

KASPERSKY LAB

Kaspersky Anti-Virus 6.0 SOS

BENUTZERHANDBUCH

KASPERSKY ANTI-VIRUS 6.0 SOS

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
1.4. Kennzeichen einer Infektion.....	13
1.5. Was tun, wenn Kennzeichen einer Infektion auftreten?	14
1.6. Sicherheitsregeln	15
KAPITEL 2. KASPERSKY ANTI-VIRUS 6.0 SOS.....	18
2.1. Was ist neu in Kaspersky Anti-Virus 6.0 SOS.....	18
2.2. Komponenten von Kaspersky Anti-Virus 6.0 SOS.....	20
2.2.1. Aufgaben zur Virensuche.....	20
2.2.2. Servicefunktionen des Programms.....	21
2.3. Hardware- und Softwarevoraussetzungen.....	22
2.4. Lieferumfang.....	23
2.5. Service für registrierte Benutzer.....	24
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS 6.0 SOS.....	25
3.1. Installation mit Hilfe des Installationsassistenten.....	26
3.2. Konfigurationsassistent	30
3.2.1. Aktivierung des Programms	30
3.2.1.1. Auswahl der Methode zur Aktivierung der Anwendung	31
3.2.1.2. Eingabe des Aktivierungscode.....	32
3.2.1.3. Download des Lizenzschlüssels	32
3.2.1.4. Auswahl einer Lizenzschlüsseldatei.....	32
3.2.1.5. Abschluss der Programmaktivierung	33
3.2.2. Konfiguration der Update-Einstellungen	33
3.2.3. Konfiguration des Zeitplans für die Virenuntersuchung	34
3.2.4. Zugriffsbegrenzung für die Anwendung.....	35
3.2.5. Abschluss des Konfigurationsassistenten	35
3.3. Installation der Anwendung aus der Befehlszeile	36
3.4. Installation über den Gruppenrichtlinienobjekt-Editor (Group Policy Object)	36

3.4.1. Installation der Anwendung	37
3.4.2. Upgrade der Anwendung	37
3.4.3. Löschen der Anwendung	38
3.5. Aktualisierung der Anwendung von Version 5.0 auf Version 6.0	38
KAPITEL 4. PROGRAMMOBERFLÄCHE	40
4.1. Symbol im Infobereich	40
4.2. Kontextmenü	41
4.3. Programmhauptfenster	42
4.4. Konfigurationsfenster der Anwendung	45
KAPITEL 5. ERSTE SCHRITTE	47
5.1. Wie der Computer auf Viren untersucht wird	47
5.2. Wie kritische Computerbereiche untersucht werden	48
5.3. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden ...	49
5.4. Wie das Programm aktualisiert wird	50
KAPITEL 6. STEUERUNG DES PROGRAMMS	51
6.1. Programm aktivieren/ deaktivieren	51
6.2. Typen der zu kontrollierenden schädlichen Programme	52
6.3. Aufbau einer vertrauenswürdigen Zone	53
6.4. Start von Aufgaben mit Rechten eines anderen Benutzers	58
6.5. Konfiguration des Zeitplans für Aufgabenstart und Senden von Benachrichtigungen	60
6.6. Leistungseinstellungen	62
KAPITEL 7. VIRENSUCHE AUF DEM COMPUTER	64
7.1. Steuerung von Aufgaben zur Virensuche	65
7.2. Erstellen einer Liste der Untersuchungsobjekte	66
7.3. Erstellen von Aufgaben zur Virensuche	67
7.4. Konfiguration von Aufgaben zur Virensuche	69
7.4.1. Auswahl der Sicherheitsstufe	69
7.4.2. Festlegen der zu untersuchenden Objekttypen	71
7.4.3. Wiederherstellen der standardmäßigen Untersuchungseinstellungen	74
7.4.4. Auswahl der Aktion für Objekte	74
7.4.5. Zusätzliche Optionen für die Virensuche	77
7.4.6. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben	79
KAPITEL 8. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS 6.0 SOS	80

8.1. EICAR-"Testvirus" und seine Modifikationen	80
8.2. Testen einer Aufgabe zur Virensuche	82
KAPITEL 9. UPDATE DES PROGRAMMS	84
9.1. Starten des Updates	86
9.2. Rückkehr zum vorherigen Update	86
9.3. Erstellen einer Update-Aufgabe	87
9.4. Update-Einstellungen	88
9.4.1. Auswahl der Updatequelle	89
9.4.2. Auswahl von Updatemodus und Update-Objekt	91
9.4.3. Konfiguration der Verbindungsparameter	93
9.4.4. Update-Verteilung	95
9.4.5. Aktionen nach dem Programm-Update	96
KAPITEL 10. ZUSÄTZLICHE OPTIONEN	98
10.1. Quarantäne für möglicherweise infizierte Objekte	99
10.1.1. Aktionen mit Objekten in der Quarantäne	100
10.1.2. Konfiguration der Quarantäne-Einstellungen	102
10.2. Sicherungskopien gefährlicher Objekte	103
10.2.1. Aktionen mit Sicherungskopien	103
10.2.2. Konfiguration der Backup-Einstellungen	105
10.3. Berichte	105
10.3.1. Konfiguration der Berichtsparameter	108
10.3.2. Registerkarte <i>Gefunden</i>	109
10.3.3. Registerkarte <i>Ereignisse</i>	110
10.3.4. Registerkarte <i>Statistik</i>	111
10.3.5. Registerkarte <i>Einstellungen</i>	111
10.4. Allgemeine Informationen über die Anwendung	113
10.5. Lizenzverwaltung	114
10.6. Technischer Support für Benutzer	115
10.7. Konfiguration der Oberfläche von Kaspersky Anti-Virus 6.0 SOS	117
10.8. Benachrichtigungen über Ereignisse von Kaspersky Anti-Virus 6.0 SOS	119
10.8.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen	120
10.8.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail	122
10.8.1.3. Parameter des Ereignisberichts	123
10.8.2. Zugriffsbeschränkung für das Programm	124

10.9. Export/Import der Einstellungen von Kaspersky Anti-Virus 6.0 SOS	125
10.10. Wiederherstellen der Standardeinstellungen	126
KAPITEL 11. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE	128
11.1. Aktivierung der Anwendung	130
11.2. Steuerung von Aufgaben	130
11.3. Virenuntersuchung von Objekten	132
11.4. Programm-Update	137
11.5. Rollback des letzten Programm-Updates	138
11.6. Export von Schutzparametern	139
11.7. Import von Schutzparametern	140
11.8. Anwendung starten	141
11.9. Anwendung beenden	141
11.10. Anlegen einer Tracing-Datei	141
11.11. Anzeige der Hilfe	142
11.12. Rückgabecodes der Befehlszeile	142
KAPITEL 12. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN	144
12.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten	144
12.2. Deinstallation des Programms aus der Befehlszeile	146
KAPITEL 13. VERWALTUNG DER ANWENDUNG ÜBER KASPERSKY ADMINISTRATION KIT	148
13.1. Anwendung verwalten	151
13.1.1. Anwendung starten / beenden	152
13.1.2. Anwendungsparameter anpassen	153
13.1.3. Spezifische Parameter anpassen	155
13.2. Aufgaben verwalten	156
13.2.1. Aufgaben starten und beenden	158
13.2.2. Aufgaben erstellen	158
13.2.2.1. Lokale Aufgabe erstellen	159
13.2.2.2. Gruppenaufgabe erstellen	161
13.2.2.3. Globale Aufgabe erstellen	161
13.2.3. Aufgabenparameter anpassen	162
13.3. Richtlinien verwalten	164
13.3.1. Richtlinie erstellen	164
13.3.2. Richtlinienparameter anzeigen und ändern	166

KAPITEL 14. HÄUFIGE FRAGEN	168
ANHANG A. ZUSÄTZLICHE INFORMATIONEN	170
A.1. Liste der Objekte, die nach Erweiterung untersucht werden.....	170
A.2. Zulässige Ausschlussmasken für Dateien	173
A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren- Enzyklopädie.....	174
A.4. Beschreibung von Parametern der Datei <i>setup.ini</i>	175
ANHANG B. KASPERSKY LAB.....	176
B.1. Andere Produkte von Kaspersky Lab	177
B.2. Kontaktinformationen	189
ANHANG C. ENDBENUTZER-STANDARDLIZENZVERTRAG.....	190

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 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-Netzes 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 und PC-Benutzern. 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 Skripts, die beim Öffnen bestimmter Webseiten automatisch gestartet werden, schädliche Aktionen auf dem Computer

ausführen, wozu Modifikation der Systemregistrierung, Diebstahl persönlicher Daten und Installation schädlicher Programme gehören.

Mit Netzwerktechnologien lassen sich Angriffe auf entfernte PCs und Unternehmensserver verwirklichen. Das Ergebnis solcher Angriffe kann die Funktionsuntüchtigkeit der Ressource, der vollständige Zugriff auf die darauf gespeicherten Informationen sowie der Missbrauch des Rechners als Teil eines Zombie-Netzes sein.

Im Bereich Kreditkartenzahlung, E-Money und Online-Banking (Internet-Shops, -Auktionen, Websites von Banken usw.) hat sich der Internetbetrug zu einem weit verbreiteten Verbrechen entwickelt.

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 ernstem 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.

Neben der Gefahr des Eindringens von Schadprogrammen besteht das Problem unerwünschter E-Mails, die Werbung enthalten (Spam). Zwar stellen unerwünschte E-Mails keine direkte Bedrohungsquelle dar, doch erhöhen sie die Belastung von Mailservern, ergeben zusätzlichen Datenverkehr, verstopfen das Benutzerpostfach, führen zu Zeitverlust und verursachen dadurch erhebliche finanzielle Schäden.

Erwähnenswert ist auch, dass Angreifer so genannte Spam-Technologien mit Massencharakter und Methoden des Social Engineering verwenden, um einen Benutzer dazu zu veranlassen, eine E-Mail zu öffnen, über einen Link aus der E-Mail zu einer bestimmten Internetressource zu

gehen usw. Deshalb ist die Möglichkeit zur Spam-Filterung auch zum Kampf gegen neue Arten des Internetbetrugs (wie beispielsweise Phishing) sowie gegen die Verbreitung von Schadprogrammen notwendig.

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 6.0 SOS 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. Vielleicht sind Sie schon auf solche Programme gestoßen, wenn beim Aufruf einer Webseiten-Adresse eine ganz andere Seite geöffnet wurde.

Scherzprogramme (Jokes)

Jokes sind Programme, die dem Computer keinen direkten Schaden zufügen, sondern Meldungen darüber anzeigen, dass Schaden verursacht wurde oder unter bestimmten Bedingungen verursacht wird. Solche Programme warnen den Benutzer 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.

Das Erkennen und Blockieren dieser Arten von Bedrohungen wird von Kaspersky Anti-Virus 6.0 SOS mit einer reaktiven Methode ausgeführt,

- die auf der Suche von schädlichen Objekten mit Hilfe der regelmäßig aktualisierten Datenbanken mit Bedrohungssignaturen beruht. Zur Realisierung dieser Methode muss mindestens eine Infektion erfolgt sein, wonach den Datenbanken die entsprechende Bedrohungssignatur

hinzugefügt und das Update der Datenbanken weitergegeben werden kann.

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.

1.4. Kennzeichen einer Infektion

Es existiert eine Reihe von Kennzeichen, die auf eine Computerinfektion hinweisen. Wenn Sie bemerken, dass sich der Computer beispielsweise auf folgende Weise "seltsam" verhält, dann ist er mit hoher Wahrscheinlichkeit von einem Virus infiziert:

- Es werden unvorhergesehene Meldungen oder Bilder auf dem Bildschirm angezeigt oder unvorhergesehene Audiosignale wiedergegeben.
- Die Schublade des CD/DVD-ROM-Laufwerks öffnet und schließt sich ohne erkennbaren Grund.
- Bestimmte Programme auf dem Computer werden willkürlich gestartet, ohne dass dies von Ihnen initiiert wurde.
- Auf dem Bildschirm werden Meldungen angezeigt, die sich auf den Versuch bestimmter Programme Ihres Computers beziehen, eine Verbindung mit dem Internet herzustellen, obwohl Sie dies nicht initiiert haben.

Außerdem gibt es einige charakteristische Merkmale für eine Virusinfektion durch E-Mails:

- Freunde oder Bekannte teilen Ihnen mit, dass sie Nachrichten von Ihnen erhalten haben, die Sie aber nicht abgeschickt haben.
- In Ihrer Mailbox befindet sich eine große Anzahl von Nachrichten ohne Antwortadresse und Betreff.

Es ist anzumerken, dass diese Merkmale nicht immer durch die Existenz von Viren hervorgerufen werden. Manchmal können sie auf andere Ursachen zurückgehen. So können beispielsweise infizierte Nachrichten zwar Ihre Adresse als Antwortadresse enthalten, aber trotzdem von einem anderen Computer aus abgeschickt worden sein.

Außerdem existieren indirekte Hinweise auf eine Infektion Ihres Computers:

- häufiges Abstürzen und Funktionsstörungen des Computers.

- verlangsamer Start von Programmen.
- das Laden des Betriebssystems ist nicht möglich.
- Verschwinden von Dateien und Ordnern oder Veränderungen ihres Inhalts.
- häufiger Zugriff auf die Festplatte (häufiges Blinken der Festplatten-LED am PC-Gehäuse).
- Der Webbrowser (z.B. Microsoft Internet Explorer) "bleibt hängen" oder verhält sich unerwartet (z.B. das Programmfenster lässt sich nicht schließen).

In 90 % der Fälle werden indirekte Symptome durch Hardware- oder Softwarestörungen verursacht. Trotz der geringen Wahrscheinlichkeit, dass solche Symptome auf eine Infektion zurückgehen, wird bei ihrem Auftreten empfohlen, den Computer vollständig zu untersuchen (s. Pkt 5.1 auf S. 47).

1.5. Was tun, wenn Kennzeichen einer Infektion auftreten?

Wenn Sie bemerken, dass sich Ihr Computer "verdächtig verhält",

1. Keine Panik! Diese goldene Regel kann Sie vor dem Verlust wichtiger Daten bewahren.
2. Trennen Sie den Computer vom Internet und vom lokalen Netzwerk, wenn er damit verbunden ist.
3. Wenn das Symptom darin besteht, dass der Systemstart von der Festplatte des Computers nicht möglich ist (der Computer gibt einen Fehler aus, wenn Sie ihn einschalten), versuchen Sie, das System im abgesicherten Modus oder von der Microsoft Windows-Rettungsdiskette zu starten, die Sie bei der Installation des Betriebssystems auf dem Computer erstellt haben.
4. Bevor Sie irgendwelche Aktionen ausführen, speichern Sie Ihre Daten auf einem externen Datenträger (Diskette, CD/DVD, Flash-Card usw.).
5. Installieren Sie Kaspersky Anti-Virus, falls er noch nicht installiert wurde.
6. Aktualisieren Sie die Bedrohungssignaturen und die Programm-Module (s. 5.4 auf S. 50). Verwenden Sie für den Download aus dem Internet möglichst nicht Ihren eigenen Computer, sondern einen virenfreien Computer (Computer eines Freundes, im Internet-Café, bei der Arbeit). Die Verwendung eines anderen Computers ist von Vorteil, da bei einer

Internetverbindung des infizierten Computers die Möglichkeit besteht, dass der Virus wichtige Informationen an die Angreifer sendet oder sich an die Adressen Ihres Adressbuchs verschickt. Gerade deshalb sollte bei einem Infektionsverdacht die Verbindung mit dem Internet sofort getrennt werden.

7. Stellen Sie die von Kaspersky Lab empfohlene Sicherheitsstufe ein.
8. Starten Sie die vollständige Untersuchung des Computers (s. 5.1 auf S. 47).

1.6. Sicherheitsregeln

Selbst die zuverlässigsten und vernünftigsten Maßnahmen können keinen hundertprozentigen Schutz vor Computerviren und Trojaner bieten. Allerdings lässt sich das Risiko einer Virusinfektion und möglicher Verluste minimieren, indem Sie folgende Regeln beachten.

Eine der wichtigsten Methoden im Kampf gegen Viren ist, wie auch in der Medizin, die rechtzeitige *Prophylaxe*. Die Computerprophylaxe umfasst wenige Regeln, welche die Wahrscheinlichkeit einer Virusinfektion und des Datenverlusts erheblich verringern.

Im Folgenden finden Sie die wichtigsten Sicherheitsregeln, die Ihnen helfen, das Risiko von Virenangriffen wesentlich zu verringern. Allerdings sollte beachtet werden, dass Kaspersky Anti-Virus 6.0 SOS dem Computer keinen Echtzeitschutz bietet.

Regel 1: *Schützen Sie Ihren Computer mit Hilfe eines Antiviren-Programms und einer Firewall.*

- Installieren Sie umgehend Kaspersky Anti-Virus.
- Aktualisieren Sie regelmäßig die Bedrohungssignaturen, die zum Umfang des Programms gehören (s. 5.4 Auf S. 50). Das Update kann beim Eintreten einer Virenepidemie mehrmals täglich vorgenommen werden. In solchen Fällen werden die Datenbanken mit den Bedrohungssignaturen auf den Kaspersky-Lab-Updateservern unverzüglich aktualisiert.
- Legen Sie die von Kaspersky Lab empfohlenen Einstellungen für die vollständige Untersuchung des Computers fest und planen Sie deren Ausführung mindestens einmal pro Woche.

Regel 2: *Verhalten Sie sich beim Speichern neuer Daten auf dem Computer vorsichtig:*

- Untersuchen Sie alle Wechseldatenträger (s. 5.3 Auf S. 49) (Disketten, CDs/DVDs-ROMs, Flash-Cards usw.) vor deren Verwendung auf das Vorhandensein von Viren.
- Gehen Sie vorsichtig mit E-Mail-Nachrichten um. Starten Sie nie Dateien, die Sie per E-Mail erhalten haben, wenn Sie nicht sicher sind, dass diese wirklich für Sie bestimmt sind, selbst wenn diese von einem Bekannten abgeschickt wurden.
- Gehen Sie vorsichtig mit allen Daten um, die Sie aus dem Internet empfangen haben. Wenn Ihnen von einer Webseite angeboten wird, ein neues Programm zu installieren, vergewissern Sie sich über das Vorhandensein eines Sicherheitszertifikats.
- Wenn Sie eine ausführbare Datei aus dem Internet oder über ein lokales Netzwerk herunterladen, dann untersuchen Sie diese unbedingt mit Kaspersky Anti-Virus.
- Verhalten Sie sich vorsichtig bei der Auswahl der von Ihnen besuchten Internetressourcen. Bestimmte Seiten sind von gefährlichen Skriptviren oder Internetwürmern infiziert.

Regel 3: *Verfolgen Sie aufmerksam die Informationen von Kaspersky Lab.*

In den meisten Fällen informiert Kaspersky Lab über den Ausbruch einer neuen Epidemie lange bevor diese ihren Höhepunkt erreicht. Die Wahrscheinlichkeit einer Infektion ist in diesem Fall noch gering und durch den Download der aktualisierten Bedrohungssignaturen können Sie sich rechtzeitig vor einem neuen Virus schützen.

Regel 4: *Verhalten Sie sich misstrauisch gegenüber falschen Viruswarnungen, Scherzprogrammen und E-Mails, die vorgeben vor Infektionen zu warnen.*

Regel 5: *Verwenden Sie den Dienst Windows Update und installieren Sie regelmäßig die Updates für das Betriebssystem Microsoft Windows.*

Regel 6: *Kaufen Sie Ihre Software nur bei offiziellen Händlern.*

Regel 7: *Beschränken Sie den Kreis der Leute, die zur Arbeit auf Ihrem Computer berechtigt sind.*

Regel 8: *Verringern Sie das Risiko unangenehmer Folgen einer möglichen Infektion: Fertigen Sie dazu rechtzeitig Sicherungskopien Ihrer Daten an. Wenn Sicherungskopien vorhanden sind, kann das System bei Datenverlust schnell wiederhergestellt werden. Distributions-CDs, Disketten, Flash-Cards und andere Datenträger mit Software und wertvollen Informationen sollten an einem sicheren Ort aufbewahrt werden.*

Regel 9: *Überprüfen Sie regelmäßig die Liste der auf Ihrem Computer installierten Programme. Dazu können Sie den Dienst **Programme ändern***

oder entfernen in der **Systemsteuerung** verwenden oder den Inhalt des Ordners **Programme** und des Ordners Autostart prüfen. Dadurch können Sie Software finden, die ohne Ihr Wissen auf dem Computer installiert wurde, während Sie beispielsweise das Internet benutzt oder ein bestimmtes Programm installiert haben. Möglicherweise befinden sich potentiell gefährliche Programme darunter.

KAPITEL 2. KASPERSKY ANTI-VIRUS 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS ist die neue Generation des Informationsschutzes.

Der Hauptunterschied zwischen Kaspersky Anti-Virus 6.0 SOS und bisherigen Produkten besteht darin, dass die Anwendung ein zusätzliches Antiviren-Schutzmittel ist, das die Funktion der Virensuche auf Befehl übernimmt. Dabei funktioniert Kaspersky Anti-Virus 6.0 SOS zusammen mit anderen Antiviren-Programmen, ohne Konflikte zu verursachen.

Kaspersky Anti-Virus 6.0 SOS gewährleistet keinen Viren-Echtzeitschutz für den Computer!

2.1. Was ist neu in Kaspersky Anti-Virus 6.0 SOS

In diesem Kapitel werden die neuen Optionen von Kaspersky Anti-Virus 6.0 SOS ausführlich beschrieben.

Neuerungen in der Virensuche

- Die Technologie für die Untersuchung von 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 Technologie iChecker™ 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 Benutzer 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 über bestimmte Ereignisse während der Programmarbeit wurde erweitert. Für jeden Ereignistyp kann eine Benachrichtigungsmethode festgelegt werden: E-Mail-Nachricht, Audiosignal, Popupmeldung, Eintrag im Ereignisbericht.
- Eine Funktion zur zentralen entfernten Verwaltung des Schutzsystems mit Hilfe einer erweiterten Verwaltungsoberfläche unter Kaspersky Administration Kit wurde hinzugefügt.

Neuerungen auf der Programmoberfläche

- Auf der neuen Oberfläche von Kaspersky Anti-Virus 6.0 SOS 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 werden Sie mit vollständigen Informationen unterstützt: Kaspersky Anti-Virus 6.0 SOS zeigt Meldungen über den Status der Untersuchungs- und Update-Aufgaben 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 6.0 SOS 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.
- Es besteht die Möglichkeit, keinen Proxyserver zu verwenden, wenn das Programm-Update über eine lokale Quelle erfolgt. Dadurch wird das Volumen des Netzwerkverkehrs über den Proxyserver erheblich vermindert.
- Eine Option zum Rollback von Updates wurde realisiert. Dadurch wird beispielsweise bei einer Beschädigung von Dateien oder bei einem Kopierfehler erlaubt, zur vorherigen 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. Komponenten von Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS umfasst:

- Aufgaben zur Virensuche (s. Pkt. 2.2.1 auf S. 20), mit deren Hilfe die Untersuchung des Computers und einzelner Dateien, Ordner, Laufwerke oder Bereiche ausgeführt wird.
- Servicefunktionen (s. Pkt. 2.2.2 auf S. 21), die die Aktualisierung der Bedrohungssignaturen gewährleisten, Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

2.2.1. Aufgaben zur Virensuche

Es ist sehr wichtig, regelmäßig die vollständige Virenuntersuchung Ihres Computers durchzuführen. Zur Virensuche verfügt Kaspersky Anti-Virus 6.0 SOS 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 Untersuchungsaufgaben zu erstellen und Zeitplan für ihren Start anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Mail-Datenbanken oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

2.2.2. Servicefunktionen des Programms

Kaspersky Anti-Virus 6.0 SOS 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, einen beliebigen Hackerangriff abzuwehren und Viren oder andere gefährliche Programme unschädlich zu machen, muss der aktuelle Zustand von Kaspersky Anti-Virus 6.0 SOS aufrechterhalten werden. Dazu ist die Komponente *Update* vorgesehen. Sie dient zur Aktualisierung der Bedrohungssignaturen und Programm-Module von Kaspersky Anti-Virus 6.0 SOS, 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 jede Untersuchungs- und Update-Aufgabe der Anwendung ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und die Arbeitsergebnisse. Unter Verwendung der Funktion *Berichte* können Sie stets Details über die Arbeit einer beliebigen Aufgabe erhalten. Sollten Probleme auftreten, dann können Sie die Berichte an Kaspersky Lab schicken, damit unsere Experten die Situation analysieren und Ihnen möglichst schnell helfen können.

Alle im Hinblick auf die Sicherheit verdächtigen Objekte werden von Kaspersky Anti-Virus 6.0 SOS in den speziellen Speicher *Quarantäne* verschoben. Sie werden dort in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können die Quarantäneobjekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen oder löschen. Außerdem können Sie verdächtige Objekte manuell in die Quarantäne verschieben. Alle Objekte, die sich aufgrund der Untersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien von Objekten gespeichert, die von der Anwendung desinfiziert und gelöscht wurden. Diese Kopien werden angelegt, um bei Bedarf die Objekte oder ein Bild ihrer Infektion wiederherzustellen. Auch die Sicherungskopien der Objekte werden in

verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können ein Backup-Objekt am ursprünglichen Ort wiederherstellen oder die Sicherungskopie löschen.

Support

Alle registrierten Benutzer von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS zu helfen.

2.3. Hardware- und Softwarevoraussetzungen

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus 6.0 SOS zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen.

Allgemeine Voraussetzungen:

- 50 MB freier Speicher auf der Festplatte
- CD-ROM-Laufwerk (zur Installation von Kaspersky Anti-Virus 6.0 SOS von CD-ROM).
- Microsoft Internet Explorer Version 5.5 oder höher (für das Update der Bedrohungssignaturen und Programm-Module über das Internet)
- Microsoft Windows Installer 2.0.

Microsoft Windows 98(SE), Microsoft Windows ME, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Prozessor Intel Pentium 300 MHz oder höher (oder ein entsprechender kompatibler Prozessor)
- 64 MB Arbeitsspeicher.

Unter Microsoft Windows 2000 Professional (Service Pack 4 oder höher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 oder höher), Microsoft Windows XP Professional x64 Edition:

- Prozessor Intel Pentium 300 MHz oder kompatibel (oder ein entsprechender kompatibler Prozessor)
- 128 MB Arbeitsspeicher.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Prozessor Intel Pentium 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
- 512 MB Arbeitsspeicher.

2.4. Lieferumfang

Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS 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 6.0 SOS 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 SOS

Kaspersky Anti-Virus 6.0 SOS kann gleichzeitig mit Antiviren-Programmen anderer Hersteller und Programmen von Kaspersky Lab installiert werden. Es werden keine Konflikte bei der Arbeit mit anderen Antiviren-Programmen verursacht. Eine Ausnahme bilden folgende Programme:

- Kaspersky Anti-Virus 6.0 und 7.0
- Kaspersky Internet Security 6.0 und 7.0
- Kaspersky Anti-Virus 6.0 for Windows Workstations
- Kaspersky Anti-Virus 6.0 for File Servers

Kaspersky Anti-Virus 6.0 SOS gewährleistet keinen Echtzeitschutz für den Computer und ist ein zusätzliches Antiviren-Programm!

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. 26). 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. 36).
- 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. 36).

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

3.1. Installation mit Hilfe des Installationsassistenten

Um Kaspersky Anti-Virus 6.0 SOS 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 Installationsvoraussetzungen für Kaspersky Anti-Virus 6.0 SOS

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 6.0 SOS 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 6.0 SOS 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 6.0 SOS 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 6.0 SOS 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 SOS – für 32-Bit-Systeme.
- <Laufwerk>\Programme (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 SOS – 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. Suche anderer Antiviren-Programme

Auf dieser Etappe erfolgt die Suche nach anderen Antiviren-Produkten.

Wenn auf Ihrem Computer ein anderes Antiviren-Programm gefunden wird, setzt Kaspersky Anti-Virus 6.0 SOS die Installation fort. Andernfalls erscheint auf dem Bildschirm eine Warnung darüber, dass das Programm keinen vollständigen Antiviren-Schutz des Computers bietet.

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

Schritt 6. Abschlussvorbereitungen für die Programminstallation

Auf dieser Etappe wird Ihnen angeboten, die Programminstallation auf Ihrem Computer abschließend vorzubereiten. Falls bei der Deinstallation der Vorgängerversion von Kaspersky Anti-Virus SOS Parameter und Bedrohungssignaturen gespeichert wurden, können Sie nun entscheiden, ob diese für die Anwendung verwendet werden sollen (Wenn Sie beispielsweise eine Beta-Version installiert hatten und jetzt eine kommerzielle Version des Programms installieren).

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

Wenn auf Ihrem Computer bereits eine ältere Version von Kaspersky Anti-Virus SOS 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 Computer kopiert.

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

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

Schritt 7. Auswahl des Installationstyps

Hier können Sie auswählen, in welchem Umfang das Programm auf Ihrem Computer installiert werden soll. Drei 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 5 beschrieben.

Benutzerdefiniert. In diesem Fall wird Ihnen angeboten, die Programmkomponenten auszuwählen, die auf Ihrem Computer installiert werden sollen. Details siehe Schritt 8.

Klicken Sie zur Auswahl eines Installationstyps auf die entsprechende Schaltfläche.

Schritt 8. 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 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. Details über die Funktionalität der gewählten Komponente und Informationen über den für ihre Installation auf der Festplatte erforderlichen Platz befinden sich im unteren Bereich dieses Installationsfensters.

Um die Installation einer Komponente abzulehnen, wählen Sie im Kontextmenü die Variante **Die Komponente wird nicht verfügbar sein**. Beachten Sie, dass Sie auf den Schutz vor einer ganzen Reihe gefährlicher Programme verzichten, wenn Sie eine bestimmte Komponente nicht installieren.

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**.

Klicken Sie im folgenden Fenster auf **Installieren**.

Schritt 9. Abschluss des Installationsvorgangs

Das Fenster **Installation wird abgeschlossen** enthält Informationen über den Abschluss des Installationsvorgangs von Kaspersky Anti-Virus 6.0 SOS auf Ihrem Computer.

Um den Konfigurationsassistenten zu starten, klicken Sie auf die Schaltfläche **Weiter** (s. Pkt. 3.2 auf S. 30).

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 SOS 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.

Sie können die Etappen des Konfigurationsassistenten bei der Programminstallation überspringen, indem Sie das Assistentenfenster schließen. Der Assistent kann später über die Programmoberfläche gestartet werden, wenn die ursprünglichen Schutzeinstellungen (s. Pkt. 10.10 auf S. 126) von Kaspersky Anti-Virus 6.0 SOS wiederhergestellt werden.

3.2.1. 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 6.0 SOS 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.

3.2.1.1. 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:

- ① **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.
- ② **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.
- ③ **Vorherigen Lizenzschlüssel verwenden.** Aktivieren Sie die Anwendung mit Hilfe einer bereits vorhandenen Lizenzschlüsseldatei für Kaspersky Anti-Virus 6.0 SOS.
- ④ **Das Programm später aktivieren.** Bei der Auswahl dieser Variante wird die Aktivierung des Programms übersprungen. Kaspersky Anti-Virus 6.0 SOS 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. 9.4.3 auf S. 93). 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. 10.5 auf S. 114). 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 Aktivierungscodes einen Lizenzschlüssel herunterzuladen.

3.2.1.2. 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 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.

3.2.1.3. 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.

3.2.1.4. Auswahl einer Lizenzschlüsseldatei

Wenn Sie bereits eine Lizenzschlüsseldatei für das Programm Kaspersky Anti-Virus 6.0 SOS 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.

3.2.1.5. 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.

3.2.2. Konfiguration der Update-Einstellungen

Die Qualität der Virensuche auf Ihrem Computer 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 6.0 SOS 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 6.0 SOS 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**.

3.2.3. 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 6.0 SOS 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 6.0 SOS statt. Die Zeitplaneinstellungen 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-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 Computers zu starten.

3.2.4. Zugriffsbegrenzung für die Anwendung

Da ein PC von mehreren Personen benutzt werden kann, die über ein unterschiedliches Maß an Fertigkeiten im Umgang mit Computern verfügen, und weil die Gefahr besteht, dass Schadprogramme versuchen, das Programm auszuschalten, bietet Kaspersky Anti-Virus 6.0 SOS eine Funktion, um den Zugriff auf das Programm mit Hilfe eines Kennworts zu beschränken. Der Kennwortschutz erlaubt es, das Programm vor Versuchen zum unerlaubten Abschalten des Programms und zum Ändern seiner Einstellungen zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus. Wenn Sie das vorhandene Kennwort ändern möchten, füllen Sie zusätzlich das Feld **Altes Kennwort** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung 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.
- Untersuchungsaufgaben anhalten/ beenden** – Das Kennwort wird abgefragt, wenn der Benutzer versucht, die Arbeit einer Untersuchungsaufgabe anzuhalten oder zu beenden.

3.2.5. Abschluss des Konfigurationsassistenten

Aktivieren Sie im letzten Fenster bei Bedarf das Kontrollkästchen **Programm starten** und klicken Sie auf die Schaltfläche **Fertig stellen**.

3.3. Installation der Anwendung aus der Befehlszeile

Geben Sie zur Installation von Kaspersky Anti-Virus 6.0 SOS in der Befehlszeile ein:

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

Der Installationsassistent (s. Pkt. 3.1 auf S. 26) wird gestartet.

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

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

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. 175), der Konfigurationsdatei *install.cfg* (s. Pkt. 11.7 auf S. 140) 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. 175), die Konfigurationsdatei *install.cfg* (s. Pkt. 11.7 auf S. 140) 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 Professional 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 5.0 SOS installiert ist, können Sie diese auf Kaspersky Anti-Virus 6.0 SOS aktualisieren.

Nach dem Start des Installationsprogramms für Kaspersky Anti-Virus 6.0 SOS 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!

Wenn Sie Kaspersky Anti-Virus SOS von Version 5.0 auf 6.0 aktualisieren und die Installation aus einem Netzwerkordner erfolgt, auf den der Zugriff mit Hilfe eines Kennworts eingeschränkt ist, wird zwar Version 5.0 deinstalliert, 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 6.0 SOS 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. 40)
- Kontextmenü (s. Pkt. 4.2 auf S. 41)
- Hauptfenster (s. Pkt. 4.3 auf S. 42)
- Konfigurationsfenster der Anwendung (s. Pkt. 4.4 auf S. 45)


Das Programm verfügt außer der Hauptoberfläche noch über eine Erweiterungskomponente (Plug-in), das in die Anwendung Microsoft Windows Explorer integriert werden kann (s. Pkt. 7.2 auf S. 66).

Das Plug-in erweitert die Möglichkeiten von Microsoft Windows Explorer, da auf seiner Oberfläche die Steuerung von Kaspersky Anti-Virus 6.0 SOS möglich ist.




4.1. Symbol im Infobereich

Sofort nach der Installation von Kaspersky Anti-Virus 6.0 SOS erscheint sein Symbol im Infobereich der Taskleiste.

Das Symbol ist ein spezieller Indikator für die Arbeit von Kaspersky Anti-Virus 6.0 SOS. Er informiert über eine Reihe wichtiger Aufgaben, die vom Programm ausgeführt werden.

Wenn das Symbol  in der Taskleiste angezeigt wird, ist Kaspersky Anti-Virus 6.0 SOS aktiv.

Abhängig von der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Anti-Virus 6.0 SOS:

	Die Untersuchung einer Datei wird ausgeführt.
	Das Update der Bedrohungssignaturen und Programm-Module von Kaspersky Anti-Virus 6.0 SOS wird ausgeführt.
	Bei der Arbeit von Kaspersky Anti-Virus 6.0 SOS ist eine Störung

aufgetreten.

Das Symbol bietet außerdem Zugriff auf die grundlegenden Elemente der Programmoberfläche: Kontextmenü (s. Pkt. 4.2 auf S. 41) und Hauptfenster (s. Pkt. 4.3 auf S. 42).

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

Um das Hauptfenster von Kaspersky Anti-Virus 6.0 SOS im Abschnitt **Virensuche** 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.

Das Menü von Kaspersky Anti-Virus 6.0 SOS 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 den Ordner **Eigene Dateien**, Autostart-Objekte, Mail-Datenbanken, alle Laufwerke Ihres Computers usw. Sie können die Liste ergänzen, Objekte zur Untersuchung auswählen und die Virensuche starten.



Abbildung 1. Kontextmenü

Update – Starten der Aktualisierung der Programm-Module und Bedrohungssignaturen für Kaspersky Anti-Virus 6.0 SOS und der Installation der Updates auf Ihrem Computer.

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 6.0 SOS wechseln.

Kaspersky Anti-Virus – Das Programmhauptfenster öffnen (s. Pkt. 4.3 auf S. 42).

Beenden – Die Arbeit von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS (s. Abb. 2) lässt sich bedingt in zwei Bereiche aufteilen:

- Die linke Seite des Fensters, der *Navigationsbereich*, erlaubt es, schnell und einfach zur Ausführung von Untersuchungs- und Update-Aufgaben oder zu den Servicefunktionen des Programms zu wechseln.
- Die rechte Seite des Fensters, der *Informationsbereich*, bietet Werkzeuge zur Ausführung der Aufgaben zur Virensuche, zur Arbeit mit Dateien in der Quarantäne und im Backup, zur Verwaltung der Lizenzschlüssel usw.

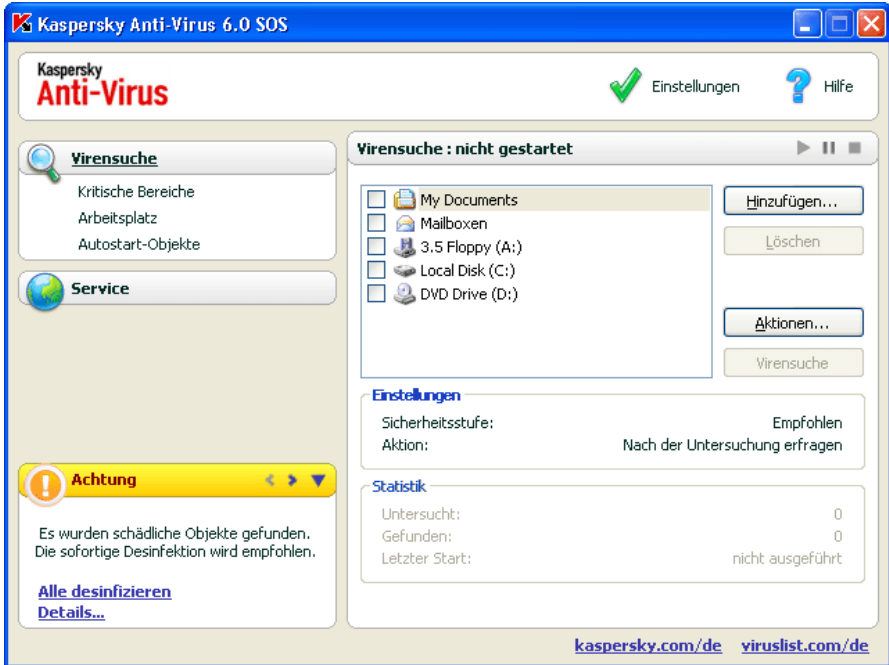


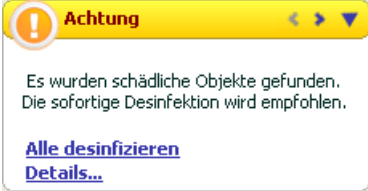


Abbildung 2. Hauptfenster von Kaspersky Anti-Virus 6.0 SOS

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>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 6.0 SOS.</p> 	<p>Hier können Sie zum Update der Anwendung wechseln, die Berichte über die Virensuche 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>
<p>Dieser Bereich begleitet Ihre Arbeit mit dem Programm durch Kommentare und Ratschläge.</p> 	<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.</p>

Jedes Element des Navigationsbereichs verfügt über ein spezielles Kontextmenü. Für 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 zum Update 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 6.0 SOS kann vom Hauptfenster aus aufgerufen werden (s. Pkt. 4.3 auf S. 42). 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 Untersuchungs- und Update-Aufgaben sowie auf die Einstellungen für die Servicefunktionen des Programms.
- Die rechte Seite des Fensters enthält eine Liste der Parameter für die auf der linken Seite ausgewählte Aufgabe usw.

Wird auf der linken Seite des Konfigurationsfensters ein bestimmter Abschnitt 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.

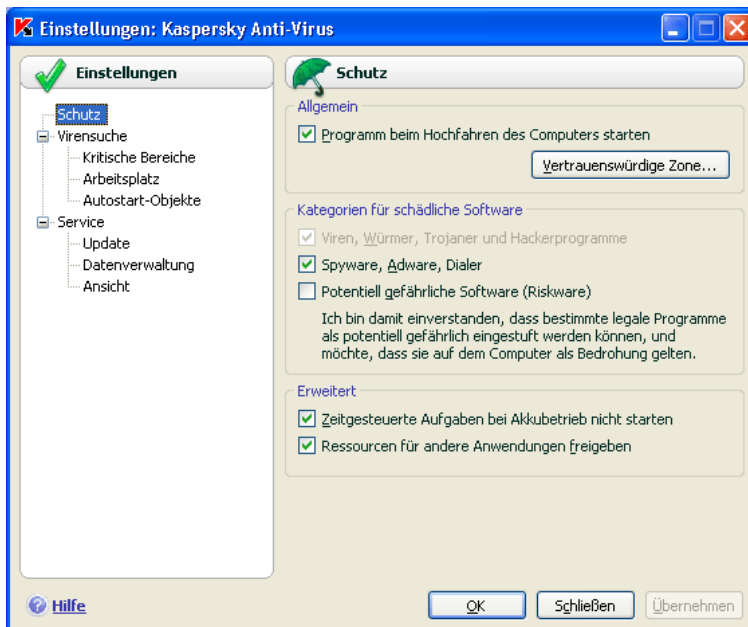


Abbildung 3. Konfigurationsfenster von Kaspersky Anti-Virus 6.0 SOS

KAPITEL 5. ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Anti-Virus 6.0 SOS bestand eine der Hauptaufgaben der Spezialisten von Kaspersky Lab in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich ausführlich mit den Einstellungen zu beschäftigen.

Allerdings können die Konfiguration Ihres Computers oder die auf diesem zu lösenden Aufgaben Besonderheiten aufweisen. Deshalb empfehlen wir Ihnen, das Programm zuerst anzupassen, um mit den Schutz mit maximaler Flexibilität genau auf Ihren Computer einzustellen.

Um die Benutzerfreundlichkeit zu erhöhen, haben wir uns bemüht, die Etappen der vorbereitenden Einstellungen in dem Konfigurationsassistenten (s. Pkt. 3.2 auf S. 30) zusammenzufassen, der am Ende der Programminstallation gestartet wird. Im Rahmen des Assistenten können Sie das Programm aktivieren, Einstellungen für das Update und den Start von Untersuchungsaufgaben vornehmen, den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken, usw.

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

- Update des Programms, wenn das Update nicht mit Hilfe des Konfigurationsassistenten oder automatisch sofort nach der Programminstallation erfolgte (s. Pkt. 5.4 auf S. 50).
- Untersuchung des Computers auf das Vorhandensein von Viren (s. Pkt. 5.1 auf S. 47).

5.1. Wie der Computer 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 Computers ausgeführt wurde, und Ihnen wird empfohlen, ihn umgehend auf Viren zu untersuchen.

Der Lieferumfang von Kaspersky Anti-Virus 6.0 SOS 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.

5.2. Wie kritische Computerbereiche untersucht werden

Auf Ihrem Computer gibt es Bereiche, die hinsichtlich der Sicherheit als kritisch gelten. Sie können zum Objekt einer Infektion durch schädliche Programme werden, die auf die Beschädigung des Computerbetriebssystems, Prozessors, Arbeitsspeichers usw. gerichtet ist.

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.

5.3. 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, auf der sich Programme und Spiele befinden, Mail-Datenbanken, die aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde, usw. Sie können ein Objekt mit den Standardmitteln von Microsoft Windows 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-Kontextmenü und wählen den Punkt **Auf Viren untersuchen** (s. Abb. 4).

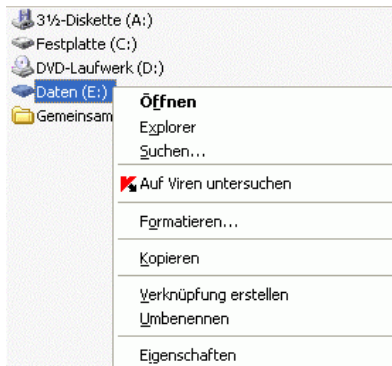


Abbildung 4. Virenuntersuchung eines Objekts, das über Microsoft Windows ausgewählt wurde

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.

5.4. Wie das Programm aktualisiert wird

Kaspersky Lab aktualisiert die Bedrohungssignaturen und die Module von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS ist eine bestehende Internetverbindung erforderlich.

Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS 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 6.0 SOS gestartet. Alle Details über den Prozess werden in einem speziellen Fenster angezeigt.

KAPITEL 6. STEUERUNG DES PROGRAMMS

Kaspersky Anti-Virus 6.0 SOS bietet Ihnen die Möglichkeit zur komplexen Steuerung seiner Arbeit:

- Aktivieren und Deaktivieren der Arbeit des Programms (s. Pkt. 6.1 auf S. 51).
- Die Typen gefährlicher Programme festlegen, vor denen Kaspersky Anti-Virus 6.0 SOS Ihren Computer schützen soll (s. Pkt. 6.2 auf S. 52).
- Erstellen einer Liste von Ausnahmen für den Schutz (s. Pkt. 6.3 auf S. 53).
- Erstellen eigener Aufgaben für die Virensuche und das Update (s. Pkt. 6.4 auf S. 58).
- Festlegen eines eigenen Zeitplans für den Aufgabenstart (s. Pkt. 6.5 auf S. 60).
- Anpassen der Leistungsparameter (s. Pkt. 6.6 auf S. 62) für den Computerschutz.

6.1. Programm aktivieren/ deaktivieren

Kaspersky Anti-Virus 6.0 SOS wird standardmäßig beim Start des Betriebssystems gestartet.

Wenn es aus einem bestimmten Grund erforderlich ist, die Arbeit von Kaspersky Anti-Virus 6.0 SOS vollständig zu beenden, wählen Sie den Punkt **Beenden** im Kontextmenü (s. Pkt. 4.2 auf S. 41) des Programms. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt.

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

Außerdem kann das Programm 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

Kaspersky Anti-Virus 6.0 SOS ermöglicht die Suche nach 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 ernsten 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 6.0 SOS den Computer schützen soll, wählen Sie im Konfigurationsfenster des Programms (s. Pkt. 4.4 auf S. 45) 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 6.0 SOS 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, führt Kaspersky Anti-Virus 6.0 SOS die Virensuche auf Ihrem Computer mit der maximalen Sicherheitsstufe aus. Wenn die zweite und dritte Gruppe deaktiviert ist, sucht das Programm nur nach 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 6.0 SOS 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. 53).

6.3. Aufbau einer vertrauenswürdigen Zone

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die das Programm Kaspersky Anti-Virus 6.0 SOS bei seiner Arbeit nicht kontrolliert. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder ein Programm) oder Objekte entsprechend der Klassifikation der Viren-Enzyklopädie (Status, der dem Objekt bei der Untersuchung vom Programm zugewiesen wird) 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 **Schutz**.
2. Klicken Sie auf die Schaltfläche **Vertrauenswürdige Zone** im Block **Allgemein**.
3. Konfigurieren Sie im folgenden Fenster (s. Abb. 5) die Ausnahmeregel für Objekte.

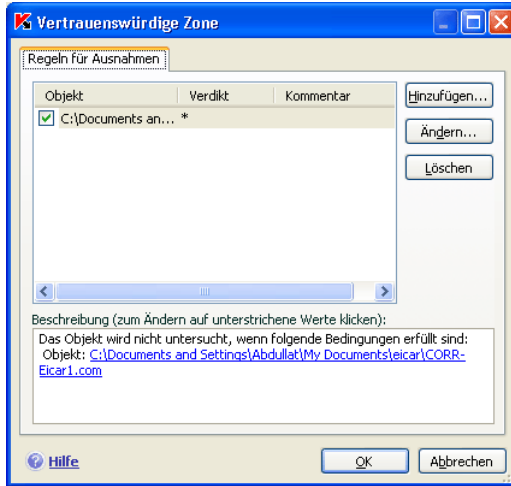


Abbildung 5. Erstellen der vertrauenswürdigen Zone

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von dem Programm Kaspersky Anti-Virus 6.0 SOS untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner) 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 6.0 SOS 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 dann bei der Ausführung von Untersuchungsaufgaben verwendet wird. 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. 6) im Abschnitt **Parameter** den Typ der Ausnahme fest:

- 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.

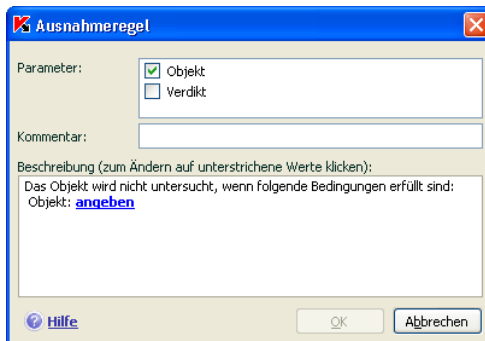


Abbildung 6. Erstellen einer Ausnahmeregel

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. 173). Aktivieren Sie das Kontrollkästchen **Unterordner einschließen**, damit das festgelegte Objekt (Datei, Dateimaske, Ordner) bei der Untersuchung rekursiv ausgeschlossen wird. Wenn Sie beispielsweise die Datei **C:\Programmewinword.exe** als Ausnahme festgelegt und das Kontrollkästchen für die Untersuchung von Unterordnern aktiviert haben, wird die Datei **winword.exe** von der Untersuchung ausgeschlossen, die sich in einem beliebigen Ordner des Verzeichnisses **C:\Programme** befinden kann.
 - 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. 174).

Für einige Klassifikationsobjekte können im Feld **Erweiterte Einstellungen** zusätzliche Bedingungen für die Verwendung der Regel festgelegt werden.

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

1. Verwenden Sie im Meldungsfenster (s. Abb. 7) 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.



Abbildung 7. Meldung über den Fund eines gefährlichen Objekts

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. 8).

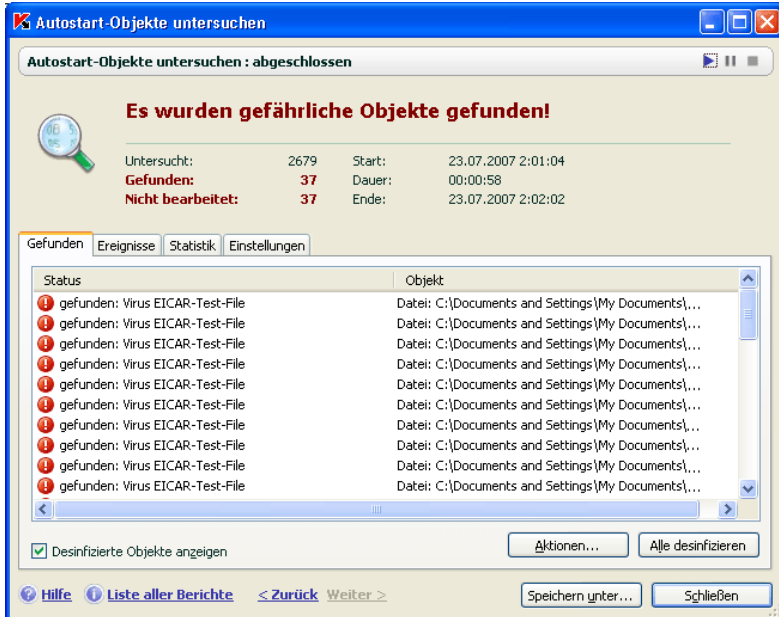


Abbildung 8. Erstellen einer Ausnahmeregel vom Bericht aus

3. Dadurch wird das Fenster zur Konfiguration der Ausnahme geöffnet. Überprüfen Sie, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden automatisch ausgefüllt, wozu Informationen aus dem Bericht dienen. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu erstellen.

6.4. Start von Aufgaben mit Rechten eines anderen Benutzers

In Kaspersky Anti-Virus 6.0 SOS 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 Benutzers zu starten, der über die erforderlichen Privilegien verfügt.

Beachten Sie, dass diese Option für das Betriebssystem Microsoft Windows 98/ME nicht zur Verfügung steht.

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. 9).

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.

Beachten Sie, dass die zeitplangesteuerte Aktualisierung mit den Rechten des aktiven Benutzerkontos ausgeführt wird, wenn der Start mit Rechten eines anderen Benutzers nicht aktiviert wurde. Sollte es vorkommen, dass zu einem bestimmten Zeitpunkt kein Benutzer auf dem Computer angemeldet ist und der Updatestart nicht mit Rechten eines anderen Benutzers geplant wurde, dann wird das Update dem Zeitplan entsprechend mit den Rechten des Benutzers SYSTEM gestartet.

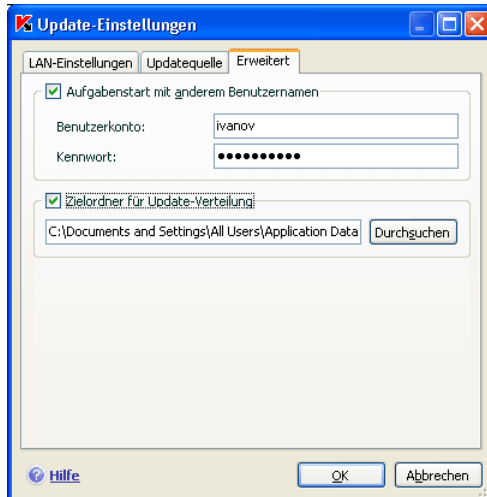


Abbildung 9. Einstellungen für den Start der Update-Aufgabe unter einem anderen Benutzerkonto

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 10) angepasst werden, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

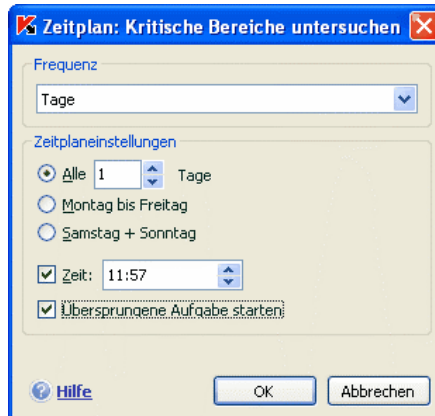





Abbildung 10. Erstellen eines Zeitplans für den Aufgabenstart

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 10) die gewünschte Variante. Geben Sie dann im Block **Zeitplaneinstellungen** die Parameter des Zeitplans für die gewählte Variante an. Folgende Varianten stehen zur Auswahl:

-  **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.
- 🕒 **Einmal.** Der 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 6.0 SOS 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).

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

Um sparsam mit der Batterie eines Laptops umzugehen und die Belastung des Prozessors und der Laufwerkssysteme zu beschränken, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

- Da die Virensuche auf dem Computer und die Programmaktualisierung relativ viel Ressourcen und Zeit benötigen, empfehlen wir Ihnen, den zeitgesteuerten Start solcher Aufgaben zu deaktivieren. Dadurch können Sie Akkustrom sparen. Bei Bedarf können Sie das Programm selbständig aktualisieren (s. Pkt. 5.4 auf S. 50) oder die Virenuntersuchung starten (s.

Pkt. 5.1 auf S. 47). Um den Dienst zum Stromsparen im Batteriebetrieb zu verwenden, aktivieren Sie das entsprechende Kontrollkästchen **Zeitgesteuerte Aufgaben bei Akkubetrieb nicht starten**.

- Das Ausführen von Untersuchungsaufgaben erhöht die Belastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält das Programm beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

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

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

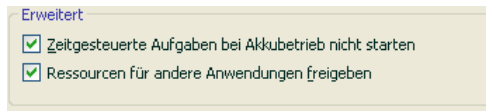


Abbildung 11. Leistungsoptionen

Um die Leistungsparameter für die Untersuchungsaufgaben anzupassen,

wählen Sie den Abschnitt **Schutz** des Anwendungshauptfensters und verwenden Sie den Link Einstellungen. Die Leistungsparameter werden im Block **Erweitert** angepasst (s. Abb. Abbildung 11).

KAPITEL 7. VIRENSUCHE AUF DEM COMPUTER

Kaspersky Anti-Virus 6.0 SOS erlaubt es, sowohl einzelne Objekte (Dateien, Ordner, Laufwerke, Wechseldataenträger) 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 den Schutzkomponenten aus bestimmten Gründen nicht erkannt wurde.

Kaspersky Anti-Virus 6.0 SOS 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. 7.4 auf S. 69) und einen Zeitplan für den Aufgabenstart festlegen (s. Pkt. 6.5 auf S. 60).

Außerdem besteht die Möglichkeit, eigene Aufgaben zur Virensuche zu erstellen (s. Pkt. 7.3 auf S. 67) und einen Startzeitplan dafür anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Mail-Datenbanken oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

Daneben können Sie ein beliebiges Objekt auf Viren untersuchen (z.B. eine Festplatte, auf der sich Programme und Spiele befinden, Mail-Datenbanken, die aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde,


usw.), ohne dafür eine spezielle Untersuchungsaufgabe zu erstellen. Das zu untersuchende Objekt kann aus dem Interface von Kaspersky Anti-Virus 6.0 SOS oder mit den Standardmitteln von Microsoft Windows (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.

7.1. 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. 60).

Um eine Untersuchungsaufgabe manuell zu starten,


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

Momentan ausgeführte Aufgaben (einschließlich Aufgaben, die über Kaspersky Administration Kit erstellt wurden) werden im Kontextmenü angezeigt (s. Pkt. 4.2 auf S. 41), das durch Rechtsklick auf das Anwendungssymbol 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.

7.2. 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. 12).

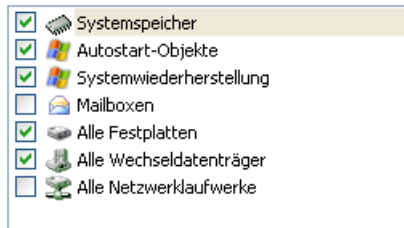


Abbildung 12. Liste der Untersuchungsobjekte

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 6.0 SOS 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 einer 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 des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen (s. Abb. 13). Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen**.



Abbildung 13. Untersuchung eines Objekts aus dem Kontextmenü von Microsoft Windows

7.3. 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!

Der Benutzer kann maximal vier Aufgaben erstellen.

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. 7.2 auf S. 66), legen Sie die Parameter fest (s. Pkt. 7.4 auf S. 69), mit denen die Aufgabe ausgeführt werden soll, und erstellen Sie den Zeitplan (s. Pkt. 6.5 auf S. 60) 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.

7.4. 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. 7.4.1 auf S. 69).
- zur detaillierten Konfiguration der Stufe wechseln:
 - die Parameter angeben, welche die Dateitypen bestimmen, die der Virusanalyse unterzogen werden (s. Pkt. 7.4.2 auf S. 71).
 - den Start von Aufgaben unter einem anderen Benutzerkonto konfigurieren (s. Pkt. 6.4 auf S. 58).
 - zusätzliche Parameter für die Untersuchung angeben (s. Pkt. 7.4.5 auf S. 77).
- die standardmäßig verwendeten Untersuchungsparameter wiederherstellen (s. Pkt. 7.4.3 auf S. 74).
- die Aktion wählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird (s. Pkt. 7.4.4 auf S. 74).
- einen Zeitplan für den automatischen Aufgabenstart erstellen (s. Pkt. 6.5 auf S. 60).
- Außerdem können Sie einheitliche Parameter für den Start aller Aufgaben festlegen (s. Pkt. 7.4.6 auf S. 79).

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

7.4.1. Auswahl der Sicherheitsstufe

Jede Aufgabe zur Virensuche gewährleistet die Untersuchung von Objekten auf einer der folgenden Stufen (s. Abb. 14):

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.

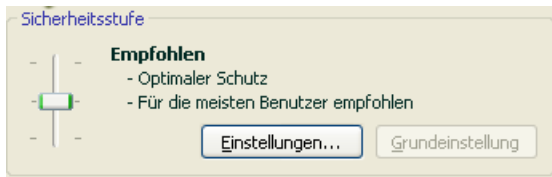


Abbildung 14. Auswahl der Sicherheitsstufe für die Virenuntersuchung von Objekten

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.

7.4.2. 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. 15). Wählen Sie eine der drei Varianten:

- ① **Alle Dateien untersuchen.** In diesem Fall werden alle Dateien ohne Ausnahme der Untersuchung unterzogen.
- ② **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.

Hinweis.

Es gibt eine Reihe von Dateiformaten, für die das Eindringen von schädlichem Code und dessen spätere Aktivierung relativ gering ist. Dazu gehören beispielsweise Dateien im txt-Format.

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

- ③ **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. 170).

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 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.

Im 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.

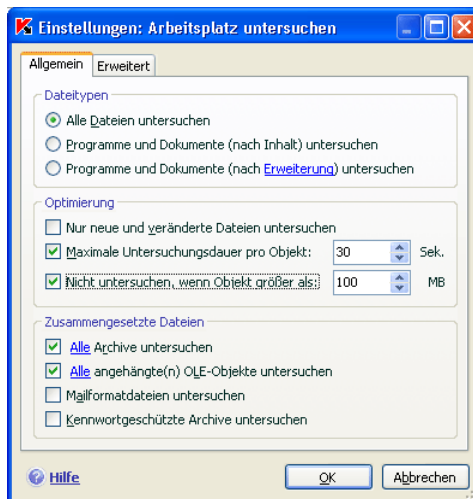


Abbildung 15. Untersuchungseinstellungen

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 6.0 SOS 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. Diese Meldung erscheint auf dem Bildschirm, nachdem die Bearbeitung von während der Untersuchung gefundenen Objekten gestartet wurde. Außerdem kann ein infiziertes Archiv auch manuell aus dem Computer entfernt 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 aktiviert ist, zerlegt Kaspersky Anti-Virus 6.0 SOS eine Mailformatdatei und analysiert jede Komponente der E-Mail (Briefkörper, Anhang) auf Viren. Wenn das Kontrollkästchen nicht angekreuzt ist, wird die Mailformatdatei als einheitliches Objekt untersucht.

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

- Kaspersky Anti-Virus 6.0 SOS 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.

7.4.3. 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**.

7.4.4. 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. 16).

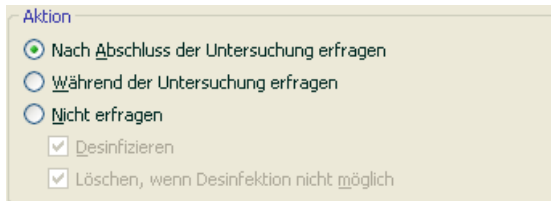





Abbildung 16. Auswahl der Aktion für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines infizierten/ möglicherweise infizierten Objekts?
 Nach Abschluss der Untersuchung erfragen	Das Programm schiebt die Bearbeitung von Objekten bis zum Ende der Untersuchung auf. Nach dem Abschluss der Untersuchung erscheint auf dem Bildschirm ein Statistik-Fenster mit einer Liste der gefundenen Objekte und Ihnen wird angeboten, die Objektbearbeitung durchzuführen.
 Während der Untersuchung erfragen	Das Programm 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.
 Nicht erfragen	Das Programm protokolliert im Bericht Informationen über die gefundenen Objekte. Die Objekte werden nicht bearbeitet und der Benutzer wird nicht benachrichtigt. 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	<p>Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, erhält das Objekt den Status <i>möglicherweise infiziert</i> und wird in die Quarantäne verschoben (s. Pkt. 10.1 auf S. 99). Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 10.3 auf S. 105). Später kann versucht werden, das Objekt zu desinfizieren.</p>
<input checked="" type="radio"/> Nicht erfragen <input checked="" type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen, wenn Desinfektion nicht möglich	<p>Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, wird das Objekt gelöscht.</p>
<input checked="" type="radio"/> Nicht erfragen <input type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen	<p>Das Programm löscht das Objekt automatisch.</p>

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus 6.0 SOS eine Sicherungskopie des Objekts an und speichert diese im Backup. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

7.4.5. Zusätzliche Optionen für die Virensuche

Neben der Konfiguration der grundlegenden Parameter für die Virenuntersuchung können Sie noch zusätzliche Parameter festlegen (s. Abb. 17):

- 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.

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 6.0 SOS bekannt ist (z.B. die Dateiformate *exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar*).

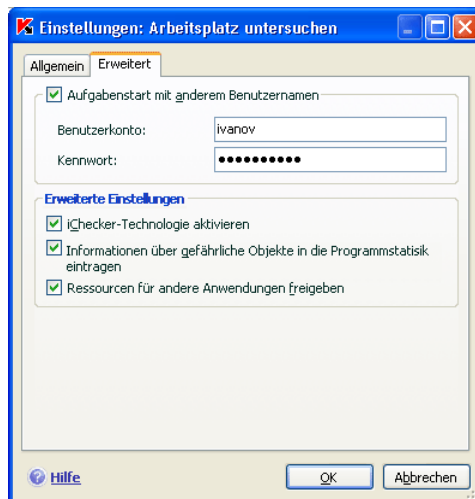



Abbildung 17. Erweiterte Untersuchungseinstellungen

- 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. 10.3.2 auf S. 109) 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.

7.4.6. 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. 7.4.1 auf S. 69), nehmen Sie die erweiterten Einstellungen für die Sicherheitsstufe vor und bestimmen Sie die Aktion für Objekte (s. Pkt. 7.4.4 auf S. 74).
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 8. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS 6.0 SOS

Nach Installation und Konfiguration von Kaspersky Anti-Virus 6.0 SOS wird empfohlen, die Korrektheit von Einstellungen und Funktion der Anwendung mit Hilfe eines "Testvirus" und seinen Modifikationen zu prüfen.

8.1. 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 6.0 SOS erkennt diese Datei bei der Virensuche, weist ihr den Typ **Virus** zu und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Reaktion von Kaspersky Anti-Virus 6.0 SOS 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 enthält einen Virus, der desinfiziert werden kann. Die Anwendung führt die Antiviren-Bearbeitung des Objekts durch.

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
	Das Objekt kann repariert werden, wobei der Text des "Viruskörpers" in CURE geändert wird.	Danach ist das Objekt vollständig repariert.
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 6.0 SOS 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.

8.2. 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. 8.1 auf S. 80) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erstellen Sie eine neue Aufgabe (s. Pkt. 7.3 auf S. 67) zur Virensuche und wählen Sie als Untersuchungsobjekt den Ordner (s. Pkt. 8.1 auf S. 80), 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. 7.1 auf S. 65).

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:



Durch die Auswahl unterschiedlicher Aktionsvarianten können Sie die Reaktion von Kaspersky Anti-Virus 6.0 SOS auf den Fund der einzelnen Objekttypen testen.

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

KAPITEL 9. UPDATE DES PROGRAMMS

Jeden Tag tauchen neue Viren, Trojaner und andere schädliche Programme auf. Deshalb ist es sehr wichtig, dass immer die aktuelle Version der Bedrohungssignaturen verwendet wird.

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 Datenbanken, die die Bedrohungssignaturen enthalten. Die Untersuchungsaufgaben 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 SOS brauchen Sie sich nicht um die Auswahl der passenden Art von Bedrohungssignaturen kümmern. Bei der Arbeit unserer Produkte werden jetzt Bedrohungssignaturen verwendet, die Schutz vor unterschiedlichen Arten schädlicher und potentiell gefährlicher Objekte bieten. Sie können aber die Typen der Schadprogramme festlegen, vor denen Kaspersky Anti-Virus 6.0 SOS den Computer schützen soll.

- **Programm-Module**

Neben den Bedrohungssignaturen können Sie auch die Programm-Module von Kaspersky Anti-Virus 6.0 SOS aktualisieren. Kaspersky Lab gibt periodisch Updatepakete heraus.

Als primäre Updatequelle für Kaspersky Anti-Virus 6.0 SOS gelten die speziellen Kaspersky-Lab-Updateserver. Für den erfolgreichen Updatedownload von den Servern ist eine Verbindung Ihres Computers 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 6.0 SOS 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 Kaspersky Anti-Virus 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 Ihrem Computer die aktuelle Version der Signaturen und Module installiert ist, erscheint auf dem Bildschirm eine Meldung über die Aktualität des Schutzes auf Ihrem Computer. 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 6.0 SOS eine Sicherungskopie davon an. Bei Bedarf können Sie zu den vorhergehenden Signaturen zurückkehren.

Die Möglichkeit des Rollbacks (s. Pkt. 9.2 auf S. 86) 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. 9.4.4 auf S. 95). 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.

9.1. Starten des Updates

Sie können das Programm-Update jederzeit starten. Die Aktualisierung erfolgt von der von Ihnen gewählten Updatequelle (s. Pkt. 9.4.1 auf S. 89).


Das Programm-Update kann gestartet werden:

- aus dem Kontextmenü (s. Pkt. 4.2 auf S. 41).
- aus dem Hauptfenster des Programms (s. Pkt. 4.3 auf S. 42).

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. 9.4.4 auf S. 95).

9.2. Rückkehr zum vorherigen Update

Jedes Mal, wenn Sie das Programm-Update starten, erstellt Kaspersky Anti-Virus 6.0 SOS 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.

9.3. Erstellen einer Update-Aufgabe

Kaspersky Anti-Virus 6.0 SOS verfügt über eine integrierte Update-Aufgabe für das Update der Bedrohungssignaturen und Programm-Module. Sie können aber auch eigene Update-Aufgaben mit anderen Parametern oder alternativem Startzeitplan erstellen.

Wenn Sie Kaspersky Anti-Virus 6.0 SOS beispielsweise auf einem Laptop installiert haben, den Sie zu Hause und im Büro nutzen, 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**. Die Aufgabe erscheint mit dem angegebenen Namen im Abschnitt **Service** des Programmhauptfensters.

Achtung!

Es können maximal Update-Aufgaben vom Benutzer erstellt werden.

Die neue Aufgabe übernimmt alle Parameter der Aufgabe, auf deren Grundlage sie erstellt wurde, unter Ausnahme des Zeitplans. Der automatische Start der neuen Aufgabe ist in der Grundeinstellung deaktiviert.

Nehmen Sie nach dem Erstellen einer Aufgabe folgende Zusatzeinstellungen vor: Angabe der Updatequelle (s. Pkt. 9.4.1 auf S. 69) und der Parameter für die Netzwerkverbindung (s. Pkt. 9.4.3 auf S. 93). Falls erforderlich, muss außerdem der Aufgabenstart mit Rechten aktiviert (s. Pkt. 6.4 auf S. 58) und der Zeitplan konfiguriert (s. Pkt. 6.5 auf S. 60) 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.

9.4. 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. 9.4.1 auf S. 89).
- in welchem Modus die Programmaktualisierung gestartet wird und welche Elemente aktualisiert werden sollen (s. Pkt. 9.4.2 auf S. 91).
- wie oft das Update gestartet werden soll, wenn der Start nach Zeitplan aktiviert ist (s. Pkt. 6.5 auf S. 60).
- unter welchem Benutzerkonto das Update ausgeführt wird (s. Pkt. 6.4 auf S. 58).
- ob die heruntergeladenen Updates in einen lokalen Ordner kopiert werden sollen (s. Pkt. 9.4.4 auf S. 95).
- welche Aktionen nach dem Programm-Update ausgeführt werden sollen (s. Pkt. 9.4.5 auf S. 96).

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

9.4.1. Auswahl der Updatequelle

Eine *Updatequelle* ist eine bestimmte Ressource, die Updates der Bedrohungssignaturen und der Module für Kaspersky Anti-Virus 6.0 SOS 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. 18).

Die Aktualisierung erfolgt standardmäßig von den Kaspersky-Lab-Updateservern. Die Serverliste kann nicht verändert werden. Beim Updateprozess greift Kaspersky Anti-Virus 6.0 SOS 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://<Benutzername>:<Kennwort>@<Host>:<Port>` angegeben werden.

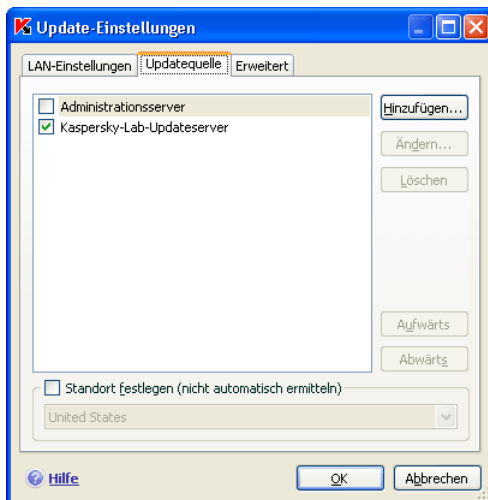


Abbildung 18. Auswahl der Updatequelle

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 6.0 SOS 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 Kaspersky-Lab-Updateserver stehen als Quellen nicht für Änderungen oder zum Löschen zur Verfügung.

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 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.

9.4.2. 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. 19) bestimmt, bestimmt, welche Elemente aktualisiert werden:

- Bedrohungssignaturen
- Programm-Module

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

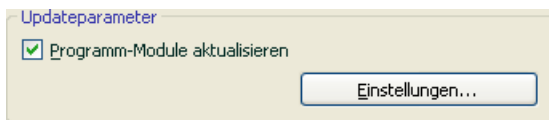


Abbildung 19. Auswahl des Update-Objekts

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. 20) bestimmt, auf welche Weise die Aktualisierung gestartet wird. Sie können im Block **Startmodus** einen der folgenden Modi wählen:

- Automatisch.** Kaspersky Anti-Virus 6.0 SOS prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Wenn neue Updates vorhanden sind, lädt Kaspersky Anti-Virus sie herunter und installiert sie auf dem Computer. Dieser Updatemodus wird standardmäßig benutzt.

Wenn als Quelle eine Netzwerkressource gewählt wurde, führt Kaspersky Anti-Virus 6.0 SOS 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 und Programm-Module versorgt, was die Möglichkeit des Eindringens gefährlicher Programme auf Ihren Computer verhindert.

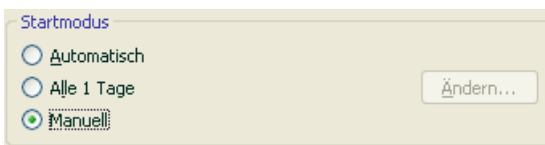



Abbildung 20. Auswahl des Startmodus für das Update

- 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. 60).

 **Manuell.** In diesem Fall starten Sie die Aktualisierung des Programms selbständig. Kaspersky Anti-Virus 6.0 SOS informiert Sie bei Bedarf über die Notwendigkeit der Aktualisierung:

- erstens wird über dem Programmsymbol im Infobereich eine entsprechende Meldung eingeblendet (wenn der Benachrichtigungsdienst aktiviert ist) (s. Pkt. 10.8 auf S. 119).
- zweitens erscheint im Bereich der Kommentare und Empfehlungen des Hauptfensters eine Empfehlung zum Programm-Update (s. Pkt. 4.3 auf S. 42).

9.4.3. 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. 21).

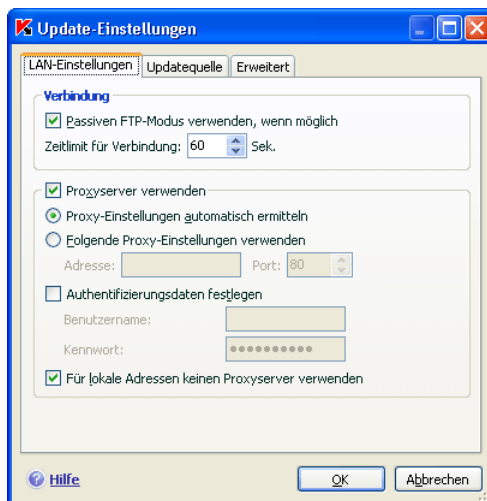


Abbildung 21. Anpassen der Netzwerkeinstellungen für das Update

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.

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 6.0 SOS 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 Anmelddaten 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. 58).

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.**

Dieser Parameter steht nicht zur Verfügung, wenn das Programm auf einem Computer mit Microsoft Windows 9X/NT 4.0 installiert ist. Allerdings wird für lokale Adressen standardmäßig kein Proxyserver verwendet.

9.4.4. Update-Verteilung

Wenn PCs zu einem lokalen Netzwerk zusammengeschlossen sind, ist es überflüssig die Updates für jeden Computer einzeln herunterzuladen und zu installieren, weil dadurch eine erhöhte Netzwerkbelastung verursacht wird. Sie können den Dienst zur Update-Verteilung verwenden, der es erlaubt, die Netzwerkbelastung zu senken, indem das Updateverfahren folgendermaßen organisiert wird:

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 22) 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.

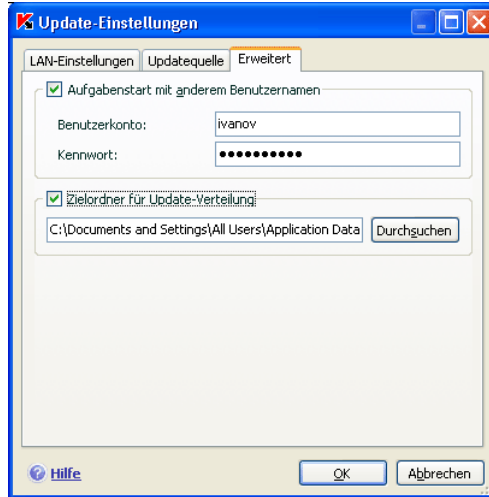


Abbildung 22. Einstellungen für den Dienst zur Update-Verteilung

Beachten Sie, dass Kaspersky Anti-Virus 6.0 SOS von den Kaspersky-Lab-Updateservern nur das Updatepaket für die Anwendungen der Version 6.0 erhält. Es wird empfohlen, die Update-Verteilung für andere Kaspersky-Lab-Anwendungen über Kaspersky Administration Kit auszuführen.

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.

9.4.5. 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. 10.1 auf S. 99). Möglicherweise kann Kaspersky Anti-Virus 6.0 SOS 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 **Quarantäne dateien 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 6.0 SOS über eine vordefinierte Aufgabe zur Untersuchung der Autostart-Objekte (s. Kapitel 7 auf S. 64). 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. 60).

KAPITEL 10. ZUSÄTZLICHE OPTIONEN

Neben dem Schutz Ihrer Daten bietet das Programm zusätzliche Dienste, welche die Funktionalität von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS verändert oder gelöscht wurden (s. Pkt. 10.2 auf S. 103). 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. 10.1 auf S. 99).

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 6.0 SOS (s. Pkt. 10.6 auf S. 115). 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 6.0 SOS (s. Pkt. 10.8 auf S. 119). Dies können einerseits Ereignisse informativen Charakters sein, andererseits aber Fehler, die unverzüglich behoben werden müssen und hohe Priorität besitzen.
- Der Dienst für die Beschränkung des Zugriffs auf das Programm bietet Schutz vor der externen Steuerung der Programmdienste und kontrolliert die Beschränkung von Rechten anderer Benutzer Ihres Computers zum Ausführen bestimmter Aktionen mit Kaspersky Anti-Virus (s. Pkt. 10.8.2 auf S. 124). Beispielsweise kann das Ändern der Sicherheitsstufe

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. 10.5 auf S. 114).

Darüber hinaus bietet das Programm ein ausführliches Hilfesystem (s. Pkt. 10.4 auf S. 113) und detaillierte Berichte (s. Pkt. 10.3 auf S. 105) über die Ausführung aller Aufgaben zur Virensuche und zum Update.

Außerdem besteht die Möglichkeit, das Aussehen von Kaspersky Anti-Virus 6.0 SOS zu ändern und die Parameter der aktuellen Programmoberfläche zu konfigurieren (s. Pkt. 10.7 auf S. 117).

Im Folgenden werden alle genannten Dienste ausführlich beschrieben.

10.1. 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 6.0 SOS 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 6.0 SOS 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 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.

10.1.1. 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 6.0 SOS 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. 23) 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, die manuell in die Quarantäne verschoben wurde, bei einer folgenden Untersuchung als virenfrei erkannt wird, ändert sich ihr Status nicht gleich 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.

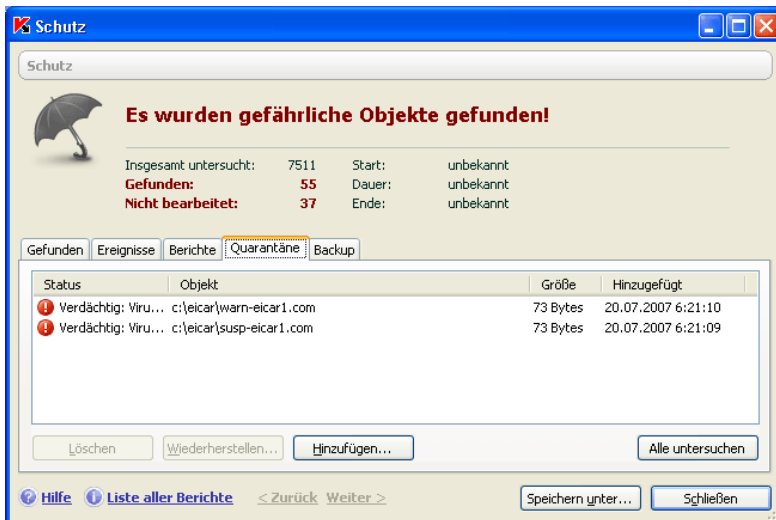


Abbildung 23. Liste der Quarantäneobjekte

- 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.

- Dateien wiederherstellen – entweder in einem vom Benutzer gewählten 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.

10.1.2. 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. 9.4.4 auf S. 95).

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 6.0 SOS mit der Schaltfläche Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie **Datenverwaltung** in der Konfigurationsstruktur.
3. Legen Sie im Block **Quarantäne und Backup** (s. Abb. 24) den Zeitraum fest, nach dem Quarantäneobjekte automatisch gelöscht werden sollen.

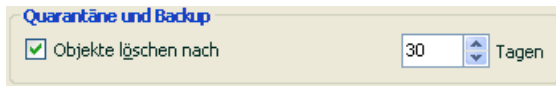


Abbildung 24. Anpassen der Speicherdauer für Quarantäneobjekte

10.2. 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.

10.2.1. 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 6.0 SOS 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. 25) 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.

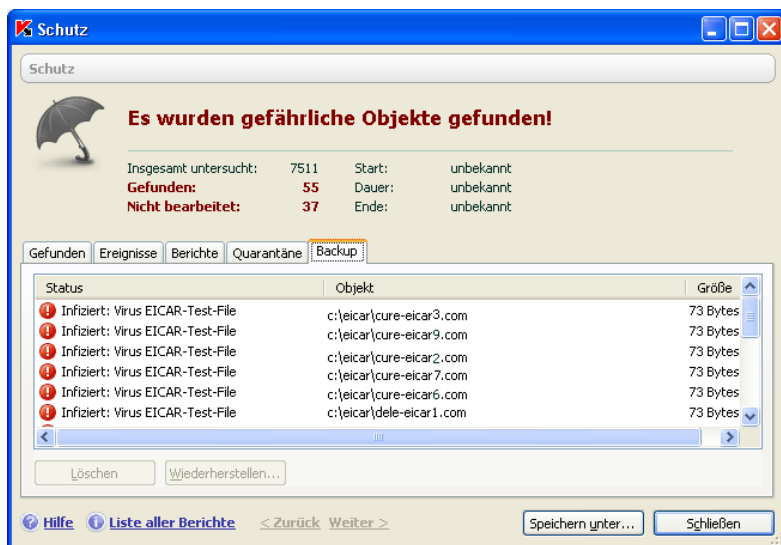


Abbildung 25. Sicherungskopien von gelöschten oder desinfizierten Objekten

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. 10.2.2 auf S. 105).

10.2.2. Konfiguration der Backup-Einstellungen

Sie können die maximale Speicherdauer der Kopien im Backup festlegen.

Standardmäßig beträgt die Speicherdauer für Kopien gefährlicher Objekte 30 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 6.0 SOS 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. 24).

10.3. Berichte

Die Ausführung jeder Aufgabe zur Virensuche und des Updates wird 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. 26). Hier befinden sich die neuesten Berichte für alle Aufgaben zur Virensuche und zum Update, die in der laufenden Sitzung von Kaspersky Anti-Virus 6.0 SOS gestartet wurden. Neben jeder 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**.

Um alle Ereignisse anzuzeigen, die im Bericht über die Ausführung einer Aufgabe aufgezeichnet wurden,

wählen Sie den Namen der Aufgabe auf der Registerkarte **Berichte** und klicken Sie auf die Schaltfläche **Details**.

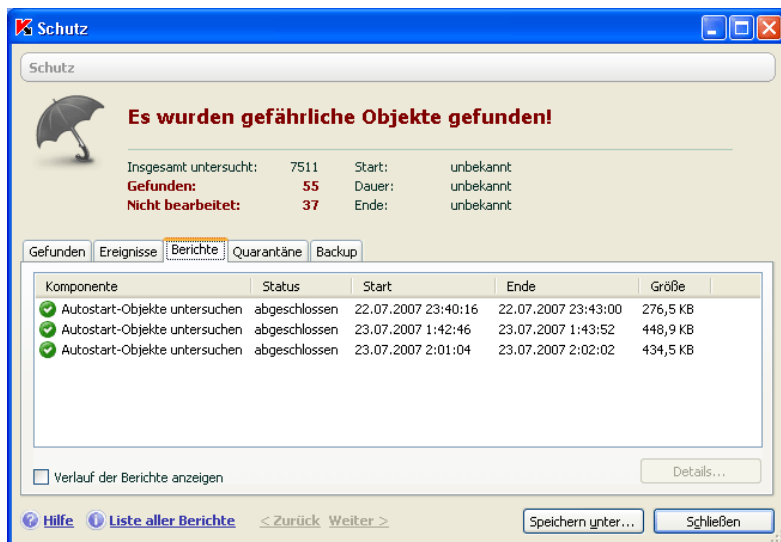


Abbildung 26. Berichte über die Arbeit einer Untersuchungsaufgabe

Dadurch wird ein Fenster geöffnet, das Detailinformationen über die Arbeit der gewählten 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 dem Ausführen einer Untersuchungsaufgabe gefunden wurden.

- Die Registerkarte **Ereignisse** informiert über die Ereignisse bei der Arbeit einer Aufgabe.
- Die Registerkarte **Statistik** umfasst eine ausführliche Statistik aller untersuchten Objekte.
- Die Registerkarte **Einstellungen** enthält die Parameter, mit denen die Aufgabe zur Virensuche oder das Update der Bedrohungssignaturen arbeitet.

Sie können den gesamten Bericht in eine Textdatei importieren. Das kann beispielsweise von Nutzen sein, wenn bei der Arbeit einer Komponente 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 Aufgabe, deren Bericht Sie geöffnet haben. Unten werden alle möglichen Punkte genannt):

- **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 6.0 SOS 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 aufsteigen oder absteigend sortieren.

10.3.1. Konfiguration der Berichtsparemeter

Zur Konfiguration der Parameter für das Erstellen und Speichern von Berichten

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus 6.0 SOS mit dem Link Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Datenverwaltung**.
3. Nehmen Sie im Block **Berichte** (s. Abb. 27) 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 30 Tage. Sie können die Speicherdauer ändern oder diese Beschränkung völlig aufheben.

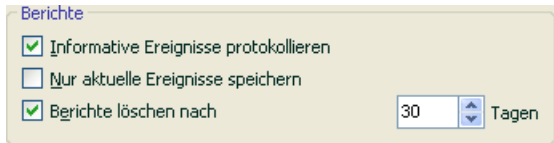


Abbildung 27. Einstellungen für das Erstellen von Berichten

10.3.2. Registerkarte *Gefunden*

Diese Registerkarte (s. Abb. 28) enthält eine Liste der gefährlichen Objekte, die von Kaspersky Anti-Virus 6.0 SOS 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**.

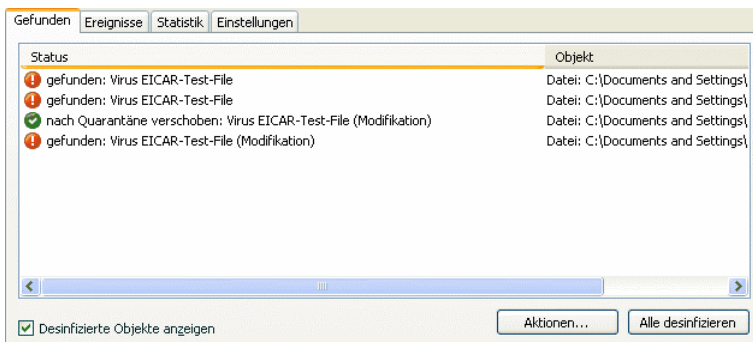


Abbildung 28. Liste der gefundenen gefährlichen Objekte

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Anti-Virus 6.0 SOS 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.

10.3.3. Registerkarte *Ereignisse*

Auf dieser Registerkarte (s. Abb. 29) wird eine vollständige Liste aller wichtigen Ereignisse 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.

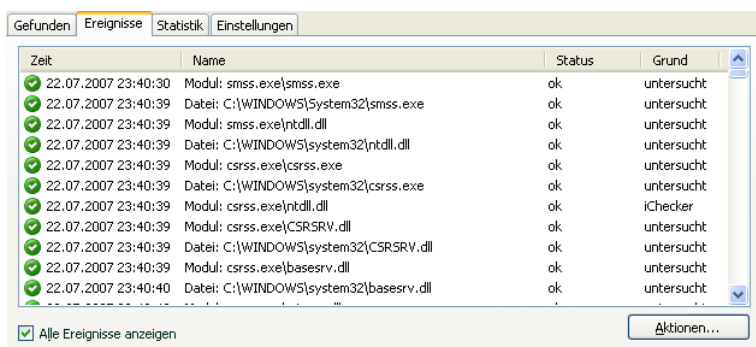


Abbildung 29. Ereignisse, die bei der Arbeit einer Komponente aufgetreten sind

Das Format der im Ereignisbericht enthaltenen Ereignisse kann in Abhängigkeit von der 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.

10.3.4. Registerkarte *Statistik*

Eine ausführliche Statistik über die Ausführung der Aufgabe zur Virensuche wird auf dieser Registerkarte aufgezeichnet (s. Abb. 30). Hier können Sie erfahren:

- Wie viele Objekte 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	Gefährlich	Nicht beseitigt	Gelöscht	Nach Quarantäne verschoben	Archive	Geprüft
Alle Objekte	1926	0	0	0	0	1	8
Systemspeicher	1505	0	0	0	0	1	1
Autostart-Objekte	419	0	0	0	0	0	7
Laufwerksbootsektoren	2	0	0	0	0	0	0

Abbildung 30. Statistik über die Arbeit einer Komponente

10.3.5. Registerkarte *Einstellungen*

Die Registerkarte **Einstellungen** (s. Abb. 31) enthält eine vollständige Übersicht der Parameter, mit denen die Untersuchungsaufgabe bzw. das Programm-Update ausgeführt wird. Sie können erfahren, welche Schutzstufe die Arbeit der Komponente 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.

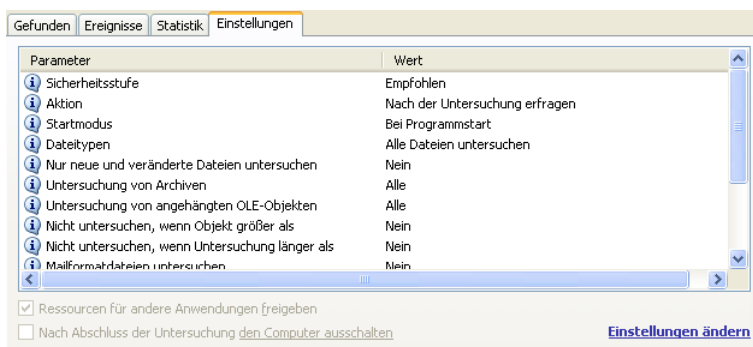


Abbildung 31. Einstellungen für die Arbeit einer Komponente

- Modus für die Arbeit des Computers nach dem Abschluss der Untersuchungsaufgabe bestimmen. Sie können festlegen, dass 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.

Diese Option ist beispielsweise dann von Nutzen, wenn Sie die Virenuntersuchung des Computers kurz vor Feierabend starten und nicht auf deren Abschluss warten möchten.

Die Verwendung dieser Option erfordert allerdings folgende zusätzlichen Vorbereitungen: Vor dem Untersuchungsstart muss die Kennwortabfrage bei der Objektuntersuchung deaktiviert werden, falls diese aktiviert war, und der Modus zur automatischen Bearbeitung gefährlicher Objekte muss festgelegt werden. Dadurch wird der interaktive Funktionsmodus des Programms abgeschaltet. Das Programm führt keine Anfragen durch, welche Ihre Reaktion erfordern und den Untersuchungsvorgang unterbrechen.

10.4. Allgemeine Informationen über die Anwendung

Allgemeine Informationen über das Programm finden Sie im Abschnitt **Service** des Hauptfensters (s. Abb. 32).

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 6.0 SOS 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. 10.6 auf S. 115).

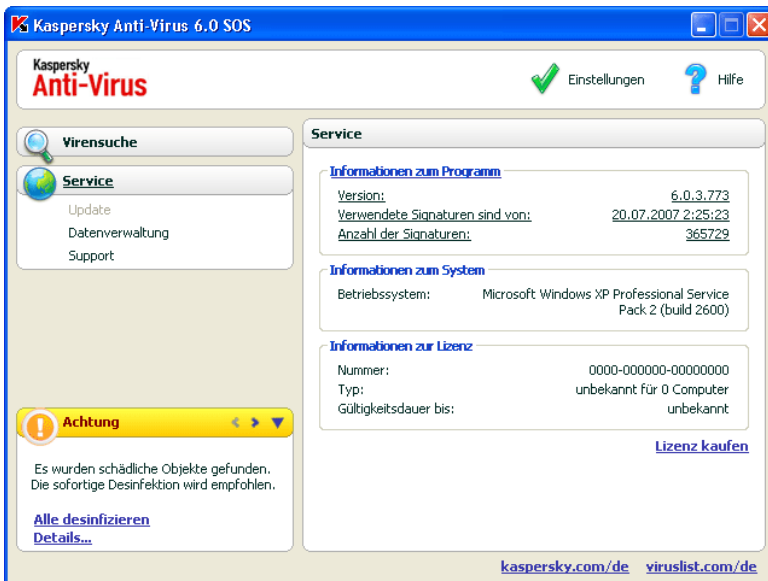


Abbildung 32. Informationen zu Programm, Programmlizenz und Betriebssystem

10.5. Lizenzverwaltung

Die Möglichkeit zur Nutzung von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS 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 6.0 SOS 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, 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 6.0 SOS 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 Kaspersky Anti-Virus 6.0 SOS 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. Abbildung 33). 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.

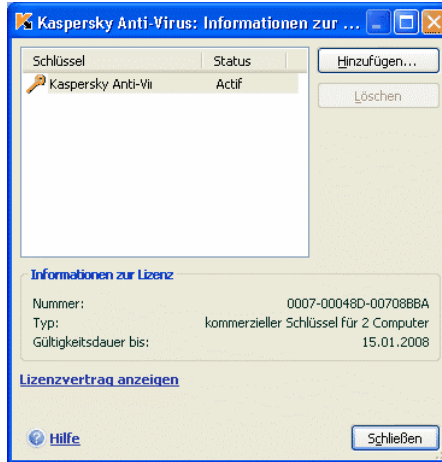


Abbildung 33. Informationen zur Lizenz

Informationen zum verwendeten Lizenzschlüssel befinden sich im Block **Informationen zur Lizenz** des Abschnitts **Service** im Hauptfenster der Anwendung. In das Fenster zur Lizenzverwaltung gelangen Sie durch Linksklick an eine beliebige Stelle des Blocks. Im folgenden Fenster (s. Abb. Abbildung 33) können Sie Informationen über den aktiven Schlüssel lesen sowie 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. 3.2.1 auf S. 30). 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](#).

10.6. Technischer Support für Benutzer

Kaspersky Anti-Virus 6.0 SOS 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. 34) im Abschnitt **Service**.

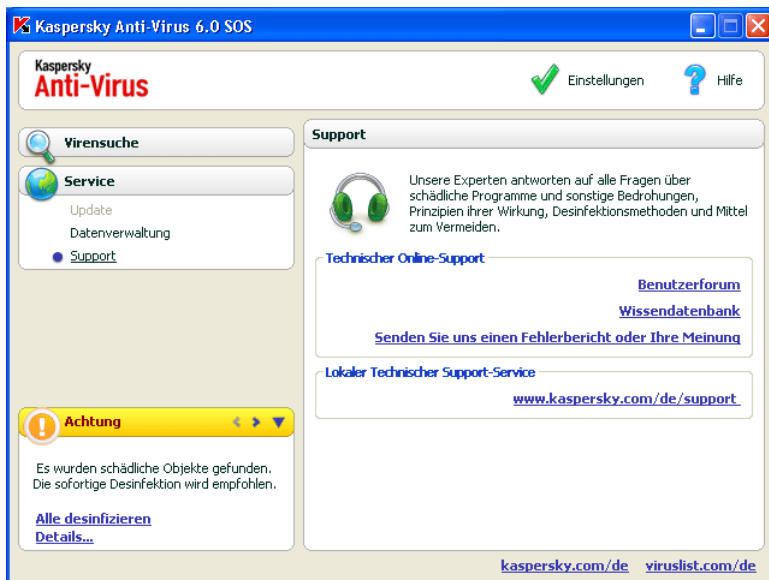


Abbildung 34. Informationen zum technischen Kundendienst

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 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 6.0 SOS 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.

10.7. Konfiguration der Oberfläche von Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS über den Link [Einstellungen](#) des Hauptfensters.
2. Wählen Sie **Ansicht** im Abschnitt **Service** der Konfigurationsstruktur des Programms (s. Abb. 35).

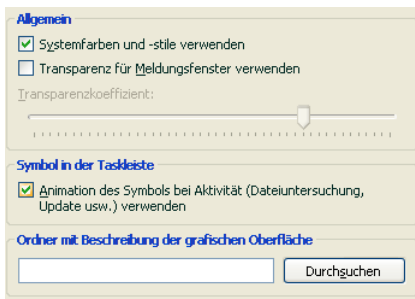


Abbildung 35. Einstellungen für die Programmoberfläche

Auf der rechten Seite des Konfigurationsfensters können Sie festlegen:

- ob das Programmsymbol im Infobereich der Taskleiste animiert werden soll oder nicht.

In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Wird beispielsweise das Update ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. 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 Status der Programms auf Ihrem Computer wieder: Wenn die Anwendung gestartet wurde, wird das Symbol in grauer Farbe angezeigt.

- Transparenzstufe der Popupmeldungen.

Alle Operationen von Kaspersky Anti-Virus 6.0 SOS, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Popupmeldung über dem Programmsymbol im Infobereich. Die Meldungsfenster sind halbtransparent, damit sie Ihre Arbeit nicht 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.

Diese Option steht nicht zur Verfügung, wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows 98/NT 4.0/ME installiert ist.

- Verwendung eigener grafischer Elemente und Farbpaletten auf der Programmoberfläche.

Alle auf der Oberfläche von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS beim Wiederherstellen der Standardeinstellungen oder bei der Deinstallation der Anwendung nicht gespeichert werden.

10.8. Benachrichtigungen über Ereignisse von Kaspersky Anti-Virus 6.0 SOS

Bei der Arbeit von Kaspersky Anti-Virus 6.0 SOS treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Anti-Virus 6.0 SOS 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. Öffnen Sie mit dem Link Einstellungen des Hauptfensters das Konfigurationsfenster des Programms.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.
3. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** im Block **Interaktion mit dem Benutzer** (s. Abb. 36).

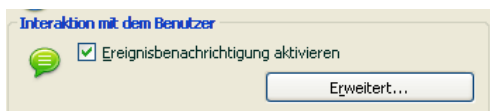


Abbildung 36. Aktivieren des Benachrichtigungsmodus

4. Legen Sie die Typen der Ereignisse von Kaspersky Anti-Virus 6.0 SOS fest, über deren Eintreten Sie benachrichtigt werden möchten, und wählen Sie eine Methode zum Senden der Benachrichtigungen (s. Pkt. 10.8.1.1 auf S. 120).
5. Passen Sie die Einstellungen für das Senden von Benachrichtigungen per E-Mail an, wenn Sie diese Benachrichtigungsmethode wünschen (s. Pkt. 10.8.1.2 auf S. 122).

10.8.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen

Bei der Arbeit von Kaspersky Anti-Virus 6.0 SOS 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: *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 37) können Sie folgende Benachrichtigungsmethoden für die oben genannten Ereignisse anpassen:

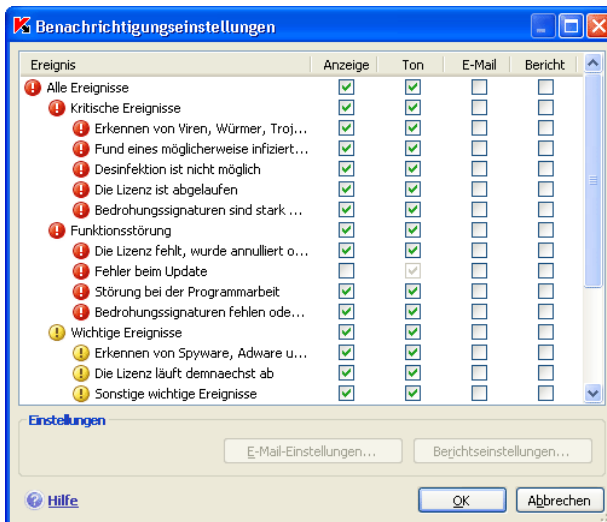


Abbildung 37. Ereignisse bei der Programmarbeit und entsprechende Benachrichtigungsmethoden

- *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. 10.8.1.2 auf S. 122).

- *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. 10.8.1.3 auf S. 123) an.

10.8.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail

Nachdem Sie die Ereignisse gewählt haben (s. Pkt. 10.8.1.1 auf S. 120), 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 **Benachrichtigungseinstellungen** (s. Abb. Abbildung 38) 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.
 - 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.

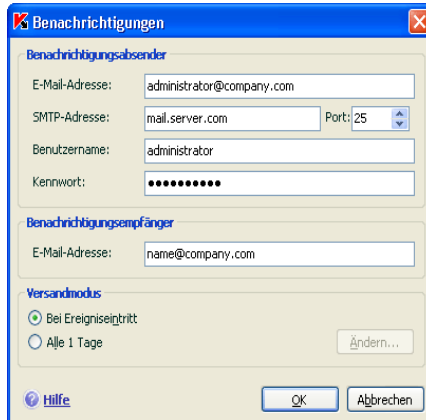


Abbildung 38. Einstellungen für E-Mail-Benachrichtigung

10.8.1.3. 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 6.0 SOS 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 6.0 SOS (**Kaspersky Event Log**) aufzuzeichnen.

Auf einem Computer mit dem Betriebssystem Microsoft Windows 98/ME ist das Führen von Ereignisberichten nicht möglich. Mit dem Betriebssystem Microsoft

Windows NT 4.0 steht der Bericht **Kaspersky Event Log** nicht zur Verfügung.

Diese Einschränkungen hängen mit Besonderheiten der genannten Betriebssysteme zusammen.

Zur Anzeige der Berichte dient das Microsoft Windows-Standardfenster **Ereignisanzeige**, das mit Hilfe des folgenden Befehls geöffnet wird: **Start** → **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Ereignisanzeige**.

10.8.2. Zugriffsbeschränkung für das Programm

Kaspersky Anti-Virus 6.0 SOS 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 einen Mechanismus zum Schutz vor externem Zugriff und zum Kennwortschutz für den Programmmzugriff.

Um den Zugriff auf das Programm zu beschränken:

1. Öffnen Sie das Konfigurationsfenster des Programms mit dem Link Einstellungen des Hauptfensters.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.
3. Aktivieren Sie im Block **Selbstschutz** (s. Abb. 39) das Kontrollkästchen **Externe Dienststeuerung verbieten**. In diesem Fall wird jeder Versuch zur Fernsteuerung von Diensten der Anwendung blockiert.

Wird versucht, das Programm fernzusteuern, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).

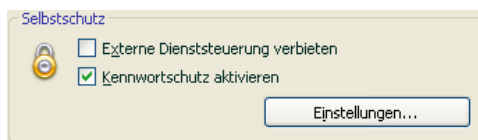


Abbildung 39. Einstellungen für den Programmschutz

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. 40). 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 6.0 SOS 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 Benutzer Ihres Computers berechtigt sein sollen, diese Aktionen auszuführen.

Beim Versuch eines beliebigen Benutzers Ihres Computers, die von Ihnen festgelegten Aktionen auszuführen, wird das Programm nun immer das Kennwort abfragen.

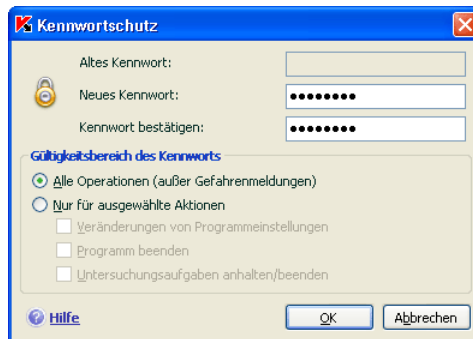


Abbildung 40. Einstellungen für den Kennwortschutz des Programms

10.9. Export/Import der Einstellungen von Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS bietet Ihnen die Möglichkeit zum Exportieren und Importieren seiner Programmeinstellungen.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie das Programm auf Ihrem Privat-PC und im Büro installiert haben. Sie können das Programm zu Hause entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

Um die aktuellen Programmeinstellungen zu exportieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Anti-Virus 6.0 SOS.
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 6.0 SOS.
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 6.0 SOS importieren möchten.

10.10. 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**.

Der Konfigurationsassistent wird gestartet. Folgen Sie den Anweisungen.

Nach dem Abschluss des Assistenten wird für alle Aufgaben 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 11. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE

Sie können mit Kaspersky Anti-Virus 6.0 SOS mit Hilfe der Befehlszeile arbeiten. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Aufgaben zur Virensuche.
- Erhalt von Informationen über den aktuellen Status von 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 Aktivierungscode
START	Starten einer Aufgabe
PAUSE	Anhalten der Arbeit einer Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die

	Programmoberfläche festgelegte Kennwort angegeben wird)
RESUME	Fortsetzen der Arbeit einer Aufgabe
STOP	Beenden der Arbeit einer Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
STATUS	Bildschirmanzeige des aktuellen Status einer Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit 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 Schutzeinstellungen für Kaspersky Anti-Virus 6.0 SOS (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXPORT	Exportieren von Schutzeinstellungen für Kaspersky Anti-Virus 6.0 SOS

Jedem Befehl entspricht eine eigene Auswahl von Parametern.

11.1. Aktivierung der Anwendung

Die Aktivierung des Programms kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscodes (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 6.0 SOS, das über die Benutzeroberfläche der Anwendung festgelegt wurde.

Beispiel:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<Kennwort>
```

11.2. Steuerung von Aufgaben

Syntax der Befehlszeile:

```
avp.com <Befehl> <Aufgabenname>
avp.com STOP|PAUSE <Aufgabenname>
/password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Beschreibung der Parameter:

<Befehl>	Die Steuerung der Aufgaben von Kaspersky Anti-Virus wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Aufgabe.
-----------------------	---

	<p>STOP – Beenden einer Aufgabe.</p> <p>PAUSE – Anhalten einer Aufgabe.</p> <p>RESUME – Fortsetzen einer Aufgabe.</p> <p>STATUS – Den aktuellen Status einer Aufgabe auf dem Bildschirm anzeigen.</p> <p>STATISTICS – Die Statistik über die Arbeit 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>
<Aufgabenname>	<p>Als Wert für den Parameter <Aufgabenname> kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Update-Aufgabe angegeben werden:</p> <p>Für die vordefinierten Aufgaben gelten folgende Werte:</p> <p>UPDATER – Update</p> <p>RetranslationCfg – Kopieren der Updates in eine lokale Quelle</p> <p>Rollback – Rollback des letzten Updates</p> <p>SCAN_OBJECTS – Aufgabe zur Untersuchung eines einzelnen Objekts (Datei, Ordner, Laufwerk)</p> <p>SCAN_MY_COMPUTER – Aufgabe zur vollständigen Untersuchung des Computers</p> <p>SCAN_CRITICAL_AREAS – Aufgabe zur Untersuchung kritischer Bereiche</p> <p>SCAN_STARTUP – Aufgabe zur Untersuchung der Autostart-Objekte</p> <p>SCAN_QUARANTINE – Aufgabe zur Untersuchung der Quarantäneobjekte</p>
<Kennwort>	<p>Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche angegeben wurde.</p>
/R[A]:<Berichtsdatei>	<p>R:<Berichtsdatei> – nur wichtige Ereignisse im</p>

	<p>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>
<p>Die aus der Befehlszeile gestarteten Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.</p>	

Beispiel:

Um die Aufgabe Arbeitsplatz zu beenden, geben Sie in der Befehlszeile ein:

```
avp.com STOP SCAN_MY_COMPUTER /password=<Kennwort>
```

11.3. 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 6.0 SOS erstellten Aufgaben verwenden, indem Sie die erforderliche Befehlszeile benutzen (s. Pkt. 11.1 auf S. 130). 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 Netzwerklauferwerke.
/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 <code>/i8</code> entspricht.</p>	
<code>/i0</code>	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
<code>/i1</code>	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
<code>/i2</code>	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).
<code>/i3</code>	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
<code>/i4</code>	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
<code>/i8</code>	den Benutzer beim Fund eines infizierten Objekts nach einer Aktion fragen
<code>/i9</code>	den Benutzer nach dem Abschluss der Untersuchung nach einer Aktion fragen
<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>	
<code>/fe</code>	nur infizierbare Dateien nach Erweiterung untersuchen.
<code>/fi</code>	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 6.0 SOS 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 Virenungersuchung festlegt.	
/iChecker=<on off>	Verwendung der Technologie iChecker 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

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
```

11.4. Programm-Update

Der Befehl für das Update der Programm-Module und Bedrohungssignaturen von Kaspersky Anti-Virus 6.0 SOS 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 Pfades ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Anti-Virus 6.0 SOS festgelegt wurden.</p>
<code>/APP=<on off></code>	<p>Update der Programm-Module aktivieren/deaktivieren.</p>

Beispiele:

Update der Bedrohungssignaturen, alle Ereignisse protokollieren:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update der Programm-Module von Kaspersky Anti-Virus 6.0 SOS, 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
```

11.5. 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 6.0 SOS, das über die Programmoberfläche festgelegt wurde.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

11.6. Export von Schutzparametern

Syntax der Befehlszeile:

```
avp.com EXPORT <Profil> <Dateiname>
```

Beschreibung der Parameter:

<Profil>	<p>Aufgabe, für die der Export von Parametern ausgeführt wird.</p> <p>Als Wert des Parameters <Profil> kann einer der in Pkt. 11.2 auf S. 130 genannten Werte verwendet werden.</p>
-----------------------	--

<Dateiname>	<p>Pfad der Datei, in welche die Parameter von Kaspersky Anti-Virus 6.0 SOS exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.</p> <p>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.</p>
--------------------------	---

Beispiel:

```
avp.com EXPORT c:\settings.dat
```

11.7. Import von Schutzparametern

Syntax der Befehlszeile:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	<p>Pfad der Datei, aus welcher die Parameter von Kaspersky Anti-Virus 6.0 SOS 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>
<Kennwort>	<p>Kennwort für Kaspersky Anti-Virus 6.0 SOS, das über die Programmoberfläche festgelegt wurde.</p>

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Kennwort>
```

11.8. Anwendung starten

Syntax der Befehlszeile:

avp.com

11.9. Anwendung beenden

Syntax der Befehlszeile:

EXIT /password=<Kennwort>

<Kennwort>	Kennwort für Kaspersky Anti-Virus 6.0 SOS, das über die Programmoberfläche festgelegt wurde.
------------	--

11.10. 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>	<p>Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden.</p> <p>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.

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
```

11.11. 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>
```

11.12. 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 12. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN

Zur Deinstallation des Programms stehen folgende Varianten zur Verfügung:

- mit Hilfe des Installationsassistenten (s. Pkt. 12.1 auf S. 144)
- aus der Befehlszeile (s. Pkt. 12.2 auf S. 146)
- 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. 38).

12.1. 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.

Das Ändern des Komponentenbestands erlaubt Ihnen, bestimmte Komponenten von Kaspersky Anti-Virus nachträglich zu installieren oder jene Komponenten zu löschen, die nicht gebraucht werden. Sie können beispielsweise den Konnektor für den Administrationsagenten von Kaspersky Administration Kit installieren oder entfernen.

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 6.0 SOS 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 SOS** → **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 6.0 SOS 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, 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, die zuvor installiert wurden, werden aktualisiert und die empfohlene Sicherheitsstufe wird eingestellt.

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 6.0 SOS 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* – Schlüsseldatei, die für die Arbeit der Anwendung erforderlich ist.

- *Bedrohungssignaturen* – vollständige Signaturen der gefährlichen Programme, Viren und anderen Bedrohungen, die beim letzten Update aktuell waren.
- *Backup-Objekte* – Sicherungskopien von gelöschten oder desinfizierten 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.
- *Programmeinstellungen* – Parameterwerte für die Arbeit des Programms.

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.

12.2. Deinstallation des Programms aus der Befehlszeile

Um Kaspersky Anti-Virus 6.0 SOS aus der Befehlszeile zu deinstallieren, geben Sie ein:

```
msiexec /x <Paketname>
```

Es wird ein Installationsassistent gestartet (s. Kapitel 12 auf S. 144), 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.
```

KAPITEL 13. 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 SOS 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 SOS über Kaspersky Administration Kit zu steuern:

- Richten Sie im Netzwerk einen *Administrationsserver* ein. Installieren Sie die *Administrationskonsole* am Arbeitsplatz des Administrators (Details siehe Administratorenhandbuch zum Einrichten von "Kaspersky Administration Kit 6.0").
- Richten Sie Kaspersky Anti-Virus 6.0 SOS und den *Administrationsagenten* (der zum Lieferumfang von Kaspersky Administration Kit gehört) auf den Netzwerkcomputern ein. Details über die Remote-Installation des Pakets Kaspersky Anti-Virus 6.0 SOS auf Netzwerkcomputern finden Sie im Administratorenhandbuch zum Einrichten von "Kaspersky Administration Kit 6.0".

Wenn Kaspersky Anti-Virus 6.0 SOS über Kaspersky Administration Kit gesteuert wird, beachten Sie folgende Besonderheiten!

Wenn auf den Netzwerkcomputern die Version 5.0 von Kaspersky Anti-Virus eingerichtet ist, sind beim Update auf Version 6.0 über Kaspersky Administration Kit folgende Vorbereitungen erforderlich:

- Beenden Sie vor der Installation die Vorgängerversion der Anwendung (das ist im entfernten Modus über Kaspersky Administration Kit möglich).
- Beenden Sie vor Beginn der Installation alle laufenden Anwendungen.
- Führen Sie die Programminstallation der Version 6.0 aus.

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. 41). Sie stellt ein standardmäßiges **Interface** dar, **das in MMC integriert ist**, und erlaubt dem Administrator folgende Funktionen auszuführen:

- entfernte Installation von Kaspersky Anti-Virus 6.0 SOS und des *Administrationsagenten* auf den Netzwerkcomputern.
- entfernte Konfiguration von Kaspersky Anti-Virus 6.0 SOS auf den Netzwerkcomputern.
- Aktualisierung der Bedrohungssignaturen und der Module von Kaspersky Anti-Virus 6.0 SOS.
- Verwaltung der Lizenzen für Kaspersky Anti-Virus 6.0 SOS auf den Netzwerkcomputern.
- Anzeige von Informationen über die Arbeit der Anwendung auf den Client-Computern.

Kaspersky Anti-Virus 6.0 SOS bietet keinen Echtzeitschutz für den Computer. Deshalb wird für Kaspersky Anti-Virus 6.0 SOS im Detailfenster der Administrationskonsole von Kaspersky Administration Kit der Status **Kritisch** (rotes Symbol neben dem Namen des Computers) angezeigt.

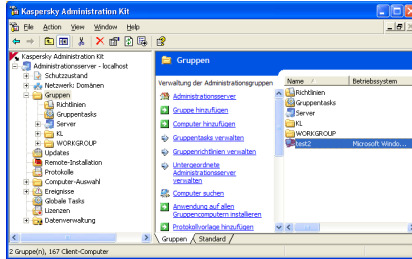


Abbildung 41. Administrationskonsole von Kaspersky Administration Kit¹

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 Aufgabenparameter, Parameter für den Backup-Speicher und die Quarantäne, Parameter für die Berichterstattung u.a. gehören.

Eine **Aufgabe** ist eine benannte Aktion, die von der Anwendung ausgeführt werden kann. Entsprechend der Funktionen werden die Aufgaben von Kaspersky Anti-Virus 6.0 SOS in Typen unterteilt (Untersuchungsaufgabe, Aufgabe zum Update der Anwendung oder zum Rollback von Updates, Aufgabe zur Installation eines Lizenzschlüssels). Jeder konkreten Aufgabe entspricht bei ihrer Ausführung eine Auswahl von Funktionsparametern der Anwendung – 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.

¹ Das Aussehen des Hauptfensters von Kaspersky Administration Kit kann in Abhängigkeit des auf Ihrem Computer verwendeten Betriebssystems variieren.

13.1. Anwendung verwalten

Kaspersky Administration Kit bietet die Möglichkeit, den Start und das Beenden von Kaspersky Anti-Virus 6.0 SOS 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. 41) 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. 42) wird eine vollständige Liste aller Kaspersky-Lab-Anwendungen angezeigt, die auf dem Client-Computer installiert sind. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 SOS** aus.

Unter der Liste mit den Anwendungen befinden sich 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. 13.1.2 auf S. 153).

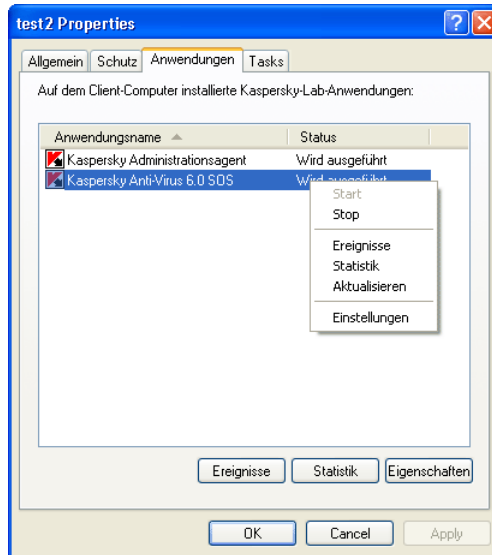


Abbildung 42. Liste der Kaspersky-Lab-Anwendungen

13.1.1. Anwendung starten / beenden

Der Start und das Beenden von Kaspersky Anti-Virus 6.0 SOS auf einem entfernten Client-Computer wird mit Hilfe der entsprechenden Befehle im Eigenschaften-Fenster des Computers verwaltet (s. Abb. 42).

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. 43).

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.

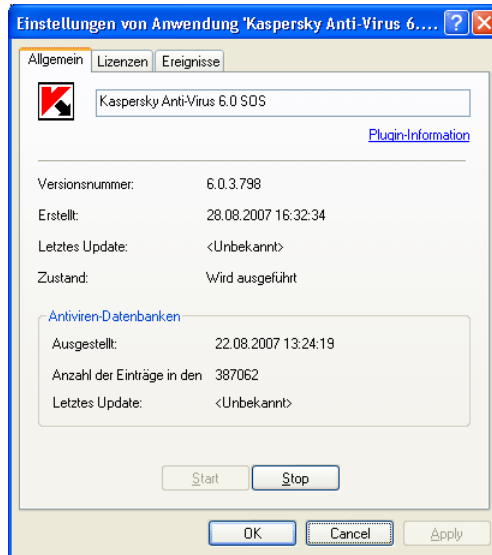


Abbildung 43. Parameter von Kaspersky Anti-Virus 6.0 SOS anpassen.
Registerkarte **Allgemein**

13.1.2. 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. 42).
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 SOS** aus und verwenden Sie die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Anwendungsparameter geöffnet (s. Abb. 44).

Alle Registerkarten (außer der Registerkarte **Einstellungen**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig und werden im entsprechenden Administratorenhandbuch ausführlich beschrieben.

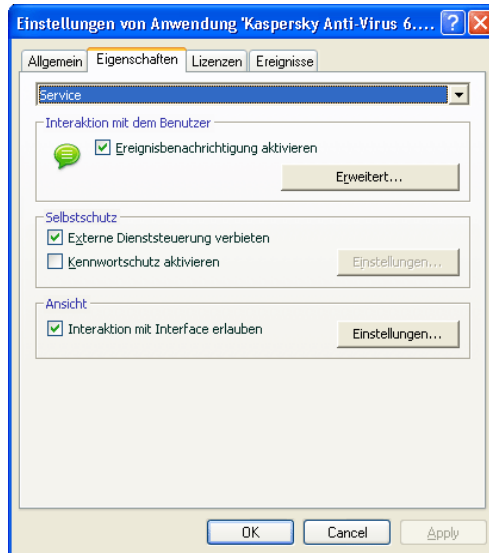


Abbildung 44. Parameter von Kaspersky Anti-Virus 6.0 SOS anpassen.
Registerkarte **Einstellungen**

Wenn für eine Anwendung eine Richtlinie erstellt wurde (s. Pkt. 13.3 auf S. 164), 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 6.0 SOS, Parameter für den Backup-Speicher, die Quarantäne und den Dienst zur Berichtsführung sowie die Netzwerkparameter angepasst werden. Wählen Sie dazu aus der Dropdown-Liste im oberen Bereich des Fensters den erforderlichen Wert aus und nehmen Sie die Einstellungen vor:

Schutz

In diesem Fenster können Sie:

- den automatischen Start der Anwendung beim Hochfahren des Computers festlegen (s. Pkt. 6.1 auf S. 51).
- eine Liste der Untersuchungsausnahmen erstellen (s. Pkt. 6.3 auf S. 53).
- die Kategorien der schädlichen Software auswählen, die von der

Anwendung untersucht werden sollen (s. Pkt. 6.2 auf S. 52).

- die Leistungsparameter für die Arbeit von Kaspersky Anti-Virus 6.0 SOS konfigurieren (s. Pkt. 6.6 auf S. 62).

Service

Die Einstellungen der Service-Parameter umfassen:

- die Konfiguration des Diensts zum Empfang von Benachrichtigungen über Ereignisse, die bei der Arbeit der Anwendung eintreten (s. Pkt. 10.8 auf S. 119).
- Konfiguration des Diensts für die Zugriffsbeschränkung auf Kaspersky Anti-Virus (s. Pkt. 10.8.2 auf S. 124).
- Konfiguration des Aussehens der Anwendung auf dem entfernten Computer. Dabei handelt es sich um eine spezifische Einstellung von Kaspersky Anti-Virus 6.0 SOS bei der Verwaltung über Kaspersky Administration Kit (s. Pkt. 10.8.2 auf S. 124).

Datenverwaltung

In diesem Fenster können Sie die Parameter für das Erstellen der Berichtsstatistik über die Arbeit der Anwendung anpassen (s. Pkt. 10.3.1 auf S. 108), sowie die Speicherdauer für Dateien im Backup-Speicher (s. Pkt. 10.1.2 auf S. 102) und in der Quarantäne (s. Pkt. 10.2.2 auf S. 105) festlegen.

13.1.3. Spezifische Parameter anpassen

Bei der Verwaltung von Kaspersky Anti-Virus 6.0 SOS 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. 42). Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 SOS** aus und verwenden Sie die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Anwendungsparameter geöffnet.

2. Gehen Sie auf die Registerkarte **Einstellungen** (s. Abb. 44), 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 6.0 SOS auf dem entfernten Computer aktivieren / deaktivieren. Dazu zählen die Anzeige des Symbols von Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS angezeigt (s. Abb. 34).

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 6.0 SOS 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.

13.2. Aufgaben verwalten

Dieser Abschnitt enthält Informationen über die Verwaltung von Aufgaben für Kaspersky Anti-Virus 6.0 SOS. Einzelheiten zur Konzeption der Aufgabenverwaltung über Kaspersky Administration Kit 6.0 finden Sie im Administratorenhandbuch für dieses Produkt.

Bei der Installation der Anwendung wird für jeden Computer des Netzwerks eine Auswahl von Systemaufgaben erstellt. Zu dieser Liste (s. Abb. 45) zählen eine

Reihe von 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 (s. Pkt. 13.2.2 auf S. 158).

Um eine Liste der Aufgaben anzuzeigen, die für einen Client-Computer erstellt wurden:

1. Wählen Sie im Ordner **Gruppen** (s. Abb. 41) den Ordner mit dem Namen der Gruppe aus, zu welcher der Client-Computer gehört.

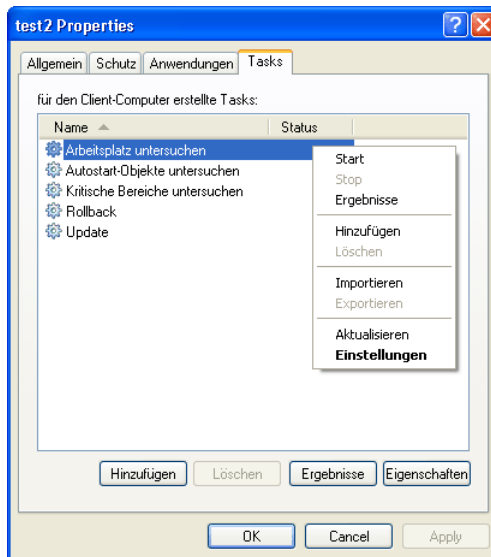


Abbildung 45. Liste der Aufgaben von Kaspersky Anti-Virus 6.0 SOS

2. Wählen Sie im Detailfenster den Computer aus, für den eine lokale Aufgabe erstellt werden soll, und verwenden Sie den Befehl **Tasks** im Kontextmenü oder den entsprechenden Punkt im Menü **Aktion**. Dadurch wird das Eigenschaften-Fenster des Client-Computers geöffnet.

3. Auf der Registerkarte **Tasks** (s. Abb. 45) befindet sich eine vollständige Liste der Aufgaben, die für diesen Client-Computer erstellt worden sind.

13.2.1. Aufgaben starten und beenden

Der Start von Aufgaben auf einem Computer wird nur dann ausgeführt, wenn die entsprechende Anwendung gestartet wurde (s. Pkt. 13.1.1 auf S. 152). Beim Beenden der Anwendung wird auch die Ausführung von gestarteten Aufgaben abgebrochen.

Der Start und das Beenden von Aufgaben erfolgt automatisch (entsprechend dem Zeitplan) oder manuell (mit Hilfe der Befehle des Kontextmenüs) sowie aus dem Fenster zur Anzeige der Aufgabeneinstellungen. Sie können den Ausführungsprozess einer gestarteten Aufgabe anhalten und später fortsetzen.

Um eine Aufgabe manuell zu starten / zu beenden / anzuhalten / fortzusetzen,

wählen Sie die gewünschte Aufgabe aus, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Starten / Beenden / Anhalten / Fortsetzen** aus oder verwenden Sie den entsprechenden Befehl im Menü **Aktion**.

Die entsprechenden Operationen können auch aus dem Konfigurationsfenster der Aufgabe auf der Registerkarte **Allgemein** (s. Abb. 46) mit Hilfe der gleichnamigen Schaltflächen initiiert werden.

13.2.2. Aufgaben erstellen

Bei der Arbeit mit Kaspersky Anti-Virus 6.0 SOS über Kaspersky Administration Kit können Sie folgende Aufgaben erstellen:

- lokale Aufgaben, die für einen einzelnen Client-Computer erstellt werden.
- Gruppenaufgaben, die für eine Gruppe von Client-Computern erstellt werden.
- globale Aufgaben, die für eine Auswahl von Client-Computern aus beliebigen Gruppen des logischen Netzwerks erstellt werden.

Sie können die Parameter der Aufgaben anpassen, die Ausführung der Aufgaben verfolgen, Aufgaben 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**.

13.2.2.1. Lokale Aufgabe erstellen

Um eine Aufgabe für einen einzelnen Client-Computer zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Tasks** (s. Abb. 45).
2. Verwenden Sie die Schaltfläche **Hinzufügen**, um eine neue Aufgabe hinzuzufügen. Dadurch wird ein Fenster zum Erstellen einer neuen Aufgabe geöffnet, das die Form eines Programmassistenten für Microsoft Windows besitzt und aus einer Reihe von Fenstern (Schritten) besteht. 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 wird die Anwendung angegeben, für welche die Aufgabe erstellt werden soll. Ihr Name lautet Kaspersky Anti-Virus 6.0 SOS. Außerdem wird der Aufgabentyp ausgewählt. Für Kaspersky Anti-Virus 6.0 SOS können folgende Aufgaben erstellt werden:

- *Virensuche* – Aufgabe zur Virensuche in benutzerdefinierten Bereichen.
- *Update* – Aufgabe zum Download und zum Übernehmen eines Updatepakets für die Anwendung.
- *Update rückgängig machen* – Aufgabe zum Rollback des letzten Updates der Anwendung.
- *Lizenzschlüssel installieren* – Aufgabe zum Hinzufügen eines neuen Lizenzschlüssels für die Arbeit der Anwendung.

Schritt 3. Parameter der gewählten Aufgabentyps anpassen

Abhängig vom Aufgabentyp, der beim vorigen Schritt ausgewählt wurde, variiert der Inhalt der folgenden Fenster folgendermaßen:

VIRENSUCHE

Im Konfigurationsfenster für die Aufgabe zur Virensuche muss die Aktion angegeben werden, die Kaspersky Anti-Virus 6.0 SOS beim Fund eines gefährlichen Objekts ausführen soll (s. Pkt. 7.4.4 auf S. 74). Außerdem wird hier die Liste der Untersuchungsobjekte angelegt (s. Pkt. 7.2 auf S. 66).

UPDATE

Für die Aufgabe zum Update der Bedrohungssignaturen und Programm-Module ist die Angabe der Quelle erforderlich, aus der die Updates heruntergeladen werden sollen (s. Pkt. 9.4.1 auf S. 89). In der Grundeinstellung erfolgt das Update vom Updateserver der Anwendung Kaspersky Administration Kit.

UPDATE RÜCKGÄNGIG MACHEN

Die Aufgabe zum Rollback des letzten Updates 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. Um den neuen Schlüssel als Reserveschlüssel hinzuzufügen, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel hinzufügen**. Der Reserve-Lizenzschlüssel wird aktiviert, wenn die Gültigkeitsdauer des momentan aktiven Lizenzschlüssels abläuft.

Informationen über den neuen Schlüssel (Nummer, Typ und Gültigkeitsdatum der Lizenz) werden im Feld auf der linken Seite angezeigt.

Schritt 4. Aufgabenstart im Namen eines anderen Benutzerkontos anpassen

Bei diesem Schritt wird Ihnen angeboten, den Start der Aufgabe unter einem anderen Benutzerkonto anzupassen, das über ausreichende Zugriffsrechte auf ein Untersuchungsobjekt oder eine Updatequelle verfügt (Details s. Pkt. 6.4 auf S. 58).

Schritt 5. Zeitplan anpassen

Nachdem Sie die Aufgabenparameter angepasst haben, wird Ihnen angeboten, den Zeitplan für den automatischen Aufgabenstart anzupassen.

Wählen Sie dazu aus der Dropdown-Liste die Frequenz für den Aufgabenstart aus und stellen Sie im unteren Teil des Fensters die Zeitplanparameter ein.

Schritt 6. Erstellen der Aufgabe abschließen

Im letzten Fenster des Assistenten werden Sie über den erfolgreichen Abschluss des Vorgangs zum Erstellen der Aufgabe informiert.

13.2.2.2. Gruppenaufgabe erstellen

Um eine Gruppenaufgabe für Kaspersky Anti-Virus 6.0 SOS 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 (s. Abb. 41), 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. 13.2.2.1 auf S. 159). 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.

13.2.2.3. Globale Aufgabe erstellen

Um eine lokale Aufgabe für Kaspersky Anti-Virus 6.0 SOS zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur das Element **Globale Tasks** aus (s. Abb. 41), 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. 13.2.2.1 auf S. 159). 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 6.0").

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 angezeigt.

13.2.3. 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. 45).
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. 46).

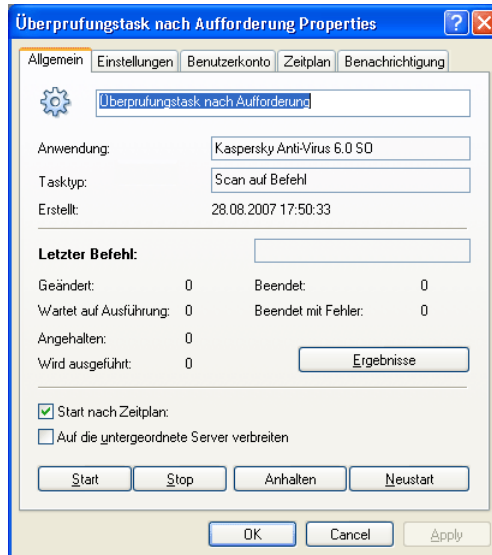


Abbildung 46. Aufgabenparameter anpassen

Alle Registerkarten (außer der Registerkarte **Einstellungen**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig und werden im entsprechenden Administratorenhandbuch ausführlich beschrieben. Die Registerkarte **Einstellungen** enthält spezifische Parameter für Kaspersky Anti-Virus 6.0 SOS. Der Inhalt variiert in Abhängigkeit vom ausgewählten Aufgabentyp.

Die Konfiguration von Aufgabenparametern der Anwendung über das Interface von Kaspersky Administration Kit entspricht der Konfiguration über das lokale Interface von Kaspersky Anti-Virus 6.0 SOS. Eine Ausnahme bilden die Parameter, die für jeden Benutzer individuell angepasst werden. Dazu zählen beispielsweise die schwarzen und weisen Listen von Anti-Spam. Eine ausführliche Beschreibung der Aufgabeneinstellungen finden Sie in Kapitel 7 – Kapitel 9 auf S. 64 – 84 des vorliegenden Handbuchs.

Wenn für die Anwendung eine Richtlinie erstellt wird (s. Pkt. 13.3 auf S. 164), in der das Ändern bestimmter Parameter verboten ist, stehen diese bei der Konfiguration von Aufgaben nicht zur Verfügung.

13.3. 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 SOS. Einzelheiten zur Konzeption der Richtlinienverwaltung über Kaspersky Administration Kit 6.0 finden Sie im Administratorenhandbuch für dieses Produkt.

13.3.1. Richtlinie erstellen

Um eine Richtlinie für Kaspersky Anti-Virus 6.0 SOS zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Gruppen** (s. Abb. 41) 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**.

Die Oberfläche 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.

Bei der Konfiguration einer Richtlinie können Sie das Verändern ihrer Parameter in den Richtlinien untergeordneter Gruppen, in den Aufgabenparametern und Anwendungsparametern vollständig oder teilweise verbieten. Klicken Sie dazu auf die Schaltfläche . Für Parameter, deren Änderung verboten ist, muss die Schaltfläche folgendes Aussehen besitzen: .

Schritt 1. Allgemeine Angaben über die Richtlinie eingeben

Das erste Fenster des Assistenten dient der Eingabe des Richtliniennamens (Feld **Name**) und der Auswahl der Anwendung **Kaspersky Anti-Virus 6.0 SOS** aus der Dropdown-Liste **Anwendungsname**.

Schritt 2. Richtlinienstatus auswählen

In diesem Fenster werden Sie dazu aufgefordert, den Status der Richtlinie festzulegen. Wählen Sie dazu die erforderliche Position des Schalters: aktive Richtlinie oder inaktive Richtlinie.

In einer Gruppe können mehrere Richtlinien für eine Anwendung erstellt werden. Allerdings kann nur eine davon als aktive Richtlinie gelten.

Schritt 3. Programm auswählen und anpassen

Auf dieser Etappe können Sie die Programmeinstellungen, die in der Richtlinie verwendet werden sollen, aktivieren/deaktivieren und anpassen.

Das Programm ist standardmäßig aktiviert. Um die Arbeit des Programms auszuschalten, deaktivieren Sie das Kontrollkästchen **Schutz**. Um die Programmeinstellungen im Detail anzupassen, wählen Sie den Punkt **Schutz** und klicken Sie auf die Schaltfläche **Einstellungen**.

Schritt 4. Parameter der Virensuche anpassen

Auf dieser Etappe wird Ihnen angeboten, die Parameter anzupassen, die von den Aufgaben zur Virensuche verwendet werden.

Wählen Sie im Block **Sicherheitsstufe** eine der drei vordefinierten Sicherheitsstufen aus (s. Pkt. 7.4.1 auf S. 69). Verwenden Sie die Schaltfläche **Einstellungen**, um die gewählte Stufe detailliert einzustellen. Um die Parameter der **Empfohlenen** Sicherheitsstufe wiederherzustellen, verwenden Sie die Schaltfläche **Grundeinstellung**.

Geben Sie im Block **Aktion** die Aktion an, die Kaspersky Anti-Virus beim Fund eines gefährlichen Objekts ausführen soll (s. Pkt. 7.4.4 auf S. 74).

Schritt 5. Update-Einstellungen anpassen

In diesem Fenster können Sie die Parameter für das Update von Kaspersky Anti-Virus 6.0 SOS anpassen.

Legen Sie im Block **Update-Einstellungen** das Update-Objekt fest (s. Pkt. 9.4.2 auf S. 71). Geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, die Parameter für das lokale Netzwerk (s. Pkt. 9.4.3 auf S. 93) und die Updatequelle (s. Pkt. 9.4.1 auf S. 89) an.

Aktivieren / deaktivieren Sie im Block **Aktion nach dem Update** die Option zur Untersuchung des Quarantänespeichers nach dem Empfang eines neuen Updatepakets (s. Pkt. 9.4.5 auf S. 96).


Schritt 6. Richtlinie übernehmen

Auf dieser Etappe wird Ihnen angeboten, die Methode zum Verteilen der Richtlinie auf die Client-Computer der Gruppe auszuwählen (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 die festgelegte Anwendung dem Ordner **Richtlinien** (s. Abb. 41) 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**.

13.3.2. 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 Richtlinienparameter Sie ändern möchten.
2. Wählen Sie den zu dieser Gruppe gehörenden Ordner **Richtlinien** aus (s. Abb. 41). Dadurch werden im Detailfenster alle Richtlinien angezeigt, die für diese Gruppe erstellt worden sind.
3. Wählen Sie in der Richtlinienliste die Richtlinie für die Anwendung **Kaspersky Anti-Virus 6.0 SOS** aus (der Anwendungsname wird im Feld **Anwendung** angegeben).

- Öffnen Sie das Kontextmenü der gewählten Richtlinie und verwenden Sie den Befehl **Eigenschaften**. Auf dem Bildschirm erscheint das Konfigurationsfenster der Richtlinie für Kaspersky Anti-Virus 6.0 SOS (s. Abb. 47).

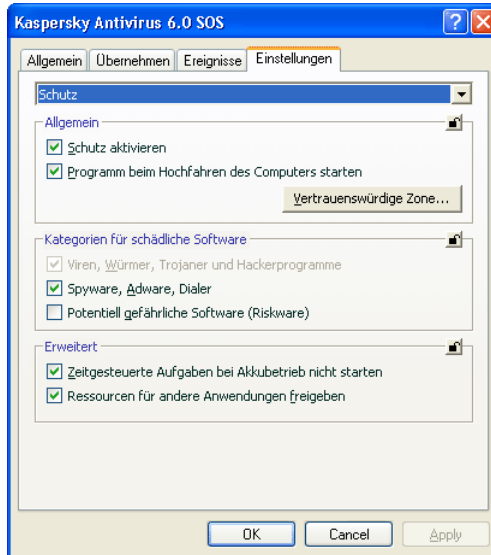


Abbildung 47. Richtlinienparameter anpassen

Alle Registerkarten (außer der Registerkarte **Einstellungen**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig und werden im entsprechenden Administratorenhandbuch ausführlich beschrieben.

Die Registerkarte **Einstellungen** enthält Richtlinienparameter für Kaspersky Anti-Virus 6.0 SOS. Die Richtlinienparameter umfassen Anwendungsparameter (s. Pkt. 13.1.2 auf S. 153) und Aufgabenparameter (s. Pkt. 13.2.3 auf S. 162).

Wählen Sie zum Anpassen der Parameter aus der Dropdown-Liste im oberen Teil des Fensters den gewünschten Wert aus und nehmen Sie die Einstellungen vor.

KAPITEL 14. HÄUFIGE FRAGEN

In diesem Kapitel behandeln wir die von Benutzern am häufigsten gestellten Fragen zu Installation, Konfiguration und Arbeit mit Kaspersky Anti-Virus 6.0 SOS und versuchen, sie eingehend zu beantworten.

Frage: *Kann Kaspersky Anti-Virus 6.0 SOS mit Antiviren-Produkten anderer Hersteller genutzt werden?*

Ja, das ist möglich. Die gleichzeitige Verwendung von Kaspersky Anti-Virus 6.0 SOS mit Antiviren-Programmen anderer Hersteller führt nicht zu Konflikten.

Frage: *Eine Datei wird von Kaspersky Anti-Virus 6.0 SOS nicht wiederholt untersucht. Warum?*

In der Tat untersucht Kaspersky Anti-Virus eine Datei nicht doppelt, wenn sie seit der letzten Untersuchung nicht geändert worden ist.

Das wird durch die Verwendung der neuen Technologien iChecker™ ermöglicht. Dabei wird eine Datenbank mit Kontrollsummen der Objekte verwendet.

Frage: *Wozu wird die Schlüsseldatei gebraucht? Funktioniert Kaspersky Anti-Virus 6.0 SOS auch ohne Schlüsseldatei?*

Kaspersky Anti-Virus kann ohne Schlüssel arbeiten. Allerdings stehen in diesem Fall das Programm-Update und die Unterstützung durch den Technischen Support-Service nicht zur Verfügung.

Wenn Sie sich noch nicht für den Kauf von Kaspersky Anti-Virus 6.0 SOS entschieden haben, können wir Ihnen einen Testschlüssel mit einer Gültigkeit von zwei Wochen oder einen Monat anbieten. Nach Ablauf der Testdauer wird der Schlüssel gesperrt.

Frage: *Nach der Installation von Kaspersky Anti-Virus 6.0 SOS verhält sich das Betriebssystem ungewöhnlich ("Einfrieren auf blauem Bildschirm", wiederholter Neustart des Computers u.a.). Was tun?*

Diese Situation tritt selten ein, kann aber durch einen Konflikt zwischen Kaspersky Anti-Virus 6.0 SOS und einem auf Ihrem Computer installierten Programm verursacht werden.

Gehen Sie folgendermaßen vor, um die Funktionsfähigkeit Ihres Betriebssystems wiederherzustellen:

1. Klicken Sie gleich nachdem der Computer gestartet wurde solange auf die Taste **F8**, bis das Auswahlmenü für die Startvarianten des Betriebssystems erscheint.
2. Wählen Sie den Punkt **Abgesicherter Modus** und laden Sie das Betriebssystem.
3. Starten Sie Kaspersky Anti-Virus 6.0 SOS.
4. Verwenden Sie im Programmhauptfenster den Link Einstellungen und wählen Sie im Konfigurationsfenster des Programms den Abschnitt **Schutz**.
5. Deaktivieren Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten** und klicken Sie auf die Schaltfläche **OK**.
6. Starten Sie das Betriebssystem im gewöhnlichen Modus neu.

Wenden Sie sich danach über die Kaspersky-Lab-Webseite an den Technischen Support-Service (Abschnitt **Dienste** → **Technischer Support** → **Anfrage an den Support senden**). Beschreiben Sie das Problem und die entsprechenden Bedingungen möglichst genau.

Fügen Sie Ihrer Anfrage unbedingt eine Datei mit dem vollständigen Speicherabbild des Betriebssystems Microsoft Windows bei. Diese Datei wird folgendermaßen erstellt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** und wählen Sie im folgenden Fenster den Punkt **Eigenschaften**.
2. Wählen Sie im folgenden Fenster **Systemeigenschaften** die Registerkarte **Erweitert** und klicken Sie im Abschnitt **Starten und Wiederherstellen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im Fenster **Starten und Wiederherstellen** im Abschnitt **Debuginformationen speichern** aus der Dropdown-Liste den Wert **Vollständiges Speicherabbild**.


Die Datei mit dem Speicherabbild wird standardmäßig unter dem Namen *memory.dmp* im Systemverzeichnis gespeichert. Sie können einen anderen Ordner zum Speichern des Dumps festlegen. Ändern Sie dazu im entsprechenden Feld den Ordernamen.

4. Wiederholen Sie den Vorgang, bei dem das mit der Arbeit von Kaspersky Anti-Virus verbundene Problem aufgetreten ist.
5. Vergewissern Sie sich, dass die Datei mit dem vollständigen Speicherabbild erfolgreich gespeichert wurde.

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 6.0 SOS verwendet werden können. Außerdem werden hier die Parameter der Datei setup.ini beschrieben, die bei der Installation der Anwendung im Silent-Modus verwendet wird.

A.1. Liste der Objekte, die nach Erweiterung untersucht werden

Wenn Sie als Untersuchungsobjekte die Variante  **Programme und Dokumente (nach Erweiterung) untersuchen** gewählt haben, dann werden beim Ausführen von Untersuchungsaufgaben 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.

*vx*d – 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, png – 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.

*md** – 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 **Untergeordnet 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 **Unterordner 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. 36) oder über den Gruppenrichtlinienobjekt-Editor (s. Pkt. 3.4 auf S. 36) 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 Programminstallation der Neustart des Computers erfolgen soll (Standardmäßig wird kein Neustart ausgeführt).

[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 Vireninfection 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 Popupfenstern 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 MI-

MEsweeper 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- STANDARDLIZENZVERTRAG

HINWEIS FÜR ALLE BENUTZER: BITTE LESEN SIE DIE FOLGENDE RECHTLICHE VEREINBARUNG ("VEREINBARUNG") ZUR LIZENZ FÜR DIE VON KASPERSKY LAB ("KASPERSKY LAB") HERGESTELLTE KASPERSKY ANTI-VIRUS S.O.S. (SECOND OPINION SOLUTION) ("SOFTWARE") SORGFÄLTIG.

WENN DIESE SOFTWARE AUF EINEM PHYSIKALISCHEN MEDIUM NICHT IN EINER SCHUTZHÜLLE VERPACKT IST, STIMMEN SIE (ALS NATÜRLICHE ODER JURISTISCHE PERSON) MIT KLICKEN AUF DIE SCHALTFLÄCHE "ANNEHMEN" DIESER VEREINBARUNG RECHTSVERBINDLICH ZU. WENN SIE NICHT MIT ALLEN LIZENZBEDINGUNGEN ÜBEREINSTIMMEN, KLICKEN SIE AUF DIE SCHALTFLÄCHE, DIE DARAUF HINWEIST, DASS SIE DIE BEDINGUNGEN DIESER VEREINBARUNG NICHT AKZEPTIEREN UND INSTALLIEREN SIE DIE SOFTWARE NICHT.

WENN DIESE SOFTWARE AUF EINEM PHYSIKALISCHEN MEDIUM IN EINER SCHUTZHÜLLE VERPACKT IST, STIMMEN SIE (ALS NATÜRLICHE ODER JURISTISCHE PERSON) DIESER VEREINBARUNG MIT AUFREISSEN DER SCHUTZHÜLLE RECHTSVERBINDLICH ZU.

WENN SIE NICHT MIT ALLEN LIZENZBEDINGUNGEN ÜBEREINSTIMMEN, LASSEN SIE DIE SCHUTZHÜLLE DER CD UNVERSEHRT. LADEN SIE DIE SOFTWARE NICHT HERUNTER UND INSTALLIEREN UND VERWENDEN SIE DIE SOFTWARE NICHT.

ALLE VERWEISUNGEN AUF "SOFTWARE" UMFASSEN AUCH DEN VON KASPERSKY LAB ALS TEIL DER SOFTWARE BEREIT GESTELLTEN SOFTWARE AKTIVIERUNGSCODE.

Lizenzgewährung. Vorbehaltlich erfolgter Zahlung der geltenden Lizenzgebühren und der in dieser Vereinbarung genannten Fristen und Bedingungen, gewährt Ihnen Kaspersky für die Dauer dieser Vereinbarung ein nicht-exklusives und nicht übertragbares Recht zur Benutzung eines Exemplars der genannten Softwareversion und der Begleitdokumentation ("Dokumentation" für Ihre eigenen internen Geschäftszwecke.

Benutzung. Sofern in diesem Abschnitt nicht anders bestimmt, darf die Software nur auf der Anzahl von Computern, die auf der Verpackung angegeben ist oder von Ihnen bei Bestellung der Software genannt wurde, und nur von einem Benutzer jeweils gleichzeitig benutzt werden. Bei der Software handelt es sich um ein zusätzliches Antivirus-Programm, das keinen Schutz des Computers in Echtzeit bietet. Die Software ist nicht zur Verwendung als einziges Antivirenprogramm im Computer bestimmt.

Die Software wird in einem Computer "benutzt", wenn sie in den Kurzspeicher (d.h. Arbeitsspeicher oder RAM) geladen oder in einem Festspeicher (z.B. Festplatte, CD-ROM oder anderer Speicher) dieses Computers installiert wird. Die Lizenz berechtigt Sie zur Anfertigung von Sicherungskopien der Software nur in der Menge, wie sie für die rechtmäßige Benutzung der Software und ausschließlich für Sicherungszwecke notwendig ist, unter der Bedingung, dass auf allen Kopien die entsprechenden Urheberrechtshinweise angegeben sind. Die Anzahl und der Aufbewahrungsort der von der Software und der Dokumentation angefertigten Kopien ist von Ihnen aufzuzeichnen und Sie haben die Software mit angemessenen Vorsichtsmaßnahmen gegen unbefugte Benutzung oder Vervielfältigung zu schützen.

Wenn sie den Computer verkaufen, in dem die Software installiert wurde, haben Sie zu gewährleisten, dass zuvor alle von der Software angefertigten Kopien vernichtet werden.

Sie dürfen diese Software auch nicht teilweise weder selbst noch durch einen Dritten dekompileieren, zurückentwickeln, zerlegen oder anderweitig auf eine visuell lesbare Form reduzieren. Auf Wunsch stellt Kaspersky Lab die zur Interoperabilität der Software mit selbständig geschaffenen Computerprogrammen notwendigen Schnittstellenangaben gegen Zahlung angemessener Kosten und Aufwandserstattung für Besorgung und Lieferung der Daten zur Verfügung. Wenn Kaspersky Lab mitteilt, dass eine Bereitstellung solcher Daten aus einem beliebigen Grund (einschließlich unter anderem Kostengründe) nicht beabsichtigt ist, sind Ihnen mit der Einschränkung, dass eine Rückentwicklung oder Dekompilierung nur in dem gesetzlich zulässigen Umfang erfolgt, eigene Maßnahmen zur Erzeugung der Interoperabilität gestattet.

Sie dürfen die Software weder selbst noch durch einen Dritten kopieren (in anderer als hierin zulässiger Weise), Fehlerbehebungen vornehmen oder anderweitig modifizieren, anpassen oder übersetzen oder aus der Software Sekundärwerke ableiten.

Sie dürfen Ihre Lizenzrechte an keine andere Person vermieten, verleihen, übertragen oder als Unterlizenz vergeben.

Sie dürfen diese Software nicht in automatischen, halbautomatischen oder manuellen Tools verwenden, die zur Erzeugung von Virussignaturen, Routinen zur Viruserkennung, anderen Daten oder Codes zur Erkennung von Malware bestimmt sind.

Support. (*)

- (i) Kaspersky stellt Ihnen die nachstehend definierten Supportleistungen ("Supportleistungen") für die Dauer von einem Jahr ab dem Zeitpunkt der Aktivierung zur Verfügung bei:

- (a) Zahlung der aktuellen Supportgebühr und

(b) erfolgreichem Ausfüllen des Abonnementformulars für Supportleistungen, das Sie mit dieser Vereinbarung erhalten oder Ihnen auf der Website von Kaspersky Lab zur Verfügung steht, in dem Sie den Aktivierungscode angeben müssen, den Sie von Kaspersky Lab zusammen mit dieser Vereinbarung erhalten haben. Die Entscheidung, ob Sie die Bedingungen für den Erhalt von Supportleistungen erfüllen, liegt ausschließlich im Ermessen von Kaspersky Lab.

Die Supportleistungen stehen unmittelbar nach Aktivierung der Software zur Verfügung. Der technische Support von Kaspersky Lab ist berechtigt, vom Endbenutzer eine weitere Registrierung als Identifizier für die Erbringung von Supportleistungen zu verlangen.

Bis zur Aktivierung der Software und/oder Erhalt des Identifiers des Endbenutzers (Kunden-ID) leistet der technische Support lediglich Unterstützung bei der Aktivierung und Registrierung des Endbenutzers.

- (ii) Mit Ausfüllen des Abonnementformulars für Supportleistungen stimmen Sie den Datenschutzbestimmungen von Kaspersky Lab zu, die Sie unter www.kaspersky.com/privacy finden können, und genehmigen gemäß dieser Datenschutzpolitik ausdrücklich den Datentransfer außerhalb Ihres eigenen Landes.
- (iii) Die Supportleistungen enden, wenn sie nicht mit Zahlung der jeweils geltenden Jahresgebühr und erneutem erfolgreichem Ausfüllen des Abonnementformulars für Supportleistungen verlängert werden.
- (iv) "Supportleistungen" umfassen:
 - a. Updates der Antiviren-Datenbanken;
 - b. kostenlose Software-Updates, einschließlich Version Upgrades;
 - c. technischer Support im Internet und über die vom Verkäufer und/oder Einzelhändler bereitgestellte Telefon-Hotline;
 - d. Updates der Viruserkennung und Virenbehebung in 24-Stundenfrist.
- (v) Supportleistungen werden nur dann erbracht, wenn Sie die neueste, auf der offiziellen Kaspersky Lab Website

(www.kaspersky.com) erhältliche Programmversion in ihrem Computer installiert haben.

Eigentumsrechte. Die Software ist durch Urheberrechte geschützt. Kaspersky Lab und deren Lieferanten besitzen alle Rechte, Eigentumsrechte und Beteiligungen in und an der Software, einschließlich Urheberrechte, Patente, Warenzeichen und andere geistigen Eigentumsrechte. Der Besitz, die Installation oder die Benutzung der Software durch Sie stellt keine Übertragung irgendwelcher Rechte oder des geistigen Eigentums an der Software dar und Sie erwerben außer wie in dieser Vereinbarung ausdrücklich genannt, keinerlei Rechte an der Software.

Vertraulichkeit. Sie vereinbaren, dass die Software und die Dokumentation zusammen mit der konkreten Gestaltung und Struktur individueller Programme vertrauliche Eigentümerdaten von Kaspersky Lab darstellen. Sie dürfen diese vertraulichen Daten ohne vorherige schriftliche Zustimmung von Kaspersky Lab Dritten in keiner Form offenlegen, übergeben oder in anderer Weise zur Verfügung stellen. Sie haben zum Schutz dieser vertraulichen Daten angemessene Sicherheitsmaßnahmen zu ergreifen, wozu ohne Einschränkung vorgenannter Bestimmungen auch alle Bemühungen zum Schutz und zur Sicherung des Aktivierungscode gehören.

Eingeschränkte Gewährleistung.

- (i) Kaspersky Lab gewährleistet sechs (6) Monate ab dem ersten Download oder ab erster Installation der auf einem physikalischen Medium erworbenen Software deren wesentliche Funktionalität gemäß den in der Dokumentation genannten Funktionen, wenn sie ordnungsgemäß und in der in der Dokumentation genannten Art und Weise betrieben wird.
- (ii) Für die Auswahl dieser Software entsprechend Ihren eigenen Anforderungen sind Sie ausschließlich selbst verantwortlich. Kaspersky Lab gewährleistet nicht, dass die Software und/oder Dokumentation für solche Anforderungen geeignet ist oder ununterbrochen und fehlerfrei betrieben werden kann.
- (iii) Kaspersky Lab gewährleistet nicht, dass diese Software alle bekannten Viren erkennt oder dass die Software nicht gelegentlich fälschlich einen Virus in einem Titel meldet, der nicht von diesem Virus infiziert ist.
- (iv) Kaspersky haftet bei einem, Kaspersky Lab oder deren Beauftragten innerhalb der Gewährleistungsfrist gemeldeten Verstoß gegen die in Absatz (i) genannte Gewährleistung ausschließlich und nach eigener Wahl mit Reparatur, Austausch oder Kaufpreiserstattung der Software. Zur Unterstützung des Lieferanten in der Lösung des defekten

Artikels haben Sie alle im angemessenen Umfang benötigten Angaben bereitzustellen.

- (v) Die in (i) genannte Gewährleistung erlischt, wenn Sie (a) ohne Einwilligung von Kaspersky Lab an der Software Änderungen vornehmen oder vornehmen lassen, (b) die Software zweckentfremdet verwenden oder (c) die Software in einer anderen, als gemäß dieser Vereinbarung zulässigen Weise benutzen.
- (vi) Die in dieser Vereinbarung genannten Gewährleistungen und Bedingungen gelten anstelle aller übrigen Bedingungen, Garantien und anderen Bedingungen im Zusammenhang mit der tatsächlichen oder angeblichen Lieferung, unterlassener oder verspäteter Lieferung der Software oder Dokumentation, die ohne den in Absatz (vi) genannten Bestimmungen zwischen Kaspersky Lab und Ihnen gelten, stillschweigend angenommen oder in diese Vereinbarung oder einen Zusatzvertrag infolge von Rechtsvorschriften, bürgerlichen Rechts oder anderweitig aufgenommen würden und die hiermit gänzlich ausgeschlossen werden (einschließlich unter anderem stillschweigende Bedingungen, Gewährleistungen oder Klauseln hinsichtlich zufriedener Qualität, Eignung für einen Zweck oder Anwendung angemessener Kenntnisse und Fähigkeiten sowie Sorgfalt).

Haftungsbeschränkung.

- (i) Diese Vereinbarung und deren Bestimmungen führen nicht zur Beschränkung oder zum Ausschluss der Haftung von Kaspersky Lab bei (i) Betrugsdelikt, (ii) Tod oder Personenschäden aufgrund eines Verstoßes gegen ihre Sorgfaltspflicht aufgrund bürgerlichen Rechts oder bei fahrlässigem Verstoß gegen eine in dieser Vereinbarung enthaltene Klausel oder (iii) eine andere Haftung, die gesetzlich nicht ausgeschlossen werden kann.
- (ii) Vorbehaltlich der in vorstehendem Absatz (i) genannten Bestimmungen übernimmt Kaspersky Lab bei einem der nachstehend genannten Verluste oder Schäden (vorausgesehen, vorhersehbar, bekannt oder anderweitig) keinerlei Haftung (Vertrags-, Delikt- Entschädigungs- und andere Haftung):
 - (a) Einkommensausfall;
 - (b) Tatsächlicher oder angenommener Gewinnausfall (einschließlich Gewinnausfall bei Verträgen);

- (c) entgangene Verwendung von Geldern;
 - (d) entgangene angenommene Einsparungen;
 - (e) entgangene Geschäfte;
 - (f) entgangene Geschäftsmöglichkeiten;
 - (g) Goodwill-Einbußen;
 - (h) Reputationseinbußen;
 - (i) Verlust, Beschädigung oder Verfälschung von Daten;
 - (j) indirekte Schäden oder Folgeschäden beliebiger Art (zur Vermeidung von Zweifelsfällen, einschließlich Schäden in der in den Absätzen (ii), (a) bis (ii), (i) beschriebenen Art).
- (iii) Kaspersky Lab haftet nicht für mögliche Verluste oder Schäden, die dadurch entstehen, dass Sie die Software als einziges Antivirus-Programm verwenden.
- (iv) Vorbehaltlich Absatz (i) bleibt die Haftung von Kaspersky Lab (Vertrags-, Delikt-, Entschädigungs- oder anderweitige Haftung) aus oder im Zusammenhang mit der Lieferung der Software auf den von Ihnen für die Software entrichteten Betrag begrenzt.

Diese Vereinbarung stellt die vollständige Vereinbarung der Vertragsparteien zum Vertragsgegenstand dar und ersetzt alle früheren, vor dieser Vereinbarung in Schriftstücken und Verhandlungen mit uns und unseren Repräsentanten ausdrücklich oder stillschweigend zustande gekommenen Abreden, Zusagen und Versprechungen zwischen Ihnen und Kaspersky Lab und alle früheren Vereinbarungen zwischen den Vertragsparteien zum vorgenannten Gegenstand enden zum Datum des Inkrafttretens.

(*)

Sobald sie eine Demosoftware benutzen, sind sie nicht berechtigt die unter 2. genannten Support Leistungen zu nutzen. Des Weiteren haben sich nicht das Recht die Software weiterzuverkaufen. Sie sind berechtigt die Software zu Testzwecken für den in der Lizenz genannten Zeitraum zu benutzen.