KASPERSKY LABS

Kaspersky Anti-Virus Personal / Personal Pro Version 4.5

BENUTZERHANDBUCH

KASPERSKY ANTI-VIRUS
PERSONAL / PERSONAL PRO
VERSION 4.5

Benutzerhandbuch

Besuchen Sie unsere Webseite: http://www.kaspersky.com/de/

Redaktion: September 2003

Inhalt

KAPITEL 1. KASPERSKY ANTI-VIRUS® PERSONAL

Achtung! Jeden Tag tauchen neue Viren auf. Um die Aktualität Ihres Produkts zu gewährleisten, sollten die Antiviren-Datenbanken täglich aktualisiert werden (ausführliche Informationen finden Sie unten). Vergessen Sie nicht, sofort nach der Installation des Produkts auf Ihrem Computer die Antiviren-Datenbanken zu aktualisieren!

Das Softwarepaket Kaspersky Anti-Virus® Personal ist für den Antiviren-Schutz von Computern mit dem Betriebssystem Windows bestimmt.

Zu dem Paket gehören folgende Programme:

- ***Kaspersky Anti-Virus® Scanner*** *– Ein Programm zur Virus-Untersuchung des Computers auf Veranlassung des Benutzers und zur Entfernung von entdeckten Viren. Das Programm findet und entfernt Viren in Dateien, Bootsektoren und im Arbeitsspeicher. Es findet Viren (entfernt diese aber nicht!) in Archiven und in lokalen Mailboxen der verbreiteten E-Mail-Systeme.*

- ***Kaspersky Anti-Virus® Monitor*** *– Ein residenter Antiviren-Monitor, mit welchem alle zu startenden bzw. zu öffnenden Dateien auf Viren überprüft werden können.*

  Beachten Sie, dass Kaspersky Anti-Virus® Scanner aus ZIP-Archiven Viren entfernen kann!

- ***Kaspersky Anti-Virus® Updater*** *– Ein Programm zur Aktualisierung der Antiviren-Datenbanken. Die Antiviren-Datenbanken werden von Kaspersky AV Scanner und Kaspersky AV Monitor bei der Suche nach Viren verwendet. Kaspersky Labs aktualisiert die Antiviren-Datenbanken täglich mit Informationen über neue Viren und stellt Updates im Internet bereit, von wo sie das Update-Programm herunterlädt.*

- ***Kaspersky Anti-Virus® Mail Checker*** *– Ein Programm das die Antiviren-Sicherheit für Benutzer von Microsoft Outlook 98/2000/XP.*

- ***Kaspersky Anti-Virus® Script Checker*** *– Das Programm schützt den Computer vor Skript-Viren und Würmern, die direkt im Arbeitsspeicher des Computers ausgeführt werden.*

- ***Kaspersky Anti-Virus® Rescue Disk*** *– Ein Programm zum Erstellen von Rettungsdisketten, die nach einem Virenangriff zur Wiederherstellung des Systems dienen.*

- ***Kaspersky Anti-Virus® Control Centre*** *– Ein Programm zur automatischen Steuerung aller Komponenten des Pakets. Control Centre ist zur Organisation der Installation und für Updates der Paketkomponenten bestimmt. Außerdem führt es die automatische Zeitsteuerung von Operationen, den Start von Paketanwendungen und eine Ergebniskontrolle durch.*

- ***Kaspersky® Report Viewer*** *– Das Programm erlaubt die Anzeige von Protokollen, die von anderen Programmen des Pakets erstellt werden.*

1.1. Was ist neu in Version 4.5?

Die im vorliegenden Benutzerhandbuch beschriebene Version des Softwarepakets Kaspersky Anti-Virus® Personal unterscheidet sich durch folgende neuen Funktionen von vorhergehenden Versionen:

- *Die Arbeitsgeschwindigkeit des Programms wurde erhöht.*

- *Die Optionen zur Desinfektion von ZIP-Archiven wurden verbessert.*

- *Der Untersuchungsalgorithmus für die an eingehende und ausgehende E - Mail-Nachrichten angefügte Dateien mit Hilfe der Komponente Kaspersky Anti-Virus® Mail Checker wurde optimiert. Dadurch wird bei der Virus-Untersuchung von E-Mails der Bedarf an Computerressourcen verringert.*

1.2. Hardware- und Softwarevoraussetzungen

Um die volle Funktionsfähigkeit des Programms zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Windows 95/98/Me

- *Prozessor Intel Pentium (oder kompatibel) mit einer Frequenz von **150Mhz** oder mehr.*
- *Mindestens **32 MB** Arbeitsspeicher (empfohlen – **64 MB**).*

Windows NT Workstation 4.0 (SP6a oder höher):

- *Prozessor Intel Pentium (oder kompatibel) mit einer Frequenz von **150Mhz** oder mehr.*
- *Mindestens **48 MB** Arbeitsspeicher (empfohlen – **64 MB**).*

Windows 2000 Professional:

- *Prozessor Intel Pentium (oder kompatibel) mit einer Frequenz von **150Mhz** oder mehr.*
- *Mindestens **64 MB** Arbeitsspeicher (empfohlen – **96 MB**).*

Windows XP Home Edition/Professional:

- *Prozessor Intel Pentium II (oder kompatibel) mit einer Frequenz von **300Mhz** oder mehr.*
- *Mindestens **128 MB** Arbeitsspeicher.*

Bei der Arbeit mit Kaspersky Anti-Virus® auf den Betriebssystemen Windows XP Home Edition und Windows XP Professional bestehen bestimmten Einschränkungen bei der Verwendung der Option **Schnelle Benutzerumschaltung**: Der Benutzer kann die Einstellungen von Kaspersky Anti-Virus® nicht ändern und erhält keine interaktiven Reaktionen von ihm (zum Beispiel Dialogfenster zur Angabe der Aktionen für infizierte Dateien).

Generelle Anforderungen für alle Betriebssysteme:

- *Verfügbarer Festplattenspeicher: mindestens **72 MB** für die Installation und mindestens **23 MB** für die Arbeit des Produkts.*
- *Das Programm Microsoft Internet Explorer, mindestens Version 5.5 mit installiertem Update SP2.*

- *Auf Ihrem Computer dürfen keine anderen Antiviren-Programme installiert sein, auch keine Produkte von Kaspersky Lab.*

Vor der Installation von Kaspersky Anti-Virus® Personal sollten alle auf Ihrem Computer installierten Antiviren-Anwendungen entfernt werden.

Außerdem muss die Bildschirmauflösung auf mindestens 800 x 600 eingestellt sein, eine kleine Schriftart gewählt und das Systemdatum richtig angegeben werden.

1.3. Lieferumfang

Kaspersky Anti-Virus® Personal kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z.B. http://www.kaspersky.com/de/, Abschnitt **BUY ON-LINE**) erworben werden.

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

- *versiegelter Umschlag mit Installations-CD, welche die Programmdateien enthält*
- *Benutzerhandbuch*
- *Lizenzschlüssel, der auf der Installations-CD gespeichert ist.*
- *Lizenzvertrag*

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

Beim Erwerb von Kaspersky Anti-Virus® Personal in einem Online-Shop kopieren Sie das Produkt von der Kaspersky Labs Internetseite. Das Distributiv enthält neben dem eigentlichen Produkt auch die vorliegende Dokumentation. Ein Lizenzschlüssel ist entweder Bestandteil des Distributivs oder wird Ihnen nach erfolgter Bezahlung per E-Mail zugesandt.

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

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit Kaspersky Anti-Virus® an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Abonnements wird an Sie zurückerstattet. Voraussetzung dafür ist, dass der versiegelte Umschlag mit der Installations-CD nicht geöffnet wurde.

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

1.4. Service für registrierte Benutzer

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

Durch den Erwerb eines Abonnements werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer Ihres Abonnements folgende Serviceleistungen in Anspruch nehmen:

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

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

1.5. Textgestaltung

Bestimmte Textteile dieser Dokumentation sind in Abhängigkeit ihrer Bedeutung durch unterschiedliche Formatierung hervorgehoben.

Formatierung	**Bedeutung**
Fette Schrift	Namen von Menüs, Menüelementen, Dialogfenstern, Elementen von Dialogfenstern, usw.
 Hinweis.	Zusatzinformationen, Hinweise.
 Achtung!	Sehr wichtige Information.
 *Um eine Aktion durchzuführen,* 1. Schritt 1. 2. …	Beschreibung einer Abfolge von Schritten und möglichen Aktionen, die der Benutzer durchführt.
 Aufgabe, Beispiel	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts
 Lösung	Lösung einer gestellten Aufgabe
[Parameter] – Funktion des Parameters.	Befehlszeilenparameter.
`Text von Hinweisen und Befehlszeilen`	Text von Konfigurationsdateien, informativen Hinweisen des Programms und Befehlszeilen

KAPITEL 2. INSTALLATION UND DEINSTALLATION DES PROGRAMMS

Vor der Installation von Kaspersky Anti-Virus® Personal sollten alle auf dem Computer laufenden Programme beendet werden.

Um den Installationsvorgang zu starten, starten Sie das Programm Setup.exe auf der Installations-CD. Das Setup-Programm funktioniert im Dialogmodus. Jedes Dialogfenster enthält eine bestimmte Auswahl an Schaltflächen zur Steuerung des Installationsvorgangs. Unten finden sie die Funktionsbeschreibung der wichtigsten Schaltflächen:

- ***OK*** *– bestätigt die entsprechende Aktion*
- ***Abbrechen*** *– bricht die entsprechende Aktion ab*
- ***Weiter*** *– einen Schritt weitergehen*
- ***Zurück*** *– einen Schritt zurückgehen*

Für die Installation des Produkts bestehen zwei Varianten: Erstinstallation und wiederholte Installation. Im Folgenden werden beide Varianten ausführlich beschrieben.

2.1. Erstinstallation

Schritt 1. Lesen des Lizenzvertrags

Das Dialogfenster **Lizenzvertrag** enthält den Text des Lizenzvertrags. Bitte lesen Sie den Vertrag sorgfältig. Wenn Sie den Bedingungen des Lizenzvertrags zustimmen, klicken Sie auf die Schaltfläche **Ja**. Andernfalls klicken Sie auf die Schaltfläche **Nein** und brechen damit den Installationsvorgang ab.

Schritt 2. Eingabe der Benutzerinformationen

Geben Sie im Dialogfenster **Benutzerdaten** die erforderlichen Angaben über den Benutzer ein. Geben Sie als **Benutzername** den Namen des Benutzers und als **Firmenname** die Bezeichnung der Firma an. Standardmäßig erscheinen in diesen Feldern die Angaben aus der Windows-Registrierung.

Schritt 3. Auswahl des Installationsordners

Wählen Sie im Dialogfenster **Auswahl des Zielordners** den Ordner, in dem die Programmkomponenten von Kaspersky Anti-Virus® Personal installiert werden sollen. Der Ordner für die Komponenten wird im Feld **Dateien in Ordner speichern** angegeben, der Ordner für gemeinsame Dateien im Feld **Ordner für gemeinsam genutzte Dateien**. Zur Ordnerauswahl dient die Schaltfläche **Ändern...**.

Schritt 4. Angabe des Namens der Programmgruppe im Menü Start\Programme

Geben Sie im Dialogfenster **Ordnerauswahl** den Namen des Ordners im Menü **Programme** an, in dem die Verknüpfungssymbole für den Start der Programmkomponenten von Kaspersky Anti-Virus® Personal angelegt werden sollen. Klicken Sie auf **Weiter**.

Schritt 5. Auswahl der Installationsart

Wählen Sie im Dialogfenster **Installationsart** eine von drei möglichen Installationsarten aus:

Benutzer-definiert	Sie können die zur Installation gewünschten Komponenten selbst in einer Liste auswählen.
Minimal	Es werden nur die wichtigsten Komponenten installiert, wie Kaspersky Anti-Virus® Scanner, Kaspersky Anti-Virus® Monitor, Antiviren-Datenbanken und Kaspersky Anti-Virus® Updater.
Standard	Alle Komponenten des Softwarepakets Kaspersky Anti-Virus® werden installiert.

Schritt 6. Auswahl der zu installierenden Komponenten von Kaspersky Anti-Virus®

Wenn Sie die Installationsart **Benutzerdefiniert** gewählt haben, geben Sie im Dialogfenster **Auswahl der Komponenten** die zur Installation gewünschten Komponenten an.

Zur Auswahl einer Komponente aktivieren Sie das Kontrollkästchen links vom Namen der Komponente.

Schritt 7. Kopieren der Dateien auf die Festplatte

Überprüfen Sie im Dialogfenster **Start des Kopiervorgangs** die Informationen über die Installation. Klicken Sie auf **Weiter**, um die Installation fortzusetzen. Dadurch wird der Installationsvorgang gestartet und die Dateien werden auf die Festplatte des Computers kopiert. Das Dialogfenster **Setup-Status** informiert über den Fortschritt des Installationsprozesses.

Schritt 8. Auswahl des Ordners zum Speichern von Protokollen

Im Dialogfenster **Parameter für Report Viewer** wird der Ordner zum Speichern der Protokolle angegeben, die von den Paketkomponenten von Kaspersky Anti-Virus® Personal erstellt werden.

Schritt 9. Angabe des Pfads der Schlüsseldateien

Geben Sie im Dialogfenster **Schlüsseldatei** den Namen und Pfad der Schlüsseldatei an.

Wenn sich diese Datei in dem Ordner befindet, aus dem die Installation erfolgt, dann erscheint der Dateiname automatisch in der **Liste der Schlüsseldateien**.

Sollte sich die Schlüsseldatei in einem anderen Ordner befinden, klicken Sie auf **Hinzufügen** und geben im folgenden Dialogfenster **Schlüsseldatei** den Namen der Schlüsseldatei und den dazugehörigen Pfad an. Gegebenenfalls können gleichzeitig mehrere Schlüsseldateien verwendet werden.

Die Schlüsseldatei ist Ihr persönlicher **Schlüssel**, der alle Service-Informationen enthält, die für die Arbeit mit Kaspersky Anti-Virus® erforderlich sind. Dazu gehören:

- *Informationen über den Verkäufer dieser Version (Firmenname, Adresse, Telefonnummern)*
- *Support-Informationen (Supportanbieter und deren Adressen)*
- *Erscheinungsdatum des Produkts*
- *Name und Nummer der Lizenz*
- *Liste der Funktionalität der einzelnen Komponenten*
- *Gültigkeitsdauer dieser Lizenz*

Schritt 10. Abschluss der Installation

Nach Abschluss der Installation des Pakets Kaspersky Anti-Virus® Personal erscheint auf dem Bildschirm das Fenster **Installation beendet**. Wählen Sie die gewünschte Aktion:

- **Ja, Computer jetzt neu starten**
- **Nein Computer später neu starten**

In diesem Fall ist für den korrekten Abschluss der Installation des Pakets Kaspersky Anti-Virus® Personal und den Beginn der Arbeit unbedingt der Neustart des Computers erforderlich.

Klicken Sie auf die Schaltfläche **Fertig**.

In Verbindung mit dem vollständigen Abschluss der Installation von Kaspersky Anti-Virus® Personal kommt es zu einer gewissen Verlangsamung beim Laden des Betriebssystems. Es besteht kein Grund zu Beunruhigung! In dieser Zeit wird Kaspersky Anti-Virus® auf Ihrem Computer registriert.

2.2. Wiederholte Installation

Sollte das Installationsprogramm zu Beginn des Installationsvorgangs eine frühere Version des Kaspersky Anti-Virus® Personal auf Ihrem Rechner finden, so erscheint das Dialogfenster **Auswahlbildschirm**, in dem folgende Optionen zur Auswahl stehen:

- ***Programm ändern*** *– Hinzufügen neuer Komponenten zu dem bereits installierten Paket*
- ***Reparieren*** *– Reparatur aller beschädigten, bereits installierten Komponenten*
- ***Entfernen*** *– Alle Komponenten des Pakets Kaspersky Anti-Virus® Personal werden von ihrem Computer gelöscht (s. Pkt. 2.3).*

Wählen Sie eine Aktion und klicken Sie auf die Schaltfläche **Weiter**.

Haben Sie den Modus **Programm ändern** gewählt, so erscheint nach Klick auf die Schaltfläche **Weiter** das Dialogfenster **Auswahl der Komponenten**, in dem Sie durch Aktivieren der entsprechenden Kontrollkästchen die gewünschten Komponenten wählen können. Nach der Auswahl der gewünschten Komponenten klicken Sie auf **Weiter**. Auf dem Bildschirm erscheinen nacheinander die Dialogfenster **Setup-Status** und **Installation beendet**.

Haben Sie **Reparieren** gewählt, so erscheinen nach Klick auf die Schaltfläche **Weiter** nacheinender die Dialogfenster **Setup-Status** und **Installation beendet**. Diese Option kann beispielsweise dann gewählt werden, wenn Sie eine zu Kaspersky Anti-Virus® Personal gehörende Datei versehentlich gelöscht haben.

Ist auf Ihrem Rechner bereits dieselbe oder eine vorhergehende Version des Programms Kaspersky AV Control Centre installiert (das zum Beispiel mit einem anderen Softwarepaket installiert wurde), dann erscheint während des Installationsvorgangs auf dem Bildschirm das Fenster **Komponente: Kaspersky Anti-Virus® Control Centre**, das eine Aktionsabfrage für die Installation der Standard-Konfigurationsdatei enthält.

Für die Installation der Konfigurationsdatei können Sie einen der folgenden Typen wählen:

- ***Zusammenfügen*** *– Hinzufügen der Standardeinstellungen zu den in der gefundenen Datei gespeicherten Einstellungen.*

- ***Überschreiben*** *– An Stelle der gefundenen Konfigurationsdatei die Standard-Konfigurationsdatei speichern.*

- ***Überspringen*** *– Die gefundene Konfigurationsdatei unverändert lassen.*

Wurde auf Ihrem Rechner bereits das Programm Kaspersky AV Updater installiert, so erscheint während des Installationsvorgangs ein Fenster mit einer Aktionsabfrage. Allerdings wird der Punkt **Zusammenfügen** nicht verfügbar sein. Sie können entweder die Standard-Konfigurationsdatei überschreiben oder die gefundene Datei speichern.

2.3. Deinstallation des Programms

Möchten Sie aus irgendeinem Grund das Programm Kaspersky Anti-Virus® Personal entfernen, wählen Sie im Dialogfenster **Auswahlbildschirm** die Option **Entfernen** und klicken Sie auf **Weiter**.

Auf dem Bildschirm erscheint nun ein Dialogfenster zur Bestätigung der Deinstallation. Zur Deinstallation klicken Sie auf **OK**. Der Deinstallationsvorgang wird gestartet und alle Programmdateien werden von der Festplatte gelöscht. Der Fortschritt des Deinstallationsvorgangs wird im Dialogfenster **Setup-Status** angezeigt.

Werden während des Deinstallationsvorgangs Dateien gefunden, die eventuell von mehreren Programmen gemeinsam genutzt werden, erscheint auf dem Bildschirm ein Dialogfenster zur Bestätigung des Löschens der entsprechenden Dateien. Um eine Datei zu löschen, klicken Sie auf **Ja**.

KAPITEL 3. KASPERSKY ANTI-VIRUS® SCANNER

Der Antiviren-Scanner Kaspersky Anti-Virus® Scanner (Kaspersky AV Scanner) ist ein Programm, mit dem nach Vorgaben des Benutzers der Computer auf Viren untersucht wird und entdeckte Viren entfernt werden können.

Kaspersky Anti-Virus® Scanner verfügt über folgende Funktionen:

- *Er erkennt und löscht Viren aller Art in den Dateien auf den zur Untersuchung ausgewählten Datenträgern, in Bootsektoren sowie im Arbeitsspeicher.*
- *Er erkennt und löscht Viren in komprimierten Dateien, die mit PKLITE, LZEXE, DIET, COM2EXE oder anderen Programmen komprimiert wurden.*
- *Er erkennt Viren (entfernt diese aber nicht!) in Archiven aller gängigen Formate (ZIP, ARJ, LHA, RAR usw.).*
- *Er erkennt Viren (entfernt diese aber nicht!) in lokalen Mailboxen der bekanntesten E-Mail-Systeme: Microsoft Outlook, Microsoft Exchange, Microsoft Internet Mail, Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail SMTP/POP3 server.*
- *Er erkennt Viren in Mail-Datenbanken von MS Outlook Express Version 5.0 (und höher) und entfernt gefundene Viren.*
- *Er verwendet einen perfektionierten heuristischen Mechanismus zur Suche nach unbekannten Viren (Erfolgsquote bis zu 92 %).*

3.1. Start des Antiviren-Scanners

Zum Starten des Programms stehen folgende Möglichkeiten zur Verfügung:

Methode 1: aus dem Windows-Hauptmenü. Klicken Sie dazu auf die Schaltfläche **Start**, wählen Sie danach den Punkt **Programme**, und klicken Sie dann in der Programmgruppe **Kaspersky Anti-Virus®** auf den Punkt **Kaspersky**

Anti-Virus® Scanner. Danach wird das Hauptfenster des Programms geöffnet (s. Pkt. 3.2.2) und das Symbol  erscheint in der Taskleiste. Durch Rechtsklick auf dieses Symbol können Sie das Systemmenü öffnen (s. Pkt. 3.2.1).

Methode 2: aus dem Programm Kaspersky AV Control Centre. Dazu wird ein spezieller Task erstellt. Der Task kann manuell gestartet werden oder der automatische Start kann durch einen Zeitplan festgelegt werden.

Methode 3: aus einer Befehlszeile. Klicken Sie dazu in der Windows-Taskleiste auf die Schaltfläche **Start**, wählen Sie den Befehl **Ausführen**..., und geben Sie im Dialogfenster **Ausführen** den vollständigen Pfad des ausführbaren Moduls avp32.exe an. Zum Beispiel:

```
C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe
```

Beim Start können Sie folgende Befehlszeilenparameter verwenden:

[/?] oder **[/H]** – vollständige Liste der Befehlszeilenparameter anzeigen.

[/P=dateiname] – Kaspersky AV Scanner mit den Einstellungen aus der Datei **dateiname** starten.

[/S] – unmittelbar nach dem Start von Kaspersky AV Scanner die Virus-Suche beginnen.

[/W] – Protokolldatei erstellen.

[/N] – Das Hauptfenster von Kaspersky AV Scanner nach dem Start sofort minimieren.

[/Q] – Das Hauptfenster von Kaspersky AV Scanner nach dem Abschluss des Scanvorgangs sofort schließen.

[/D] – Kaspersky AV Scanner wird nicht gestartet, wenn am selben Tag bereits ein Scanvorgang durchgeführt und erfolgreich abgeschlossen wurde (d.h. das Scannen wurde nicht abgebrochen und es wurden keine Viren gefunden).

[/@[!]=dateiname] – nur die Dateien und/oder Ordner scannen, die in der Datei **dateiname** angegeben sind. Dies ist eine normale Textdatei (ASCII) in der sich eine Liste der zu scannenden Dateien befindet. Jede Zeile darf nur einen Datei- bzw. Ordnernamen (mit vollständiger Pfadangabe) enthalten. Enthält der Parameter das Zeichen **!** (d.h. **/@!=dateiname**), dann wird die Datei **dateiname** nach dem Abschluss des Scannens gelöscht. Wird das Zeichen **!** nicht angegeben (d.h. **/@=dateiname**), wird diese Datei nicht gelöscht.

[/redundant] – Verwendung des redundanten Suchmodus (Details s. Pkt. A.2). Dieser Modus sollte verwendet werden, wenn beim normalen Scannen keine Viren entdeckt wurden, das System sich aber weiterhin ungewöhnlich verhält (wenn sich der Computer z.B. wiederholt von selbst neu startet, wenn Anwendungen ungewöhnlich langsam ausgeführt werden usw.). Sonst wird das Aktivieren dieses Modus nicht empfohlen, weil dabei der Suchvorgang erheblich verlangsamt wird.

[/virlist=dateiname] – Die Datei **dateiname** anlegen und in ihr eine Namensliste der bekannten Viren speichern, die zur Zeit von Kaspersky AV Scanner entdeckt werden können.

[datei-_und_ordnernamen] – Scannen der angegebenen Dateien und Ordner. Sollte der Name einer Datei oder eines Ordners Leerzeichen enthalten, so ist dieser Name in Anführungszeichen anzugeben. Die Verwendung von Zugriffsmasken, die in Dateinamen die Zeichen ***** oder **?** enthalten (z.B. Ausdrücke wie ***.exe**, **av?32.exe**) sind nicht zulässig.

Wenn in der Befehlszeile ein Ordner oder ein Dateiname mit einer Dateiliste (**/@=file_list.lst**) angegeben wird, dann wird das Scannen auch ohne den Parameter **/S** automatisch gestartet.

[/EL] –- Beim Scannen die Objekte überspringen, die in der Datei **dateiname** in Parameter **[/@[!]=dateiname]** angegeben sind.

[/EF] – Beim Scannen die Dateien und/oder Ordner überspringen, die in der Befehlszeile angegeben sind. Der Parameter **/EF** kann nicht nur in der Befehlszeile, sondern auch in den Zeilen der Datei **dateiname** des Parameters **/@=dateiname** verwendet werden. Steht der Parameter **/EF** in einer Zeile bedeutet, dass eine Datei (oder ein Ordner) nicht gescannt werden soll. Enthält ein Dateiname Leerzeichen, dann muss in der Zeile der Parameter vor dem Dateinamen stehen. Steht er nach dem Dateinamen, dann ist der Dateiname in Anführungszeichen anzugeben. Enthält der Dateiname keine Leerzeichen, kann der Parameter an beliebiger Stelle der Zeile stehen.

Mit Hilfe der Parameterkombinationen **/EF**, **/EL**, **/@** und der Datei- und Ordnerliste können Sie in der Befehlszeile verschiedene Scanbereiche bestimmen.

Es folgen einige Beispiele zur Verwendung der Befehlszeilenparameter:

Beispiel 1. Programmstart und Suche nach Viren in den Dateien des Ordners **Eigene Dateien**.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" /S "C:\Eigene Dateien"
```

Beispiel 2. Programmstart, Erstellen einer Virus-Liste in der Datei *E:\virlist.txt* und anschließendes Beenden des Programms.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" /virlist=E:\virlist.txt /q
```

Beispiel 3. Programmstart mit anschließender Virus-Suche, wenn die letzte Suche am vorigen Tag durchgeführt wurde, oder wenn bei einer Suche am gleichen Tag Viren entdeckt wurden. Beenden des Programms nach Abschluss des Scannens.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" /s/d/q
```

Beispiel 4. Programmstart und Virus-Suche in allen Dateien des Ordners **Eigene Dateien**, mit Ausnahme der Dateien, welche in der Datei *exclude.txt* aufgelistet sind.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" "C:\Eigene Dateien" /EL
/@=C:\exclude.txt
```

3.2. Benutzeroberfläche

3.2.1. Systemmenü

Beim Programmstart wird das Hauptfenster des Programms (s. Pkt. 3.2.2) geöffnet, und in der Taskleiste erscheint das Symbol  . Durch Rechtsklick auf dieses Symbol, können Sie das Systemmenü (s. Bild 1) öffnen. Das Systemmenü besteht aus folgenden Elementen:

- ***Kaspersky Anti-Virus® Scanner Einstellungen…*** *– Öffnet das Hauptfenster des Programms.*
- ***Scannen starten / Scannen abbrechen*** *– Startet den Scanvorgang / bricht den Scanvorgang ab*
- ***Scanvorgang anhalten / Scanvorgang fortsetzen*** *– Hält den Scanvorgang an / setzt den Scanvorgang fort.*
- ***Scan-Priorität setzen*** *– Ändert die Priorität des Scanvorgangs (dieses Element ist nur bei laufendem Scanvorgang verfügbar).*

- ***Report anzeigen*** *– Öffnet das Report-Dialogfenster mit den Ergebnissen der Programmoperationen.*

- ***Antiviren-Datenbanken aktualisieren*** *– Startet das Programm Kaspersky AV Updater zur Aktualisierung der Antiviren-Datenbanken.*

- ***Über...*** *– Öffnet das Fenster mit Informationen über das Programm.*

- ***Kaspersky Anti-Virus® Scanner beenden*** *– Beendet das Programm und entfernt es aus dem Arbeitsspeicher.*

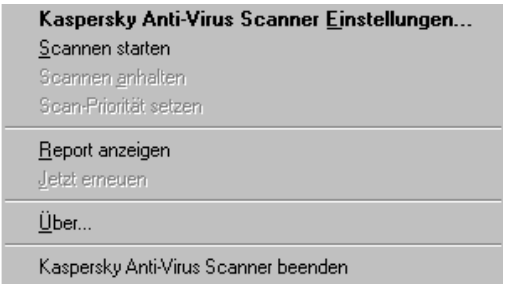


Bild 1. Systemmenü

3.2.2. Hauptfenster

Im Hauptfenster des Programms Kaspersky AV Scanner können Sie die Scanner-Einstellungen ändern, den Scanvorgang starten bzw. beenden, und das Ergebnisprotokoll öffnen. Sie können das Hauptfenster schließen, ohne das Programm aus dem Arbeitsspeicher zu entfernen.

Im Hauptfenster von Kaspersky AV Scanner befinden sich folgende Bedienungselemente: Menü, Symbolleiste, Arbeitsbereich, Statuszeile. Im Folgenden betrachten wir die einzelnen Elemente des Programmhauptfensters ausführlich:

3.2.3. Menü

Das Menü befindet sich im oberen Bereich des Hauptfensters. Einige Menübefehle sind sowohl als Tastenkombinationen wie auch als Schaltflächen in der Symbolleiste vorhanden (s. Pkt. 3.2.4). Die Tastenkombinationen sind im Menü

rechts vom jeweiligen Menübefehl angegeben. Die Zuordnung von Tastenkombinationen und Symbolleisten-Schaltflächen zu den Menübefehlen wird in Punkt 3.2.4. erläutert.

Menübefehl	**Funktion**
Datei → Profil laden	Lädt die Einstellungen aus der Konfigurationsdatei (s. Pkt. 3.3.4).
Datei → Profil speichern	Speichert die Einstellungen in der Konfigurationsdatei (s. Pkt. 3.3.4).
Datei → Profil speichern unter	Speichert die gewählten Einstellungen in einer anderen Konfigurationsdatei (s. Pkt. 3.3.4).
Datei → Profil als Standard speichern	Speichert die gewählten Einstellungen als Standard (s. Pkt. 3.3.4).
Datei → Zuletzt geladene Profile	Auswahl der zu ladenden Konfigurationsdatei aus einer Liste der zuletzt verwendeten Dateien.
Datei → Kaspersky AV Scanner beenden	Entfernt Kaspersky AV Scanner aus dem Arbeitsspeicher.
Datei → Fenster schließen	Schließt das Hauptfenster des Programms.
Scan → Scannen starten / Scannen beenden	Startet / beendet den Scanvorgang (s. Pkt. 3.4.1).
Scan → Scannen anhalten / Scannen fortsetzen	Hält den Scanvorgang an / setzt den Scanvorgang fort (s. Pkt. 3.4.1).
Scan → Scan-Priorität ändern	Ändert die Priorität des Scanvorgangs (dieses Element ist nur verfügbar, wenn der Scanvorgang läuft. Siehe Pkt. 3.4.2).
Scan → Scan-Vorschau	Zeigt die Scan-Einstellungen als fortlaufenden Text (s. Pkt. 3.3.5) an.
Tools → Antiviren-Datenbanken aktualisieren	Aktualisiert die Antiviren-Datenbanken (s. Pkt. 3.5).

Menübefehl	Funktion
Tools → Report anzeigen	Öffnet das Report-Fenster (s. Pkt. 3.4.3).
Tools → Virus-Liste erstellen	Erstellt eine Liste aller zur Zeit bekannten Viren (s. Pkt. 3.6).
Hilfe → Inhalt	Öffnet das Hilfesystem.
Hilfe → Kaspersky Anti-Virus® im Internet	Öffnet das Browserfenster mit Informationen über Kaspersky Lab.
Hilfe → Über Kaspersky Anti-Virus® Scanner	Zeigt kurze Informationen zum Programm.

3.2.4. Symbolleiste

Die *Symbolleiste* enthält Schaltflächen. Durch Klick auf eine Schaltfläche wird die entsprechende Funktion ausgeführt.

Schalt-fläche	Menü → Befehl	Funktion
	Datei → Profil laden	Lädt die Einstellungen aus der Konfigurationsdatei
	Datei → Profil speichern	Speichert die Einstellungen in der Konfigurationsdatei
	Datei → Profil als Standard speichern	Speichert die gewählten Einstellungen als Standardeinstellungen in der Konfigurationsdatei.
	Scan → Scannen starten	Startet den Scanvorgang
	Scan → Scannen anhalten / Scannen fortsetzen	Hält den Scanvorgang an / setzt den Scanvorgang fort

Schalt-fläche	Menü → Befehl	Funktion
	Scan → Scannen beenden	Bricht den Scanvorgang ab
	Scan → Scan-Vorschau	Zeigt die aktuellen Scan-Einstellungen als fortlaufenden Text an
	Tools → Report anzeigen	Öffnet das Report-Fenster
	Tools → Antiviren-Datenbanken aktualisieren	Startet die Aktualisierung der Antiviren-Datenbanken
	Datei → Kaspersky Anti-Virus® Scanner beenden	Beendet das Programm und entfernt es aus dem Arbeitsspeicher

3.2.5. Arbeitsbereich

Der Arbeitsbereich des Hauptfensters besteht aus zwei Teilen. Auf der linken Seite sind die Kategorienliste und deren Symbole angeordnet. Auf der rechten Seite werden die Inhalte der Kategorien angezeigt. Es gibt vier Kategorien: **Objekte**, **Optionen**, **Anpassen** und **Statistik**.

Die Kategorie **Objekte** dient zum Festlegen des Scanbereichs (Liste der Dateien und Ordner), der zu scannenden Objekte (zum Beispiel Sektoren, Dateien, Mailboxen) und der Regeln zur Behandlung infizierter Objekte (s. Pkt. 3.3.1). Alle diese Einstellungen sind in Form eines speziellen Bedienungselements organisiert, das *Konfigurationsbaum der Objekthierarchie* genannt wird.

In der Kategorie **Optionen** können allgemeine Einstellungen vorgenommen werden. Die Kategorie **Anpassen** bietet die Möglichkeit spezieller Programm-einstellungen mit Hilfe des *Konfigurationsbaumes* (s. Pkt. 3.3.2, 3.3.3).

Die Kategorie Statistik erlaubt die Anzeige von Ergebnissen der Programm-operationen in Tabellenform (s. Pkt. 3.4.4).

Die Elemente des Konfigurationsbaums verfügen über ein *Kontextmenü*, mit dessen Hilfe auf das entsprechende Element bezogene Operationen ausgeführt werden können.

Um das Kontextmenü eines bestimmten Hierarchie-Elements zu öffnen,

Zeigen Sie mit dem Mauszeiger auf das betreffende Element.

Klicken Sie mit der rechten Maustaste. Dann wird das Kontextmenü des Elements (s. Bild 2) eingeblendet.

Bild 2. Kontextmenü eines Elements des Konfigurationsbaums

3.2.6. Statuszeile

Am unteren Rand des Hauptfensters befindet sich die *Statuszeile*. In der Statuszeile werden folgende Informationen angezeigt:

- *Kontextbezogener Hilfetext / Name des gescannten Objekts;*
- *Fortschrittsanzeige des Scanvorgangs.*

3.3. Konfiguration der Scan-Parameter

Dieser Abschnitt enthält eine ausführliche Beschreibung der Einstellungen aller Scan-Parameter, die von Kaspersky AV Scanner verwendet werden.

3.3.1. Einstellungen für das Scannen von Objekten. Kategorie *Objekte*

Die Kategorie **Objekte** (s. Bild 3) des Arbeitsbereichs wird zur Auswahl des Scanbereichs und der zu scannenden Objekte verwendet. Die Auswahl von Bereich und Objekten wird mit Hilfe des Konfigurationsbaums vorgenommen. Für die Darstellung des Konfigurationsbaums stehen ein vereinfachter Modus und ein Expertenmodus zur Verfügung. Zur Änderung bzw. zum Umschalten des Darstellungsmodus dienen die Schaltflächen **Standard** und **Experte** im Hauptfenster.

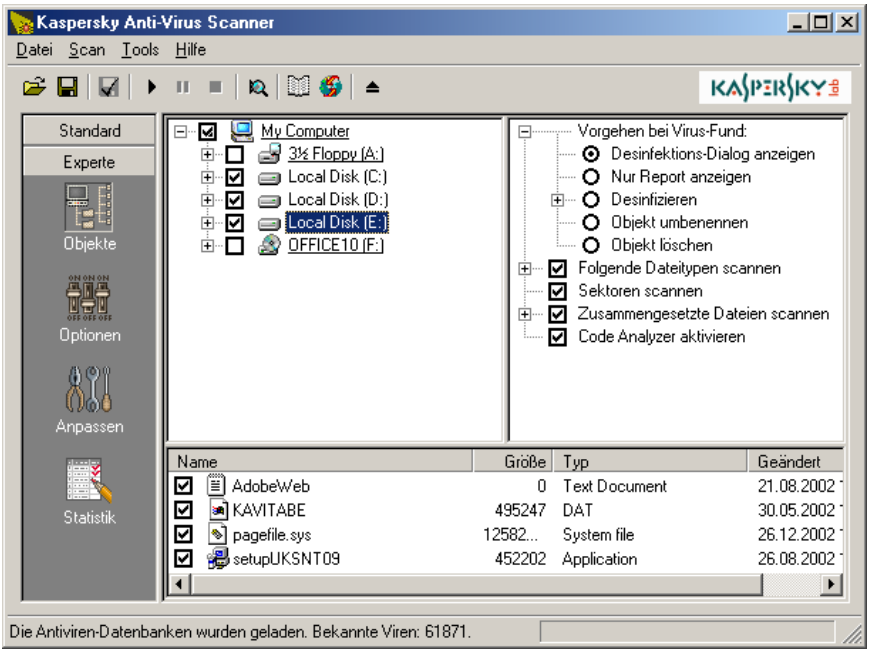


Bild 3. Kategorie **Objekte**

Im Standardmodus besteht der Baum für Objekteinstellungen aus zwei Feldern: Das linke Feld enthält die Liste der Computerlaufwerke. Das rechte Feld enthält den Konfigurationsbaum des aus der linken Liste ausgewählten Objekts (s. Bild 4).

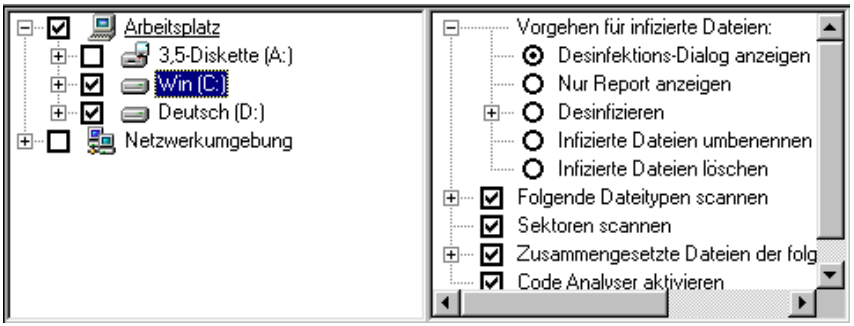


Bild 4. Ansichtsmodus **Standard**

Im Expertenmodus besteht der Konfigurationsbaum aus drei Feldern: das linke Feld enthält die Hierarchie des Computerdateisystems. Das rechte Feld enthält den Konfigurationsbaum für das aus der Hierarchie ausgewählte Objekt. Im unteren Feld befindet sich eine Liste der Dateien, die sich im Verzeichnis des aus der Hierarchie gewählten Objekts befinden (s. Bild 5).

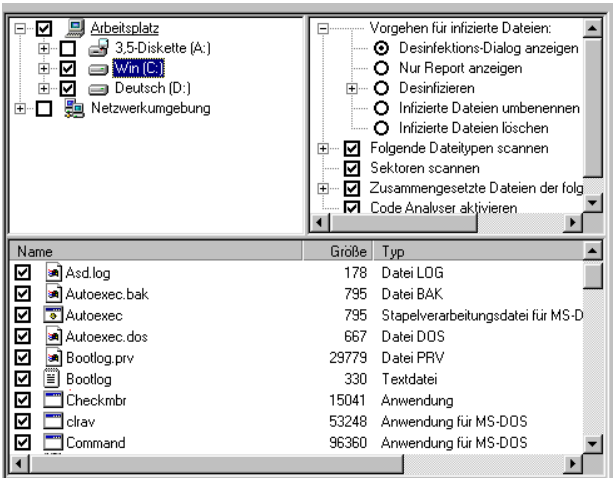


Bild 5. Ansichtsmodus **Experte**

Der Scanbereich wird im linken Feld ausgewählt, das die Hierarchie des Computerdateisystems und Kontrollkästchen für das Scannen jedes einzelnen Dateisystembereichs enthält. Das Scan-Kontrollkästchen kann entweder aktiviert werden: ☑, was die Anweisung zur Untersuchung des gewählten Bereichs

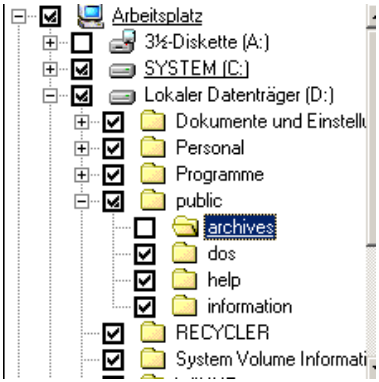
bedeutet, oder es kann deaktiviert werden: ☐, was der Anweisung zum Überspringen des betreffenden Bereichs entspricht.

Wenn das Programm einen Bereich des Dateisystems scannen soll, ist es notwendig, das Scan-Kontrollkästchen zu aktivieren, das sich links vom Namen des Bereichs befindet.

Um eine Gruppe von Laufwerken zum Scannen auszuwählen, markieren Sie im Feld mit der Dateisystemhierarchie die Zeile **Arbeitsplatz** und aktivieren Sie im rechten Feld mit dem Konfigurationsbaum die entsprechenden Kontrollkästchen:

- ☑ **Austauschbare Datenträger scannen –** Zum Scannen aller Wechseldatenträger. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** aus zugegriffen werden. Das Aktivieren dieses Kontrollkästchens bedeutet die Untersuchung aller Wechseldatenträger.
- ☑ **Lokale Festplatten scannen –** Zum Scannen aller lokalen Festplatten. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** aus zugegriffen werden. Das Aktivieren dieses Kontrollkästchens bedeutet die Untersuchung aller lokalen Festplatten.

Bei der Untersuchung eines bestimmten Dateisystembereichs wird automatisch der gesamte Bereich analysiert, der sich in dem ausgewählten Bereich befindet. Im Expertenmodus besteht allerdings die Möglichkeit, bestimmte Ordner oder Dateien vom Scannen auszuschließen.



Sie haben zum Beispiel die Laufwerke C: und D: zum Scannen gewählt, wollen aber den Ordner *D:\public\archives* nicht untersuchen, weil Sie sicher sind, dass der Inhalt virusfrei ist. Dann können Sie die Kontrollkästchen links von den Namen der Laufwerke C: und D: aktivieren, öffnen dann in der Dateihierarchie das Laufwerk D: und deaktivieren dort das Kontrollkästchen des Ordnernamens *D:\public\archives*.

Wenn Sie einen Ordner vom Scannen ausgeschlossen haben, werden alle Kontrollkästchen mit einem Haken ☑, die zu einem übergeordneten Bereich des Dateisystems gehören, durch ein Kontrollkästchen mit einem Haken und einem Dreieck in der rechten unteren Ecke ersetzt: ☑. Dadurch stellt das Programm eine Situation dar, in der innerhalb eines aktivierten Bereichs des Dateisystems ein Teilbereich enthalten ist, der auf andere Weise überprüft wird, als der

gesamte Bereich. Solche Unterschiede der Untersuchungsregeln innerhalb eines Bereichs können aufgehoben oder langfristig beibehalten werden. Weitere Informationen darüber finden Sie in Punkt 8.3.

Für jeden Bereich des Dateisystems können Sie eigene Scan-Einstellungen vornehmen. Die zu überprüfenden Objekte werden für jeden zu scannenden Bereich mit Hilfe des Konfigurationsbaums im rechten Feld festgelegt.

3.3.1.1. Zu scannende Objekte. Arbeitsspeicher, Sektoren und Dateien.

Jede Hierarchieebene des Computerdateisystems verfügt über eigene Einstellungsmöglichkeiten. Der Bereich **Arbeitsplatz** besitzt den Konfigurationsbaum mit einer maximalen Anzahl möglicher Einstellungen. In die Liste der Einstellungen sind Scan-Optionen für den Arbeitsspeicher, Bootsektoren, Laufwerkgruppen und Datenbanken von MS Outlook Express (Version 5.0 und höher) eingeschlossen.

Die Untersuchungsparameter eines Laufwerks erlauben nur das Scannen der Bootsektoren dieses Laufwerks, sowie das Aktivieren bzw. Deaktivieren des Kontrollkästchens für das Scannen des Dateisystems der Laufwerke. Die Untersuchungsparameter eines Ordners erlauben das Deaktivieren des Kontrollkästchens für das Scannen des Dateisystems nicht. Ebenso wie auf allen höheren Ebenen sind aber auch bei den Untersuchungsparametern für Ordner die Auswahl der Behandlung infizierter und verdächtiger Objekte, die Auswahl des Typs der zu scannenden Dateien und die Auswahl zusätzlicher Suchfunktionen möglich.

☑ **Folgende Dateitypen scannen –** Scannen von bestimmten Dateitypen eines Objekts (einschließlich Dateien mit den Attributen *System*, *Versteckt* und *Schreibgeschützt*). Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** und der Laufwerke aus zugegriffen werden. Das Deaktivieren ist für die Objekte des Typs "Ordner" und "Datei" nicht möglich. Wählen Sie einen der folgenden Dateitypen:

- ⊙ **Alle infizierbaren** – Zum Scannen aller Dateien, die Viren enthalten können.
- ⊙ **Alle** – Zum Scannen aller Dateien.
- ⊙ **Nach Maske** – Zum Scannen der Dateien, die den Masken entsprechen, welche in den unten angebrachten Textfeldern festgelegt werden. Die Anzahl der Masken ist unbegrenzt. In jedem Textfeld darf jedoch nur ein Wert angegeben werden.

- ☑ **Nach Maske ausschließen** – Die Dateien, die den Masken, welche in den unten angebrachten Textfeldern festgelegt werden, werden vom Scannen ausgeschlossen. Die Anzahl der Masken ist unbegrenzt. In jedem Textfeld darf jedoch nur ein Wert angegeben werden.

☑ **Sektoren scannen –** Zum Scannen des Master-Bootsektors und der Bootsektoren von Laufwerken. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** und der Laufwerke aus zugegriffen werden.

☑ **Arbeitsspeicher scannen –** Zum Scannen des Arbeitsspeichers. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** aus zugegriffen werden.

☑ **MS Outlook Express Datenbanken scannen –** Zum Scannen der Datenbanken von MS Outlook Express Version 5.0 und höher. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** aus zugegriffen werden. Details über das Scannen von Mail-Datenbanken anderer Formate s. Pkt. 3.3.1.3.3.

Kaspersky Anti-Virus® Scanner untersucht nur dbx-Dateien, die sich im Arbeitsverzeichnis von MS Outlook Express befinden und die folglich bei jedem Start von MS Outlook Express geöffnet werden. *.dbx-Dateien, die sich in anderen Verzeichnissen befinden, werden vom Programm als gewöhnliche Mail-Datenbanken betrachtet. Zwar findet Kaspersky Anti-Virus® Scanner in diesen Datenbanken Viren, kann diese jedoch nicht entfernen.

☑ **Beim Systemstart auszuführenden Objekte scannen** – Zum Scannen von Objekten, die unmittelbar nach dem Start vom Betriebssystem automatisch ausgeführt werden. Auf dieses Kontrollkästchen kann nur vom Konfigurationsbaum des Objekts **Arbeitsplatz** aus zugegriffen werden.

3.3.1.2. Aktionen mit infizierten und verdächtigen Objekten

Vorgehen bei Virus-Fund – Wenn ein infiziertes oder verdächtiges Objekt gefunden wird, führt das Programm folgende Aktionen aus:

- ⊙ **Desinfektions-Dialog anzeigen** – Beim Fund eines Virus öffnet Kaspersky AV Scanner ein Dialogfenster (s. Bild 6). Dieses Dialogfenster enthält den Namen der infizierten Datei, den Namen des entdeckten Virus und eine Liste der möglichen Aktionen zur Behandlung des infizierten Objekts (mit Ausnahme der Aktion ⊙ **Desinfektions-Dialog anzeigen**). Außerdem enthält dieses Dialogfenster das Kontrollkästchen **Auf alle infizierten Objekte anwenden**, durch dessen Aktivieren Sie die in diesem Dialog gewählten Aktionen

auf alle infizierten Objekte anwenden können, die später entdeckt werden und für die das Öffnen des Dialogfensters als Aktion festgelegt wurde. Das Dialogfenster wird dann beim Fund des nächsten infizierten Objekts nicht mehr angezeigt. Die drei folgenden Schaltflächen sind am unteren Rand des Dialogfensters angeordnet: **OK** (gewählte Aktionen bestätigen), **Abbrechen** (Dialogfenster schließen und Virus-Suche fortsetzen) und **Beenden** (Virus-Suche beenden).

- **Nur Report anzeigen** – Keine Aktionen mit Objekten durchführen, nur die Informationen im Protokoll aufzeichnen. Das Untersuchungsprotokoll kann mit Hilfe von Kaspersky® Report Viewer angezeigt werden (s. Kapitel 7).

- **Desinfizieren** – alle infizierten Objekte ohne vorherige Anfrage reparieren. Durch die Desinfektion werden alle Viren entfernt und die Funktionsfähigkeit des Objekts wird wiederhergestellt. Zusätzlich zur Desinfektion von Objekten können Sie folgende Aktionen wählen:

  - ☑ **Sicherungskopie der Originaldatei anfertigen** – Vor einem Desinfektionsversuch eine Kopie des infizierten Objekts anlegen. Das Verzeichnis für die Kopie ist im Konfigurationsbaum der Kategorie **Optionen** anzugeben (s. Pkt. 3.3.2.2). Die Sicherheitskopie wird nach der Desinfektion nicht gelöscht.

  - **Wenn Desinfektion nicht möglich** – Nicht alle infizierten Objekte können repariert werden, weil Computerdaten durch bestimmte Viren irreversibel beschädigt werden. In diesem Fall kann Kaspersky AV Scanner eine der drei folgenden Methoden anwenden:
    - **Nur Report anzeigen** – über erfolglose Desinfektionsversuche informieren,
    - **Objekt umbenennen** – irreparable Dateien umbenennen
    - **Objekt löschen** – beschädigte Dateien löschen.

- **Objekt umbenennen** – alle infizierten Objekte umbenennen. Die Regeln für das Umbenennen werden im Konfigurationsbaum der Kategorie **Optionen** festgelegt (s. Pkt. 3.3.2.2).

- **Objekt löschen** – alle infizierten Objekte ohne Vorwarnung löschen.

Die Regeln **Objekt löschen** und **Objekt umbenennen** werden auf zusammengesetzte Dateien nur dann angewandt, wenn das Kontrollkästchen **Löschen oder Umbenennen infizierter zusammengesetzter Dateien aktivieren** auf der Registerkarte **Optionen** aktiviert wurde. Sonst wird die gewählte Aktion – Löschen oder Umbenennen von zusammengesetzten Dateien – nicht ausgeführt.

Bild 6. Dialogfenster zur Auswahl einer Aktion beim Fund eines infizierten Objekts

3.3.1.3. Zusätzliche Suchfunktionen

3.3.1.3.1. Scannen zusammengesetzter Objekte

Zum Scannen von Archiven, komprimierten Dateien, E-Mail-Datenbanken, Dateien in Mailformaten und eingebundenen Objekten stehen Ihnen zusätzliche Modi zur Verfügung. Diese Funktionen sind in einer Gruppe zusammengefasst:

- ☑ **Zusammengesetzte Dateien scannen** – verbundene Objekte als Ordner behandeln, die eine Auswahl an Objekten enthalten.

In bestimmten Fällen kann das Programm einen Virus in einer verbundenen Datei (Archiv, Mail-Datenbank, Datei im Mailformat) finden, diesen aber nicht entfernen. Wenn Sie als Aktion für infizierte Objekte das Löschen oder Umbenennen gewählt haben, wird deshalb bei der Arbeit mit verbundenen Objekten empfohlen, das Kontrollkästchen ☑ **Zusammengesetzte Dateien scannen** zu aktivieren und das Kontrollkästchen ☑ **Löschen oder Umbenennen infizierter zusammengesetzter Dateien aktivieren** auf der Registerkarte Optionen zu deaktivieren. In diesem Fall wird beim Fund eines infizierten Objekts in einer verbundenen Datei ein entsprechender Eintrag im Protokoll vorgenommen, die verbundene Datei wird aber nicht gelöscht oder umbenannt. Sie können die Datei entpacken, den Scanner starten und die entpackten Dateien von Viren säubern.

Wird das Kontrollkästchen **Löschen oder Umbenennen infizierter zusammengesetzter Dateien aktivieren** aktiviert, dann kann es zum Verlust von Daten kommen, deren Wiederherstellung möglich wäre.

3.3.1.3.2. Untersuchung von Archiven und selbstentpackenden Dateien

Das Erkennen von Viren in Archiven ist eine sehr wichtige Aufgabe, weil Viren in diesen monate- oder sogar jahrelang folgenlos abgelegt werden, sich aber dann schnell ausbreiten und große Probleme verursachen können.

☑ **Archive** – Virus-Suche in Archivdateien, die mit den Archivierungsprogrammen ZIP, ARJ, LHA, RAR, CAB u. a. angelegt wurden.

In Archiven erkennt Kaspersky Anti-Virus® Viren zwar, löscht die Viren aber nicht. Außerdem kann Kaspersky Anti-Virus® durch Kennwort geschützte Archive nicht entpacken.

☑ **SFX Archive** – Virus-Suche in selbstentpackenden Archiven, d.h. in ausführbaren Dateien, die beim Start die in ihnen enthaltenen Dateien entpacken. Bestimmte selbstentpackende Archive können außerdem die aus dem Archiv extrahierten Dateien starten.

Der Extraktionsmechanismus funktioniert auch mit mehrfach gepackten Archiven korrekt. Ebenso funktioniert er mit bestimmten Versionen von Datei-Immunisatoren. Das sind Programme, die ausführbare Dateien durch Anhängen von Kontrollblöcken (CPAV und F-XLOCK) und Verschlüsselungsprogrammen (CryptCOM) vor Infektion schützen.

3.3.1.3.3. Untersuchung von Mail-Datenbanken und Dateien in Mailformaten

Mit diesem Programm können Sie Ihre Mail-Datenbanken und Dateien in Mailformaten überprüfen.

☑ **Mail-Datenbanken** – Virus-Suche in Mail-Datenbanken. Es werden Mail-Datenbanken in folgenden Formaten überprüft:

- *Microsoft Outlook, Microsoft Exchange (Dateien *.pst und *.pab, Archivtyp MS Mail)*
- *Microsoft Internet Mail (Dateien *.mbx, Archivtyp MS Internet Mail)*
- *Eudora Pro & Lite*
- *Pegasus Mail*
- *Netscape Navigator Mail*

- *JSMail SMTP/POP3 server (Benutzer-Datenbank)*

Bei Überprüfung von Mail-Datenbanken untersucht das Programm jeden Eintrag der E-Mail-Datenbanken und scannt angehängte Dateien auf Viren. Dabei werden folgende Formate unterstützt: UUEncode; XXEncode; btoa (bis 5.0); btoa 5.*; BinHex 4.0; ship; NETRUN 3.10; NETSEND 1.0 (nicht gepackt); NETSEND 1.0C (gepackt); MIME base64.

☑ **Text-Mail-Formate** – Virus-Suche in E-Mail-Dateien der Formate Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail, Benutzer-datenbanken auf SMTP/POP3-Servern.

In diesem Modus durchsucht Kaspersky Anti-Virus® jede Datei nach einem E-Mail-Header und, nachdem er diesen gefunden hat, nach angehängten Daten (UUEncode, XXEncode, usw.), und untersucht diese auf Viren.

Bei Aktivierung der Virus-Suche in Mail-Datenbanken und insbesondere bei der Untersuchung von Dateien in Text-Mail-Formaten kann die Arbeits-geschwindigkeit von Kaspersky AV Scanner sinken. Deshalb empfehlen wir nicht, diese Funktionen bei einer normalen Untersuchung aller Dateien Ihres Rechners zu verwenden.

Kaspersky AV Scanner kann Viren aus Mail-Datenbanken und Dateien in Text-Mail-Formaten nicht entfernen, sondern diese nur finden. Allerdings kann das Programm im speziellen Suchmodus ☑ **Outlook Express Datenbanken überprüfen** in den Datenbanken von MS Outlook Express (Version 5.0 und höher) Viren nicht nur finden, sondern auch löschen.

3.3.1.3.4. Virus-Suche in eingebetteten Objekten

Mit diesem Programm lassen sich nicht nur Dateien, sondern auch die mit ihnen verbundenen OLE -Objekte überprüfen. Aktivieren Sie dazu das Kontroll-kästchen ☑ **Eingebettete Objekte** – Virus-Suche in OLE-Objekten, die in zu untersuchende Dateien eingebettet sind.

3.3.1.3.5. Code Analyzer

Zum Entdecken von Viren, die dem Programm noch unbekannt sind (die noch nicht in die Antiviren-Datenbanken aufgenommen wurden), steht der die heuris-tische Scan-Funktion von Dateien zur Verfügung. Aktivieren Sie das Kontroll-kästchen ☑ **Code Analyzer aktivieren** – Zur Auswahl der Untersuchung mit dem Heuristischen Analyzer.

3.3.2. Allgemeine Optionen. Kategorie *Optionen*

Die Kategorie **Optionen** (s. Bild 7) enthält Einstellungen für die Protokollierung der Scan-Ergebnisse in einer Datei, Einstellungen für das Umbenennen infizierter Dateien und für die Stufe der Scan-Priorität.

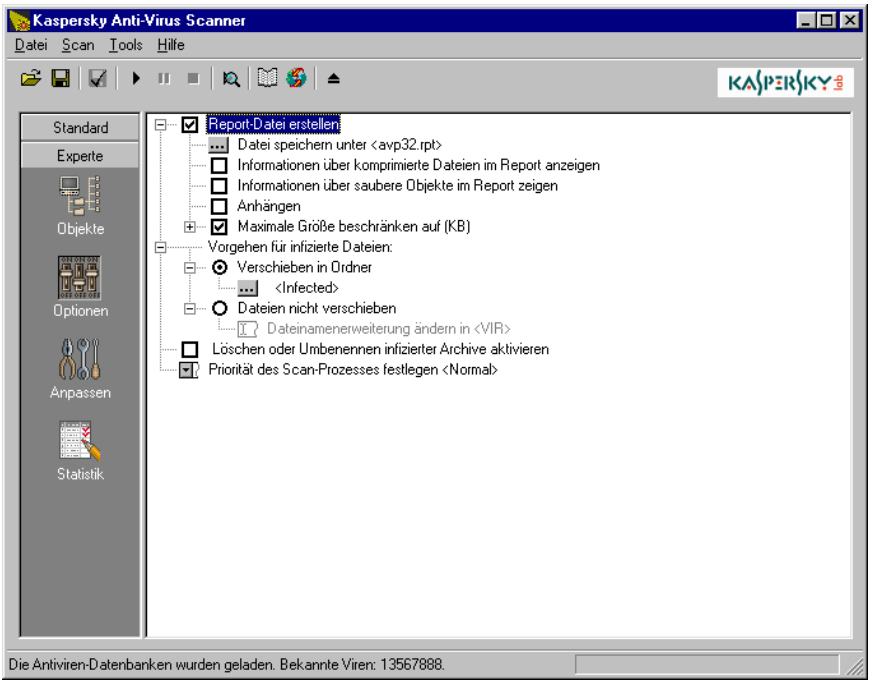


Bild 7. Kategorie **Optionen**

3.3.2.1. Report-Optionen

☑ **Report-Datei erstellen** – Report in einer Datei speichern. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie mit Hilfe von Kaspersky® Report Viewer (s. Kapitel 7) die Arbeit von Kaspersky Anti-Virus® verfolgen. Bei der Anzeige der Ergebnisse verwendet dieses Programm alle Einstellungen des Unterbaums **Report-Datei erstellen**.

Datei speichern unter – vollständiger Pfad der Report-Datei.

Als Standard wird der Report im Verzeichnis erstellt, das bei der Programm-Installation angegebenen wird. Läuft das Programm ohne Verbindung mit Control Centre, dann können Sie den Ordner ändern, indem Sie den vollständigen Pfad für die Report-Datei angeben. Andernfalls ist das Ändern des Standardpfads nicht möglich.

- **Informationen über komprimierte Dateien im Report anzeigen** – Zur Anzeige von Informationen über komprimierte Objekte und Archive im Report. Die Informationen werden in der Tabelle von Kaspersky® Report Viewer wie folgt dargestellt: Der Name des Objekts steht in der Spalte **Objekt**, der Hinweis **Komprimiert** oder **Archiv** steht in der Spalte **Ergebnis**, der Name des Komprimierungs- oder Archivierungsprogramms steht in der Spalte **Beschreibung**.
- **Informationen über saubere Objekte im Report anzeigen** – Zur Anzeige von Informationen über virusfreie Objekte im Report. Die Informationen werden in der Tabelle von Kaspersky® Report Viewer folgendermaßen dargestellt: Der Name des Objekts steht in der Spalte **Objekt**, der Hinweis **OK** steht in der Spalte **Ergebnis**.
- **Anhängen** – Die Untersuchungsergebnisse werden an die bereits vorhandene Report-Datei angehängt. Dadurch bleiben alle Ergebnisse früherer Untersuchungen erhalten. Wenn Sie dieses Kontrollkästchen deaktivieren, dann wird die Protokolldatei bei jedem Start von Kaspersky AV überschrieben.
- **Maximale Größe beschränken auf (KB)** – Beschränkung der Dateigröße auf den in dem Eingabefeld angegebenen Wert. Als Standard wird der Wert 2048 KB verwendet.

3.3.2.2. Optionen für das Umbenennen, Kopieren und Löschen von Objekten

Vorgehen bei Virus-Fund – Eine Schaltflächengruppe, die das Vorgehen beim Umbenennen infizierter Objekte festlegt. Das Programm verwendet die gewählte Aktion zur Behandlung von Objekten, für die im Konfigurationsbaum der Kategorie **Objekte** die Option **Umbenennen** gewählt wurde (s. Pkt. 3.3.1).

- **Verschieben in Ordner** – Infizierte Objekte in ein gesondertes Verzeichnis verschieben, das im Feld unter der Schaltfläche angegeben wird. In diesem Fall werden infizierte Dateien in einen speziellen Ordner verschoben, wobei Name und Erweiterung unverändert bleiben.

- **Dateien nicht verschieben** – Infizierte Objekte im ursprünglichen Verzeichnis belassen. Dabei wird die Erweiterung durch die im Feld **Dateinamenerweiterung ändern in…** angegebene Erweiterung ersetzt.

☑ **Löschen oder Umbenennen infizierter zusammengesetzter Dateien aktivieren** – Löschen oder Umbenennen von infizierten verbundenen Objekten, wenn deren Desinfektion erfolglos war und auf der Registerkarte **Objekte** die Aktion **Infizierte Dateien löschen** oder **Infizierte Dateien umbenennen** aktiviert wurde. Auf infizierte verbundene Objekte wird diese Aktion nur angewandt, wenn dieser Modus aktiviert ist. Es wird nicht empfohlen, diesen Modus zu aktivieren, weil dadurch Daten verloren gehen können, deren Wiederherstellung mit Spezialprogrammen möglich ist.

3.3.2.3. Priorität des Scanvorgangs

Scan-Priorität festlegen <...> – Prioritätsstufe des Scanvorgangs. Die Auswahl der drei folgenden Werte aus der Liste ist möglich: *Hoch* steht für hohe Priorität, bei der das Betriebssystem das Programm Kaspersky AV Scanner im Vergleich zu anderen laufenden Anwendungen bevorzugt behandelt. *Normal* steht für gewöhnliche Priorität, bei der Kaspersky AV Scanner vom Prozessor wie andere laufende Anwendungen behandelt wird. *Niedrig* steht für niedrige Priorität, bei der jede andere laufende Anwendung die Arbeit von Kaspersky AV Scanner verlangsamt.

3.3.3. Zusätzliche Optionen. Kategorie *Anpassen*

Die Kategorie **Anpassen** (s. Bild 8) enthält zusätzliche Optionen für die Programmfunktion.

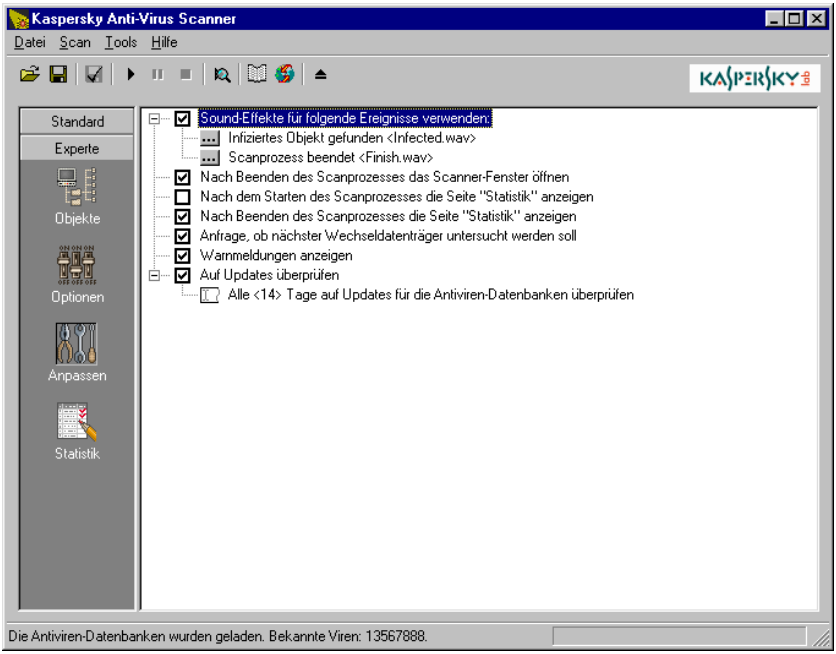


Bild 8. Kategorie **Anpassen**

☑ **Sound-Effekte für folgende Ereignisse verwenden** – In diesem Modus werden bei bestimmten Programmoperationen Klangsignale abgespielt.

- … **Infiziertes Objekt gefunden** – Wählen Sie den Namen der Klang-Datei aus, die gespielt werden soll, wenn ein infiziertes Objekt entdeckt wird. Nach der Auswahl der Datei in der Dateiliste, können Sie durch Klick auf die Schaltfläche **Test** den Sound anhören.
- … **Scanprozess beendet** – Wählen Sie den Namen der Klang-Datei aus, die nach Abschluss des Scanvorgangs gespielt wird soll. Nach der

Auswahl der Datei in der Dateiliste, können Sie durch Klick auf die Schaltfläche **Test** den Sound anhören.

- ☑ **Nach Beenden des Scanprozesses das Scanner-Fenster öffnen –** Zur Anzeige der Ergebnisse sofort nach dem Beenden des Programms. Wurde der Scanvorgang aus dem Systemmenü gestartet, während das Hauptdialogfenster von Kaspersky AV Scanner geschlossen war, dann wird nach dem Beenden des Scanvorgangs das Hauptdialogfenster geöffnet.
- ☑ **Nach dem Starten des Scanprozesses die Seite "Statistik" anzeigen –** Nach dem Start des Scannens wird automatisch in die Kategorie **Statistik** gewechselt, um den Fortschritt der Programmoperation anzuzeigen.
- ☑ **Nach Beenden des Scanprozesses die Seite "Statistik" anzeigen –** Nach dem Beenden des Scanvorgangs wird automatisch in die Kategorie **Statistik** gewechselt, um die Ergebnisse der Programmoperation anzuzeigen.
- ☑ **Anfrage, ob nächster Wechseldatenträger untersucht werden soll –** Anfrage auf Untersuchung des nächsten Wechseldatenträgers durchführen. Diese Anfrage erscheint nur, wenn nur Wechseldatenträger als Scanbereich angegeben wurden.
- ☑ **Warnmeldungen anzeigen –** andere Warnhinweise auf dem Bildschirm anzeigen.
- ☑ **Auf Updates überprüfen** – Kaspersky Anti-Virus® Updater nach Ablauf der im Eingabefeld **Alle <> Tage auf Updates für die Antiviren-Datenbanken überprüfen** angegebenen Anzahl von Tagen automatisch starten (Das Eingabefeld wird aktiviert, wenn Sie diese Option wählen).

Wenn Sie in Kaspersky AV Control Centre mit der Kategorie **Anpassen** arbeiten, dann steht ein Teil der Einstellungen nicht zur Verfügung, dann steht ein Teil der Einstellungen der Kategorie **Anpassen** nicht zur Verfügung. Dies betrifft Einstellungen, die bei der Programmoperation in Verbindung mit Kaspersky AV Control Centre überflüssig sind.

3.3.4. Speichern und Laden von Einstellungen in/aus einer Konfigurationsdatei

Die Einstellungen von Kaspersky AV Scanner können in einer Konfigurationsdatei auf der Festplatte gespeichert werden, um sie später zur Ausführung bestimmter Operationen zu laden. Sie können bestimmte Einstellungen unter

dem Namen **Untersuchung von Wechseldatenträgern** speichern und diese zur Virus-Untersuchung von Disketten laden. Für eine redundante Untersuchung aller Dateien bei dem Verdacht auf Eindringen eines Virus in Ihren Computer können Sie eine andere Konfigurationsdatei unter dem Namen **Vollständige Untersuchung aller Datenträger** speichern usw.

Sie können eine standardmäßig zu ladende Konfigurationsdatei festlegen. Die Einstellungen werden dann bei jedem Start von Kaspersky AV Scanner aus dieser Konfigurationsdatei geladen.

	Hauptmenü	**Symbolleiste**	**Tastatur**
Einstellungen laden	Datei → Profil laden		**<STRG>+<O>**
Einstellungen speichern	Datei → Profil speichern, Datei → Profil speichern unter		**<STRG>+<S>**
Einstellungen als Standard speichern	Datei → Profil als Standard speichern		

Die Standardendung für Konfigurationsdateien von Kaspersky AV Scanner lautet **.klr**. Wird keine Standard-Konfigurationsdatei angegeben, dann verwendet Kaspersky AV Scanner interne Einstellungen.

3.3.5. Vorschau der Einstellungen vor dem Starten des Scannens

Die Scan-Einstellungen können als fortlaufender Text angezeigt werden. Dieser Text enthält die Regeln für die Behandlung aller Objekte des Dateisystems (von **Arbeitsplatz** bis zu einzelnen Dateien). Unterscheiden sich beispielsweise die Regeln für die Datei *autoexec.bat* von den Regeln für das übergeordnete Objekt **System-Laufwerk (C:)**, so wird eine separate Liste der Regeln für diese Datei angezeigt.

Zur Anzeige der Scan-Optionen als fortlaufender Text wählen Sie im Menü **Scan** den Menübefehl **Scan-Vorschau**, oder klicken Sie in der Symbolleiste auf die Schaltfläche  .

Dann wird das Fenster **Scan-Optionen** geöffnet (s. Bild 9), welches die Werte der Scan-Einstellungen für die Kategorien **Objekte** und **Optionen** enthält. Die Einstellungen können überprüft und kopiert werden. Klicken Sie zum Schließen des Fensters auf **OK**.

Die Scan-Optionen sind außerdem am Anfang der Report-Datei als fortlaufender Text gespeichert.

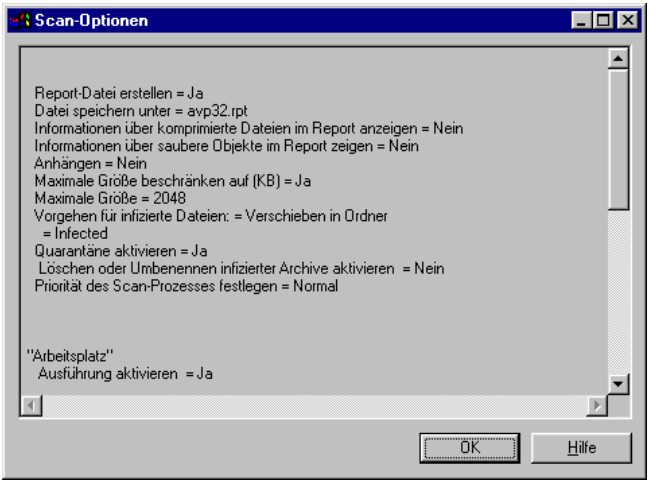


Bild 9. Kategorie **Scan-Optionen**

3.4. Suche und Löschen von Viren

3.4.1. Start und Beenden des Scanvorgangs

Der Scanvorgang kann entweder automatisch oder manuell mit Hilfe von Kaspersky AV Control Centre, oder manuell aus dem Hauptfenster von Kaspersky AV Scanner gestartet bzw. beendet werden.

Nach dem Beginn des Scannens können Sie den Scanvorgang anhalten und fortsetzen, seine Priorität ändern oder das Scannen beenden.

	Hauptmenü	**Systemmenü**	**Symbolleiste**
Starten	Scan → Scannen starten	Scannen starten	
Beenden	Scan → Scannen beenden	Scannen beenden	
Anhalten	Scan → Scannen anhalten	Scannen anhalten	
Fortsetzen	Scan → Scannen fortsetzen	Scannen fortsetzen	

Betrachten wir die Operationen, die Kaspersky AV Scanner sofort nach dem Start ausführt: Unmittelbar nach dem Start lädt das Programm die Antiviren-Datenbanken und untersucht sich selbst auf Viren. Nach erfolgreichem Laden wird in der Statuszeile des Programmfensters folgende Meldung angezeigt:

```
Antiviren-Datenbanken wurden geladen. Bekannte Viren: XXXX
```

XXXX steht hier für die Anzahl der bekannten Viren. Sollte das Programm selbst infiziert sein, dann wird ein Reparaturversuch unternommen. Ist die Reparatur erfolgreich, wird das Programm neu gestartet und ein Hinweis über das Löschen des Virus aus dem Programm wird angezeigt. Wenn die Reparatur nicht möglich ist, wird das Programm nicht gestartet und ein entsprechender Hinweis wird auf dem Bildschirm angezeigt. Wenn Sie über eine virusfreie Kopie von Kaspersky Anti-Virus® verfügen, entfernen Sie die infizierte Kopie des Programms und führen eine Neuinstallation von Kaspersky Anti-Virus® durch.

Nach Abschluss des Scannens liefert Kaspersky AV Scanner Rückgabewerte, die Sie beim Erstellen von Paketdateien verwenden können. Das Programm kann einen der folgenden Werte ausgeben:

- **0** – Es wurden keine Viren gefunden.
- **1** – Das Scannen wurde nicht abgeschlossen.
- **2** – Es wurden Objekte entdeckt, die einen modifizierten oder defekten Virus enthalten.
- **3** – Es wurden Objekte entdeckt, die verdächtig sind, Viren zu enthalten.

- **4** – Ein bekannter Virus wurde entdeckt.
- **5** – Alle entdeckten Viren wurden gelöscht.
- **7** – Kaspersky AV Scanner ist beschädigt.
- **10** – Interner Fehler von Kaspersky AV Scanner.

3.4.2. Ändern der Scan-Priorität

Die Priorität des Scanvorgangs kann geändert werden, ohne das Scannen zu beenden. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie im Menü **Scan** den Menübefehl **Scan-Priorität ändern**.

2. Wählen Sie im folgenden Dialogfenster (s. Bild 10) einen Prioritätswert (*Hoch*, *Normal*, *Niedrig*) aus der Dropdown-Liste (Details s. Pkt. 3.3.2.3).

Bild 10. Dialogfenster zur Auswahl der Priorität des Scanvorgangs

Andere Optionen können während des Scanvorgangs nicht geändert werden! Möchten Sie die Einstellungen ändern, dann beenden Sie zuerst den Scanvorgang und wählen Sie dann die gewünschten Optionen. Danach kann der Scanvorgang neu gestartet werden.

3.4.3. Anzeige des Reports

Wurden die Parameter für die Reporterstellung aktiviert (s. Pkt. 3.3.2.1), dann können Sie mit Hilfe von Kaspersky® Report Viewer den Arbeitsverlauf von Kaspersky AV Scanner verfolgen. Wählen Sie zum Starten im Menü **Tools** den Befehl **Report anzeigen** oder klicken Sie in der Symbolleiste auf die Schaltfläche  . Danach wird das Hauptfenster des Programms Kaspersky® Report Viewer geöffnet, in dem Sie die Informationen über den Verlauf des Scannens überprüfen können (s. Kapitel 7).

3.4.4. Anzeige der Statistik. Kategorie ***Statistik***

Wenn Sie die Parameter das Erstellen des Reports nicht aktiviert haben, dann können die Veränderungen der Statistik in der Tabelle der Kategorie **Statistik** verfolgt werden (s. Bild 11).

Die Tabelle besteht aus zwei Teilen: **Gescannt** und **Gefunden**. Der obere Teil (**Gescannt**) enthält die Anzahl der untersuchten Sektoren, Dateien, Ordner, Archive und komprimierten Dateien. Der untere Teil (**Gefunden**) enthält Angaben über die Anzahl folgender Kategorien:

- *Bekannte Viren*
- *Virus-Körper, d.h. die Anzahl der durch einen bekannten Virus infizierten Dateien*
- *Desinfizierte Objekte, d.h. Objekte, aus denen Viren korrekt entfernt wurden*
- *Gelöschte Objekte*
- *Umbenannte Objekte*
- *Warnungen, d.h. Hinweise auf Objekte, die ähnliche Codes wie bekannte Virus-Versionen enthalten*
- *Verdächtiger Objekte, d.h. der Meldungen des Code Analyzers*

- *Beschädigte Objekte*
- *Eingabe/Ausgabe-Fehler*

Die Operationsgeschwindigkeit (in KB/Sek) und die Gesamtzeit der Untersuchung aller Objekte werden im unteren Bereich der Tabelle angezeigt.

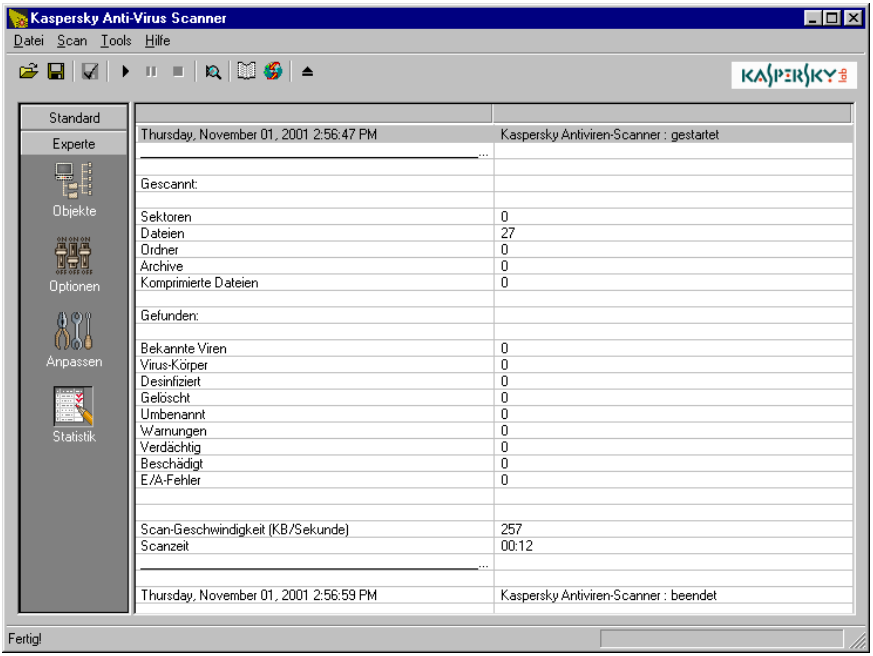


Bild 11. Kategorie **Statistik**

3.5. Starten des Updaters für die Antiviren-Datenbanken

Das Programm zur Aktualisierung der Antiviren-Datenbanken kann aus dem Hauptfenster von Kaspersky AV Scanner gestartet werden. Wählen Sie dazu im Menü **Tools** den Befehl **Antiviren-Datenbanken aktualisieren** oder klicken Sie in der Symbolleiste auf die Schaltfläche  .

3.6. Erstellen einer Liste der bekannten Viren

Um eine Liste aller dem Programm momentan bekannten Viren zu erstellen,

1. Wählen Sie im Menü **Tools** den Befehl **Virus-Liste erstellen**. Danach wird **Kaspersky Virus List Generator** gestartet.

2. Geben Sie im folgenden Dialogfenster **Kaspersky Virus List Generator** (s. Bild 12) den Namen der Datei an, in der die Virenliste gespeichert werden soll. Zur Angabe des Dateinamens dient die Schaltfläche **Durchsuchen**.

3. Klicken Sie auf **Erstellen**.

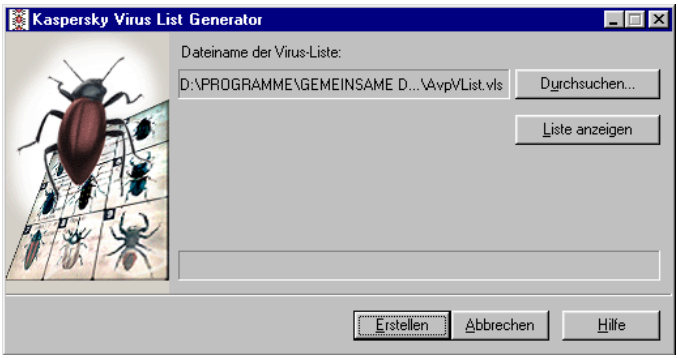


Bild 12. Dialogfenster von Kaspersky Virus List Generator

Zur Anzeige der Liste wird mit der Schaltfläche **Liste anzeigen** Kaspersky® Report Viewer gestartet.

Klicken Sie zum Schließen von **Kaspersky Virus List Generator** auf die Schaltfläche **Abbrechen**.

Sie können **Kaspersky Virus List Generator** auch autonom starten. Klicken Sie dazu in der Windows-Taskleiste auf die Schaltfläche **Start** und gehen Sie zum Untermenü **Programme**. Danach wählen Sie in der Gruppe **Kaspersky Anti-Virus®** den Punkt **Kaspersky Virus List Generator**.

KAPITEL 4. KASPERSKY ANTI-VIRUS® MONITOR

Der Antiviren-Monitor Kaspersky Anti-Virus® Monitor (Kaspersky AV Monitor) ist ein Programm, das sich ständig im Arbeitsspeicher Ihres Rechners befindet und den Zugriff auf Dateien und Sektoren (Master-Bootsektor und Bootsektoren) überwacht. Bevor der Zugriff auf ein Objekt erlaubt wird, untersucht Monitor dieses auf Viren. Ist das Objekt infiziert, dann versucht das Programm (in Abhängigkeit der von Ihnen vorgenommenen Einstellungen) die Desinfektion des Objekts, löscht es, oder blockiert den Zugriff auf das Objekt. Dadurch kann Kaspersky AV Monitor Viren vor einer realen Infektion des Systems entdecken und entfernen.

An dieser Stelle ist anzumerken, dass es für ähnliche Programme wie Kaspersky AV Monitor von Kaspersky Labs unterschiedliche Bezeichnungen gibt. Sie werden zum Beispiel als residente Scanner, Antiviren-Filter oder On-Access-Scanner o.ä. bezeichnet.

4.1. Start und Beenden des Antiviren-Monitors

Es gibt verschiedene Möglichkeiten für den Start des Antiviren-Monitors, die im Folgenden ausführlich beschrieben werden:

Methode 1: aus dem Windows-Hauptmenü: Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, zeigen Sie auf **Programme**, dann auf **Kaspersky Anti-Virus®**, und klicken Sie auf **Kaspersky Anti-Virus® Monitor**.

Das Monitor-Symbol  erscheint im Infobereich der Taskleiste. Das Monitor-Systemmenü kann durch Rechtsklick auf dieses Symbol geöffnet werden (s. Pkt. 4.2.1).

Methode 2: automatisch beim Start des Betriebssystems, wenn Sie bei der Installation von Kaspersky Anti-Virus® auf Ihrem Computer eine Verknüpfung von Kaspersky AV Monitor zum Windows-Menü **Autostart** erstellt haben.

Methode 3: aus Kaspersky AV Control Centre, wenn Sie Kaspersky AV Control Centre installiert haben und in dessen Einstellungen den automatischen Start von Kaspersky AV Monitor festgelegt haben. Allerdings wird in diesem Fall das Verknüpfungssymbol nicht in der Taskleiste erscheinen.

Methode 4: aus einer Befehlszeile: Gehen Sie dazu in den Ordner, in den Kaspersky Anti-Virus® installiert wurde, und führen die Datei *avpm.exe* aus.

Ist Kaspersky AV Monitor aktiviert, dann:

- erscheint im Infobereich der Taskleiste das Symbol  .
  - erscheint die Popupinformation **Kaspersky Anti-Virus® Monitor aktiv**, wenn der Mauszeiger auf das Symbol  geführt wird.
  - enthält das Systemmenü von Kaspersky AV Monitor den Befehl **Monitoring deaktivieren**.

Ist Kaspersky AV Monitor deaktiviert, dann:

- erscheint im Infobereich der Taskleiste das Symbol  .
  - erscheint die Popupinformation **Kaspersky Anti-Virus® Monitor inaktiv**, wenn der Mauszeiger auf das Symbol  geführt wird.
  - enthält das Systemmenü von Kaspersky AV Monitor den Befehl **Monitoring aktivieren**.

Es wird nicht empfohlen, auf einem Computer gleichzeitig zwei Antiviren-Monitore unterschiedlicher Hersteller zu verwenden, da dies zu Konflikten und Fehlalarm führen kann.

Wenn Sie Monitor von Kaspersky AV Control Centre aus starten, kann nur über Kaspersky AV Control Centre auf die Monitor-Einstellungen zugegriffen werden!

4.2. Programmoberfläche

Dieser Abschnitt enthält eine Beschreibung der Benutzeroberfläche von Kaspersky Anti-Virus® Monitor: Systemmenü, Hauptfenster, Arbeitsbereich usw.

Während der Arbeit mit dem Programm Kaspersky Anti-Virus® Monitor erscheinen unterschiedliche Servicefenster auf dem Bildschirm, z.B. Hinweise über den Fund eines infizierten Objekts oder sonstige Informationen, die Ihre Antwort verlangen. Wenn das Beenden der Computersession erforderlich ist, dann schließen Sie vorher alle Hinweisfenster, falls solche auf dem Bildschirm angezeigt werden.

4.2.1. Systemmenü

Nach dem Programmstart wird das Hauptfenster des Programms geöffnet (s. Pkt. 3.2.2) und im Infobereich der Taskleiste erscheint das Verknüpfungssymbol  . Um das Systemmenü (s. Bild 13) zu öffnen, klicken Sie mit der rechten Maustaste auf dieses Symbol. Das Systemmenü enthält folgende Befehle:

- ***Kaspersky Anti-Virus® Monitor Einstellungen*** – *Öffnet das Hauptfenster des Programms.*
- ***Monitoring deaktivieren / Monitoring aktivieren*** – *Deaktiviert/aktiviert das Monitor-Programm.*
- ***Report anzeigen*** – *Öffnet das Report-Fenster mit den Arbeitsergebnissen des Programms.*
- ***Antiviren-Datenbanken aktualisieren*** – *Startet Kaspersky AV Updater, das Programm zur Aktualisierung der Datenbanken.*
- ***Über...*** – *Öffnet ein Dialogfenster, mit Informationen über das Programm Kaspersky AV Monitor.*
- ***Kaspersky Anti-Virus® Monitor beenden*** – *Beendet das Programm und entfernt es aus dem Arbeitsspeicher.*

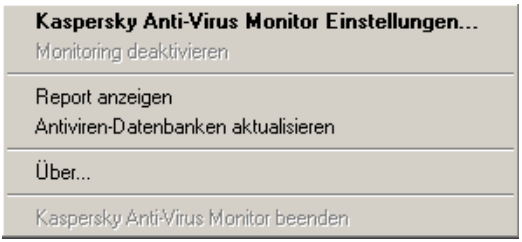


Bild 13. Systemmenü

4.2.2. Hauptfenster

Das Hauptfenster des Programms Kaspersky AV Monitor dient zum Ändern der Monitor-Einstellungen, zum Aktivieren / Deaktivieren von Monitor, und zum Öffnen des Ergebnisprotokolls (s. Bild 14). Sie können das Hauptfenster schließen, ohne dass das Programm aus dem Arbeitsspeicher entfernt wird.

Das Hauptfenster von Kaspersky AV Monitor enthält folgende Elemente: Menü, Symbolleiste, Arbeitsbereich, die Schaltflächen **OK**, **Abbrechen**, **Übernehmen** und **Hilfe**

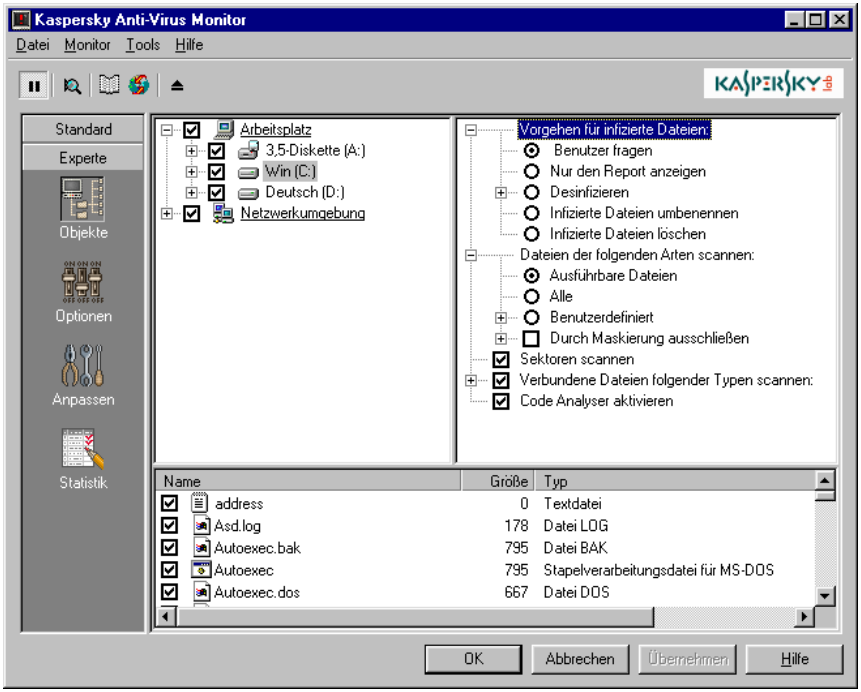


Bild 14. Das Hauptfenster von Kaspersky AV Monitor

4.2.3. Menü

Im oberen Bereich des Hauptfensters befindet sich das *Menü*. Bestimmte Menüpunkte sind sowohl als Tastenkombinationen wie auch als Symbolleisten-Schaltflächen vorhanden. Die Tastenkombinationen sind im Menü rechts vom jeweiligen Menübefehl angegeben. Die Zuordnung von Tastenkombinationen und Symbolleisten-Schaltflächen zu den Menübefehlen wird in Punkt 4.2.4 erläutert.

Menüpunkt	**Funktion**
Datei → Kaspersky Anti-Virus® Monitor beenden	Beendet Kaspersky AV Monitor und entfernt ihn aus dem Arbeitsspeicher.
Datei → Fenster schließen	Schließt das Hauptfenster von Kaspersky AV Monitor.
Monitor → Monitoring aktivieren / Monitoring deaktivieren	Aktiviert / deaktiviert das Programm zur Virus-Überwachung (s. Pkt. 4.4).
Monitor → Scan-Optionen anzeigen	Zeigt die Monitor-Einstellungen als Fließtext an (ähnlich wie Punkt 3.3.5).
Tools → Antiviren-Datenbanken aktualisieren	Aktualisierung der Antiviren-Datenbanken (s. Pkt. 3.5).
Tools → Report anzeigen	Öffnet das Report-Fenster (s. Pkt. 3.4.3).
Tools → Virus-Liste erstellen	Erstellt eine Liste der zur Zeit bekannten Viren (s. Pkt. 3.6).
Hilfe → Inhalt	Öffnet das Hilfesystem.
Hilfe → Kaspersky Anti-Virus® im Internet	Startet Ihren Web-Browser und öffnet die Internetseite von Kaspersky Lab.
Datei → Über Kaspersky Anti-Virus® Monitor...	Zeigt Informationen über das Programm an.

4.2.4. Symbolleiste

Die *Symbolleiste* enthält Schaltflächen. Durch Klick auf eine Schaltfläche wird die entsprechende Funktion ausgeführt.

Schalt–fläche	Menü → Befehl	Funktion
	Monitor → Monitoring aktivieren / Monitoring deaktivieren	Aktiviert / Deaktiviert das Programm zur Virus-Überwachung
	Monitor → Scan-Optionen anzeigen	Anzeige der Monitor-Einstellungen als fortlaufender Text
	Tools → Antiviren-Datenbanken aktualisieren	Aktualisierung der Antiviren-Datenbanken
	Tools → Report anzeigen	Öffnet das Report-Fenster
	Datei → Kaspersky Anti-Virus® Monitor beenden	Beendet Kaspersky AV Monitor und entfernt ihn aus dem Arbeitsspeicher

4.2.5. Arbeitsbereich

Der Arbeitsbereich des Hauptfensters besteht aus zwei Teilen. Auf der linken Seite sind die Kategorienliste und deren Symbole angeordnet. Auf der rechten Seite werden die Inhalte der Kategorien angezeigt. Es gibt vier Kategorien: **Objekte**, **Optionen**, **Anpassen** und **Statistik**.

Die Kategorie **Objekte** dient zum Festlegen des Überwachungsbereichs und der Regeln zur Behandlung infizierter Objekte. Alle diese Einstellungen sind in Form eines speziellen Bedienungselements organisiert, das *Hierarchiebaum der Objekteinstellungen* genannt wird.

In der Kategorie **Optionen** können allgemeine Einstellungen vorgenommen werden. Die Kategorie **Anpassen** bietet die Möglichkeit spezieller Programmeinstellungen mit Hilfe des *Konfigurationsbaumes (s. Pkt. 3.3.2, 3.3.3).*

Die Kategorie **Statistik** erlaubt die Anzeige von Ergebnissen der Programmoperationen in Tabellenform (s. Pkt. 3.4.4).

Die Elemente des Konfigurationsbaums verfügen über ein *Kontextmenü*, mit dessen Hilfe auf das jeweilige Element bezogene Operationen ausgeführt werden können.

Um das Kontextmenü eines bestimmten Elements des Konfigurationsbaums zu öffnen,

1. Zeigen Sie mit dem Mauszeiger auf das betreffende Element.

2. Klicken Sie mit der rechten Maustaste. Dann wird das Kontextmenü des Elements eingeblendet.

4.3. Konfiguration der Monitor-Einstellungen

Die Einstellungen für den Antiviren-Monitor entsprechen weitgehend den Einstellungen für Kaspersky Anti-Virus® Scanner (s. Pkt. 3.3).

Unterschiede bestehen in folgenden Punkten: In der Kategorie **Objekte** sind die Parameter **Datenbanken von MS Outlook Express scannen** und **Beim Systemstart auszuführende Objekte scannen** nicht vorhanden. Somit steht auch die Möglichkeit, entsprechende Objekte zu überwachen, nicht zur Verfügung. Dies bedeutet, dass im Überwachungsmodus kein Mail-Datenbanken desinfiziert werden können. Das Programm kann aber in diesen Objekten Viren entdecken, wenn Sie die Kontrollkästchen **Mail-Datenbanken** und **Text-Mail-Formate** aktivieren.

In der Kategorie **Optionen** fehlt die Option **Scan-Priorität festlegen**, was auf funktionellen Unterschieden zwischen Kaspersky AV Monitor und Kaspersky AV Scanner beruht. Zusätzlich ist die Option **Die Größe der zu scannenden zusammengesetzten Dateien einschränken** vorhanden, die dazu dient, die Überwachung umfangreicher Archive usw. zu beschleunigen. Die Maximalgröße für verbundene Dateien wird im Zahlenfeld neben dem Kontrollkästchen **Die Größe der zu scannenden zusammengesetzten Dateien (KB) einschränken** eingegeben.

In dieser Version von Kaspersky Anti-Virus® werden von Kaspersky AV Monitor neben gewöhnlichen Objekten auch ZIP-Archive auf Viren untersucht und desinfiziert.

In der Kategorie **Anpassen** sind die Optionen **Nach Beenden des Scanprozesses das Scanner-Fenster öffnen**, **Nach dem Starten des Scanprozesses die Seite "Statistik" anzeigen**, **Nach Beenden des Scanprozesses die Seite "Statistik" anzeigen**, und **Anfrage, ob nächster Wechseldatenträger untersucht werden soll** nicht vorhanden.

Aktivieren Sie die Kontrollkästchen **Sektoren scannen** und **Arbeitspeicher scannen**, so werden beim Start des Monitors die Sektoren und der Arbeitsspeicher ein Mal gescannt. Außerdem wird durch das Aktivieren des Kontrollkästchens **Arbeitsspeicher scannen** die Überwachung des für gestartete Programme verwendeten Arbeitsspeichers aktiviert. Kaspersky AV Monitor führt diese Kontrolle gleich nach dem Start aus, sowie nach jedem Update der Antiviren-Datenbanken auf Ihrem Rechner. Sollte ein infizierter Programmspeicher nicht zu reparieren sein, wird das betroffene Programm zwangsweise abgebrochen.

4.4. Start und Beenden von Monitor

Kaspersky AV Monitor kann entweder automatisch mit Hilfe des Programms Kaspersky AV Control Centre, oder manuell aus dem Programm Kaspersky AV Control Centre, oder manuell aus dem Hauptfenster von Kaspersky AV Monitor gestartet bzw. beendet werden.

Nach dem Beginn der Überwachung kann diese deaktiviert und wieder aktiviert werden.

	Hauptmenü → Befehl	**Systemmenü**	**Symbolleiste**
Deaktivieren	Monitor → Monitoring deaktivieren	Überwachung anhalten	
Aktivieren	Monitor → Monitoring aktivieren	Überwachung einschalten	

4.5. Anzeige der Statistik

Die Veränderungen der Statistik können in der Tabelle der Kategorie **Statistik** verfolgt werden (s. Bild 15).

Die Statistik-Tabelle besteht aus zwei Feldern: **Gescannt** und **Gefunden**. Das Feld **Gescannt** zeigt die Anzahl der untersuchten Sektoren, Dateien, Ordner,

Archive und komprimierter Dateien. Der untere Teil (**Gefunden**) informiert über die Anzahl folgender Kategorien:

- *Bekannte Viren*
- *Virus-Körper, d.h. die Anzahl der durch einen bekannten Virus infizierten Dateien*
- *Desinfizierte Objekte, d.h. Objekte, aus denen Viren korrekt entfernt wurden*
- *Gelöschte Objekte*
- *Umbenannte Objekte*
- *Warnungen, d.h. Hinweise auf Objekte, die ähnliche Codes enthalten wie eine bekannte Virus-Version*
- *Verdächtige Objekte, d.h. der Meldungen des Code Analyzers*
- *Beschädigte Objekte*
- *Eingabe/Ausgabe-Fehler.*

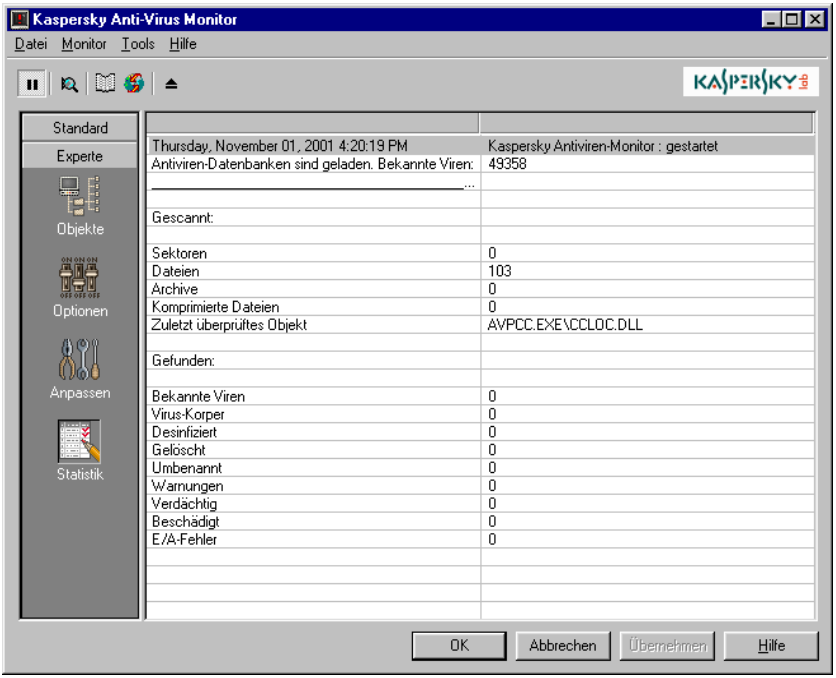


Bild 15. Kategorie **Statistik**

4.6. Start des Updateprogramms für die Antiviren-Datenbanken

Das Update-Programm für die Antiviren-Datenbanken kann im Hauptfenster von Kaspersky AV Monitor gestartet werden. Wählen Sie dazu im Menü **Tools** den Befehl **Antiviren-Datenbanken aktualisieren** oder klicken Sie in der Symbolleiste auf die Schaltfläche  .

KAPITEL 5. KASPERSKY ANTI-VIRUS® UPDATER

Das Aktualisierungsprogramm Kaspersky Anti-Virus® Updater (Kaspersky AV Updater) ist eine Komponente von Kaspersky Anti-Virus® und dient der automatischen Aktualisierung der Antiviren-Datenbanken, in denen Virus-Definitionen und Reparaturmethoden enthalten sind, und dem Update der Paketkomponenten.

Der Download der Antiviren-Datenbanken und der ausführbaren Module wird von dem Update-Programm über das Internet (über Netzwerk- oder Remote-Verbindung), aus einem lokalen Ordner oder von einem Antiviren-Netzwerkserver, der unter Kaspersky® Administration Kit arbeitet, durchgeführt.

5.1. Start des Updateprogramms

Es bestehen mehrere Möglichkeiten für den Start von Kaspersky Anti-Virus® Updater:

Methode № 1: aus dem Windows-Hauptmenü. Klicken Sie dazu in der Windows-Taskleiste auf die Schaltfläche **Start**, zeigen Sie auf **Programme**, und klicken dann in der Programmgruppe **Kaspersky Anti-Virus®** auf den Punkt **Kaspersky Anti-Virus® Updater**.

Methode № 2: aus Kaspersky AV Control Centre. Für den automatischen Start des Updateprogramms kann ein Task erstellt werden (Details zu Kaspersky AV Control Centre s. Kapitel 6).

Methode № 3: aus einer Befehlszeile. Wechseln Sie dazu in den gemeinsam genutzten Ordner von Kaspersky Anti-Virus® (**KAV Shared Files**) und führen Sie die Datei *avpupd.exe* aus. Der gemeinsam genutzte Ordner kann sich unter folgendem Pfade befinden: **C:\Program Files\Common Files\KAV Shared Files**.

5.2. Benutzeroberfläche von des Updateprogramms

Die Benutzeroberfläche von Kaspersky AV Updater ist ähnlich wie ein Programmassistent für Windows (Windows Wizard) gestaltet und besteht aus einer Abfolge von Fenstern (Schritten), zwischen denen mit Hilfe der Schaltflächen **Zurück** und **Weiter** gewechselt wird. Zum Abschluss der Aktualisierung dient die Schaltfläche **Fertig**stellen. Mit der Schaltfläche **Abbrechen** kann das Programm an einem beliebigen Punkt abgebrochen werden.

In der Mitte jedes Fensters ist ein Konfigurationsbaum platziert (zur Funktionsweise des Baums siehe Kapitel 8). Dieses Bedienungselement enthält Einstellungen, die als hierarchischer Baum angeordnet sind.

5.2.1. Schritt 1. Das erste Fenster des Aktualisierungsassistenten von Kaspersky AV Updater

Gleich nach dem Start des Update-Programms wird das erste Fenster des Assistenten geöffnet: **Willkommen bei Kaspersky AV Updater Wizard** (s. Bild 16).

Bild 16. Fenster **Willkommen**

In diesem Fenster wird angezeigt, welche Paketkomponenten aktualisiert werden und von welcher Quelle das Update empfangen werden soll. Zum Ändern von Programmeinstellungen, wird das Kontrollkästchen **Einstellungen ändern** aktiviert. Andernfalls werden die unten beschriebenen Schritte übersprungen, die mit dem Ändern von Einstellungen zusammenhängen.

5.2.2. Schritt 2. Fenster *Verbindung*

Im Fenster **Verbindung** (s. Bild 17) können bei Bedarf die Standard-Einstellungen geändert werden.

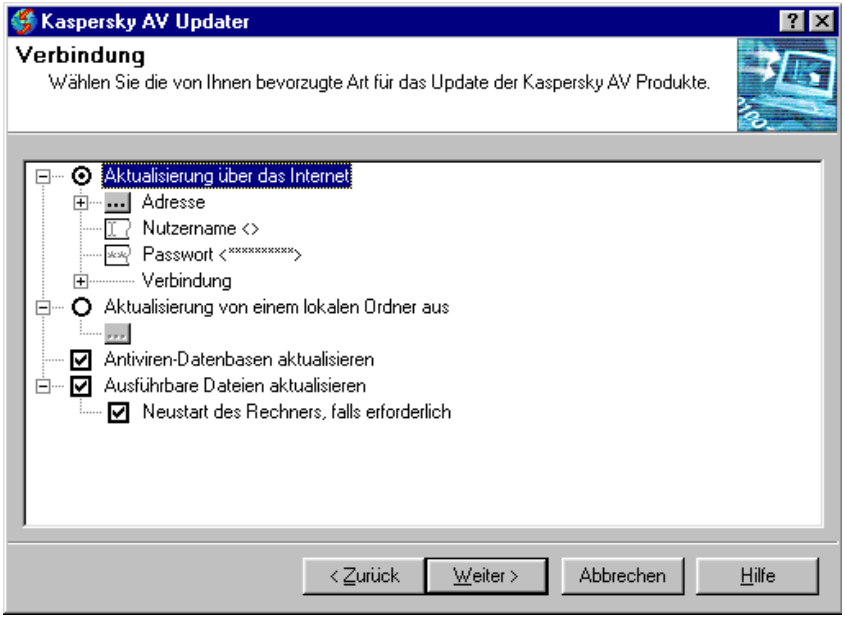


Bild 17. Fenster **Verbindung**

Das Fenster **Verbindung** enthält Einstellungen für die Art und das Objekt der Aktualisierung. Unten werden die Funktionen jedes Befehls auf der ersten Ebene des Konfigurationsbaums erläutert (s. Bild 18).

- **Aktualisierung über das Internet** – Update über das Internet vornehmen
- **Aktualisierung aus lokalem Ordner** – Update aus einem lokalen Ordner durchführen

- **Antiviren-Datenbanken aktualisieren** – Aktualisierung der Antiviren-Datenbanken
- **Ausführbare Dateien aktualisieren** – ausführbare Module von Kaspersky Anti-Virus® aktualisieren
  - **Neustart des Rechners, falls erforderlich** – Computer neu starten, wenn dies nach der Aktualisierung ausführbarer Module des Softwarepakets erforderlich ist.

Klicken Sie auf **Weiter**, nachdem Sie die Einstellungen vorgenommen haben.

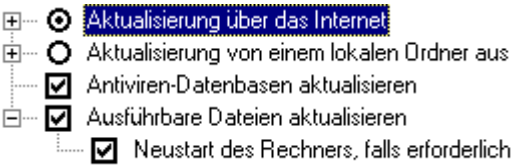


Bild 18. Allgemeine Einstellungen des Updaters

5.2.2.1. Einstellungen für das Internet-Update

Haben Sie **Aktualisierung über das Internet** gewählt, dann ist die Konfiguration dieser Funktion erforderlich. Öffnen Sie den Ast **Aktualisierung über das Internet** des Konfigurationsbaums (s. Bild 19). Unten werden die einzelnen Einstellungen erläutert:

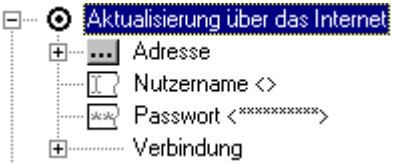


Bild 19. Einstellungen für die Aktualisierung über das Internet

Adresse – Einstellung der Update-Quelle (Protokoll, Servername ...).

Benutzername – Benutzername für den Zugriff auf den Update-Server.

Passwort – Kennwort für den Zugriff auf den Update-Server.

Verbindung – Einstellungen für die Verbindung mit dem Remote-Server.

Wenn Microsoft Internet Explorer im Offlinebetrieb arbeitet, kann das Programm auch dann keine Updates aus dem Internet empfangen, wenn die Verbindungsparameter manuell eingestellt wurden.

5.2.2.1.1. Auswahl der Adresse

Sie können die Aktualisierung über einen in die Liste eingetragenen Update-Server vornehmen. Um die Liste einzusehen, öffnen Sie den Ast **Adresse** des Konfigurationsbaums (s. Bild 20).

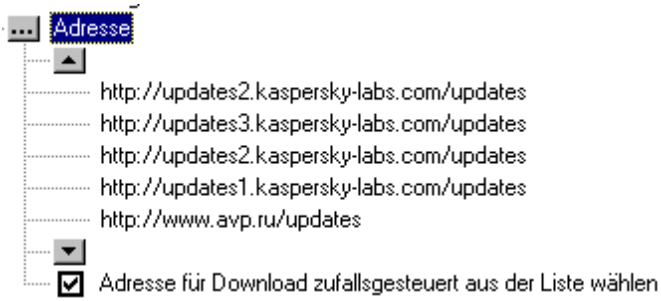


Bild 20. Einstellungen für die Adresse des Update-Servers

Als Standard wird bei der Aktualisierung die Adresse des ersten Servers in der Liste verwendet. Bei erfolgslosem Versuch wird auf den zweiten Server zugegriffen, usw. Eine Meldung über einen Fehler beim Server-Zugriff erscheint nur, wenn zu keinem der Server eine Verbindung hergestellt werden konnte. Wenn Sie das Kontrollkästchen ☑ **Adresse für Download zufallgesteuert aus der Liste wählen** aktivieren, wird als erster Server eine zufällig gewählte Server-Adresse aus der Liste verwendet.

Klicken Sie zum Ändern der Serverliste auf die Schaltfläche … **Adresse**. Danach erscheint auf dem Bildschirm das Dialogfenster **Bearbeiten der Adressen-Liste** (s. Bild 21).

Zur Bearbeitung der Liste dienen folgende Schaltflächen des Dialogfensters oder die entsprechenden Punkte des Kontextmenüs:

– neue Adresse in die Liste aufnehmen

– aktuelle Adresse ändern

– aktuelle Adresse löschen

 – aktuelle Adresse um eine Zeile nach oben verschieben

 – aktuelle Adresse um eine Zeile nach unten verschieben

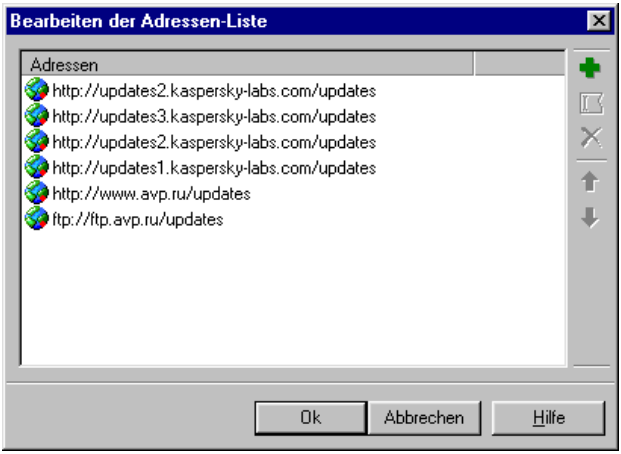


Bild 21. Dialogfenster **Bearbeiten der Adressen-Liste**

5.2.2.1.2. Konfiguration der Verbindungsparameter mit dem Internet-Provider

Die Einstellungen für die Verbindung mit dem Internet-Provider sind abhängig von der Art der Verbindung mit dem Update-Server, die Sie verwenden möchten (s. Bild 22):

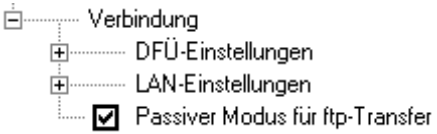


Bild 22. Einstellungen der Internet-Verbindung

DFÜ-Einstellungen – Einstellungen für die DFÜ-Verbindung zu einem Internet-Provider

LAN-Einstellungen – Einstellungen der Verbindung mit dem Internet-Provider unter Verwendung eines lokalen Netzwerks

☑ **Passiver Modus für ftp-Transfer** – Für die Verbindung mit dem FTP-Server den passiven Modus verwenden (dies ist besonders wichtig für Benutzer, welche die Verbindung zu ihrem Internet-Provider über Proxyserver oder Firewall herstellen).

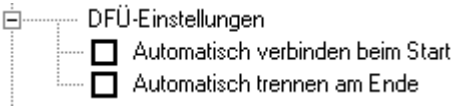


Bild 23. DFÜ-Einstellungen

Für die Einstellung der DFÜ-Verbindung können folgende Optionen aktiviert werden (s. Bild 23):

☑ **Automatisch verbinden beim Start** – DFÜ-Verbindung mit dem Internet-Provider sofort nach dem Start des Update-Vorgangs herstellen

☑ **Automatisch trennen am Ende** – Nach Abschluss des Aktualisierungsvorgangs die Verbindung automatisch trennen (Modem ausschalten)

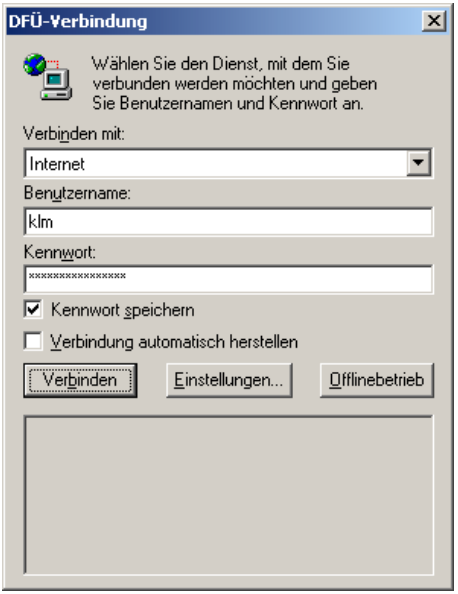


Bild 24. Dialogfenster **DFÜ-Verbindung**

Haben Sie den automatischen Aufbau der DFÜ-Verbindung mit einem Internet-Provider gewählt, dann ruft das Programm nach dem Start des Aktualisierungsvorgangs das Standard-DFÜ-Dienstprogramm auf (falls Sie kein anderes Programm gewählt haben).

Zum Aufbau der Verbindung zu einem Internet-Provider füllen Sie das Dialogfenster **DFÜ-Verbindung** aus (s. Bild 24) und klicken Sie auf **Verbinden**. Danach wird eine Verbindung mit dem Remote-Server hergestellt.

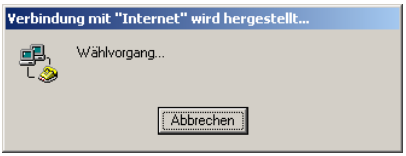


Bild 25. Fenster **Verbindung mit "Internet" wird hergestellt**. Wählvorgang

Während des Wählvorgangs wird auf dem Bildschirm das Dialogfenster **Verbindung mit "Internet" wird hergestellt** mit dem Hinweis **Wählvorgang**... angezeigt (s. Bild 5).

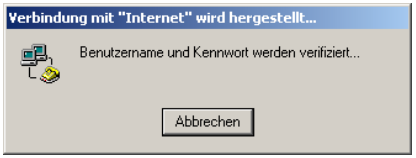


Bild 26. Fenster "**Verbindung mit "Internet" wird hergestellt**". Überprüfung von Benutzername und Kennwort

Nach dem Wählvorgang werden Benutzername und Kennwort überprüft.
Der Hinweis **Benutzername und Kennwort werden verifiziert…** wird angezeigt (s. Bild 26).

Bild 27. Fenster **User Logon**

Falls der Benutzer auf Grund seiner Angaben nicht identifiziert werden kann, erscheint das Fenster **Verbindung mit "Internet" herstellen (User Logon)** (s. Bild 27), in dem die Verbindungseinstellungen **Benutzername**, **Kennwort** und **Anmeldedomäne** einzugeben sind.

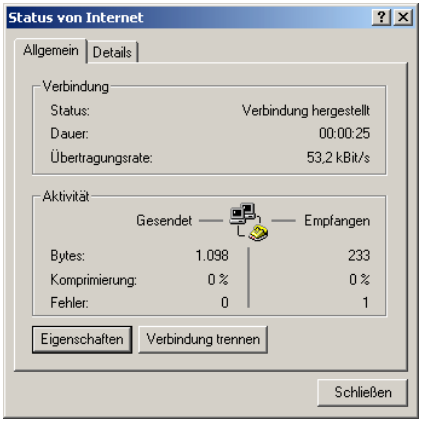


Bild 28. Dialogfeld **Status von Internet**. Verbindungparameter

Nachdem eine Verbindung mit dem Internet hergestellt wurde, erscheint ein entsprechendes Symbol in der Taskleiste. Die Eigenschaften der Verbindung können durch Doppelklick auf das Symbol in der Taskleiste angezeigt werden (s. Bild 28).

Wenn Sie ein lokales Netzwerk (LAN) für die Verbindung zu einem Internet-Provider verwenden, können Sie entweder die Einstellungen aus der Systemsteuerung benutzen oder die Verbindung manuell konfigurieren (s. Bild 29):

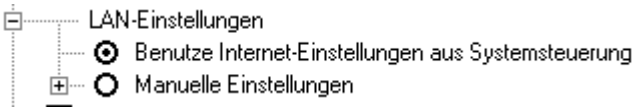


Bild 29. Parameter für LAN-Verbindung

- **Benutze Internet-Einstellungen aus Systemsteuerung** – Einstellungen für die Verbindung aus der Systemsteuerung übernehmen;
- **Manuelle Einstellungen** – Verbindungseinstellungen manuell konfigurieren.

Wurde die manuelle Einstellung gewählt, dann ist die Konfiguration folgender Parameter erforderlich (s. Bild 30):

Bild 30. Manuelle Einstellungen

- **Proxy verwenden (Firewall)** – für die Verbindung mit dem Internet-Provider einen Proxyserver oder eine Firewall benutzen
  - **Adresse** – Adresse des Proxyservers (oder der Firewall) für die Verbindung. Die Adresse kann in Dezimalform (zum Beispiel: 125.5.29.1), als vollständige Domänenangabe (zum Beispiel: test.russia.ru) oder als Kurzform (zum Beispiel: test) eingegeben werden.
  - **Port** – Port für die Verbindung mit dem Proxyserver (oder der Firewall)
- **Authentifizierung** – Individuelle Benutzereinstellungen
  - **Benutzername** – Benutzername für Proxyserver (oder Firewall)
  - **Passwort** – Passwort für Proxyserver (oder Firewall)
- **HTTP-Proxy mit Unterstützung für FTP** – Zugriff auf FTP-Server über HTTP-Proxyserver (CERN-Proxy)

Um detaillierte Informationen über die genannten Einstellungen der Internet-Verbindung zu erhalten, wenden Sie sich bitte an Ihren Systemadministrator.

5.2.2.2. Aktualisierung aus einem lokalen Ordner

Wenn Sie einen lokalen Ordner als Quelle für das Update gewählt haben, dann ist die Angabe des vollständigen Pfads des Ordners erforderlich. Klicken Sie dazu auf die Schaltfläche ... (s. Bild 31). Danach wird das Dialogfenster **Ordner suchen** geöffnet, in dem der Update-Ordner gewählt wird.

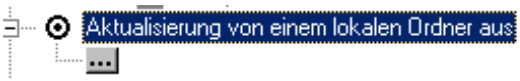


Bild 31. Aktualisierung aus einem lokalen Ordner

5.2.2.3. Auswahl der zu aktualisierenden Objekte

Im untersten Teil des Konfigurationsbaums befinden sich die folgenden zwei Optionen (Bild 32):

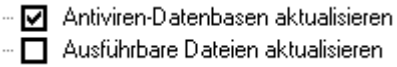


Bild 32. Auswahl des zu aktualisierenden Objektes

- **Antiviren-Datenbanken aktualisieren** – Antiviren-Datenbanken vom Update-Server kopieren und installieren
- **Ausführbare Dateien aktualisieren** – ausführbare Module vom Update-Server kopieren und installieren
  - **Rechner neu starten (falls erforderlich)** – nach der Installation von Programm-Updates den Rechner automatisch neu starten (falls erforderlich)

5.2.3. Schritt 3. Das Fenster *Optionen*

Im Fenster **Optionen** können zusätzliche Funktionen des Update-Programms für die Antiviren-Datenbanken eingestellt werden (s. Bild 33).

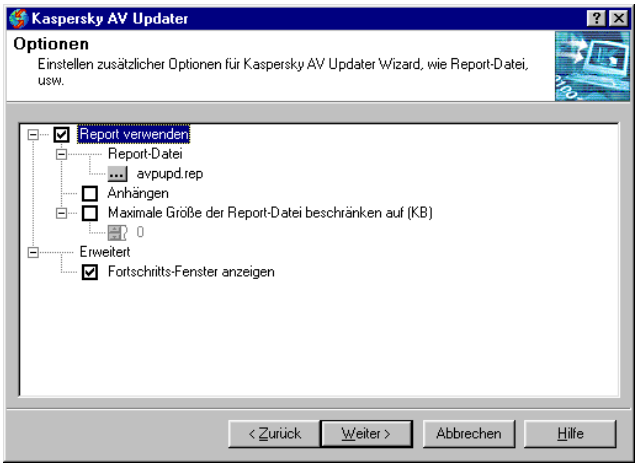


Bild 33. Fenster **Optionen**

☑ **Report verwenden** – Update-Protokoll erstellen

- **Report-Datei** – Angabe von Name und Pfad der Report-Datei
- ☑ **Anhängen** – Daten an die bestehende Report-Datei anhängen oder jedes Mal eine neue Datei erstellen
- ☑ **Maximale Größe der Report-Datei beschränken auf (KB)** – Maximale Größe der Report-Datei. Wird diese Größe erreicht, dann wird die Datei überschrieben.

Erweitert – Anpassung der Benutzeroberfläche

- ☑ **Fortschritt-Fenster anzeigen** – das Fenster Aktualisierung läuft anzeigen (siehe unten)

Klicken Sie auf Weiter, um die Aktualisierung fortzusetzen.

5.2.4. Schritt 4. Das Fenster *Aktualisierung läuft*

Das Fenster **Aktualisierung läuft** (s. Bild 34) wird nur angezeigt, wenn Sie im Fenster **Optionen** bei dem Element **Erweitert** das Kontrollkästchen **Fortschritt-Fenster anzeigen** aktiviert haben.

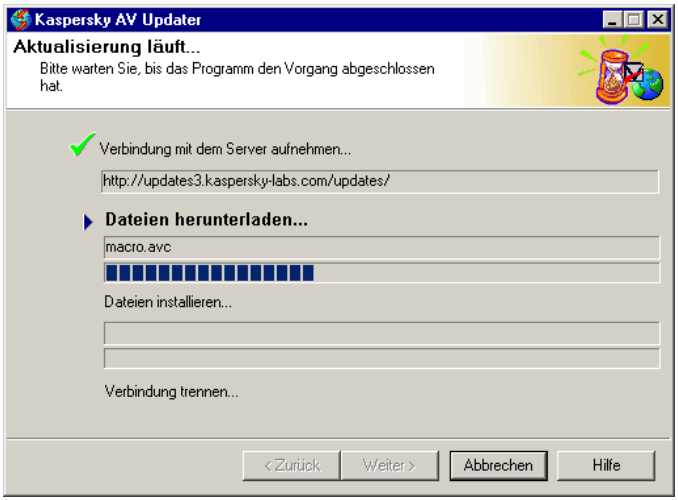


Bild 34. Fenster **Aktualisierung läuft**

Das Fenster besteht aus vier Teilen, die das jeweilige Stadium des laufenden Update-Vorgangs der Antiviren-Datenbanken anzeigen:

- ***Verbindung mit dem Server aufnehmen...*** *– Die Verbindung mit dem Server für den Datei-Download wird hergestellt.*

- ***Dateien herunterladen...*** *– Die Dateien werden vom Server auf den Computer kopiert (oben wird der Name der kopierten Datei, unten der Fortschrittsanzeige des Aktualisierungsvorgangs angezeigt).*

- ***Dateien installieren…*** *– Die Dateien werden auf dem Computer installiert (oben wird der Name der installierten Datei angezeigt, unten die Fortschrittsanzeige der Installation).*

- ***Verbindung trennen…*** *– Die Verbindung wird getrennt.*

Das Stadium des Update-Vorgangs wird durch Symbole dargestellt, die links von den oben genannten Hinweisen erscheinen (Wird kein entsprechendes Symbol angezeigt, dann hat das Update-Programm diesen Teil des Vorgangs noch nicht erreicht). Das Symbol ✓ zeigt den erfolgreichen Abschluss des betreffenden Update-Stadiums an, während ▶ anzeigt, dass der Updater diesen Vorgang im Moment ausführt.

5.2.5. Schritt 5. Das Fenster zum Abschluss des Aktualisierungsassistenten

Im letzten Fenster des Update-Assistenten **Kaspersky AV Updater Wizard beenden** (s. Bild 35) kann durch Klick auf die Schaltfläche **Report** das Update-Protokoll geöffnet werden.

Bild 35. Fenster **Aktualisierung beenden**

Klicken Sie zum Abschluss des Update-Vorgangs auf die Schaltfläche **Beenden**. Wenn Sie das Kontrollkästchen **Kaspersky Labs Webseite mit den neuesten Infos über Kaspersky AV Produkte öffnen** aktiviert haben, wird automatisch Ihr Browser mit der Internetseite von Kaspersky Labs geöffnet.

KAPITEL 6. KASPERSKY ANTI-VIRUS® CONTROL CENTRE

Das Programm Kaspersky Anti-Virus® Control Centre (Kaspersky AV Control Centre) erfüllt die Funktion einer Kontrollzentrale und dient zur Organisation der Installation und der Aktualisierung der Paketkomponenten von Kaspersky Anti-Virus® Personal. Außerdem führt es die automatische Zeitsteuerung von Tasks und eine Ergebniskontrolle der Taskausführung durch.

Die Möglichkeit, eine Übersicht der installierten Komponenten und deren Versionen zu erstellen, erleichtert die Zusammenarbeit zwischen Benutzer und Support-Service von Kaspersky Labs und gewährleistet die rechtzeitige Aktualisierung.

Mit Kaspersky AV Control Centre können Sie die Antiviren-Programme des Pakets zeitgesteuert starten. So können Sie die Produktivität steigern und gleichzeitig Ihr System nachhaltig vor Viren schützen.

Die Option für den automatisierten Start externer Programme erlaubt es, Kaspersky AV Control Centre auch als konventionellen Task-Planer einzusetzen. Meist ist der Einsatz weiterer Dienstprogramme für den automatischen Start nicht erforderlich, was zur Ersparnis von Ressourcen Ihres Computers beiträgt. Außerdem wird die exakte Synchronisation von Prozessen gewährleistet, die mit dem Antiviren-Sicherheitssystem und sonstigen Tasks verbunden sind, und Konflikte zwischen den Prozessen werden vermieden.

6.1. Start von Kaspersky AV Control Centre

Es gibt folgende Varianten für den Start von Kaspersky AV Control Centre:

Methode № 1: aus dem Windows-Hauptmenü: Klicken Sie dazu auf die Schaltfläche **Start**, zeigen Sie auf das Untermenü **Programme,** und klicken Sie in der Programmgruppe **Kaspersky Anti-Virus®** auf den Punkt **Kaspersky Anti-Virus® Control Centre**.

Methode № 2: automatischer Start nach dem Start des Betriebssystems vor dem Anmeldevorgang (Logon-Prozedur), wenn Kaspersky Anti-Virus® Control Centre installiert wurde.

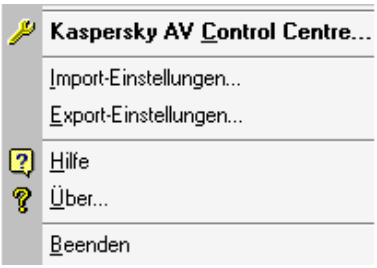


Bild 36. Menü von Kaspersky AV Control Centre in der Taskleiste

Nach dem Start von Kaspersky AV Control Centre erscheint im Infobereich der Taskleiste das Symbol . Durch Rechtsklick kann das Kontextmenü (s. Bild 36) geöffnet werden, das folgende Befehle enthält:

- ***Kaspersky AV Control Centre…*** *– Programmhauptfenster öffnen*
- ***Import-Einstellungen…*** *– Importieren von Programmeinstellungen aus einer vorher gespeicherten Datei (siehe unten).*
- ***Export-Einstellungen…*** *– Speichern der Programmeinstellungen in einer speziellen Datei mit der Erweiterung .dat. Die Einstellungen können später aus dieser Datei importiert werden (siehe oben).*
- ***Hilfe*** *– Öffnen des Hilfefensters*
- ***Über…*** *– Anzeige von Informationen über dieses Softwareprodukt, Lizenzname, Gültigkeitsdauer der Lizenz u.a. (s. Bild 37)*
- ***Beenden*** *– Beenden des Programms*

Die Befehle **Export-Einstellungen** und **Import-Einstellungen** dienen zur Übertragung von Einstellungen von Kaspersky AV Control Centre zwischen verschiedenen Rechnern, d.h. Sie können das Programm auf einem Computer konfigurieren, die vorgenommenen Einstellungen dann in einem gemeinsam genutzten Ordner auf dem Server speichern, und diese später auf einem anderen Computer laden.

Im oberen Bereich des Benutzermenüs befindet sich (oberhalb der Linie) eine Liste der Tasks, die manuell gestartet werden können. Diese Tasks können durch die entsprechenden Menüpunkte gestartet werden, ohne das Hauptfenster von Kaspersky AV Control Centre zu öffnen.

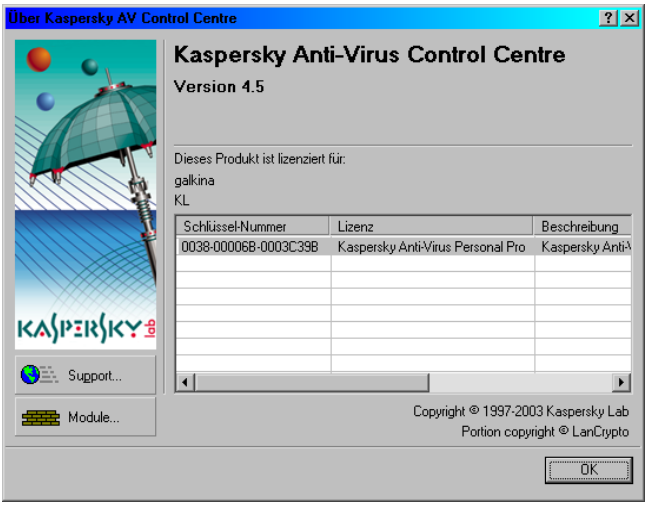


Bild 37. Fenster **Über Kaspersky Anti-Virus® Control Centre**

An dieser Stelle möchten wir auf einige funktionelle Besonderheiten des Programms hinweisen. Kaspersky AV Control Centre besteht aus zwei Teilen: dem Serviceteil, welcher bereits vor der Anmeldung als Systemdienst gestartet wird, und dem Interfaceteil, die ein grafisches Interface darstellt und der Kommunikation mit dem Benutzer dient. Wird der Interfaceteil aus dem Arbeitsspeicher entfernt, dann werden die in den Einstellungen von Kaspersky AV Control Centre festgelegten Tasks nach wie vor ausgeführt. Allerdings kann der Anwender keine weiteren Einstellungen vornehmen oder neue Tasks erstellen. Wird auch der Serviceteil aus dem Arbeitsspeicher entfernt, wird Kaspersky AV Control Centre die festgelegten Tasks nicht ausführen.

Methode № 3: aus einer Befehlszeile. Wechseln Sie dazu in den gemeinsam genutzten Ordner von Kaspersky Anti-Virus® (**KAV Shared Files**) und führen Sie die Datei *avpcc.exe* aus. Der gemeinsam genutzte Ordner kann sich unter folgendem Pfade befinden: **C:\Program Files\Common Files\KAV Shared Files**.

6.2. Benutzeroberfläche von Kaspersky AV Control Centre

Das Hauptfenster enthält vier Registerkarten: **Tasks**, **Komponenten**, **Einstellungen** und **Quarantäne** (Beschreibung siehe unten).

Zum Ausführen einer bestimmten Aktion wird das Kontextmenü oder die Symbolleiste verwendet.

Im unteren Bereich des Fensters sind die Schaltflächen **OK**, **Abbrechen**, **Übernehmen** und  angebracht. Durch Klick auf die Schaltfläche **OK** werden alle vorgenommenen Einstellungen gespeichert. Bei Klick auf **Abbrechen** werden die Änderungen verworfen. In beiden Fällen wird das Hauptfenster geschlossen. Durch Klick auf die Schaltfläche **Übernehmen** werden die Änderungen gespeichert, das Hauptfenster bleibt aber geöffnet und Sie können weitere Einstellungen vornehmen. Für aktive residente Tasks werden die vorgenommenen Einstellungen sofort in das ausführbare Modul geladen. Die Schaltfläche  dient zum Öffnen des Hilfesystems.

6.2.1. Registerkarte *Tasks*

Die Registerkarte **Tasks** (s. Bild 38) wird zur Verwaltung der Tasks verwendet. Unter *Task* wird die Ausführung eines bestimmten Programms verstanden. Dieses Programm wird zu einem bestimmten Zeitpunkt, beim Eintreten eines bestimmten Ereignisses, oder durch direkte Benutzereingabe mit vorgegebenen Parametern und Einstellungen gestartet.

Die Registerkarte besteht aus drei Bereichen:

- *Auf der linken Seite werden die Task-Liste und der Status der Tasks angezeigt.*
- *Auf der rechten Seite wird die Statistik der Programmaktionen angezeigt*[1].
- *Im unteren Bereich befindet sich eine Ereignis-Liste (Fehler, Warnungen, Hinweise).*

Betrachten wir die einzelnen Teile der Registerkarte genauer. Die Task-Liste besteht aus zwei Spalten: **Name** und **Status**. Die Spalte **Name** enthält eine Liste der Tasks, die Spalte **Status** den Ausführungsstatus des entsprechenden Tasks. Es gibt folgende Varianten für den Status:

- ***In Betrieb*** *– Der Task wird momentan ausgeführt.*

1 Statistik der Programmaktionen – eine Kurzform des Reports über die Programmaktionen.

- ***Fertig!*** *– Der Task wurde erfolgreich ausgeführt.*
- ***Erfolglos*** *– Die Ausführung des Tasks ist gescheitert.*
- ***Abgebrochen*** *– Der Task wurde vom Benutzer abgebrochen.*
- ***Pause*** *– Der Task wurde angehalten.*
- ***Start*** *– Der Task wurde gestartet.*
- ***Stopp*** *– Der Task wurde beendet.*
- ***Startfehler*** *– Fehler beim Starten des Tasks.*
- ***Erneut starten*** *– Der Task wird erneut gestartet.*

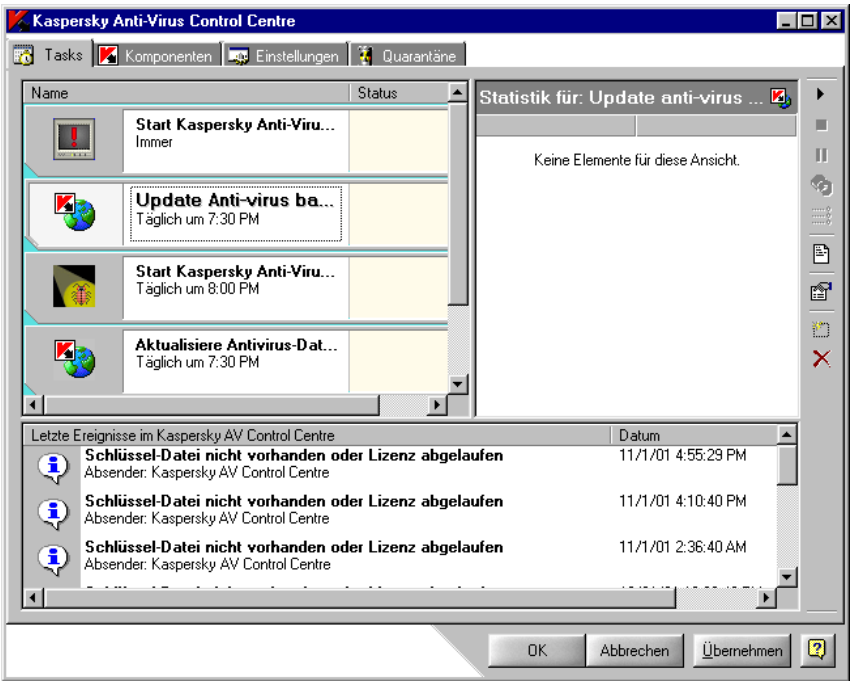


Bild 38. Registerkarte **Tasks**

Auf der rechten Seite des Fensters befindet sich die Programmstatistik. Der Inhalt der Statistik hängt von der Art des Tasks ab.

Für einen Task zum automatischen Update enthält die Statistik zum Beispiel folgende Elemente: **Datum**, **Zeit**, **Aktion**, **Ergebnis** und **Objekt**, die jeweils anzeigen, an welchem Datum und zu welcher Zeit der Task gestartet wurde, welche Aktionen ausgeführt wurden, deren Ergebnisse, und auf welche Objekte die Aktionen angewandt wurden.

Im unteren Bereich des Fensters befindet sich eine Liste der Ereignisse mit Angabe des Datums und der Zeit ihres Eintretens, sowie der betreffenden Komponente. Die Ereignisse werden von allen aktiven Komponenten des Softwarepakets an das Kaspersky AV Control Centre geschickt. In der Liste erscheinen nur kritische Ereignisse. Die Ereignisse können nach Namen oder Datum, sowie aufsteigend oder absteigend sortiert werden. Wird ein Ereignis aus der Liste gewählt, dann wird der entsprechende Task hervorgehoben.

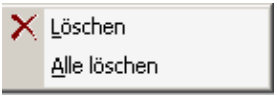


Bild 39. Kontextmenü in der Ereignisliste

Die Liste verfügt über ein Kontextmenü (s. Bild 39). Die Punkte des Kontextmenüs haben folgende Funktionen:

- ***Löschen*** *– Löscht das ausgewählte Ereignis (nach Bestätigung)*
- ***Alles löschen*** *– Löscht alle Ereignisse aus der Liste (nach Bestätigung)*

Zur Steuerung der Tasks (zum Beispiel: Erstellen, Konfiguration, Entfernen, Start und Beenden eines Tasks) werden das Kontextmenü und die Schaltflächen der Symbolleiste (s. Bild 40) verwendet.

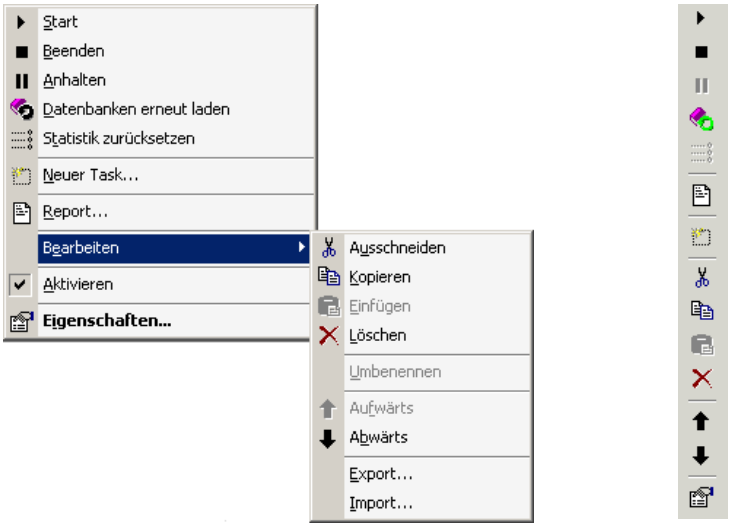


Bild 40. Kontextmenü der Task-Liste und Symbolleiste auf der Registerkarte **Tasks**

Das Kontextmenü wird durch Rechtsklick auf die linke Seite des Fensters geöffnet, d.h. dort, wo Task-Liste und Statusanzeige befinden.

- ***Start*** – *Task starten*
- ***Beenden*** – *Ausführung beenden und den Task aus dem Arbeitsspeicher entfernen.*
- ***Anhalten*** – *Ausführung des Tasks anhalten. Dabei verbleibt der Task im Arbeitsspeicher, aber die Ausführung wird angehalten.*
- ***Datenbanken erneut laden*** – *Antiviren-Datenbanken neu laden. Dieser Befehl dient nur für residente Tasks, in die neue Antiviren-Datenbanken zu laden sind, ohne den Task neu zu starten.*
- ***Statistik zurücksetzen*** – *Die Statistik über die Task-Ausführung löschen (nur für residente Tasks)*
- ***Neuer Task*** – *Neuen Task erstellen. Wenn Sie diesen Punkt wählen, wird der Task-Assistent gestartet (s. 6.3).*

- ***Report*** *– Im Fenster von Kaspersky® Report Viewer (s. Kapitel 7) den Task-Report öffnen.*

- ***Aktivieren*** *– Den Task in den Zeitplaner aufnehmen oder aus dem Zeitplaner ausschließen. Wenn Sie einen Task aus dem Zeitplaner ausschließen, wird er zwar in der Liste angezeigt, aber vom Zeitplaner nicht mehr gestartet.*

- ***Eigenschaften*** *– Einstellungen des Tasks anzeigen*

- ***Bearbeiten*** *– Task-Einstellungen anpassen. Dieses Element besteht aus einem Untermenü mit folgenden Einträgen:*

    - **Ausschneiden** – Den Task aus der Liste "ausschneiden" und in der internen Zwischenablage von Kaspersky AV Control Centre speichern. Dabei werden der Name des Tasks, die Einstellungen und der Zeitplan für seinen Start gespeichert.

    - **Kopieren** – Den Task in die interne Zwischenablage kopieren.

    - **Einfügen** – Den Task aus der internen Zwischenablage in die Task-Liste einfügen.

    - **Löschen** – Den Task aus der Liste löschen.

    - **Umbenennen** – Den Task umbenennen.

    - **Aufwärts** – Den Task in der Liste um eine Zeile nach oben verschieben.

    - **Abwärts** – Den Task in der Liste um eine Zeile nach unten verschieben.

    - **Export** – Den Task in einer Datei speichern. Wenn Sie diesen Punkt wählen, wird ein Fenster zum Speichern der Task-Einstellungen in einer Datei mit der Erweiterung .tsk geöffnet.

    - **Import** – Den Task aus einer Datei laden.

Die Befehle **Export** und **Import** dienen zum Austausch von Tasks zwischen verschiedenen Rechnern, d.h. Sie können einen Task auf einem Computer erstellen, in einem gemeinsamen Ordner auf dem Server ablegen, und ihn auf einem anderen Computer laden.

Einzelne Befehle können für bestimmte Tasktypen nicht verfügbar sein. Die Position der Tasks in der Liste bestimmt die Reihenfolge, in der sie gestartet werden. Zur Steuerung der Tasks werden außerdem die Schaltflächen in der Symbolleiste verwendet. Die Schaltflächen entsprechen folgenden Punkten des Kontextmenüs:

Schalt-fläche	Punkt im Kontextmenü
	Starten
	Abbrechen
	Anhalten
	Datenbanken erneut laden
	Statistik zurücksetzen
	Report anzeigen
	Neuer Task
	Eigenschaften
	Löschen

Wenn Sie mit dem Mauszeiger auf eine Schaltfläche zeigen, erscheint ein Infotext, der die Funktion der Schaltfläche erläutert.

Zusätzlich können die Tasks mit Hilfe folgender Funktionen kontrolliert werden:

- Buchstabentasten – *Durch Drücken einer bestimmten Buchstabentaste gelangen Sie zu den Listeneinträgen, die mit dem gewählten Buchstaben beginnen.*
- *Tasten für Schnellzugriff (Hot Keys):*

- ***<EINFÜGEN>*** *– Einen neuen Task erstellen. Wenn sie diese Taste drücken, wird das Fenster* ***Neuer Task*** *geöffnet (Details siehe Pkt. 6.3).*
- ***<ENTFERNEN>*** *– Einen Task aus der Liste entfernen (nach Bestätigung).*
- ***<LEERTASTE>*** *– Eigenschaften des ausgewählten Tasks anzeigen. Wenn Sie diese Taste drücken, wird das Fenster* ***Eigenschaften*** *geöffnet (Details s. Pkt. 6.2.1.1).*

Wenn zum Beispiel der Task **Automatisches Update** in der Liste vorhanden ist und Sie die Taste  auf der Tastatur drücken, erscheint dieser Task in der Liste und wird markiert.

6.2.1.1. Fenster *Eigenschaften*

Dieses Fenster wird durch Klick auf die Schaltfläche  oder mit dem Punkt **Eigenschaften** im Kontextmenü aufgerufen. Das Aussehen des Fensters hängt von der Art des Tasks ab, den es beschreibt.

In dieser Version des Softwareprodukts gibt es folgende Fenster:

- *Fenster der Eigenschaften für Kaspersky AV Scanner Task*
- *Fenster der Eigenschaften für Kaspersky AV Monitor Task*
- *Fenster der Eigenschaften für Kaspersky AV Updater Task*

6.2.1.1.1. Fenster der Eigenschaften für Kaspersky AV Scanner Task

Das Fenster mit Eigenschaften für die Tasks von Kaspersky AV Scanner (s. Bild 41) enthält Kategorien mit einer Liste der Einstellungen.

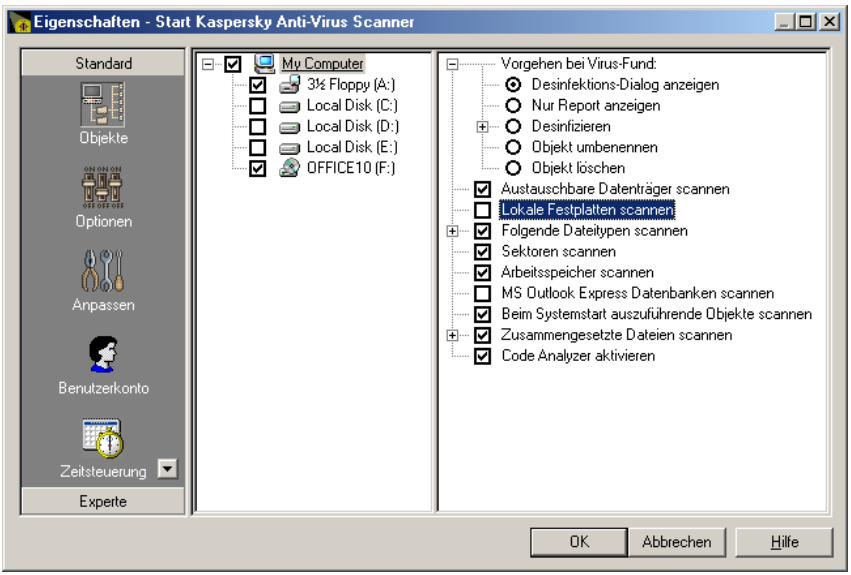


Bild 41. Fenster der Eigenschaften für Kaspersky AV Scanner Task

Das Fenster besteht aus folgenden Kategorien:

Kategorie	Beschreibung
Objekte	s. Pkt. 3.3.1
Optionen	s. Pkt. 3.3.2
Anpassen	s. Pkt. 3.3.3
Benutzerkonto	s. Pkt. 6.3.5
Zeitsteuerung	s. Pkt. 6.3.3
Alarme	s. Pkt. 6.3.4

6.2.1.1.2. Fenster der Eigenschaften für Kaspersky AV Monitor Task

Das Fenster der Eigenschaften für Kaspersky AV Monitor Task (s. Bild 42) besteht aus Kategorien, welche die Task-Einstellungen enthalten. Ein Teil der Kategorien stimmt mit den Kategorien der entsprechenden Komponente überein, andere charakterisieren lediglich Tasks von Kaspersky AV Control Centre.

Kategorie	Beschreibung
Objekte, Optionen, Anpassen	s. Pkt. 3.3.1, 3.3.2, 3.3.3.
Zeitsteuerung	s. Pkt. 6.3.2.
Alarme	s. Pkt. 6.3.4.

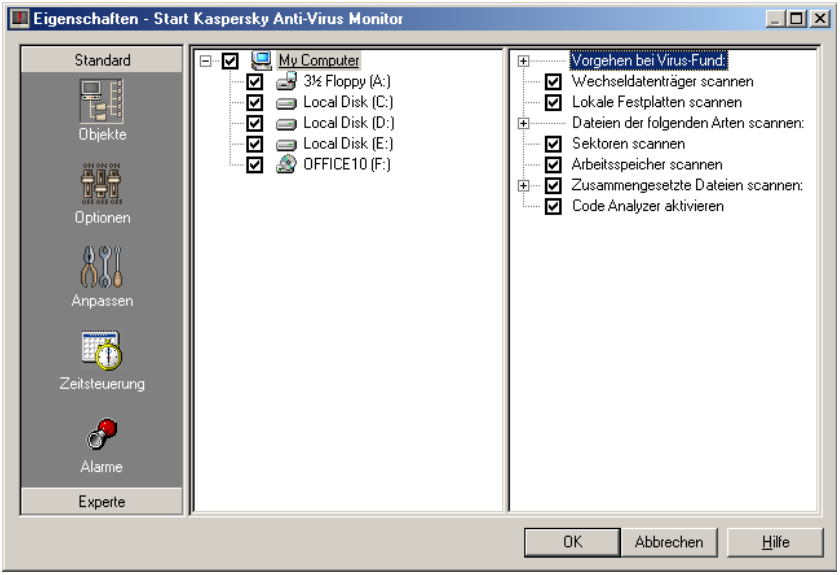


Bild 42. Fenster der Eigenschaften für Kaspersky AV Monitor Task

6.2.1.1.3. Fenster der Eigenschaften für Kaspersky AV Updater Task

Das Fenster der Eigenschaften für Kaspersky AV Updater Task besteht aus einer Reihe von Registerkarten mit Einstellungen (s. Bild 43).

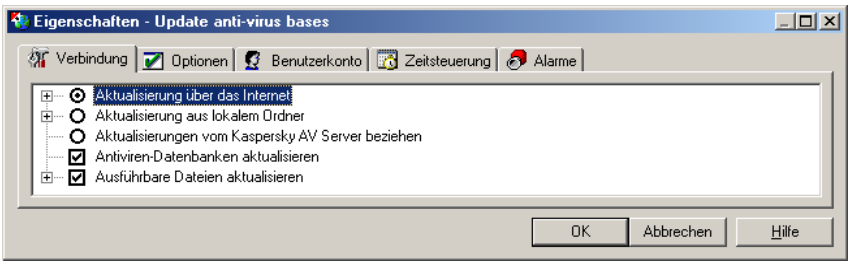


Bild 43. Fenster der Eigenschaften für Kaspersky AV Updater Task

Registerkarte	Beschreibung
Verbindung	s. Pkt. 5.2.2
Optionen	s. Pkt. 5.2.3
Benutzerkonto	s. Pkt. 6.3.5
Zeitsteuerung	s. Pkt. 6.3.3
Alarme	s. Pkt. 6.3.4

Die Registerkarte **Verbindung** im Fenster Eigenschaften enthält die zusätzliche Option **Aktualisierung von Kaspersky AV Server beziehen**. Diese Option erlaubt die Aktualisierung der Antiviren-Datenbanken und ausführbaren Module in einen Ordner auf dem Kaspersky AV Server.

6.2.2. Registerkarte *Komponenten*

Auf der Registerkarte **Komponenten** (s. Bild 44) befindet sich die Liste der Komponenten[2] des Pakets Kaspersky Anti-Virus®. Auf der rechten Seite der Registerkarte befindet sich die Symbolleiste. Durch Rechtsklick kann das Kontextmenü geöffnet werden (s. Bild 45).

Die Schaltflächen der Symbolleiste entsprechen den Befehlen im Kontextmenü (siehe unten).

2 Eine Komponente ist ein Programm, ein Dienstprogramm, eine Bibliothek oder eine Datenbank aus dem Paket Kaspersky Anti-Virus, das jeweils für ein genau abgegrenztes Aufgabengebiet zuständig ist.

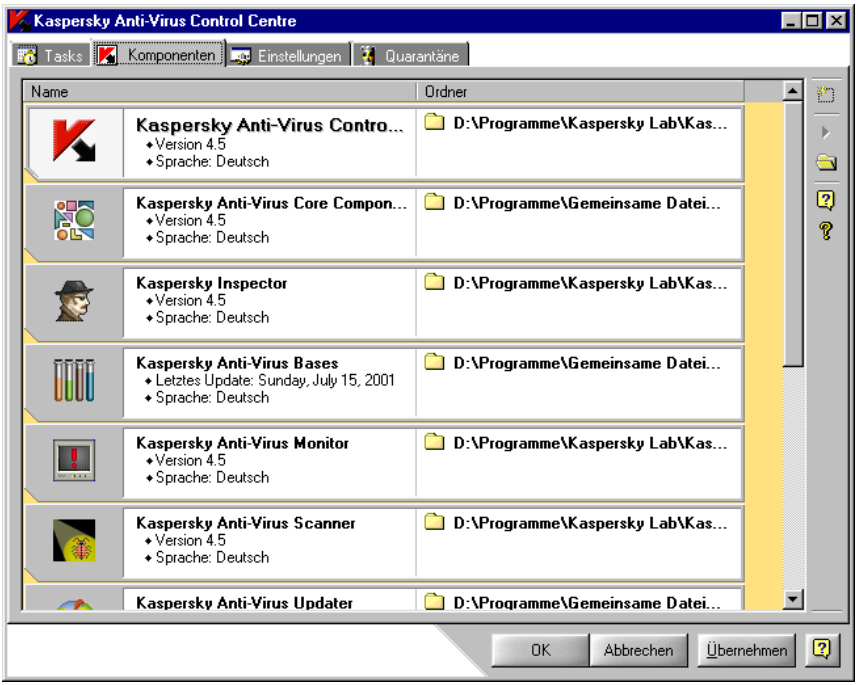


Bild 44. Registerkarte **Komponenten**

Schalt-fläche	Befehl im Kontextmenü	Beschreibung
	**Neuer Task...**	Erstellt basierend auf der gewählten Komponente einen neuen Task. Durch Klick auf diese Schaltfläche oder Auswahl des Menüpunkts wird das Fenster **Neuer Task** geöffnet (Details s. Pkt. 6.3).
	**Ausführen…**	Startet die Task-Ausführung.
	**Komponenten -Ordner öffnen**	Öffnet den Komponentenordner in einem MS Windows Standardfenster.
	**Komponenten -Hilfe**	Startet das Hilfesystem für die gewählte Komponente.

Schalt-fläche	Befehl im Kontextmenü	Beschreibung
	Über...	Anzeige von Informationen über Produktversion, letztes Update der Antiviren-Datenbanken und anderes. Wenn sie auf diese Schaltfläche klicken oder den Menüpunkt wählen, wird das Fenster **Über das Programm** geöffnet.

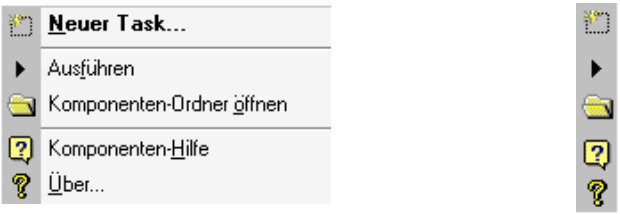


Bild 45. Kontextmenü und Symbolleiste auf der Registerkarte **Komponenten**

6.2.3. Registerkarte *Einstellungen*

Die Registerkarte **Einstellungen** (s. Bild 46) dient zur Auswahl der Einstellungen von Kaspersky AV Control Centre. Die Einstellungen sind in vier Kategorien unterteilt. Jede Kategorie fasst die Einstellungen für eine genau abgegrenzte Art von Funktionen zusammen.

Die Liste der Einstellungskategorien befindet sich auf der linken Seite des Fensters. Durch die Auswahl einer bestimmten Kategorie, wird rechts der entsprechende Konfigurationsbaum angezeigt (zur Funktionsweise des Konfigurationsbaums s. Kapitel 8).

Ist die Fenstergröße nicht für die Anzeige aller Kategorien ausreichend, dann erscheinen die Schaltflächen ▲ und ▼, die zum Umblättern der Liste dienen.

Kategorie	Funktion
 Sicherheit	Diese Kategorie enthält Einstellungen für die Systemsicherheit und die Zugriffskontrolle auf Einstellungen und Komponenten von Kaspersky AV Control Centre.
 Alarme	Diese Kategorie enthält Einstellungen für die Bearbeitung von Hinweisen auf kritische Ereignisse bei Ausführung der Tasks von Kaspersky AV Control Centre.
 Quarantäne	Diese Kategorie enthält Einstellungen für den Quarantäne-Ordner, der auf dem Computer oder auf einem Server angelegt wird (nur für Arbeit mit Kaspersky® Administration Kit). Details über Quarantäne siehe unten.
 Anpassen	Diese Kategorie enthält Einstellungen für die Benutzeroberfläche von Kaspersky AV Control Centre.

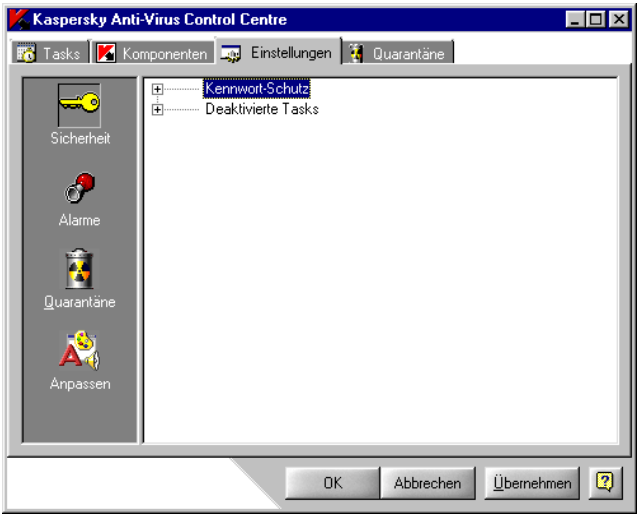


Bild 46. Registerkarte **Einstellungen**

6.2.3.1. Kategorie *Sicherheit*

Bild 47. Registerkarte **Einstellungen**. Kategorie **Sicherheit**

Diese Kategorie (s. Bild 47) enthält Einstellungen für die Funktionen der Systemsicherheit. Hier werden Kennwörter und Zugriffsrechte für bestimmte Task-Arten festgelegt.

Kaspersky AV Control Centre erlaubt den Kennwort-Schutz für bestimmte ausführbare Aktionen. Dadurch kann der Zugriff auf die Ausführung bestimmter Befehle beschränkt werden.

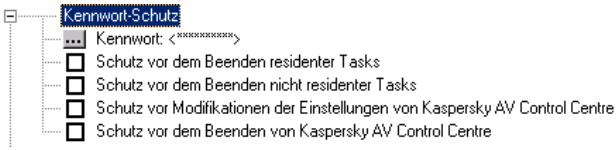


Bild 48. Abschnitt **Kennwortschutz**

Diese Funktionen werden, wie oben erwähnt, im Abschnitt **Kennwortschutz** festgelegt (siehe Bild 48):

Dieser Abschnitt enthält folgende Parameter:

Kennwort – Festlegen des Kennworts zur Verwaltung von **Kaspersky Anti-Virus®** mit Hilfe von Kaspersky Anti-Virus® Control Centre, sowie zur Beschränkung des Zugriffs auf bestimmte Programmfunktionen (eine Liste der Funktionen befindet sich im unteren Bereich des Konfigurationsbaums).

Durch Klick auf die Schaltfläche erscheint das Fenster **Kennwort ändern**.

Dieses Dialogfenster (s. Bild 49) dient zur Angabe und Änderung des Kennworts. Geben Sie in das Feld **Neues Kennwort** Ihr Kennwort ein und wiederholen Sie die Eingabe im Feld **Kennwort wiederholen**.

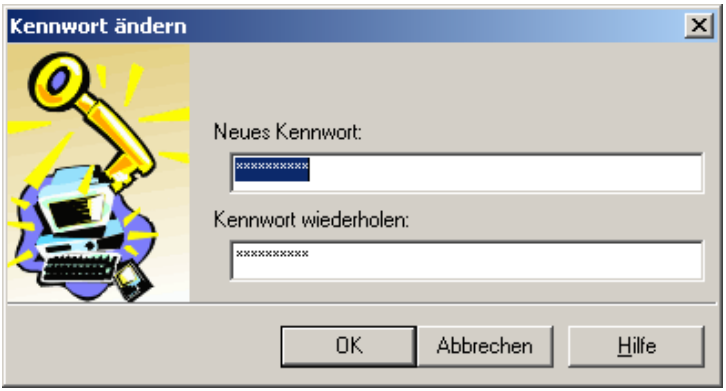
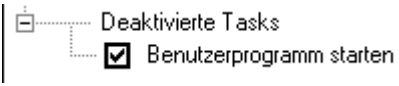


Bild 49. Dialogfenster **Kennwort ändern**

- **Schutz vor dem Beenden residenter Tasks** – Zum Abbrechen eines residenten Tasks ist die Kennworteingabe erforderlich. Wenn beispielsweise auf Ihrem Rechner der Anti-Virus Monitor läuft und diese Option aktiviert wurde, muss das Kennwort eingegeben werden, um die Arbeit des Monitors abzubrechen.
- **Schutz vor dem Beenden nicht residenter Tasks** – Zum Abbrechen eines nicht residenten Tasks ist die Kennworteingabe erforderlich. Wurde diese Option aktiviert, dann ist zum Abbrechen nicht residenter Tasks (z.B. Start von Kaspersky AV Scanner oder Kaspersky AV Updater) die Eingabe des Kennworts erforderlich.
- **Schutz vor Modifikationen der Einstellungen von Kaspersky AV Control Centre** – Kennwortschutz für das Öffnen und für Einstellungsänderungen von Kaspersky AV Control Centre.
- **Schutz vor dem Beenden von Kaspersky AV Control Centre** – Kennwortschutz für das Entfernen von Kaspersky AV Control Centre aus dem Arbeitsspeicher.

Vergessen Sie bei der Auswahl der zu schützenden Aktionen nicht, das Kennwort in das Feld **Kennwort** einzugeben!

Ferner können Sie auf dieser Registerkarte die Ausführung bestimmter Tasks verbieten, die bei Remote-Administration im Falle eines unerlaubten Zugriffs (Systemeinbruch) eine Gefahr darstellen könnten.



Diese Option wird im Abschnitt **Deaktivierte Tasks** (s. Bild 50) festgelegt.

Bild 50. Element **Deaktivierte Tasks**

In der aktuellen Version des Programms existiert nur ein solcher Tasktyp:

- **Benutzerprogramm starten** – Ist diese Option aktiviert, können Benutzeranwendungen nicht als Tasks von Kaspersky AV Control Centre gestartet werden.

6.2.3.2. Kategorie *Alarme*

Die Kategorie **Alarme** (s. Bild 51) dient den Einstellungen für die Bearbeitung von Warnungen, die von Tasks erzeugt werden.

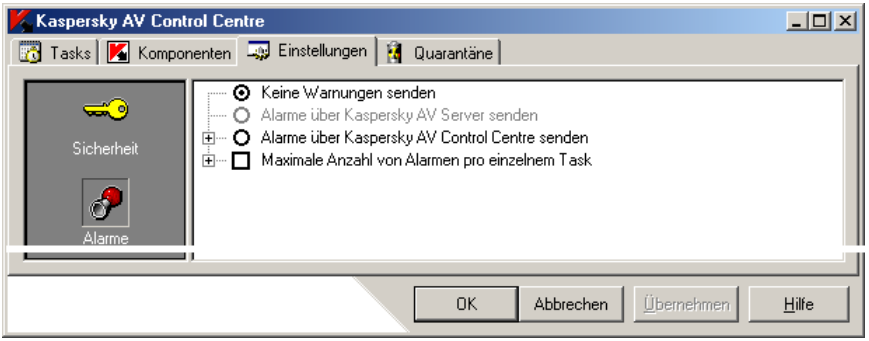


Bild 51. Registerkarte **Einstellungen**. Kategorie **Alarme**

Für die Alarme stehen folgende Varianten zu Auswahl:

- **Keine Warnungen senden** – Das Senden von Meldungen verbieten.
- **Alarme über Kaspersky AV Server senden** – Warnungen über Kaspersky AV Server senden. – Kaspersky AV Server ist die Server-Komponente des Systems zur Remote-Administration des Pakets Kaspersky Anti-Virus®.
- **Alarme über Kaspersky AV Control Centre senden** – Warnmeldungen mit Hilfe von Kaspersky AV Control Centre senden.

Zur Beschränkung der Meldungen eines Tasks kann die Option ☑ **Maximale Anzahl von Alarmen pro einzelnem Task** aktiviert und der gewünschte Wert festgelegt werden.

So ist beispielsweise auf Bild 52 eine Situation dargestellt, in der die maximale Anzahl von Warnmeldungen von einem Task auf 10 beschränkt ist. Dies bedeutet, dass beim Empfang der elften Meldung von einem bestimmten Task an Kaspersky AV Control Centre die Liste der eingegangenen Warnmeldungen automatisch gelöscht wird.

Wurde die Option **Alarme über Kaspersky AV Control Centre senden** aktiviert, dann ist die Anpassung von Einstellungen für das Senden von Meldungen erforderlich. Um das Senden von Meldungen per E-Mail zu aktivieren, wird das Kontrollkästchen **E-Mail-Nachrichten senden** aktiviert. Nehmen Sie dann folgende Einstellungen vor:

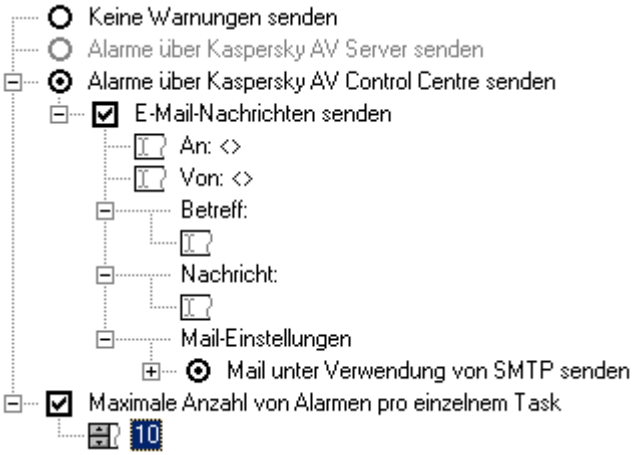


Bild 52. Option zum Senden von Meldungen mit Hilfe von Kaspersky AV Control Centre

An: Tragen Sie hier die E-Mail-Adresse des Empfängers ein.

Von: Tragen Sie hier den Namen oder die Adresse ein, die in der Zeile **Von** der E-Mail-Nachricht erscheinen soll. Hier kann eine beliebige Zeichenkette stehen. Diese Einstellung wird bei der Arbeit mit bestimmten SMTP-Servern benötigt und dient zur Benutzerauthentifizierung.

Betreff: Betreff der E-Mail-Nachricht.

Nachricht: Der Text, den die E-Mail enthalten soll.

Mail-Einstellungen In diesem Abschnitt sind Einstellungen für das E-Mail-System vorzunehmen, welche die Art des Sendens von Alarmen betreffen. Es gibt zwei Methoden zum Senden:

- *unter Verwendung von MAPI*
- *unter Verwendung von SMTP*

Nähere Informationen über SMTP und MAPI erhalten Sie von Ihrem Netzwerkadministrator.

6.2.3.2.1. Einstellungen für das Senden von Alarmen mit SMTP

Um Alarme unter Verwendung von SMTP zu senden, wählen sie die Option **Mail unter Verwendung von SMTP senden** (s. Bild 53) und tragen die folgenden Angaben ein:

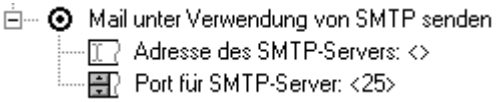


Bild 53. SMTP-Einstellungen

Adresse des SMTP-Servers Enthält die Adresse des SMTP–Servers, die in Dezimalform (z.B. 125.5.29.1), als vollständige Domäne (z.B. test.mail.ru) oder in Kurzform (z.B. test) angegeben werden kann.

Port für SMTP-Server Gibt den Port des SMTP-Servers an. Der voreingestellte Wert ist **25**.

Wir wollen an einem Beispiel verdeutlichen, wie die Einstellungen der Registerkarte **Alarme** verwendet werden. Im Beispiel sollen unter Verwendung eines E-Mail-Gateways SMS-Nachrichten über kritische Netzwerk-Ereignisse an das Mobiltelefon des Systemadministrators geschickt werden.

Eingabedaten:

- *Handynummer des Administrators – **1234567** (direkte Rufnummer)*
- *Netzbetreiber – z.B. Beeline GSM (d.h. die Netzvorwahl der direkten Rufnummer – **7 901**)*
- *Adresse des SMTP-Servers – **mysmtp.home.ru***
- *Port des SMTP-Servers – **25***

Dabei ist es notwendig, dass

- *die Nachricht unter dem Namen von Control Centre gesendet wurde.*
- *die Nachricht die Überschrift* Alarm *besaß.*
- *die Nachricht folgenden Text enthielt: Warnung! Kritisches Ereignis eingetreten!*

Nehmen Sie folgende Einstellungen vor (siehe Bild 54).

Bild 54. Einstellungen für das Senden von SMS über kritische Ereignisse

Die Adresse des E-Mail-Gateways sowie die Netzvorwahl des Mobilnetzbetreibers können je nach Standort variieren.

6.2.3.2.2. Einstellungen für das Senden von Alarmen mit MAPI

Wenn Ihr Computer mit dem Betriebssystem Windows 95 OSR2/98 arbeitet, können Sie mit Kaspersky AV Control Centre das Senden von Nachrichten mittels MAPI festlegen.

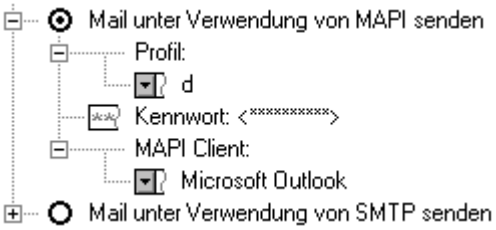


Bild 55. MAPI-Einstellungen

Zur Anpassung der MAPI-Einstellungen wählen Sie die Option **Mail unter Verwendung von MAPI senden** (s. Bild 55) nehmen folgende Einstellungen vor:

Profil — Name des Profils (Konfigurationsdatei) des MAPI-Clients

Kennwort — Kennwort für den Zugriff auf das Profil

MAPI Client — Name des MAPI-Clients, der verwendet wird, um Warnmeldungen zu senden.

Einige MAPI-Clients benutzen keine Profile. Lassen Sie in diesem Fall die Zeilen **Konfiguration** und **Kennwort** leer.

6.2.3.3. Kategorie *Anpassen*

Bild 56. Registerkarte **Einstellungen**. Kategorie **Anpassen**

Die Kategorie **Anpassen** (siehe Bild 56) enthält Einstellungen für die Programmoberfläche. In dieser Kategorie können Sie akustische Signale, die bei bestimmten Aktionen abgespielt werden, und die Farbeinstellungen des Programms festlegen.

Die Kategorie **Anpassen** besteht aus zwei Abschnitten: **Bei Ereignis Sound spielen** und **Darstellung**:

- **Bei Ereignis Sound spielen** – Einstellungen für die akustischen Signale, die nach der Ausführung (oder nach dem Beenden der Ausführung) bestimmter Operationen abgespielt werden (Details s. Pkt. 6.2.3.3.1).

- **Darstellung** – Einstellungen für die farbliche Gestaltung der Programmoberfläche (Details s. Pkt. 6.2.3.3.2).

6.2.3.3.1. Sound-Einstellungen

Kaspersky AV Control Centre erlaubt die Zuordnung von akustischen Signalen zu bestimmten Ereignissen. Dies verleiht ihrem Programm zusätzliche Servicefunktionen.

Die Sound-Einstellungen werden im Abschnitt **Bei Ereignis Sound spielen** vorgenommen (s. Bild 57).

Bild 57. Sound-Einstellungen

Um einen Sound zu aktivieren, wird dessen Kontrollkästchen aktiviert. Dann wird durch Klick auf die Schaltfläche ... das Fenster zur Auswahl der Audio-Datei geöffnet. Diese Datei sollte im Format WAV vorliegen. Die einzelnen Soundeffekte haben folgende Funktionen:

- **Task starten** – Sound sofort nach dem Start des Tasks abspielen (unabhängig von der Art des Tasks).

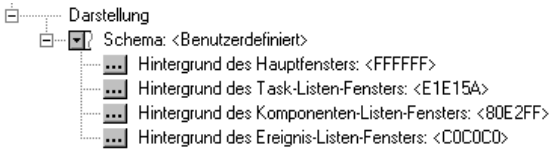
- **Task erfolgreich beendet** – Diesen Sound nach erfolgreichem Abschluss des Tasks abspielen, d.h. falls der Task nicht vom Benutzer abgebrochen und nicht mit einem Fehler beendet wurde.

- **Task vom Benutzer abgebrochen** – Diesen Sound abspielen, wenn der Task vom Benutzer abgebrochen wurde.

- **Task fehlgeschlagen** – Sound wird abgespielt bei unvorhergesehenem Task-Abbruch.

6.2.3.3.2. Farbeinstellungen

Mithilfe von Kaspersky AV Control Centre können Sie die farbliche Gestaltung der Benutzeroberfläche ändern.



Die Farbeinstellung der Oberflächenelemente werden, wie oben erwähnt, im Abschnitt **Darstellung** geändert (s. Bild 58).

Bild 58. Darstellung

Um dem Benutzer die Farbeinstellungen zu erleichtern, bietet das Programm eine Auswahl an standardmäßigen Farbschemata. Zur Auswahl eines Farbschemas dient das **Schema <...>**. Jedes Schema verfügt über folgende Einstellungen:

- **Hintergrund des Hauptfensters** – Hintergrundfarbe des Hauptfensters der Anwendung
- **Hintergrund des Task-Listen-Fensters** – Hintergrundfarbe der Task-Liste auf der Registerkarte **Tasks**
- **Hintergrund des Komponenten-Listen-Fensters** – Die Hintergrundfarbe der Komponenten-Liste auf der Registerkarte **Komponenten**
- **Hintergrund des Ereignis-Listen-Fensters** – Die Hintergrundfarbe des Ereignis-Fensters auf der Registerkarte **Tasks**

Auf den folgenden Abbildungen (s. Bild 59) ist das Farbschema **Lila** dargestellt. Zusätzlich werden die Parameter des Farbschemas angegeben.

Bild 59. Einstellungen für farbliche Darstellung

6.2.3.4. Kategorie *Quarantäne*

Die Kategorie **Quarantäne** enthält Einstellungen für den Quarantäne-Ordner – einer speziellen Ablage, in der Kaspersky Anti-Virus® Scanner und Kaspersky Anti-Virus® Monitor infizierte und verdächtige Dateien speichern (s. Bild 60).

Damit Kaspersky Anti-Virus® Scanner und Kaspersky Anti-Virus® Monitor Dateien in diesem Ordner speichern, muss in der Kategorie **Optionen** für diese Komponenten das Kontrollkästchen **Quarantäne aktivieren** aktiviert werden. In diesem Modus werden infizierte Dateien in den Quarantäne-Ordner kopiert, ohne aus ihrem ursprünglichen Ordner gelöscht zu werden. Das Programm wird infizierte Dateien nur dann löschen, wenn in den Einstellungen von Kaspersky Anti-Virus® Scanner und Kaspersky Anti-Virus® Monitor zur Behandlung von infizierten Dateien die Option **Löschen** gewählt wurde.

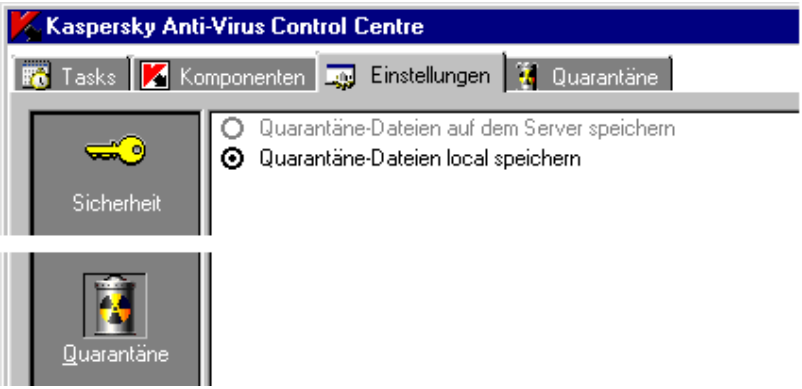


Bild 60. Kategorie **Quarantäne**

Die in Quarantäne abgelegten Dateien werden in verschlüsselter Form gespeichert, wodurch:

- *das Risiko einer Infektion ausgeschlossen wird (der ausführbare Code kann in verschlüsselter Form nicht gestartet werden).*

- *die Antiviren-Programme effektiver arbeiten (Dateien im Quarantäne-Format werden nicht als infiziert definiert).*

Die im Quarantäne-Ordner abgelegten Dateien können später zusätzlich untersucht und dann entweder in ihrer ursprünglichen Form wiederhergestellt oder gelöscht werden.

Um Dateien in den Quarantäne-Ordner zu verschieben, der sich auf Ihrem Computer befindet (*lokale* Quarantäne), wählen Sie die Variante **Quarantäne-Dateien lokal speichern**. Die Arbeit mit unter lokaler Quarantäne stehenden Dateien wird im folgenden Abschnitt ausführlich beschrieben.

6.2.4. Registerkarte *Quarantäne*

Auf der Registerkarte **Quarantäne** (s. Bild 61) wird der Inhalt des lokalen Quarantäne-Ordners angezeigt (zu lokaler Quarantäne s. oben Pkt. 6.2.3.4).

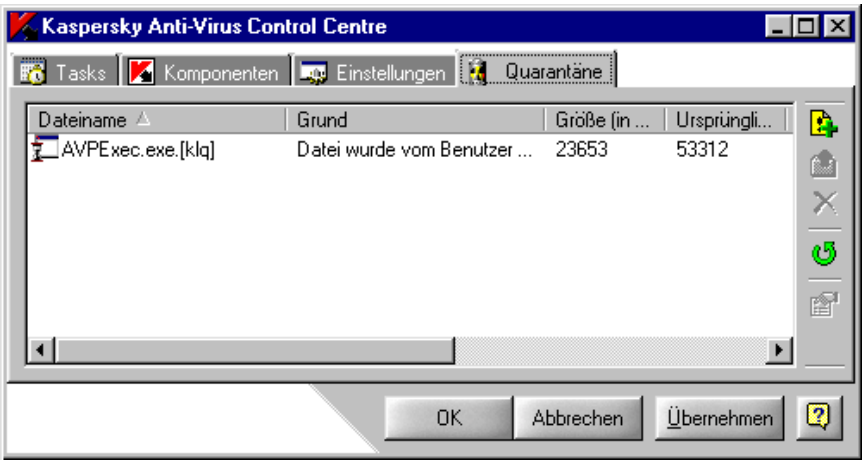


Bild 61. Registerkarte **Quarantäne**

Auf dieser Registerkarte können Sie die Darstellungsart der Dateien ändern sowie verschiedene Aktionen mit den Dateien vornehmen. Dazu dient das Kontextmenü der Registerkarte (s. Bild 62).

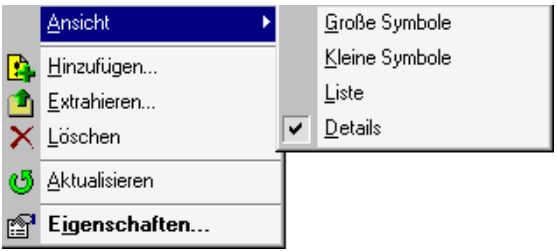


Bild 62. Kontextmenü der Registerkarte **Quarantäne**

Alle Menüpunkte außer **Ansicht** besitzen entsprechende Schaltflächen auf Symbolleiste am rechten Rand der Registerkarte.

Mit Hilfe der Befehle des Untermenüs **Ansicht** können Sie die Symbole und die Darstellung der Liste (Tabelle oder nur Dateinamen) anpassen.

Um die Eigenschaften einer Datei zu überprüfen,

1. Markieren Sie den Dateinamen, und klicken Sie auf die Schaltfläche oder wählen Sie im Kontextmenü den Punkt **Eigenschaften**.

2. Ein Fenster mit Informationen über die Datei wird geöffnet (der Umfang der Informationen entspricht dem in der Tabelle dargestellten. Allerdings sind die Informationen übersichtlicher angeordnet, s. Bild 63)

Bild 63. Informationen über eine Quarantänedatei

Um die Dateiliste des Quarantäne-Ordners zu aktualisieren, wählen Sie im Kontextmenü den Punkt **Aktualisieren** oder klicken Sie auf die Schaltfläche .

Um eine bestimmte Datei aus dem Quarantäne-Ordner zu wiederherzustellen,

1. Wählen Sie den Dateinamen, und klicken Sie auf der rechten Seite des Dialogfensters die auf Schaltfläche oder wählen Sie den Punkt **Extrahieren** im Kontextmenü des Listenelements.

2. Wählen Sie im folgenden Fenster des Assistenten einen Zielordner, in den die entnommene Datei verschoben werden soll (s. Bild 64). Klicken Sie dazu auf die Schaltfläche .

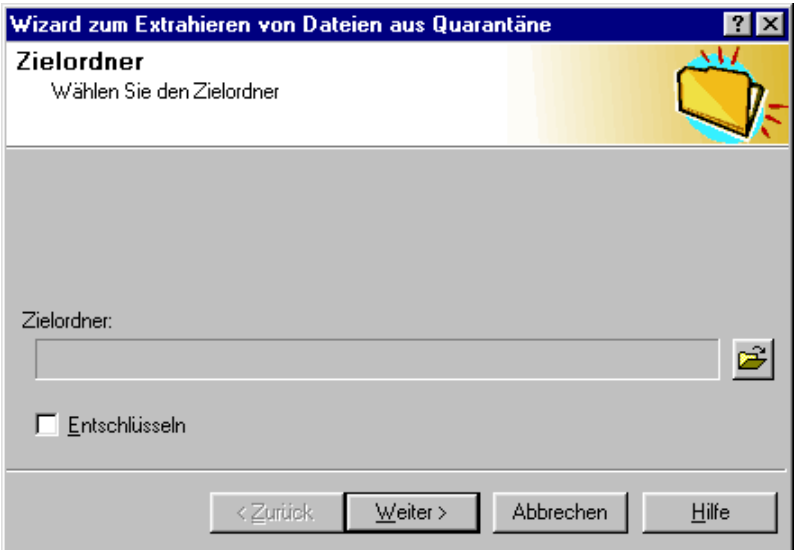


Bild 64. Assistent zur Entnahme von Dateien aus Quarantäne

3. Aktivieren Sie das Kontrollkästchen **Entschlüsseln**.

4. Klicken Sie auf **Weiter >**.

5. Ein Fenster, das über den Fortschritt der Operation informiert, wird geöffnet. Nach Abschluss der Operation klicken Sie auf **Fertig**.

Um eine Datei aus dem Quarantäne-Ordner zu löschen,

1. Markieren Sie den Dateinamen, und klicken Sie die auf Schaltfläche  oder wählen Sie im Kontextmenü der entsprechenden Datei den Punkt **Löschen**.

2. Ein Fenster zur Bestätigung des Löschvorgangs wird geöffnet. Klicken Sie auf **Ja**.

Die Datei wird dabei nur aus dem Quarantäne-Ordner entfernt und nicht aus ihrem ursprünglichen Ordner. Die infizierte Datei wird nur dann endgültig gelöscht, wenn Sie als Aktion für infizierte Dateien die Option **Löschen** aktiviert haben.

Um eine Datei manuell unter Quarantäne zu stellen:

1. Wählen Sie im Kontextmenü den Punkt **Hinzufügen** oder klicken Sie auf die Schaltfläche  . Das Fenster des Assistenten zum Verschieben einer Datei nach Quarantäne wird geöffnet (s. Bild 65).

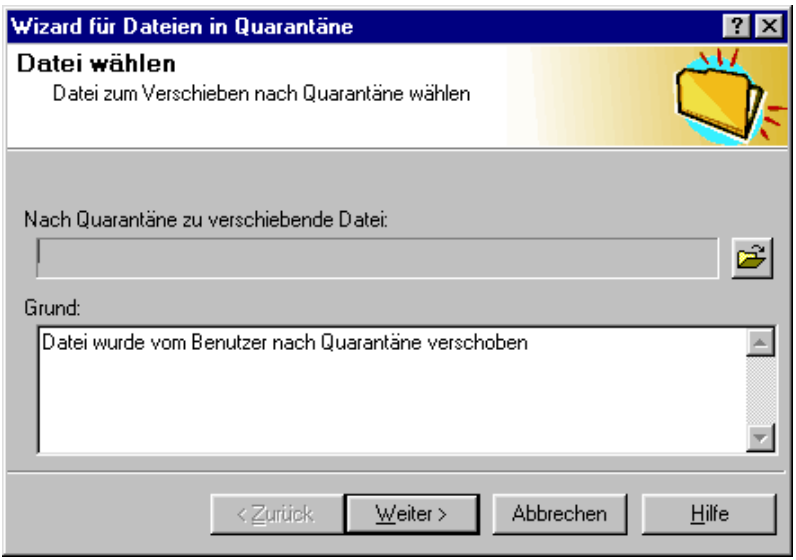


Bild 65. Assistent zum Verschieben einer Datei nach Quarantäne

2. Klicken Sie auf die Schaltfläche  und wählen Sie im folgenden Windows-Standarddialog den Dateinamen.

3. Ändern Sie bei Bedarf im Feld **Grund** den Text, der die Ursache angibt, aus welchem die Datei unter Quarantäne gestellt wurde, und klicken Sie auf **Weiter**.

4. Ein Fenster, das über den Fortschritt der Operation informiert, wird geöffnet. Nach Abschluss der Operation klicken Sie auf **Fertig**.

6.3. Assistent zum Erstellen eines neuen Tasks

Die zeitgesteuerte Ausführung einer bestimmten Anwendung mit einer vorgegebenen Liste von Parametern und Einstellungen kann als ein gesonderter Task des Zeitplaners festgelegt werden.

Der Assistent für neue Tasks wird gestartet, wenn Sie im Kontextmenü den Punkt **Neuer Task** auswählen oder in der Symbolleiste der Registerkarten **Tasks** oder **Komponenten** auf die Schaltfläche  klicken.

Das Erstellen eines neuen Tasks in Kaspersky AV Control Centre funktioniert wie ein Windows-Assistent (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). In jedem Fenster sind bestimmte Aktionen erforderlich.

Um von einem Fenster des Assistenten zum anderen zu wechseln, klicken Sie auf die Schaltflächen **Weiter** (einen Schritt vorwärts) oder **Zurück** (einen Schritt rückwärts). Das Erstellen eines Tasks wird abgeschlossen durch Klick auf **Fertig stellen**. Um das Erstellen eines Tasks abzubrechen, klicken Sie auf **Abbrechen**. Um zu dem jeweiligen Schritt Hilfe zu erhalten, klicken Sie auf **Hilfe**.

6.3.1. Fenster *Task*

In Abhängigkeit der zu lösenden Aufgaben, der zu startenden Programme und der Besonderheiten ihrer Einstellungen können Tasks in zwei Gruppen eingeteilt werden:

- *Tasks, die bei ihrer Ausführung den Start von Anwendungen aus dem Paket Kaspersky Anti-Virus® vorsehen.*

- *andere Tasks.*

Das Fenster **Task** dient der Angabe von Taskname und Tasktyp (siehe Bild 66).

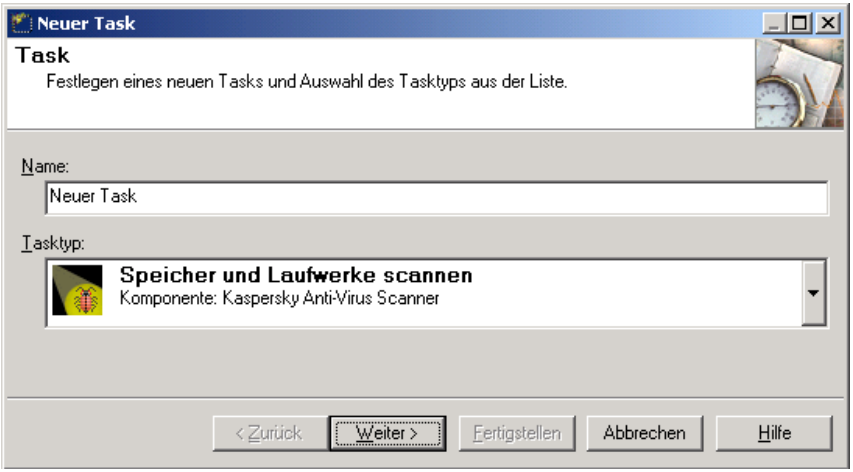


Bild 66. Fenster **Task**

Es gibt zum Beispiel folgende Tasktypen:

- ***Speicher und Laufwerke scannen*** *– Start von Kaspersky AV Scanner mit der Möglichkeit individueller Scan-Einstellungen für jeden Task. Die Tasks können automatisch nach Zeitplan, bei Eintreten eines bestimmten Ereignisses oder durch direkte Benutzereingabe gestartet werden.*

- ***Echtzeit-Scannen*** *– Starten von Kaspersky Anti-Virus® Monitor und/oder vorübergehende Änderung der Monitor-Einstellungen, ohne den Computer neu zu starten. Die Gültigkeitsdauer bestimmter Einstellungen kann genau nach Zeitplan festgelegt, vom Eintreten bestimmter Ereignisse im System abhängig gemacht oder vom Benutzer beim Wechsel zu einer anderen Aktivität festgelegt werden (zum Beispiel während der Installation neuer Software, beim Kopieren externer Programme und Dokumente, bei E-Mail-Empfang usw.).*

- ***Update der Antiviren-Datenbanken*** *– Automatisiertes Update der Datenbank mit den neuen Virus-Definitionen. Das Update kann über das*

Internet oder über ein lokales Netzwerk erfolgen. Letzteres verringert die Verbindungskosten, erhöht die Geschwindigkeit des Updateprozesses und vereinfacht die Administration des Pakets.

- ***Benutzerprogramm starten*** *– Dazu zählen beliebige Programme, die von Kaspersky AV Control Centre aus gestartet werden können.*

- ***Neue Programme installieren*** *– Starten des Assistenten zur Installation von Windows-Anwendungen.*

6.3.2. Fenster *Zeitsteuerung* für Kaspersky AV Monitor Task

Bild 67. Fenster **Zeitsteuerung** für Kaspersky Anti-Virus® Monitor Task

Beim Erstellen eines Tasks für Kaspersky AV Monitor ist im Fenster **Zeitsteuerung** (s. Bild 67) die Angabe der Start- und Stoppintervalle erforderlich. Um den Task beim Start von Kaspersky AV Control Centre auszuführen, wählen Sie **Immer**. Um den Task zeitgesteuert zu starten und zu stoppen, wählen Sie **Intervall** und stellen Sie die Zeitpunkte für Start und Stopp ein. Um einzustellen, wann die Anwendung gestartet werden soll, klicken Sie auf die Schaltfläche **Start**. Ein Fenster wird geöffnet, das dem Fenster **Zeitsteuerung** für Kaspersky AV Scanner Task gleicht (Beschreibung dieses Fensters s. unten).

Nach Klick auf die Schaltfläche **Stopp** können die Einstellungen für das Beenden der Taskausführung eingestellt werden.

6.3.3. Fenster *Zeitsteuerung* für Kaspersky AV Scanner und Kaspersky AV Updater Tasks

Beim Erstellen eines Tasks für Kaspersky AV Scanner sind im Fenster **Zeitsteuerung** Bedingungen und Frequenz des Starts festzulegen (s. Bild 68).

Für den Start bestehen folgende Möglichkeiten:

- **Nach Ereignis** – Task wird gestartet, wenn ein bestimmtes Ereignis eintritt oder auf Grund einer Benutzereingabe (s. Pkt. 6.3.3.1)
- **Nach Bedingung** – Task wird gestartet, wenn die angegebene Bedingung beim Beenden eines bestimmten Tasktyps erfüllt wird (s. Pkt. 6.3.3.2)
- **Stündlich** – Task wird zum gewählten Zeitpunkt in stündlichem Abstand gestartet (s. Pkt. 6.3.3.3)
- **Täglich** – Task wird jeden Tag zum gewählten Zeitpunkt gestartet (s. Pkt. 6.3.3.4)
- **Wöchentlich** – Task wird jede Woche zum gewählten Zeitpunkt gestartet (s. Pkt. 6.3.3.5)
- **Monatlich** – Task wird an den gewählten Tagen zu den gewählten Zeitpunkten gestartet (s. Pkt. 6.3.3.6)

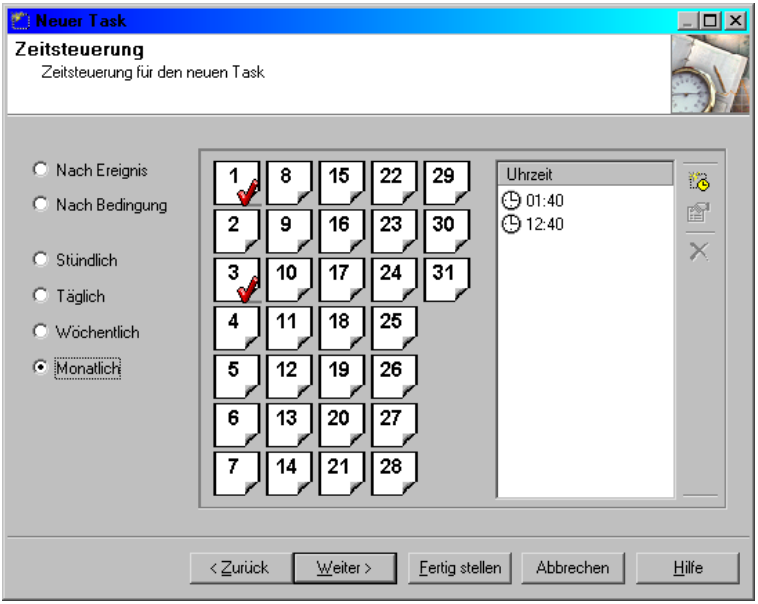


Bild 68. Fenster **Zeitsteuerung** für Kaspersky AV Scanner und Kaspersky AV Updater Tasks

Wählen Sie auf der linken Seite des Dialogfensters die gewünschte Startvariante. Nehmen Sie dann, wie in den folgenden Abschnitten beschrieben, die Einstellung der Zeitsteuerung vor.

6.3.3.1. Ereignisgesteuerter Start von Tasks

Kaspersky AV Control Centre erlaubt es, den Task bei Eintritt eines bestimmten System-Ereignisses oder durch Benutzereingabe zu starten.

Um diese Art des Starts zu wählen, aktivieren Sie das Kontrollkästchen **Nach Ereignis**. Danach erscheint auf der rechten Seite des Fensters **Zeitsteuerung** eine Liste mit Bedingungen (s. Bild 69).

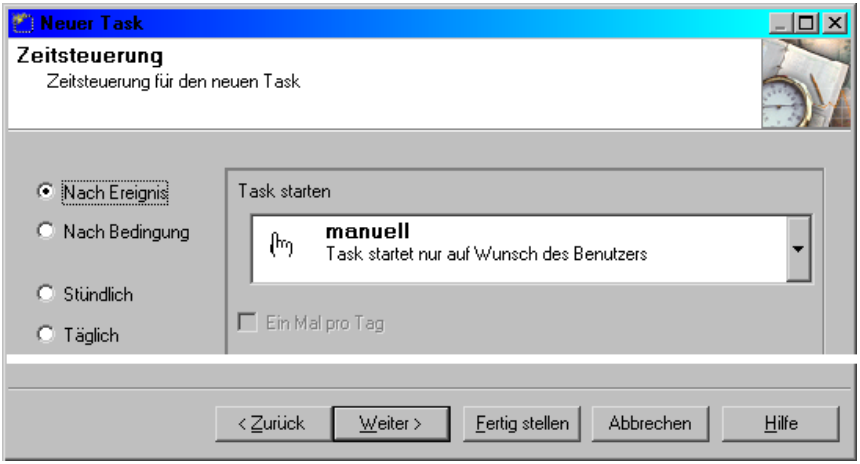


Bild 69. Einstellungen für ereignisgesteuerten Start

Wählen Sie eine Startbedingung aus der Liste. Es gibt folgende Varianten:

Manuell	Der Task wird durch Benutzereingabe in Kaspersky AV Control Centre gestartet.
Beim Start von Control Centre	Der Task wird beim Start von Kaspersky AV Control Centre ausgeführt, d.h. faktisch bei der Systemanmeldung des Benutzers.

Beim Start des Bildschirmschoners	Der Task wird beim Start des Bildschirmschoners ausgeführt.
Bei Autostart von Kaspersky AV Control Centre	Der Task wird beim Start des Systemdiensts Kaspersky AV Control Centre ausgeführt, d.h. faktisch beim Systemstart.

Für alle Tasktypen kann der Start ein Mal täglich oder jedes Mal bei Eintritt des gewählten Ereignisses festgelegt werden.

6.3.3.2. Bedingungsgesteuerter Start von Tasks

Kaspersky AV Control Centre erlaubt es, einen Task in Abhängigkeit davon zu starten, ob bei der Arbeit ausgewählter Paketkomponenten bestimmte Bedingungen erfüllt werden.

In dieser Version des Produkts wird dies folgendermaßen realisiert: Der Benutzer kann einen Task erstellen, der gestartet wird, wenn eine bestimmte Komponente von Kaspersky Anti-Virus® seine Ausführung mit einem festgelegten Exit-Code beendet.

Wählen Sie auf der linken Seite des Fensters **Zeitsteuerung** die Option **Nach Bedingung**, um den Task auf diese Art zu starten (s. Bild 70).

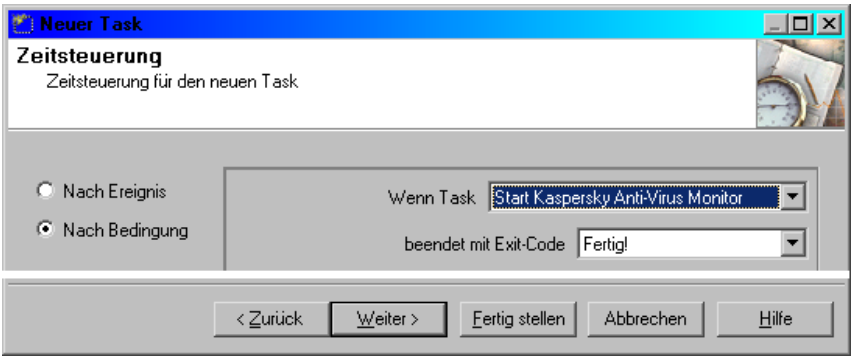


Bild 70. Einstellungen für bedingungsgesteuerten Start

Wählen Sie dann im Eingabefeld **Wenn Task** den Task-Status, von dem die Bedingung abhängen soll, und wählen Sie in der Liste **beendet mit Exit-Code** den Rückgabewert, mit dem der Task abgeschlossen werden soll.

Der Task-Status, von dem die Bedingung abhängt, wird als *Haupttask* bezeichnet, und der Rückgabewert des Haupttasks als *Ergebnis des Haupttasks*.

Es gibt folgende Typen von Haupttasks:

- *Start Kaspersky AV Monitor*
- *Aktualisierung der Antiviren-Datenbanken*
- *Start Kaspersky AV Scanner*

Das Programm bearbeitet folgende Ergebnisse des Haupttasks:

- ***Beliebig** – Der erstellte Task wird sofort nach der Ausführung des Haupttasks ungeachtet von dessen Ergebnis ausgeführt.*
- ***Fertig!** – Der erstellte Task wird nur ausgeführt, wenn der Haupttask erfolgreich beendet wurde.*
- ***Erfolglos** – Der erstellte Task wird nur ausgeführt, wenn bei der Ausführung des Haupttasks ein Fehler auftritt.*
- ***Abgebrochen** – Der erstellte Task wird ausgeführt, wenn der Haupttask vom Benutzer abgebrochen wird.*

Bestimmte Computerviren können den Antiviren-Monitor infizieren. In diesem Fall sollten Sie die Viren mit anderen Mitteln entfernen.

Mit dieser Registerkarte kann zum Beispiel ein Task erstellt werden, der Kaspersky AV Scanner nur dann startet, wenn Kaspersky AV Monitor beim Start eine Fehlermeldung generiert hat.

6.3.3.3. Task jede Stunde starten

Um den erstellten Task jede Stunde zu starten, wählen Sie auf der linken Seite des Fensters **Zeitsteuerung** den Punkt **Stündlich** (s. Bild 71) und stellen dann auf der rechten Seite des Fensters die Startzeit ein.

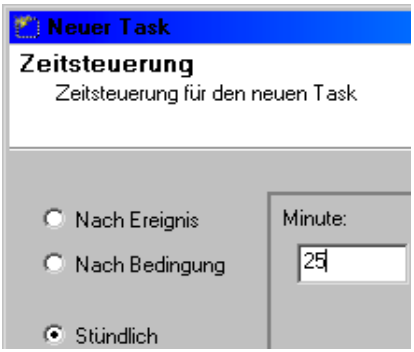


Bild 71. Einstellung für stündlichen Taskstart

Auf Bild 71 wird ein Beispiel für die Einstellungen des stündlichen Taskstarts jeweils zur 25. Minute einer Stunde gezeigt. Wenn Sie beispielsweise um 12:00 Uhr den Wert 25 eintragen, startet der Task um 12:25, 13:25, 14:25 usw.

6.3.3.4. Task jeden Tag starten

Um den Task täglich zu einer bestimmten Zeit zu starten, wählen Sie den Punkt **Täglich** im Fenster **Zeitsteuerung** (s. Bild 72) und geben Sie dann die Startzeit an.

Die Einstellung der Startzeit wird in der Liste **Uhrzeit** vorgenommen. Benutzen Sie dazu folgende Funktionen der Symbolleiste und des Kontextmenüs.

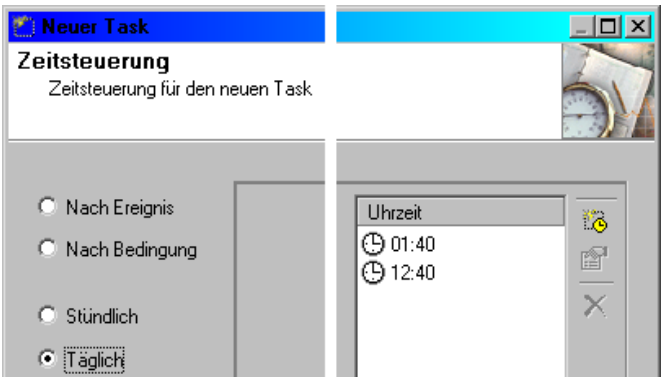


Bild 72. Einstellung für täglichen Taskstart

Schaltfläche in der Symbolleiste	Eintrag im Kontextmenü	Funktion
	**Hinzufügen…**	Eine neue Startzeit eintragen. Durch Auswahl dieses Befehls wird das Fenster **Uhrzeit hinzufügen** geöffnet, in dem die Startzeit des Tasks eingegeben wird. Dieses Fenster kann auch durch Doppelklick auf eine beliebige freie Stelle in der Liste **Uhrzeit** oder mit der Taste **<EINFG>** geöffnet werden.
	**Ändern…**	Ändern des Werts einer Startzeit des Tasks. Durch Auswahl dieses Befehls wird das Fenster **Uhrzeit ändern** geöffnet, in dem der Wert der Startzeit geändert werden kann. Dieses Fenster kann auch durch Doppelklick auf die zu ändernde Zeile oder mit der Taste **<LEERZEICHEN>** geöffnet werden.
	**Löschen…**	Löschen eines Startzeit-Eintrags aus der Liste. Wird die gewünschte Zeile markiert, dann kann hierzu auch die **<ENTF>** verwendet werden.

6.3.3.5. Task jede Woche starten

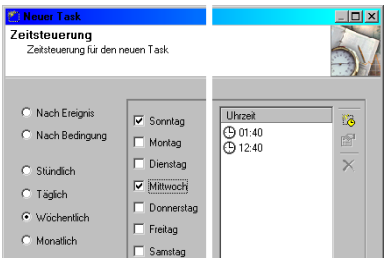


Bild 73. Einstellung für wöchentlichen Taskstart

Um den Task jede Woche an bestimmten Tagen und zu einer bestimmten Uhrzeit zu starten, wählen Sie im Fenster **Zeitsteuerung** (siehe Bild 72) den Punkt **Wöchentlich** und geben Sie dann auf der rechten Seite des Fensters Starttage und Startzeit an.

Zur Angabe der Tage und Stunden für den Taskstart werden die gewünschten Wochentage aktiviert und die Uhrzeit in der Liste **Uhrzeit** angegeben.

Das Vorgehen zur Angabe der Uhrzeit wird in Pkt. 6.3.3.4 beschrieben.

Bild 73 zeigt ein Beispiel für die Einstellungen zum Taskstart sonntags (3:40 und 1:40 Uhr) und donnerstags (3:40 und 1:40 Uhr).

6.3.3.6. Task jeden Monat starten

Um den Task jeden Monat an festgelegten Tagen und zu festgelegten Zeiten zu starten, wählen Sie auf der Registerkarte **Zeitsteuerung** (s. Bild 74) den Punkt **Monatlich**.

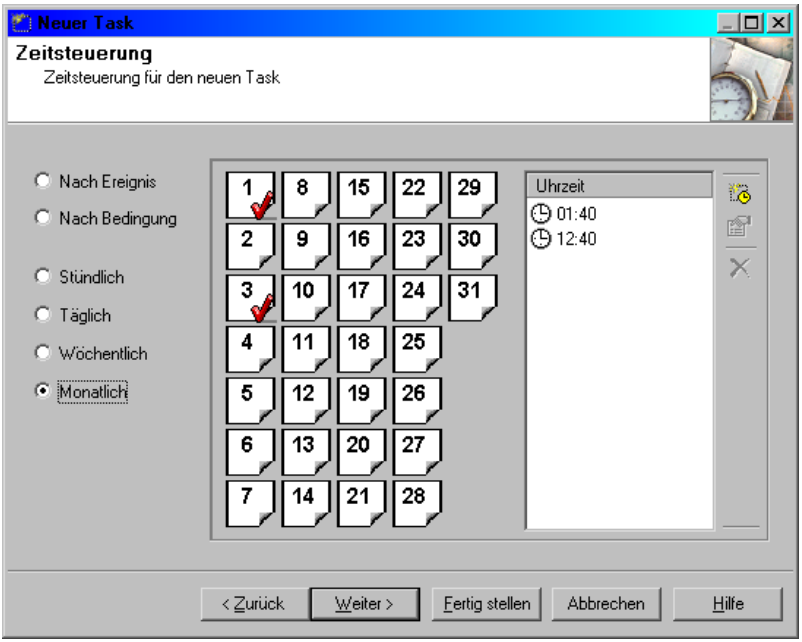


Bild 74. Einstellung für monatlichen Taskstart

Benutzen Sie Ihre Maus, um die Tage zu markieren, an denen der erstellte Task gestartet werden soll. Geben Sie danach in der Liste **Uhrzeit** den Startzeitpunkt an (zur Angabe der Uhrzeit s. 6.3.3.4).

Die Tage, an denen der Task gestartet wird, sind mit ✔ markiert. Bild 74 zeigt ein Beispiel für die Einstellungen zum Taskstart am ersten, dritten, dreizehnten und dreißigsten jeden Monats um 3:40 und 10:40 Uhr.

6.3.4. Fenster *Alarme*

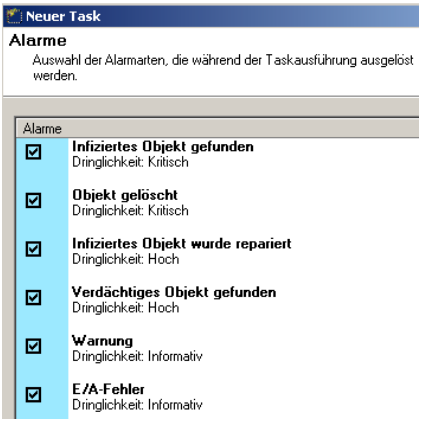


Bild 75. Auswahl der Alarmtypen

Wählen Sie im Fenster **Alarme** (siehe Bild 75) die Alarmtypen, die von diesem Task erzeugt werden.

Alarme sind, wie oben erwähnt, Nachrichten, die von Tasks erzeugt werden.

Zur Auswahl eines bestimmten Alarms wird das Kontrollkästchen neben seinem Namen aktiviert.

6.3.5. Fenster *Benutzerkonto*

Kaspersky AV Control Centre kann als Windows-Systemdienst vor der Benutzeranmeldung gestartet werden. Geben Sie in diesem Fall das Benutzerkonto an, das von diesem Task benutzt werden soll.

Das Benutzerkonto enthält Informationen über den Benutzer (z.B. vollständiger Name, Kennwort usw.). Das Konto kann im Fenster **Benutzerkonto** (s. Bild 76) konfiguriert werden.

Sie können folgende Konten benutzen:

Konto für lokales System	Windows-Konto
Derzeit angemeldetes Benutzerkonto	Das aktuelle Benutzerkonto
Dieses Konto	Konto des Benutzers, dessen Einstellungen in den Zeilen **Benutzername**, **Kennwort** und **Kennwort wiederholen** angegeben werden.

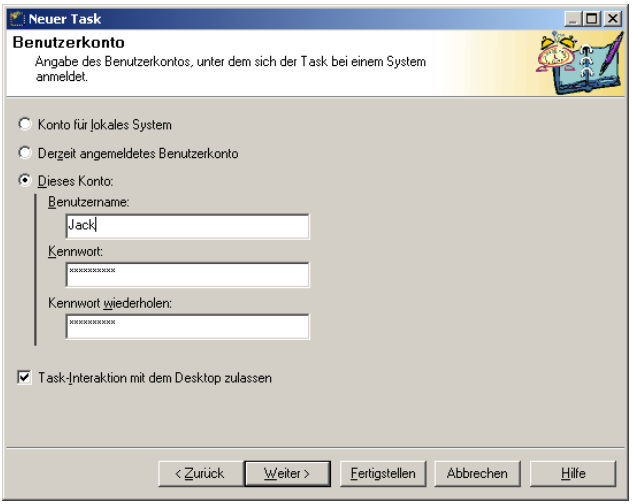


Bild 76. Konfiguration des Benutzerkontos für den Taskstart

Wird der Task von einem Konto gestartet, das sich vom aktuellen Konto unterscheidet, dann werden die von diesem generierten Warnungen nur dann auf dem Bildschirm angezeigt, wenn Sie das Kontrollkästchen **Task-Interaktion mit dem Desktop zulassen** aktivieren.

6.3.6. Task-Einstellungen

Dieser Schritt der Task-Erstellung erfordert die Konfiguration der für diesen Tasktyp charakteristischen Einstellungen. Grundsätzlich entsprechen diese Einstellungen den betreffenden Registerkarten.

Dieser Schritt umfasst folgende Tasktypen und Fenster:

Tasktyp	Fenster-Reihenfolge	Beschreibung
Task zum Start von Kaspersky AV Scanner und Kaspersky AV Monitor	1. Objekte	s. Pkt. 3.3.1
	2. Optionen	s. Pkt. 3.3.2
	3. Anpassen	s. Pkt. 3.3.3

Tasktyp	Fenster-Reihenfolge	Beschreibung
Kaspersky AV Updater	1. Verbindung	Siehe Beschreibung in Pkt. 5.2.2. In diesem Fenster sind zwei zusätzliche Optionen vorhanden, welche die Installation von Antiviren-Datenbanken und ausführbaren Modulen im angegebenen Ordner auf dem Kaspersky AV Server erlauben.
	2. Optionen	s. Pkt. 5.2.3.

6.3.6.1. Fenster *Eigenschaften* für Kaspersky AV Scanner und von Kaspersky AV Monitor Tasks

Das Fenster **Anpassen** für Kaspersky AV Scanner und Kaspersky AV Monitor Tasks gleicht hinsichtlich seiner Optionen dem Fenster **Anpassen** der entsprechenden Programme (Beschreibung dieses Fensters s. Kap. 3.3.2).

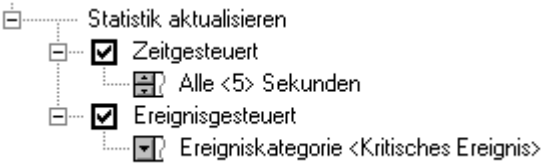


Bild 77. Dialogfenster **Anpassen** für Kaspersky AV Scanner Task

Ein Unterschied besteht im Abschnitt **Statistik aktualisieren** des Konfigurationsbaums (s. Bild 77), in dem die Aktualisierungsreihenfolge der Statistik in der Komponente Kaspersky® Report Viewer eingestellt wird.

Die Statistik kann zeitgesteuert aktualisiert werden (dazu wird das Kontrollkästchen **Zeitgesteuert** aktiviert und im Eingabefeld das Aktualisierungsintervall in Sekunden angegeben) und beim Eintritt eines System-Ereignisses (dazu wird das Kontrollkästchen **Ereignisgesteuert** aktiviert und die Ereigniskategorie gewählt). In dieser Version des Produkts kann die Statistik bei kritischen Ereignissen und anderen Ereignissen aktualisiert werden.

KAPITEL 7. KASPERSKY® REPORT VIEWER

Kaspersky® Report Viewer ist ein Programm zur Ansicht und Verwaltung von Protokollen, die von den Komponenten des Softwarepakets Kaspersky Anti-Virus® erstellt werden.

Kaspersky® Report Viewer wird gestartet durch die Auswahl des Punktes **Report anzeigen** im Hauptfenster des Programms Kaspersky AV Scanner, Kaspersky AV Monitor, Kaspersky AV Inspector, sowie durch Klick auf die Schaltfläche **Report** im Fenster **Aktualisierung abgeschlossen** des Update-Programms Kaspersky AV Updater und im Hauptfenster des Programms Kaspersky® Office Guard.

Das Hauptfenster von Kaspersky® Report Viewer (s. Bild 78) besteht aus folgenden Elementen: Menü, Symbolleiste, Sessionsliste der aktuellen Report-Datei (es kann jeweils nur eine Report-Datei geöffnet werden!), Report-Tabelle und Statuszeile.

Um den Report einer Session anzuschauen, markieren Sie die gewünschte Session auf der linken Seite des Fensters. Danach erscheint rechts das entsprechende Protokoll.

In den Spalten der Tabelle finden Sie folgende Informationen:

- ***Objekt*** *– Objekt, mit dem eine Aktion vorgenommen wurde.*
- ***Ergebnis*** *– Arbeitsergebnis*
- ***Beschreibung*** *– Beschreibung der ausgeführten Aktion.*

Rechts oben befindet sich das Hauptmenü. Unter dem Menü ist die Symbolleiste angebracht, welche Schaltflächen zur Steuerung der Grundfunktionen enthält. Jede Schaltfläche verfügt über einen Popup-Tipp mit einem kurzen Hilfetext. Der Tipp wird eingeblendet, wenn mit dem Mauszeiger auf die Schaltfläche gezeigt wird. Es ist zu erwähnen, dass bestimmte Schaltflächen der Symbolleiste über analoge Menübefehle verfügen.

Bild 78. Report-Fenster

Die Zuordnung von Schaltflächen und Menübefehlen und deren Funktionen werden in der folgenden Tabelle dargestellt.

Schaltfläche	Menü	Funktion
	Ansicht → Immer im Vordergrund	Positioniert das Programmfenster über alle anderen Programmfenster auf dem Windows-Desktop.
	Datei→ Öffnen	Öffnet eine gespeicherte Reportdatei.
	Datei→ Speichern unter…	Speichert den Report unter anderem Namen in einer Datei.
	Datei→ Löschen	Löscht alle Daten in der Report-Datei.
	Datei→ Drucken	Druckt den Report aus.
	Ansicht→ Aktualisieren	Erneutes Laden des Reports aus der Datei.
	Bearbeiten→ Suchen	Suche einer Zeile oder eines Teils davon im Report. Durch Klick auf diese Schaltfläche wird das Such-Fenster geöffnet (s. unten)

Schaltfläche	Menü	Funktion
	Bearbeiten→ Weitersuchen	Suche der nächsten Zeile (oder eines Teils davon), die mit dem Vorgabe übereinstimmt.
	Ansicht→ Automatisch aktualisieren	Automatisches Verfolgen des Reports (wenn Sie diese Option aktivieren, wird der Report beim Eintreffen neuer Daten automatisch auf die letzte Zeile positioniert).
	Ansicht→ Letzte Session anzeigen	Anzeige eines Reports der letzten Session.
	Ansicht→ Nur Statistik anzeigen	Zeigt nur die Statistik an.
	Ansicht→ Kommentare...	Zeigt nur Kommentare an.
	Hilfe	Hilfesystem.

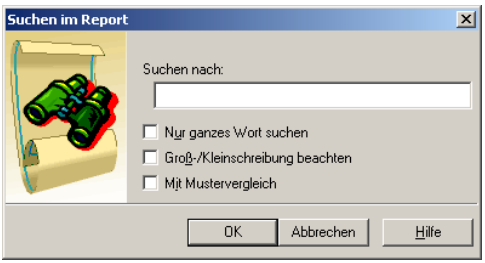


Bild 79. Fenster **Suchen im Report**

Das Suchfenster (s. Bild 79) wird durch Klick auf die Schaltfläche in der Symbolleiste oder durch Auswahl des Punktes **Suchen** im Menü **Bearbeiten** geöffnet. Um eine Zeile (oder einen Teil davon) zu suchen, geben Sie den gesuchten Text im Eingabefeld **Suchen nach** an, wählen Sie die gewünschten Suchoptionen und klicken Sie auf **OK**.

Für die Suche sind folgende Einstellungen möglich:

- ***Nur ganzes Wort suchen*** *– Im Report nach allen Wörtern suchen, die dem angegebenen Muster entsprechen.*

- ***Groß-/Kleinschreibung beachten*** *– Zwischen Groß- und Kleinschreibung unterscheiden.*

- ***Mit Mustervergleich*** *– Suche nach Reportzeilen, die genau mit dem Muster übereinstimmen.*

Um das Fenster zu schließen, klicken Sie auf **Abbrechen**. Um Hilfe zu erhalten, klicken Sie auf **Hilfe**.

Nachdem die erste Zeile (oder ein Teil davon) des Musters gefunden wurde, können Sie den Rest der Zeichenkette (oder Teilzeile) suchen.

Klicken Sie dazu auf  oder wählen Sie im Menü **Bearbeiten** den Befehl **Suchen**.

KAPITEL 8. KONFIGURATIONS-BAUM

Auf der Benutzeroberfläche der Programme von Kaspersky Labs wird häufig ein Element verwendet, in dem alle Daten in Form eines Baumes mit unterschiedlichen Bedienungselementen als Zweigen (Schaltflächen, Dropdown-Listen, Kontrollkästchen usw.) dargestellt sind.

Diese Technologie bietet ein übersichtliches Bild der Wechselbeziehungen zwischen verschiedenen Einstellungen und trägt zur Bedienungsfreundlichkeit des Programms bei.

In diesem Handbuch ist neben der Bezeichnung eines Bedienungselements jeweils das entsprechende Symbol abgebildet.

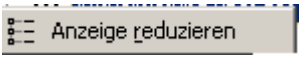
8.1. Konfigurationsbaum

Jede Gabelung des Konfigurationsbaumes kann Zweige besitzen. Wenn ein Zweig geöffnet ist, zeigt die entsprechende Gabelung das Symbol  . Ist ein Zweig geschlossen, zeigt die Gabelung das Symbol  .

Zum Ändern von Einstellungen muss der betreffende Zweig geöffnet sein.

Zum Öffnen oder Schließen eines Zweiges dienen folgende Methoden:

Aktion	Methode
Öffnen eines Zweiges (Gabelung mit dem Zeichen )	Taste → auf der Tastatur. Befehl  (bzw. Aufklappen, Zeigen) im Kontextmenü. Taste + auf dem numerischen Ziffernblock (alle Zweige der Gabelung werden geöffnet).

Aktion	Methode
Schließen eines Zweiges (Gabelung mit dem Zeichen)	Taste ← auf der Tastatur. Befehl  (bzw. Zuklappen, Ausblenden) im Kontextmenü. Taste – auf dem numerischen Ziffernblock (alle Zweige der Gabelung werden geschlossen).

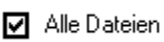
8.2. Bedienungselemente

Zur Konfiguration von Einstellungen dienen verschiedene Arten von Bedienungselementen.

8.2.1. Kontrollkästchen

Ein **Kontrollkästchen** kann zwei unterschiedliche Zustände annehmen:

 – Kontrollkästchen ist deaktiviert. Untersuchung wird nicht durchgeführt.

 – Kontrollkästchen ist aktiviert. Untersuchung wird durchgeführt.

Der Zustand eines Kontrollkästchens kann auf folgende Arten geändert werden:

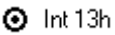
Aktion	Methode
Aktivieren eines Kontrollkästchens	Taste **<LEERZEICHEN >** auf Ihrer Tastatur. Befehl  (bzw. Aktivieren) im Kontextmenü. Ein Klick auf das Kontrollkästchen.

Aktion	Methode
Deaktivieren eines Kontrollkästchens	Taste **<LEERZEICHEN >** auf Ihrer Tastatur. Befehl  (bzw. Deaktivieren) im Kontextmenü. Klick auf das Kontrollkästchen.

8.2.2. Optionsfeld

Optionsfelder gehören zu einer Gruppe von mindestens zwei Optionsfeldern. Jedes Optionsfeld entspricht einer möglichen Einstellungsvariante. Ein Optionsfeld kann zwei Zustände annehmen:

 – deaktiviertes Optionsfeld

 – aktiviertes Optionsfeld

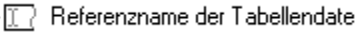
Innerhalb einer Gruppe kann jeweils nur ein Optionsfeld aktiviert sein.

Der Zustand eines Optionsfeldes kann auf folgende Arten geändert werden:

Aktion	Methode
Aktivieren eines Optionsfeldes	Taste **<LEERZEICHEN >** auf der Tastatur. Befehl  (bzw. Aktivieren) im Kontextmenü. Klick auf das Optionsfeld.
Deaktivieren eines Optionsfeldes	Aktivieren eine anderen Optionsfeldes.

8.2.3. Textfeld

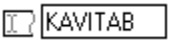
Die Angabe eines Werts in einem **Textfeld** erfolgt direkt über die Tastatur. Der aktuelle Wert des Textfeldes wird in eckigen Klammern rechts vom Namen des Textfeldes angezeigt.



– Textfeld.

Methoden zum Ändern des Werts in einem Textfeld:

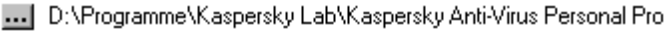
- Klick auf das Symbol des Feldes.
- Befehl 

im Kontextmenü.
- Taste <F2>. Danach nimmt das Textfeld folgendes Aussehen an: 

Drücken Sie nach dem Bearbeiten des Werts die Taste **<EINGABE>** oder klicken Sie an eine Stelle außerhalb des Eingabefeldes. Um den vorherigen Feldwert wiederherzustellen, drücken Sie die Taste **<Esc>**.

8.2.4. Eingabefeld für Pfade

Der Wert im **Eingabefeldes für Pfade** wird in einem konventionellen Windows-Dialogfenster geändert.



– Eingabefeld für Pfade.

Methoden zum Ändern des Wertes in einem Textfeld zur Pfadangabe:

- Klick auf das Symbol des betreffenden Feldes.
- Befehl 

im Kontextmenü.
- Taste **<F2>**.

8.2.5. Eingabefeld für Zahlenwerte

Die Angabe eines Werts in einem **Eingabefeld für Zahlenwerte** erfolgt direkt über die Tastatur oder wird durch Klick auf die Pfeilelemente vorgenommen. Der aktuelle Wert des Zahlenfeldes wird in eckigen Klammern rechts vom Namen des Zahlenfeldes angezeigt.

– Eingabefeld für Zahlenwerte.

Methoden zum Ändern des Werts in einem Zahlenfeld:

- *Klick auf das Symbol des betreffenden Feldes.*
- *Befehl* 

im Kontextmenü.
- *Taste* ***<F2>***.

Ist die zuerst eingegebene Ziffer eine Null, dann interpretiert das Programm diese als Oktalzahl und rechnet sie danach in die entsprechende Dezimalzahl um.

8.2.6. Dropdown-Liste

Die Dropdown-Liste dient der Auswahl eines Elements aus einer Liste (siehe Bild 80). Zur Navigation innerhalb einer Liste können die Tasten ↑ und ↓ verwendet werden. Um die Liste automatisch aufwärts bzw. abwärts zu blättern, werden die Tastenkombinationen Strg + ↑ bzw. Strg + ↓ verwendet.

Bild 80. Dropdown-Liste

8.3. Kontrollindikatoren

Bei der Einstellung des Programms zur Virus-Suche werden in der Laufwerkhierarchie sogenannte "Folge-Regeln" verwendet, d.h. bei der Auswahl bestimmter Einstellungen für das Objekt **Arbeitsplatz** (s. Bild 81) werden diese Einstellungen automatisch auf alle Laufwerke Ihres Computers angewandt.

Bild 81. Laufwerkshierarchie

Jedem Hierarchie-Element entspricht ein *Kontrollindikator,* der aktiviert oder deaktiviert werden kann, und *Regeln*, die auf das Element angewendet werden. Der Kontrollindikator zeigt, ob für ein Hierarchie-Element der Untersuchungsmodus aktiviert oder deaktiviert ist. Die Regeln bestimmen die Überprüfungsmethode.

Standardmäßig *erben alle Elemente die Regel der Gruppe*, der sie angehören. Wird die Regel der Gruppe geändert, so ändern sich auch die Regeln der zu ihr gehörenden Elemente.

Sie können für bestimmte Elemente individuelle Regeln festlegen oder den Zustand ihrer Kontrollindikatoren ändern. Diese Elemente *verfügen dann über eigene Regeln*. Werden die Regeln der Gruppe geändert, bleiben die individuellen Regeln dieser Elemente unverändert. Wird aber der Zustand des Kontrollindikators einer Gruppe geändert, so wird für die Elemente dieser Gruppe erneut der Vererbungsmodus aktiviert.

Sie können den Vererbungsmodus für ein Element ganz abschalten. Wählen Sie dazu im Kontextmenü den Punkt **Exakt** setzen. Danach wird der Kontrollindikator die Form eines roten Kästchens mit schwarzem Haken annehmen. Diese Elemente werden dann nach *festen eigenen Regeln behandelt*. Diese Elemente werden auch dann ihre individuellen Regeln beibehalten, wenn Kontrollindikatoren ihrer Gruppe geändert werden. Sie können den Vererbungsmodus wieder aktivieren, indem Sie im Kontextmenü den Punkt **Exakt** entfernen wählen.

Ein Kontrollindikator kann folgendes Aussehen haben:

Indikator	Beschreibung	Bedeutung
☑	Quadrat mit Häkchen. Das Quadrat kann rot oder schwarz sein.	Der Such-Modus ist aktiviert. Rotes Quadrat – deaktivierter Erbmodus. Schwarzes Quadrat – aktivierter Erbmodus.
☑	Quadrat mit Häkchen und Dreieck in der rechten unteren Ecke. Das Dreieck kann rot oder schwarz sein.	Der Erbmodus ist aktiviert, aber bestimmte Objekte sind aus der Gruppe ausgeschlossen und besitzen ihre individuellen Einstellungen. Rotes Dreieck – der Erbmodus ist für ein oder mehrere Objekte deaktiviert. Schwarzes Dreieck – für ein oder mehrere Objekte wurde eine Regel geändert.
☐	Quadrat ohne Häkchen, aber mit Dreieck in der rechten unteren Ecke. Das Dreieck kann rot oder schwarz sein.	Der Such-Modus ist deaktiviert, aber für ein oder mehrere Objekte ist der Such-Modus aktiviert. Rotes Dreieck – der Erbmodus ist für ein oder mehrere Objekte deaktiviert. Schwarzes Dreieck – für ein oder mehrere Objekte wurde eine Regel geändert.

KAPITEL 9. KASPERSKY ANTI-VIRUS® SCRIPT CHECKER

Kaspersky Anti-Virus® Script Checker ist ein Antiviren-Programm, das Ihren Computer vor dem Eindringen von Skript-Viren und Würmern schützt, die direkt im Arbeitsspeicher ausgeführt werden. Während der Installation des Softwarepakets Kaspersky Anti-Virus® Personal wird dieses Programm automatisch in das Betriebssystem integriert und muss danach nicht mehr manuell gestartet werden.

Verschiedene Programme, die Microsoft Windows Script Host verwenden (z.B. Microsoft Explorer, Microsoft Internet Explorer, Microsoft Outlook u.a.), senden Skripte (wie VB Script und Java Script) zur Verarbeitung und zur weiteren Ausführung an das Script Hosting. Vor dem Ausführen dieser Skript-Dateien sendet Script Checker diese zur Überprüfung an Kaspersky Anti-Virus® Monitor (vorausgesetzt, er wurde installiert und gestartet) und, falls Monitor keine Viren entdeckt, führt er eine heuristische Analyse[3] des Skript-Codes durch. Falls es sich um eine verdächtige Datei handelt, sendet Script Checker eine Warnung und verbietet die Ausführung des Skripts.

Script Checker verwendet die Antiviren-Datenbanken nicht. Die Antiviren-Datenbanken werden von Kaspersky AV Scanner und Kaspersky AV Monitor benutzt. Der Vorteil von Script Checker besteht im Vergleich zu anderen Antiviren-Programmen darin, dass er den Benutzer vor einer möglichen Infektion mit einem neuen Virus warnt, der noch nicht in den Antiviren-Datenbanken verzeichnet ist.

Im Betriebssystem Windows werden Skript-Dateien im Arbeitsspeicher ausgeführt, ohne dass vorher auf die Festplatte zugegriffen wird. Deshalb können Programme wie Antiviren-Monitore die Skript-Dateien nicht vor ihrer Ausführung überprüfen. Script Checker erlaubt es, die Ausführung der Skript-Dateien abzufangen und sie zur Untersuchung an einen Monitor zu übergeben. Auf diese Weise bietet Script Checker in Kombination mit einem Antiviren-Monitor einen vollständigen Schutz gegen alle Arten von Viren.

Die Funktion von Script Checker soll an einem Beispiel verdeutlichet werden.

---

3 Heuristische Analyse – Analyse der Befehlsabfolge im untersuchten Objekt. Diese setzt sich zusammen aus Statistiken und einer Entscheidung der Art “möglicherweise infiziert” oder “nicht infiziert” (zu Details siehe www.viruslist.com).

Nehmen wir an, sie rufen eine Internetseite auf, die einen Skript-Virus enthält, ähnlich wie LoveLetter[4]. Ist Internet-Browser auf eine niedrige Sicherheitsstufe eingestellt, so wird der Virus sofort ausgeführt. Script Checker verhindert jedoch die Ausführung des infizierten Skripts und schützt Ihren Computer dadurch vor einem Virenangriff. Dabei gibt Script Checker eine Warnung der folgenden Art aus (s. Bild 82):

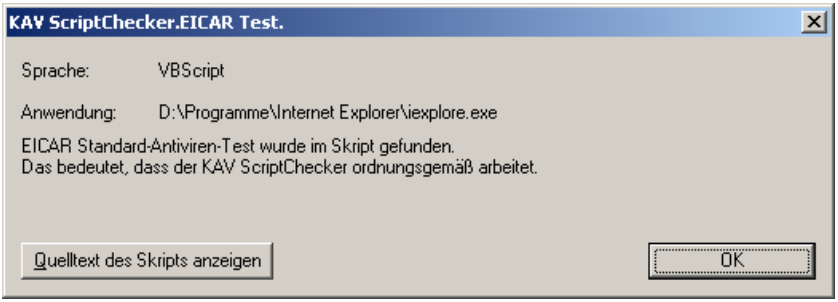


Bild 82. Warnung vor einem mutmaßlichen Virus

4 LoveLetter ist ein gefährlicher Internet-Wurm, der im Mai 2000 zu einer massenhaften Infektion von Computern führte. Der Wurm wurde durch E-Mail-Nachrichten verbreitet. Nach seiner Aktivierung verschickt er sich selbst an alle Adressen, die im Adressbuch von Microsoft Outlook gespeichert sind (zu Einzelheiten siehe www.viruslist.com).

KAPITEL 10. KASPERSKY ANTI-VIRUS® RESCUE DISK

Zu dem Paket Kaspersky Anti-Virus® gehört **Kaspersky Anti-Virus® Rescue Disk**, ein spezielles Programm, das dem Erstellen eines *Rettungsdiskettensatzes* dient.

Mit den Rettungsdisketten kann die Funktionsfähigkeit des Systems nach einem Virenangriff wiederhergestellt werden. Die Disketten umfassen:

- *Systemdateien des Betriebssystems Linux*
- *Antiviren-Scanner*
- *Antiviren-Datenbanken*

Die Rettungsdisketten funktionieren nach folgendem Prinzip: Nehmen wir an, Ihr Rechner kann nach einem Virenangriff nicht mehr hochgefahren werden. In diesem Fall ist der Start des Computers mit Hilfe der Bootdiskette aus dem Rettungsdiskettensatz erforderlich. Die Diskette lädt zuerst das Betriebssystem Linux und startet dann den Antiviren-Scanner. Falls notwendig, fordert das Bootprogramm zum Einlegen der Disketten mit den Antiviren-Datenbanken auf. Wird ein Virus gefunden, dann fragt der Antiviren-Scanner, welche Aktion er durchführen soll: einen Versuch zum Entfernen des Virus aus der Datei, die Datei vollständig löschen, oder nur einen entsprechenden Eintrag im Protokoll vornehmen.

10.1. Erstellen der Rettungsdisketten

Das Programm zum Erstellen der Rettungsdisketten von Kaspersky Anti-Virus® Rescue Disk wird im Windows-Hauptmenü in der Programmgruppe **Kaspersky Anti-Virus®** gestartet. Zum Starten des Programms wählen Sie den Punkt **Kaspersky Anti-Virus® Rescue Disk**. Danach wird das Begrüßungsfenster des Assistenten für die Rettungsdiskettenerstellung geöffnet (s. Bild 83). Um zum nächsten Fenster des Assistenten zu gelangen, klicken Sie in diesem und den folgenden Dialogfenstern jeweils auf die Schaltfläche **Weiter**.

Bild 83. Dialogfenster **Willkommen**

Im Fenster **Konfiguration** (s. Bild 84) wird angegeben, welche Disketten des Rettungsdiskettensatzes erstellt werden sollen:

- ☑ **Bootfähige Diskette mit ausführbaren Dateien** – Eine Bootdiskette mit dem Betriebssystem Linux und den ausführbaren Dateien des Antiviren-Scanners.
- ☑ **Disketten mit Antiviren-Datenbanken** – Die Disketten, welche Virusdefinitionen und Methoden zur Virusdesinfektion enthalten. Es wird empfohlen, regelmäßig Disketten mit aktualisierten Antiviren-Datenbanken anzufertigen.

Es ist ausreichend, die Bootdiskette, welche die Systemdateien des Betriebssystems Linux und die ausführbaren Dateien von Kaspersky Anti-Virus® enthält, nur beim ersten Mal zu erstellen. Dagegen wird empfohlen, die Diskette mit den Antiviren-Datenbanken jeweils beim Erscheinen eines Updates neu zu erstellen.

Wählen Sie in der Gruppe **Einstellungen der Antiviren-Datenbanken** die Methode für das Erstellen der Disketten mit den Antiviren-Datenbanken:

- ⊙ **Löschen aller Dateien auf der Diskette vor dem Kopieren** – Vor dem Kopieren der Antiviren-Datenbanken werden alle Dateien auf der Diskette gelöscht.

- **Nur aktualisierte Antiviren-Datenbanken kopieren** – Nur aktualisierte Antiviren-Datenbanken werden kopiert. In diesem Modus wird die Diskette vor dem Kopieren nicht gelöscht, sondern die auf der Diskette vorhandenen Datenbanken werden mit jenen verglichen, die kopiert werden sollen. Sind Datenbanken identisch, dann werden sie nicht kopiert.

Wenn Sie die Option **Nur aktualisierte Antiviren-Datenbanken kopieren** gewählt haben, sind die Disketten mit den Antiviren-Datenbanken in der gleichen Reihenfolge einzulegen, in der sie erstellt wurden.

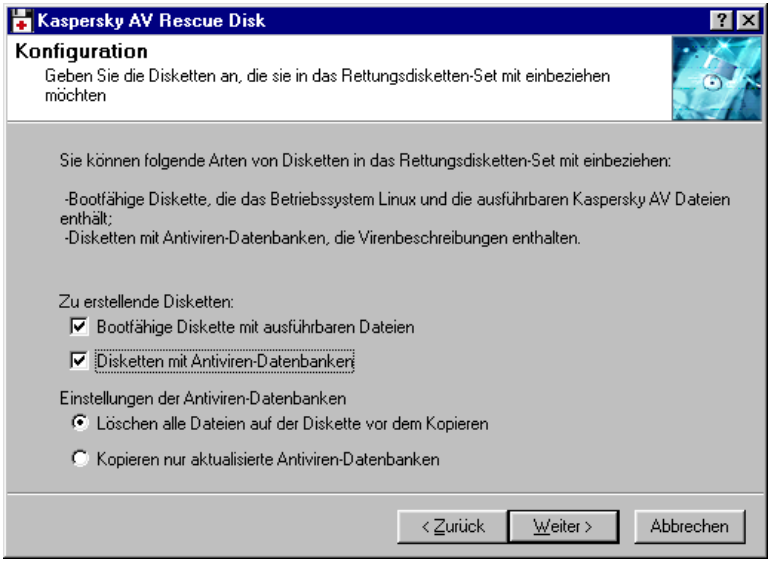


Bild 84. Dialogfenster **Konfiguration**

Geben Sie im folgenden Dialogfenster **Antiviren-Datenbanken** (s. Bild 85) den Pfad der Datei *AVP.SET* an. Diese Datei gehört zu Kaspersky Anti-Virus® und enthält eine Liste der verfügbaren Antiviren-Datenbanken.

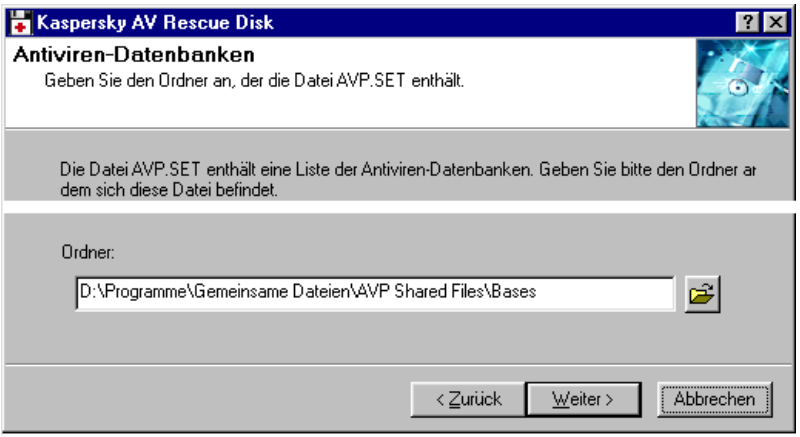


Bild 85. Dialogfenster **Antiviren-Datenbanken**

Wählen sie im Dialogfenster **Ziel** (s. Bild 86) das logische Laufwerk, auf das die Dateien kopiert werden sollen.

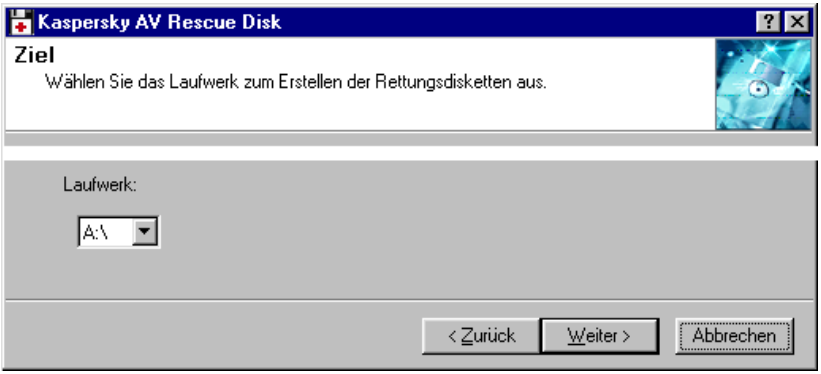


Bild 86. Dialogfenster **Ziel**

Danach werden die Dateien auf das gewählte logische Laufwerk kopiert (siehe Bild 87). Während des Kopiervorgangs werden Sie aufgefordert, weitere Disketten einzulegen.

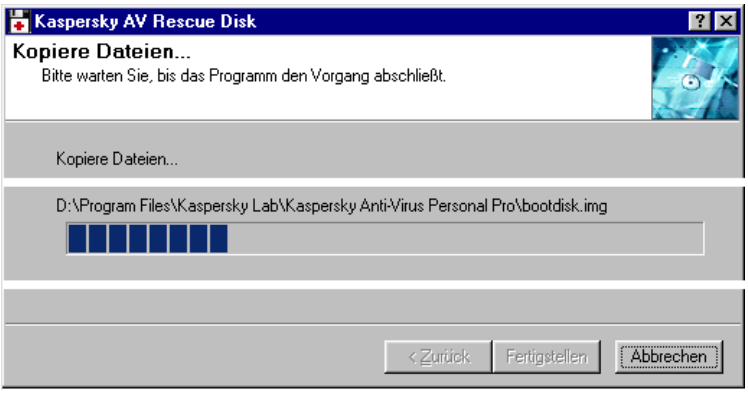


Bild 87. Fenster **Kopiere Dateien…**

Nach dem Abschluss des Kopiervorgangs erscheint das Dialogfenster **Erstellung der Rettungsdiskette wird abgeschlossen** (s. Bild 88). Dies bedeutet, dass das Programm zum Erstellen der Rettungsdisketten seine Arbeit beendet hat.

Bild 88. Dialogfenster **Erstellung der Rettungsdiskette wird abgeschlossen**

Sie verfügen nun über einen Rettungsdiskettensatz, der für den Fall eines Virenangriffs benötigt wird.

10.2. Verwendung der Rettungsdisketten

Für den Einsatz der Rettungsdisketten wird folgendes Vorgehen empfohlen:

1. Legen Sie die Rettungsdiskette in das Diskettenlaufwerk ein und führen Sie einen Neustart durch. Nachdem das Betriebssystem geladen wurde, wird der Antiviren-Scanner gestartet, der die Bootsektoren und den Master-Bootsektor Ihres Computers überprüft. Gefundene Viren werden vom Programm automatisch gelöscht. Danach erscheint auf dem Bildschirm folgende Anfrage:

   ```
   Please select a device for swapping.
   N …
   1. /dev/ide/host0/bus0/target0/lun0/part 1
   2. /dev/ide/host0/bus0/target0/lun0/part 5
   0. No swap (Recommended)
   Please enter the preferred partition number and press
   ENTER.
   ```

   Hier wird das Laufwerk gewählt, auf dem vom Betriebssystem temporäre Daten gespeichert werden, und dessen Nummer einzugeben. Die Namen der Laufwerke werden im Linux-Format angezeigt. Danach erscheint eine ähnliche Anfrage nach dem Laufwerk zum Speichern der Report-Datei.

Beachten Sie, dass über der Zeile mit der Laufwerkanfrage für die temporären Daten auf dem Bildschirm Details über die Namen der Laufwerke Ihres Computers im Format des Betriebssystems Linux erscheinen. Diese Namen benötigen Sie später, wenn Sie den Antiviren-Scanner selbständig starten möchten. Die Informationen haben folgendes Format:

```
Remounting root filesystem in read-write mode.

/dev/ide/host0/bus0/target0/lun0/part1 (Vfat) has been
mounted to /mnt/disk1
```

Es wird nicht empfohlen, die Rettungsdisketten im NTFS-Dateisystem zu benutzen. Wenn als Gerätetyp die Zeile **ntfs** angegeben wird, sollte für dieses Gerät beim Scannen keine Virus-Desinfektion festgelegt werden.

2. Legen Sie auf Anforderung die entsprechenden Disketten des Rettungsdiskettensatzes in das Laufwerk ein. Nach dem Kopieren der Datenbanken von der Diskette wird die nächste Diskette eingelegt und dreimal auf die Taste **<EINGABE>** gedrückt. Danach wird die Virus-Suche gestartet.

3. Wird ein Virus gefunden, dann stellt das Programm eine Anfrage mit folgendem Aussehen:

   ```
   File <Dateiname> Infected by virus:<Name_des_Virus>
   Actions – Report only (Ok,
   disInfect/Delete/Cancel/Stop)
   ```

   wobei:

   `<Dateiname>` – Name der infizierten Datei;

   `<Name_des_Virus>` – Bezeichnung des gefundenen Virus. Wählen Sie die Aktion, die das Programm mit der infizierten Datei durchführen soll. Geben Sie dazu einen der folgenden Buchstaben ein:

   O oder keine Eingabe – Es werden lediglich Informationen über den Virus im Protokoll aufgezeichnet.

   I – Desinfektionsversuch mit der infizierten Datei durchführen.

   D – Löschen der infizierten Datei.

   C – Nichts unternehmen.

   S – Scanprozess abbrechen.

Danach führt das Programm eine Anfrage für die Anwendung der gewählten Aktion auf alle infizierten Objekte durch, die später gefunden werden:

```
Apply to all infected objects? – Yes/No
```

Geben Sie als Antwort einen der folgenden Buchstaben ein:

Y – Die gerade gewählte Aktion soll auf alle gefundenen infizierten Objekte angewandt werden.

N – Beim Fund eines infizierten Objekts soll eine Anfrage durchgeführt werden.

4. Nach dem Abschluss des Scannens und der Desinfektion erscheint auf dem Bildschirm eine Tabelle mit den Untersuchungsergebnissen. Drücken Sie zum Schließen der Tabelle die Taste **<EINGABE>.**

   - **Sector objects** – untersuchte Sektoren
   - **Files** – untersuchte Dateien
   - **Folders** – untersuchte Ordner

- **Archives** – untersuchte Archive
- **Packed** – untersuchte gepackte ausführbare Module
- **Known viruses** – bekannte Viren
- **Viruses bodies** – gefundene Viruskörper
- **Disinfected** – desinfizierte Objekte
- **Deleted** – gelöschte Objekte
- **Warnings** – Warnungen
- **Suspicious** – verdächtige Dateien
- **Corrupted** – beschädigte Dateien
- **I/O errors** – Eingabe/Ausgabe-Fehler
- **Speed (Kb/sec)** – Durchschnittsgeschwindigkeit der Untersuchung in KB/Sekunde
- **Scan time** – Gesamtzeit der Untersuchung

5. Auf dem Bildschirm erscheint ein Menü mit den Möglichkeiten der folgenden Aktion:

```
1: Run kavscanner
2: See config
3: See report
4: Exit
Your choice [1,2,3,4]>
```

Wählen Sie durch Eingabe der entsprechenden Ziffer eine Aktion:

1 – Erneutes Starten des Antiviren-Scanners. Nach der Eingabe dieser Ziffer erscheint folgende Anfrage auf dem Bildschirm:

```
Enter directories for scanning>
```

Geben Sie die zu scannenden Verzeichnisse an. Verwenden Sie dabei das Format des Betriebssystems Linux. Dem Verzeichnis *work* auf Laufwerk C: kann zum Beispiel der Eintrag */mnt/disk1/work* entsprechen. Die

Namen der Laufwerke werden nach der Bearbeitung der ersten Diskette aus dem Rettungsdiskettensatz auf dem Bildschirm angezeigt (s. oben).

Nach der Angabe der Verzeichnisse fordert das Programm die Disketten mit den Antiviren-Datenbanken an. Danach beginnt des Scannen des von Ihnen gewählten Bereichs.

2 – Anzeige der Konfigurationsdatei des Antiviren-Scanners.

3 – Anzeige des Protokolls mit den Ergebnissen des letzten Scanvorgangs.

4 – Beenden des Programms.

6. Nachdem der Scanner die Untersuchung und Desinfektion abgeschlossen hat, drücken Sie zum Neustart des Computers die Tastenkombination **<STRG>+<ALT>+<ENTF>** und entfernen Sie die Rettungsdiskette aus dem Laufwerk.

KAPITEL 11. KASPERSKY ANTI-VIRUS® MAIL CHECKER

Das Programm Kaspersky Anti-Virus® Mail Checker (Kaspersky AV Mail Checker) für Programme, die mit Microsoft Exchange Client kompatibel sind, gewährleistet den Antiviren-Schutz für Personalcomputer, die zum Senden und Empfang von E-Mails Microsoft Outlook 98/2000/XP verwenden.

Zur Zeit ist Kaspersky AV Mail Checker nicht mit den Programmen Outlook Express und TheBat! kompatibel.

Kaspersky AV Mail Checker verfügt über folgende Funktionen:

- *Untersuchung aller ein- und ausgehenden E-Mails auf Viren. Das Programm überprüft alle Nachrichten, in dem Moment, in dem diese eingehen oder abgesandt werden, auf Viren. Dabei werden Viren sowohl in den Nachrichten selbst, als auch in Anlagen gesucht.*

  Ferner sucht Kaspersky AV Mail Checker in eingebetteten Archiven und komprimierten exe-Dateien, sowie in eingebetteten Mail-Format-Dateien und Dateien von Mail-Datenbanken nach Viren.

- *Virus-Untersuchung von Nachrichten, die sich vor der Installation von Kaspersky AV Mail Checker in der Mailbox befanden. Solche Nachrichten werden überprüft, wenn sie geöffnet werden.*

- *Desinfektion von infizierten Dateien, die an E-Mails angehängt sind.*

- *Löschen von infizierten Objekten aus E-Mail-Nachrichten. Sind alle Objekte der E-Mail infiziert, dann wird die gesamte Nachricht gelöscht.*

Die Einstellungen für den Antiviren-Schutz werden in dem Programm vorgenommen, das für den E-Mail-Verkehr verwendet wird.

Für die Behandlung eingebundener Mailboxen verfügt das Programm über eine eingeschränkte Funktionalität: Nachrichten werden nicht bei ihrem Eingang in solche Mailboxen untersucht, sondern nur wenn der Benutzer eine E-Mail öffnet.

11.1. Konfiguration von Kaspersky AV Mail Checker

Die Einstellungen des Antiviren-Schutzes für den Empfänger können auf der Registerkarte **Kaspersky Anti-Virus® Mail Checker** des Dialogfensters **Optionen** überprüft und geändert werden. Das Dialogfenster wird aus dem E-Mail-Programm Microsoft Outlook 98/2000/XP aufgerufen.

*Um das Dialogfenster **Optionen** mit Hilfe des Programms Microsoft Outlook zu öffnen,*

1. Starten Sie Microsoft Outlook.
2. Wählen Sie im Menü **Extras** den Punkt **Optionen**.
3. Öffnen Sie die Registerkarte **Kaspersky Anti-Virus® Mail Checker**.

Auf der Registerkarte **Kaspersky Anti-Virus® Mail Checker** (s. Bild 89) können Sie:

- mit Hilfe des Kontrollkästchens ☑ **Schutz aktivieren** den Antivirenschutz für Ihre eingehende oder ausgehende Mail aktivieren oder deaktivieren.
- mit Hilfe des Kontrollkästchen ☑ **Bei Fund Alarm-Benachrichtigung anzeigen** die Anzeige von informativen Hinweisen regulieren, die beim Versuch, eine infizierte Mail abzusenden ausgegeben werden.

In der aktuellen Version von Kaspersky Anti-Virus® Personal/Personal Pro besteht keine Möglichkeit zur erweiterten Konfiguration des Programms Kaspersky Anti-Virus® MailChecker. Dadurch wird das einheitliche Vorgehen zur Bearbeitung von infizierten E-Mail-Nachrichten realisiert.

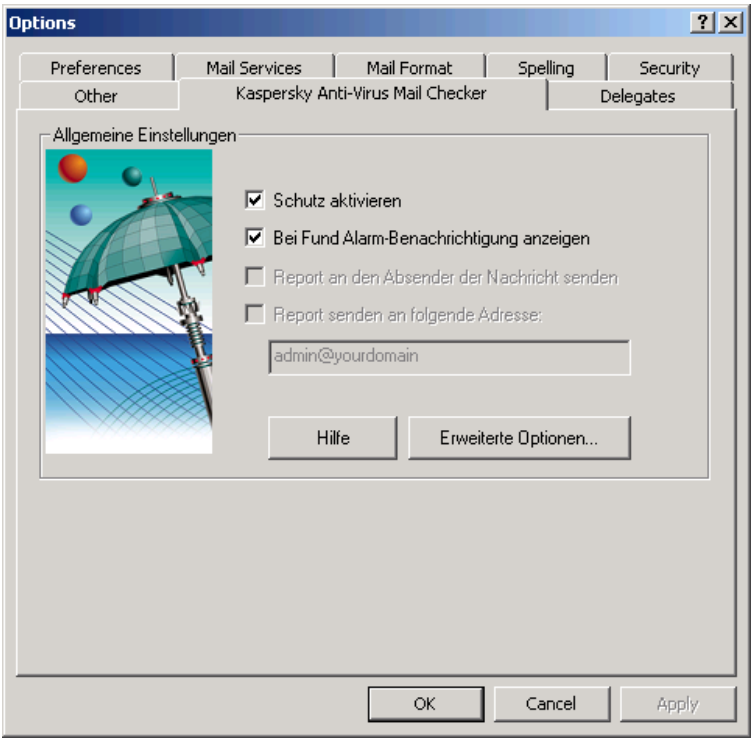


Bild 89. Registerkarte **Kaspersky Anti-Virus® MailChecker** im Dialogfenster **Optionen**

11.2. Start der Virus-Suche in E-Mail-Nachrichten

Nach der Installation von Kaspersky AV Mail Checker wird das Programm Sie nur dann über einen Virusfund in einer ausgehenden E-Mail-Nachricht informieren, wenn das Kontrollkästchen ☑ **Bei Fund Alarm-Benachrichtigung anzeigen** aktiviert wurde.

Im Folgenden werden gewisse Besonderheiten näher betrachtet, die hinsichtlich der Programmfunktion bei der Untersuchung und Bearbeitung von eingehendem und ausgehendem E-Mail-Verkehr existieren.

11.2.1. Eingehende E-Mail-Nachrichten

Eingehende Nachrichten werden im Moment ihres Eingangs in der Mailbox automatisch untersucht. Virenfreie E-Mails werden umgehend an Sie weitergeleitet. Beim Fund eines infizierten Objekts in einer E-Mail-Nachricht versucht Kaspersky Anti-Virus®, das Objekt zu desinfizieren. Kann das Objekt nicht desinfiziert werden, dann wird es aus der Nachricht gelöscht. Bei erfolgreicher Desinfektion wird die Nachricht zusammen mit dem desinfizierten Objekt sofort nach der Bearbeitung an Sie weitergeleitet.

Beachten Sie, dass Sie vom Programm nicht darüber informiert werden, wenn ein Objekt aus einer an Sie adressierten E-Mail-Nachricht desinfiziert / gelöscht wird.

Sind alle Objekte einer E-Mail-Nachricht infiziert, dann wird die Nachricht nur dann an Sie weitergeleitet, wenn mindestens ein Objekt desinfiziert werden kann. Andernfalls wird die gesamte Nachricht gelöscht.

Sie werden nicht über das Löschen der E-Mail-Nachricht informiert.

11.2.2. Ausgehende E-Mail-Nachrichten

Von der Mailbox ausgehende E-Mail-Nachrichten werden im Moment des Sendens untersucht. Wenn eine ausgehende Nachricht infiziert ist, versucht das Programm sie zu desinfizieren (falls dieser Modus aktiviert wurde).

Wenn das Kontrollkästchen ☑ **Bei Fund Alarm-Benachrichtigung anzeigen** deaktiviert ist, wird die ausgehende Nachricht im Hintergrundmodus bearbeitet. Dabei ist Ihre Teilnahme nicht erforderlich. Virusfreie Nachrichten werden an die Adressaten weitergeleitet. Infizierte Nachrichten werden der Antiviren-Bearbeitung unterzogen und anschließend:

- weitergeleitet*, wenn sie erfolgreich desinfiziert wurden.*
- *weitergeleitet, nachdem irreparable Anlagen gelöscht wurden.*
- *gelöscht*, wenn die Nachricht oder ALLE ihre Anlagen irreparabel sind.

Wenn das Kontrollkästchen **Bei Fund Alarm-Benachrichtigung anzeigen** aktiviert ist, sind folgende Anfragen des Programms zu beantworten:

Wenn die Desinfektion einer Anlage erfolglos ist, gibt das Programm einen Warnhinweis aus (s. Bild 90).

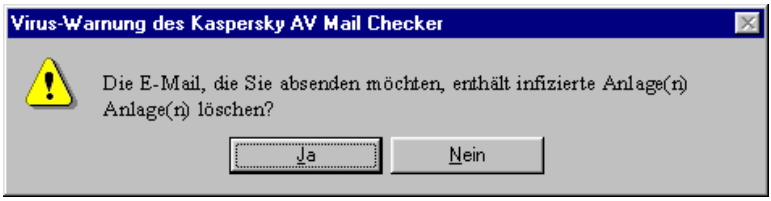


Bild 90. Warnhinweis über das Löschen von infizierten Anlagen aus einer ausgehenden Nachricht

- Klicken Sie auf die Schaltfläche **Ja**, um die infizierten Anlagen zu löschen. Danach wird die virusfreie Nachricht an den Adressaten weitergeleitet.

- Klicken Sie auf die Schaltfläche **Nein**, wenn Sie die Nachricht nicht ohne Anlage senden möchten. Danach erscheint ein Warnhinweis darüber, dass die von Ihnen abgesandte Nachricht infiziert ist (s. Bild 91). Das Absenden der infizierten Nachricht kann durch Klick auf die Schaltfläche **Nein** verworfen werden.

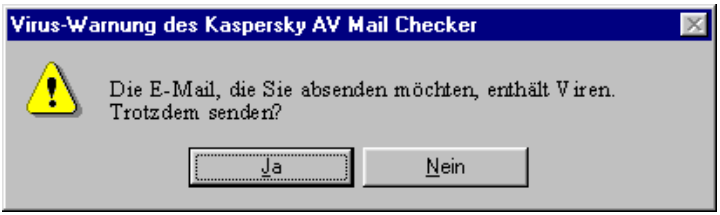


Bild 91. Warnung über den Versuch, eine infizierte Nachricht abzuschicken

11.2.3. Alte E-Mail-Nachrichten

Das Programm Kaspersky AV Mail Checker führt eine Virus-Untersuchung der E-Mail-Nachrichten durch, die sich vor der Installation des Programms in der Mailbox befanden. Diese Untersuchung findet in dem Moment statt, wenn eine solche Nachricht geöffnet wird. Danach wird die von Ihnen gewählte Nachricht auf gleiche Weise bearbeitet wie jede andere eingehende E-Mail.

KAPITEL 12. KASPERSKY ANTI-VIRUS® PERSONAL PRO

Das Programmpaket Kaspersky Anti-Virus® Personal Pro wurde speziell für den umfassenden Antiviren-Schutz von PCs entwickelt, die mit den Betriebssystemen Windows 95 OSR2/98/ME und Windows 2000/NT, mit Business-Anwendungen der MS Office 2000 Suite, sowie mit den E-Mail-Programmen Outlook und Outlook Express arbeiten. Kaspersky Anti-Virus® Personal Pro enthält dieselben Komponenten wie Kaspersky Anti-Virus® Personal (s. Kapitel 1) sowie zwei zusätzliche Komponente:

- ***Kaspersky® Office Guard*** *schützt Office 2000 Dokumente vor bekannten und unbekannten Makroviren. Kaspersky® Office Guard kontrolliert in Microsoft Office 2000 Anwendungen die Aktivitäten von Makros, die mit Visual Basic for Application geschrieben sind. Wird versucht, einen verdächtigen Makrobefehl auszuführen, dann kann Kaspersky® Office Guard in Abhängigkeit der Programmeinstellungen eine der vier folgenden Aktionen durchführen: Verbot oder Erlaubnis der Befehlsausführung, das Makro komplett deaktivieren, oder dem Benutzer eine der drei genannten Optionen zur Auswahl anbieten.*

- ***Kaspersky® Inspector*** *ist ein Antiviren-Programm zur Überwachung von Laufwerken, das für die Arbeit mit den Betriebssystemen Microsoft Windows 95 OSR2/98/ME® und Microsoft Windows NT/2000® bestimmt ist. Kaspersky® Inspector untersucht Laufwerke auf Veränderungen von Datei- und Ordnerinhalten. Das Programm kann sowohl als zusätzlicher Virus-Schutz, als auch zur Kontrolle von Laufwerkmodifikationen verwendet werden.*

Die Installation des Pakets Kaspersky Personal Pro ist identisch mit der Installation des Pakets Kaspersky Anti-Virus® Personal.

KAPITEL 13. KASPERSKY® OFFICE GUARD

Kaspersky® Office Guard dient dem Schutz von Dokumenten für Microsoft Office 2000 vor bekannten und unbekannten Makroviren. Enthält ein Dokument einen Makrovirus, dann wird er von Kaspersky® Office Guard erkannt und behandelt.

Das Programm Kaspersky® Office Guard verfügt über folgende Funktionen:

- *Kontrolle der Aktionen von Makros, die mit Visual Basic for Application (VBA) geschriebenen sind, in den Microsoft Office 2000 Anwendungen. Sobald ein Makro gestartet wird, fängt das Programm jeden von ihm auszuführenden Befehl ab und überprüft, ob dieser in der Liste* verdächtiger Makrobefehle *vorhanden ist, d.h. Befehle, die von einem Virencode ausgeführt werden können.*

  Eine Liste verdächtiger Befehle, deren Beschreibung und Angaben über die Verwendungshäufigkeit solcher Befehle durch Viren befindet sich im Hilfesystem.

- *Versucht ein Makro, einen verdächtigen Befehl auszuführen, dann geht Kaspersky® Office Guard entsprechend den von Ihnen vorgegebenen Sicherheitseinstellungen (s. Pkt. 13.3.1) vor und kann eine von folgenden vier Aktionen ausführen: Ausführung des Befehls verbieten oder erlauben, das Makro vollständig deaktivieren, oder den Benutzer fragen, damit dieser eine der drei genannten Varianten wählt. Sie können das Programm z.B. so einrichten, dass es automatisch die Ausführung aller Makrobefehle abbricht, die versuchen, verdächtige Makrobefehle auszuführen.*

  Kaspersky® Office Guard entdeckt garantiert die Aktivitäten eines beliebigen Makrovirus in Microsoft Office 2000 Dokumenten. Trotzdem kann er nicht mit vollständiger Sicherheit feststellen, ob eine Datei durch einen Virus infiziert ist oder ob sie nur ein harmloses Makro enthält, das Befehle verwendet, die manchmal auch von Viren benutzt werden. Die endgültige Entscheidung darüber, ob ein Makro sicher ist und ausgeführt werden soll, liegt bei Ihnen oder Ihrem Systemadministrator. Das Hilfesystem enthält Informationen, die Ihnen bei dieser Entscheidung von Nutzen sein können.

13.1. Kaspersky® Office Guard – Programm zum Schutz vor unbekannten Makroviren

Zur Automatisierung von sich wiederholenden Operationen wurden in viele Textverarbeitungs-, Tabellenkalkulations-, Grafikprogramme und technische Anwendungen Makrosprachen integriert. Makrosprachen können über eine komplexe Struktur und eine umfangreiche Auswahl an Befehlen verfügen.

Ein **Makrovirus** ist ein in einer Makrosprache geschriebenes Programm, das destruktive Aktionen ausführt und seinen Code aus einer infizierten Datei (Dokument oder Arbeitsmappe) in andere Dateien überträgt.

Bis Ende 2000 waren bestimmte Systeme bekannt, die von Makroviren betroffen sind. Dazu gehören die folgenden Basisanwendungen von Microsoft Office, welche die Makrosprache VBA (Visual Basic for Applications) unterstützen:

- *Textverarbeitungsprogramm Microsoft Word (in Microsoft Word 6/7 ist die Sprache WordBasic integriert, in Microsoft Word 8 und höher VBA)*
- *Tabellenkalkulation Microsoft Excel*
- *Datenbankverwaltung Microsoft Access*
- *Präsentationserstellungsprogramm Microsoft PowerPoint*
- *Projektmanager Microsoft Project*
- *Diagrammassistent Microsoft Visio*

Auch das Textverarbeitungsprogramm AmiPro, das eine spezielle Skriptsprache benutzt, ist von Makroviren betroffen.

Am weitesten verbreitet sind Makroviren für Microsoft Office (Word, Excel und PowerPoint). In anderen Anwendungen von Microsoft Office kommen relativ selten Makroviren vor. Für AmiPro ist nur ein Makrovirus bekannt.

13.1.1. Funktionsweise von Makroviren

Alle Microsoft Office Anwendungen unterstützen Automakros. Das sind Makros, die automatisch aufgerufen werden, wenn ein bestimmtes Ereignis eintritt. Automakros sind durch ihre Namen an Ereignisse "gebunden". Nach diesen Namen entscheidet eine Anwendung, welches Makros in welcher Situation aufgerufen wird. In Microsoft Word wird zum Beispiel beim Öffnen einer Datei automatisch das Makro AutoOpen ausgeführt, falls es im aktiven Dokument vorhanden ist. Beim Drucken eines Dokumentes wird das Makro FilePrint ausgeführt.

Automatisch (d.h. ohne Zutun des Benutzers) werden auch Makros/Funktionen ausgeführt, welche mit einer Taste, einer bestimmten Uhrzeit oder einem Datum verknüpft sind, d.h. eine Anwendung ruft bei Betätigung einer Taste (oder einer Tastenkombination) oder zu einem bestimmten Zeitpunkt ein Makro oder eine Funktion auf.

Makroviren, die Microsoft Office Dokumente infizieren, nutzen i.d.R. eine der oben genannten Eigenschaften aus. Entweder enthält der Virus ein Automakro (Autofunktion), oder ein Virusmakro wird automatisch aufgerufen, wenn eine Taste oder Tastenkombination betätigt wird. Außerdem gibt es Semi-Viren, die keine dieser Techniken benutzen und sich nur ausbreiten, wenn sie vom Benutzer gestartet werden.

Ist ein Dokument infiziert, dann startet die Anwendung beim Aufruf eines Automakros an dessen Stelle den Viruscode. Enthält ein Virus Makros mit Standardnamen, werden diese bei der Auswahl des entsprechenden Menübefehls (Menü **Datei**, Befehl **Öffnen**; Menü **Datei**, Befehl **Schließen**; Menü **Datei**, Befehl **Speichern unter**) aktiviert. Ist das Virusmakro mit einer Taste (oder Tastenkombination) verknüpft, wird der Virus nur bei Betätigung der entsprechenden Taste aktiviert.

Die meisten Makroviren enthalten ihre gesamten Funktionen in Form von Standardmakros für Microsoft Office 97. Allerdings gibt es auch Viren, die für ihren Code Tarnmethoden verwenden und den Code nicht in Form von Makros speichern. Die drei bekannten Techniken nutzen dabei die Fähigkeit von Makros, andere Makros zu erstellen, zu verändern und auszuführen. Diese Viren enthalten i.d.R. einen kleinen (manchmal polymorphen) Lademechanismus für Virusmakros, der einen integrierten Makro-Editor aufruft. Der Editor erstellt ein neues Makro, füllt es mit dem Basiscode des Virus, führt diesen aus und löscht ihn dann meist, um die Anwesenheitsspuren des Virus zu verwischen. Der Basiscode solcher Viren liegt entweder in Form von (teilweise verschlüsselten) Textzeilen im eigentlichen Virusmakro vor oder wird im Bereich von Dokumentenvariablen oder im Auto-Text-Bereich gespeichert.

Alle Microsoft Office Anwendungen lassen die Verschlüsselung der in einem Dokument vorhandenen Makros zu. Deshalb können bestimmte Viren in verschlüsselter Form in infizierten Dokumenten enthalten sein.

Viren für Microsoft Office können nicht nur IBM-PCs, sondern auch Computer eines beliebigen Typs infizieren. Eine Infektion ist möglich, wenn auf dem Rechner eine Anwendung installiert ist, die voll mit der entsprechenden Microsoft Office Anwendung kompatibel ist (zum Beispiel: Microsoft Word für Macintosh).

13.1.2. Verdächtige Makrobefehle

Als *verdächtig* gelten Makrobefehle, die einem Virus erlauben, eine Kopie von sich zu erstellen oder destruktive Aktionen auszuführen. Solche Befehle können auch durch Arbeitsmakros ausgeführt werden, wobei dies eher selten vorkommt. Unten finden Sie eine Liste aller verdächtigen Makrobefehle (s. Bild 92), die vom Programm kontrolliert werden. Die Makrobefehle sind nach ihrer Funktion geordnet: Auf der untersten Hierarchie-Ebene befinden sich die Namen der verdächtigen Makrobefehle, die in verschiedene Gruppen zusammengefasst werden.

Makrobefehle lassen sich in vier Gruppen einteilen:

Makro-Operationen. Gewöhnliche Makros verändern nur selten den Code anderer Makros und ihren eigenen Code praktisch nie. Deshalb weisen Code-Veränderungen mit hoher Wahrscheinlichkeit auf einen Makrovirus hin. Makro-Operationen lassen sich in zwei Untergruppen gliedern. Die erste Gruppe besteht aus Modul-Operationen: Erstellen, Hinzufügen, Kopieren, Export und Import von Modulen. Die zweite Gruppe bilden Veränderungen des Makrocodes: Einfügen von Zeilen in ein Makro, Löschen von Zeilen, Kopieren von Zeilen, Einfügen von Zeilen aus einer Datei.

Datei-Operationen. Auch Dateibefehle gelten als verdächtig. Zum Beispiel kann das Löschen von Dateien zum totalen Verlust Ihrer Daten führen, wenn dieser Befehl von einem Virus ausgeführt wird.

Andere Befehle. Diese Gruppe umfasst verdächtige Makrobefehle wie das Ändern des Antiviren-Schutzes eines Dokuments, den Start externer Anwendungen (den Befehl Shell), die Arbeit mit ActiveX-Objekten und die Nachahmung von Tastatureingaben. Solche Makrobefehle können auch von Viren verwendet werden.

Aufruf von API-Funktionen. Durch den Aufruf von Funktionen und Prozeduren des Betriebssystems und anderer Anwendungen über das API-Interface

können Viren schädliche Aktionen ausführen, ohne analoge Standardbefehle der Sprache Visual Basic zu benutzen.

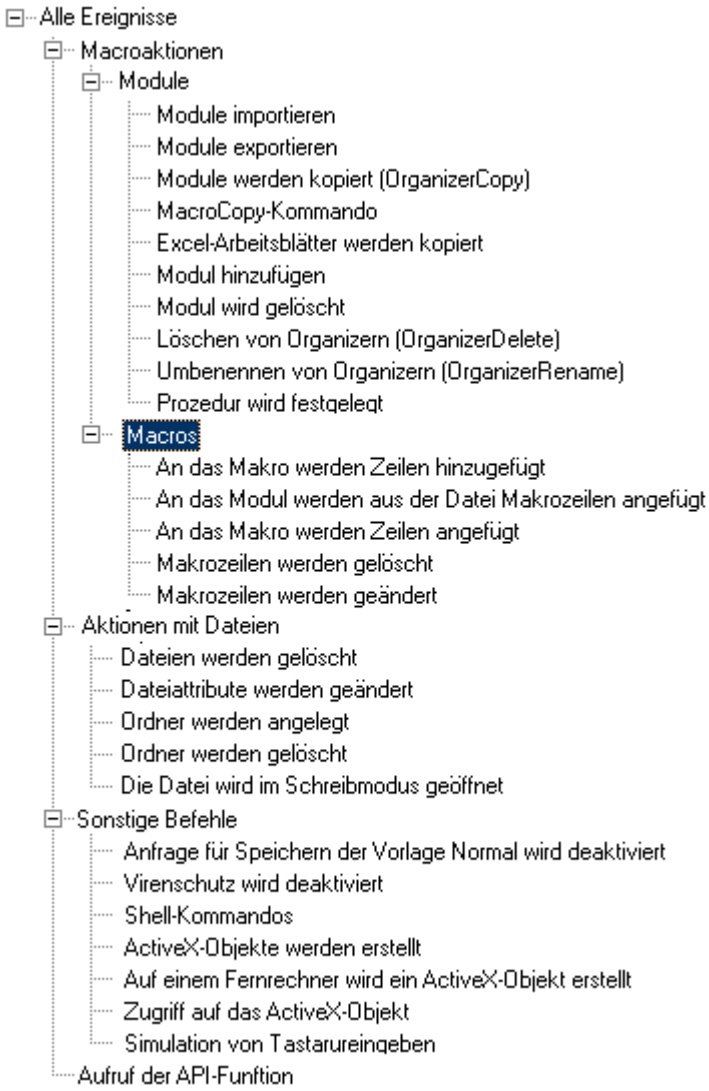


Bild 92 Liste verdächtiger Makrobefehle

13.1.3. Makroviren-Abwehr durch Kaspersky® Office Guard. Regeln für verdächtige Makrobefehle

Kaspersky® Office Guard besitzt die vollständige Kontrolle über Makroaktionen in Microsoft Office 2000 Anwendungen. Wird ein beliebiges Makro gestartet und versucht einen verdächtigen Makrobefehl aufzurufen, greift Kaspersky® Office Guard sofort ein und übernimmt die Verwaltung. Entsprechend seinen Einstellungen (s. Pkt. 13.3.1) führt Kaspersky® Office Guard eine der folgenden vier Aktionen aus: Erlaubnis oder Verbot der Ausführung des verdächtigen Makrobefehls, vollständiges Deaktivieren des Makros, oder Benutzeranfrage nach dem weiteren Vorgehen. Die einem Makrobefehl entsprechende Aktion von Kaspersky® Office Guard wird *Regel für den Makrobefehl* genannt. Zur Markierung der Regeln werden folgende Symbole verwendet:

 (Klingel) – Benutzeranfrage nach weiteren Aktionen

 ("Halteverbot") – Vollständiger Abbruch Makroaktion

 (rotes Fähnchen) – Verbot des verdächtigen Makrobefehls

 (grünes Fähnchen) – Freigabe des verdächtigen Makrobefehls

Sie können zum Beispiel folgende Regeln festlegen: automatisch alle Makros abbrechen, die sehr gefährliche Befehle auszuführen versuchen; Benutzeranfrage für den Makrobefehl zum Kopieren von Microsoft Excel Arbeitsmappen; Erlaubnis für den Makrobefehl zum Erstellen von Prozeduren; Ignorieren aller anderen verdächtigen Makrobefehle. Dieses Beispiel wird auf der folgenden Abbildung illustriert. Links vom Namen jedes Befehls befindet sich ein Symbol, das die für ihn gültige Regel angibt (s. Bild 93).

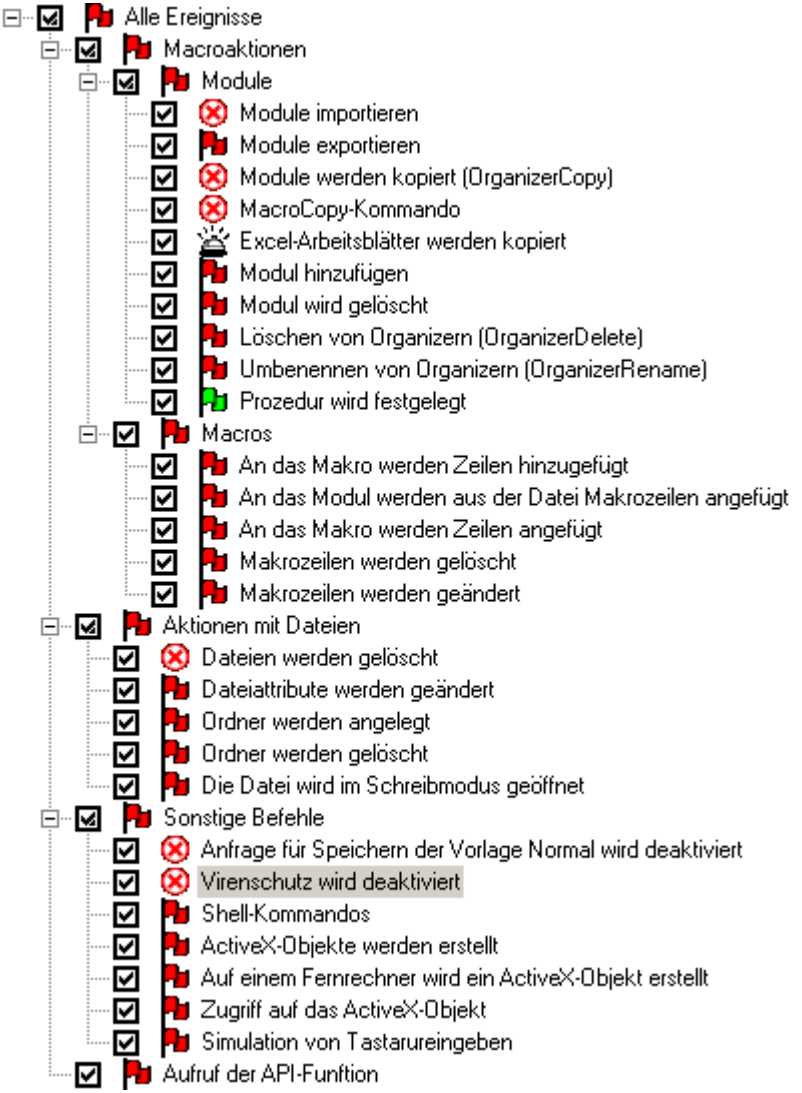


Bild 93. Beispiel. Regeln für verdächtige Makrobefehle

13.2. Benutzeroberfläche

13.2.1. Programmstart

Bei jedem Start einer Microsoft Office 2000 Anwendung wird gleichzeitig der sogenannte *Serviceteil von Kaspersky® Office Guard* gestartet, der als eigentlicher Antiviren-Wächter dient. Eben dieser Teil wird beim Versuch, verdächtige Makrobefehle auszuführen, aktiviert. Der zweite Teil, der Interfaceteil *von Kaspersky® Office Guard*, wird entweder dann gestartet, wenn der Serviceteil einen verdächtigen Befehl findet, oder vom manuell zum Ändern der Antiviren-Einstellungen.

Um den Interfaceteil von Kaspersky® Office Guard manuell zu starten,

1. Klicken Sie auf die Schaltfläche **Start**.
2. Wählen Sie den Menüpunkt **Programme**.
3. Wählen Sie im folgenden Untermenü den Punkt **Kaspersky Anti-Virus®** und dort den Punkt **Kaspersky Anti-Virus® Office Guard**.

Nachdem der Interfaceteil von Kaspersky® Office Guard gestartet wurde, erscheint im Infobereich der Windows-Taskleiste (links der Uhr) das Symbol .

*Um das Hauptfenster von Kaspersky® Office Guard zu öffnen, wählen Sie im Systemmenü (s. Pkt. 13.2.2) den Punkt **Einstellungen**, oder doppelklicken Sie auf das Symbol in der Windows-Taskleiste (s. Bild 94).*

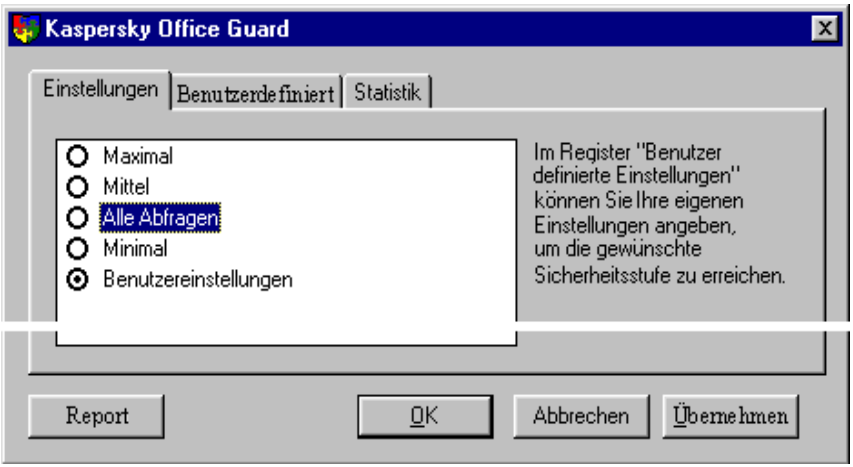


Bild 94. Hauptfenster

13.2.2. Systemmenü

Die Benutzeroberfläche von Kaspersky® Office Guard wird über das *Systemmenü* (s. Bild 95) gesteuert.

Um das Systemmenü der Benutzeroberfläche von Kaspersky® Office Guard zu öffnen, zeigen Sie mit der Maus in der Windows-Taskleiste auf das Symbol und klicken Sie mit der rechten Maustaste.

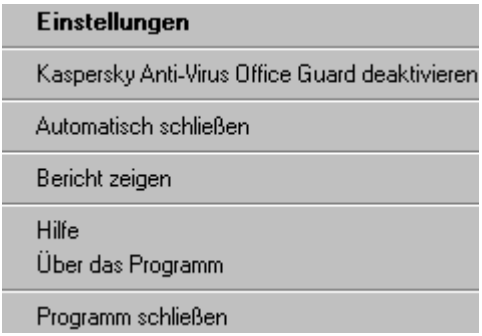


Bild 95. Systemmenü

Das Systemmenü enthält folgende Punkte:

- ***Einstellungen*** *– Öffnet das Hauptfenster von Kaspersky® Office Guard.*
- ***Kaspersky Anti-Virus® Office Guard deaktivieren / Kaspersky Anti-Virus® Office Guard aktivieren*** *– Hält die Arbeit von Kaspersky® Office Guard an/setzt die Arbeit von Kaspersky® Office Guard fort. Wurde das Programm angehalten, werden die Aktionen der Makros nicht überwacht.*
- ***Automatisch schließen*** *– Beendet den Interfaceteil von Kaspersky® Office Guard, wenn alle VBA-gestützten Microsoft Office 2000 Anwendungen geschlossen wurden.*
- ***Hilfe*** *– Öffnet das Hilfesystem.*
- ***Über das Programm*** *– Öffnet das Fenster mit Angaben über die Schlüssel.*
- ***Programm schließen*** *– Beendet den Interfaceteil von Kaspersky® Office Guard.*

Durch Auswahl des Punktes **Programm beenden** wird der Serviceteil nicht aus dem Arbeitsspeicher entfernt.

13.2.3. Hauptfenster

Das Hauptfenster von Kaspersky® Office Guard enthält drei Registerkarten: **Einstellungen**, **Benutzerdefiniert** und **Statistik**. Die Registerkarte **Einstellungen** dient der Auswahl der Sicherheitsstufe, die vom Programm gewährleistet werden soll. Auf der Registerkarte **Statistik** werden die Arbeitsergebnisse dargestellt. Auf der Registerkarte **Benutzerdefiniert** können Sie die Regeln für die gewählte Sicherheitsstufe einsehen und, wenn Sie die auf der Registerkarte **Einstellungen** die Option **Benutzerdefiniert** gewählt haben, die Regeln ändern.

Alle Aktionen werden über Kontextmenüs gesteuert, deshalb befinden sich im Hauptfenster keine üblichen Menüs.

13.2.4. Beenden des Programms

*Um die Benutzeroberfläche von Kaspersky® Office Guard zu schließen, wählen Sie im Systemmenü den Punkt **Programm schließen**.*

Nach dem Schließen des Interfaceteils bleibt der Serviceteil weiter aktiv.

13.2.5. Hilfesystem

Für die Arbeit mit Kaspersky® Office Guard steht ein *Hilfesystem* zur Verfügung.

*Um das Hilfesystem zu starten, wählen Sie im Systemmenü den Punkt **Hilfe**.*

Um zu einem Interface-Element eine Popupinformation zu erhalten, klicken Sie mit der rechten Maustaste darauf oder verwenden Sie die Tastenkombination <Umschalt>+<F1>.

13.3. Einstellungen

13.3.1. Auswahl der Sicherheitsstufe

Um die gewünschte Sicherheitsstufe einzustellen,

1. Wechseln Sie auf die Registerkarte **Einstellungen** (siehe Bild 94).

2. Wählen Sie die gewünschte Sicherheitsstufe:

   - **Maximal** – Höchste Sicherheitsstufe für den Antiviren-Schutz (s. Pkt. 13.3.2).

   - **Mittel** – Mittlere Sicherheitsstufe für den Antiviren-Schutz (s. Pkt. 13.3.3).

- **Alle abfragen** – In dieser Sicherheitsstufe fragt Kaspersky® Office Guard bei Ausführung jedes verdächtigen Befehls um Erlaubnis (s. Pkt. 13.3.4).

- **Minimal** – Niedrige Sicherheitsstufe für den Antiviren-Schutz (s. Pkt. 13.3.5).

- **Benutzerdefiniert** – In dieser Sicherheitsstufe können Sie für jeden zu kontrollierenden Befehl eigene Einstellungen vornehmen. Die Konfiguration erfolgt auf der Registerkarte **Benutzerdefiniert** (s. Pkt. 13.3.6).

Das Optionsfeld **Benutzerdefiniert** ist nur bei Vorhandensein eines registrierten Schlüssels verfügbar.

Für die meisten Anwender ist die mittlere Stufe des Antiviren-Schutzes geeignet. Die Auswahl der niedrigsten Sicherheitsstufe ist nicht empfehlenswert.

13.3.2. Maximale Sicherheitsstufe

In der höchsten Sicherheitsstufe für den Antiviren-Schutz wird Kaspersky® Office Guard automatisch die Ausführung aller Makros abbrechen, die einen verdächtigen Befehl auszuführen versuchen (s. Bild 96).

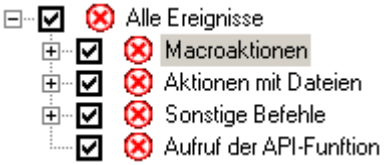


Bild 96.Regelliste für die höchste Sicherheitsstufe
(Symbol – Makroaktion abbrechen)

13.3.3. Mittlere Sicherheitsstufe

In der mittlere Sicherheitsstufe für den Antiviren-Schutz wird Kaspersky® Office Guard die Ausführung der meisten verdächtigen Makrobefehle verbieten und jene Makros vollständig deaktivieren, die versuchen, einen besonders gefährlichen Befehl auszuführen (**Module importieren, Module kopieren, Befehl MacroCopy, Excel-Arbeitsblätter kopieren, Dateien löschen, Anfrage**

vor Speichern der Vorlage Normal abschalten, Virenschutz abschalten (s. Bild 97).

Die mittlere Sicherheitsstufe ist für die meisten Anwender geeignet.

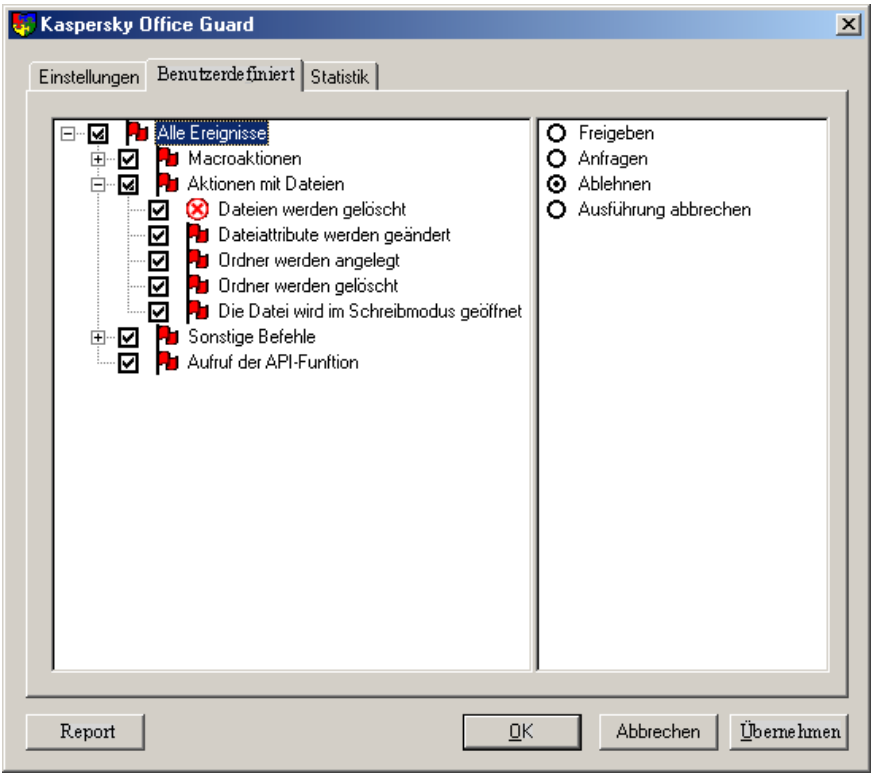


Bild 97. Regelliste für die mittlere Sicherheitsstufe (Symbol – Makro-Ausführung abbrechen; – verdächtigen Makrobefehl verbieten)

13.3.4. Sicherheitsstufe mit Benutzeranfragen

Im Anfragemodus wird Kaspersky® Office Guard für die Ausführung jedes verdächtigen Makrobefehls ihre Erlaubnis einholen (s. Bild 98).

Bild 98. Regeln für die Sicherheitsstufe mit Benutzeranfragen (Symbol – Benutzeranfrage für weiteres Vorgehen)

13.3.5. Minimale Sicherheitsstufe

In der niedrigen Sicherheitsstufe für den Antiviren-Schutz wird Kaspersky® Office Guard die Ausführung aller Makroaktionen, unter Ausnahme sehr gefährlicher, automatisch erlauben. In sehr gefährlichen Fällen wird der Benutzer nach dem weiteren Vorgehen gefragt (s. Bild 99).

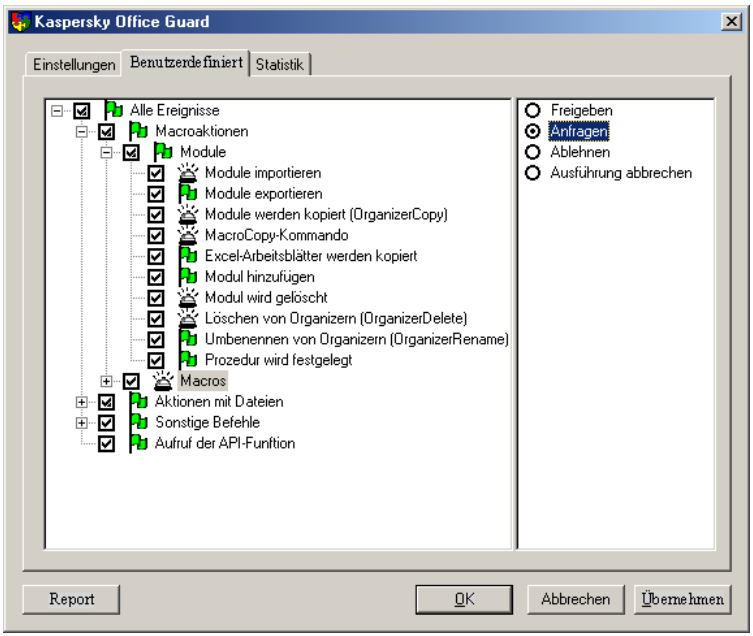


Bild 99. Regelliste für die niedrige Sicherheitsstufe (Symbol – Makroaktion abbrechen, – Freigabe eines verdächtigen Makrobefehls)

13.3.6. Benutzerdefinierte Sicherheitsstufe

In bestimmten Situationen ist es erforderlich, dass der Benutzer die Regeln für verdächtige Befehle selbst konfiguriert.

Beispiel: In Ihrer täglichen Arbeit benutzen Sie ein Makro, das einen verdächtigen Befehl aufruft. Kaspersky® Office Guard fragt Sie regelmäßig, ob der verdächtige Befehl ausgeführt werden soll. Um dies zu verhindern, können Sie die benutzerdefinierte Sicherheitsstufe so konfigurieren, dass die vom Makro ausgeführte verdächtige Aktion als standardmäßig erlaubt wird.

Um die Sicherheitsstufe optimal an Ihre Bedürfnisse anzupassen,

1. Wählen Sie auf der Registerkarte **Einstellungen** den Wert **Benutzerdefiniert** (s. Bild 100).

2. Wechseln Sie auf die Registerkarte **Benutzerdefiniert** und stellen Sie im *Konfigurationsbaum* die Regeln für verdächtige Befehle ein (Details siehe unten).

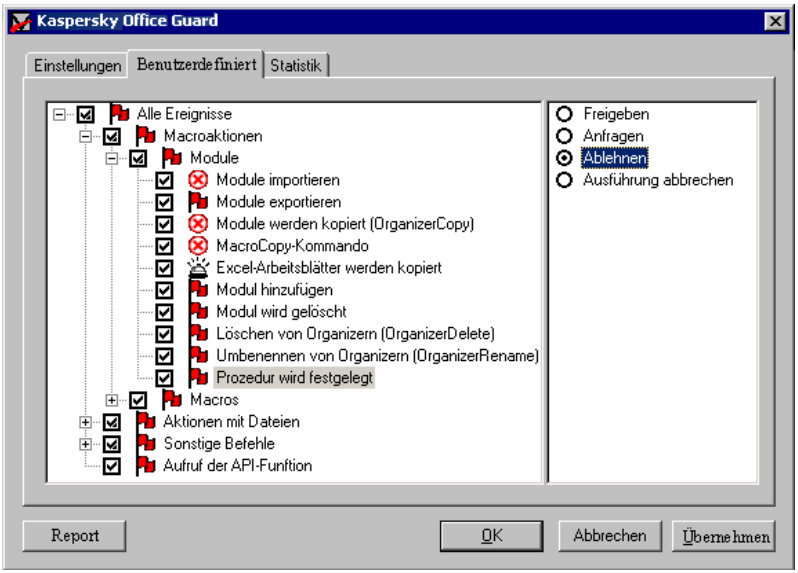


Bild 100. Benutzerdefinierte Einstellungen des Antiviren-Schutzes

Auf der Registerkarte **Benutzerdefiniert** befindet sich ein Konfigurationsbaum. Im linken Feld sind alle verdächtigen Makrobefehle aufgelistet. Jedem Befehl ist ein *Kontrollindikator* und ein Symbol der für ihn gültigen Regel zugeordnet. Im rechten Feld befinden sich eine Gruppe von Optionsfeldern, die zur Auswahl der gewünschten Regel dienen.

Im Konfigurationsbaum können die Kontrollindikator aktiviert und deaktiviert, und die Regeln für Makrobefehle und Gruppen geändert werden.

Abhängig davon, welche Änderungen Sie vornehmen, ändert sich der Konfigurationsbaum unterschiedlich: Makrobefehle können die Gruppenregel erben, individuelle Regeln oder feste eigene Regeln besitzen, d.h. nicht der Vererbungsregel unterliegen.

Um den Zustand des Kontrollindikators eines gewählten Makrobefehls oder einer Gruppe zu ändern,

1. Markieren Sie die gewünschte Zeile im Konfigurationsbaum.

2. Aktivieren / deaktivieren Sie das Kontrollkästchen durch Mausklick, oder drücken Sie die Leertaste, oder wählen Sie im Kontextmenü den Punkt **Aktivieren** bzw. **Deaktivieren**.

Der Kontrollindikator eines Makrobefehls kann verschiedene Zustände aufweisen (s. Pkt. 8.3).

Um eine Regel für einen verdächtigen Makrobefehl oder eine Gruppe festzulegen,

1. Markieren Sie die gewünschte Zeile im Konfigurationsbaum.

2. Legen Sie die Regel fest, die das Programm anwenden soll:

   - **Freigeben** – Ausführung des verdächtigen Makrobefehls erlauben (Wird diese Regel gewählt, erscheint rechts neben dem Kontrollindikator ein "grünes Fähnchen" ).

   - **Anfragen** – Den Benutzer um Erlaubnis für die Ausführung des verdächtigen Makrobefehls fragen (Wird diese Regel gewählt, erscheint rechts neben dem Kontrollindikator ein Klingelsymbol ).

   - **Ablehnen** – Ausführung des verdächtigen Makrobefehls verbieten und zum folgenden Befehl gehen (Wird diese Regel

gewählt, erscheint rechts neben dem Kontrollindikator ein "rotes Fähnchen").

- **Ausführung abbrechen** – Ausführung des Makrobefehls abbrechen (Wird diese Regel gewählt, erscheint rechts neben dem Kontrollindikator das "Verkehrszeichen Halteverbot").

Abhängig davon, ob Sie die Einstellungen für eine ganze Gruppe oder nur für einen einzelnen Befehl ändern, ändert sich der Konfigurationsbaum unterschiedlich.

13.4. Abfangen verdächtiger Makrobefehle

Sofort wenn ein Makro versucht, einen verdächtigen Makrobefehl auszuführen, wird dieser Befehl von Kaspersky® Office Guard abgefangen und entsprechend der für diesen Makrobefehl festgelegten Regel (s. Pkt. 13.3.1) behandelt. Dafür bestehen vier Möglichkeiten: Makrobefehl verbieten und zum nächsten Befehl gehen, Ausführung des Makrobefehls erlauben, Makro abbrechen oder Benutzeranfrage nach dem weiteren Vorgehen.

Wird für einen verdächtigen Befehl die Benutzeranfrage für das weitere Vorgehen festgelegt, erscheint folgendes Dialogfenster auf dem Bildschirm: **Kaspersky® Office Guard – Ausführung freigeben?** (s. Bild 101).

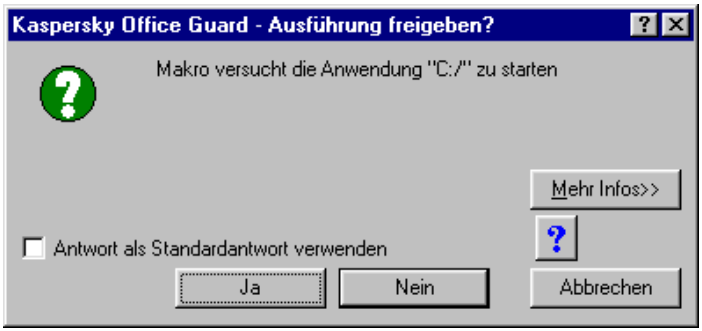


Bild 101. Benutzeranfrage für das weitere Vorgehen

Im oberen Bereich des Dialogfensters befinden sich Informationen über den verdächtigen Befehl, den das Makro auszuführen versucht. Durch Klick auf **Mehr Infos** erhalten Sie ausführliche Informationen über den Befehl. Durch Klick auf

die Schaltfläche  erhalten Sie Informationen über die Gefährlichkeit des Befehls.

Im unteren Bereich des Dialogfensters befinden sich drei Schaltflächen, die zur Auswahl des weiteren Vorgehens dienen:

- ***Ja*** *– Ausführung des verdächtigen Befehls freigeben.*
- ***Nein*** *– Ausführung des verdächtigen Befehls verbieten.*
- ***Abbrechen*** *– Ausführung des verdächtigen Makros abbrechen.*

Damit die Aktion, die Sie durch Klick auf eine der Schaltflächen wählen, in Zukunft für diesen verdächtigen Befehl als Regel gilt, aktivieren Sie das Kontrollkästchen ***Antwort als Standardantwort verwenden.***

Das Kontrollkästchen **Antwort als Standardantwort verwenden** ist mit gültigem Schlüssel verfügbar.

Wenn Sie das Kontrollkästchen **Antwort als Standardantwort verwenden** aktivieren, wird die für den verdächtigen Makrobefehl gewählte Regel im Konfigurationsbaum gespeichert. Die vorgenommenen Änderungen werden im Konfigurationsbaum anschaulich dargestellt.

Besaß ein Makrobefehl die Regel **Anfragen** mit dem Status "feste eigene Regel", so erhält die neue Regel den Status einer gewöhnlichen "selbständigen Regel".

Die Entscheidung darüber, ob eine verdächtige Aktion von einem Makrovirus ausgeführt wird, liegt bei Ihnen. Danach können Sie den Viruscode aus dem Makro entfernen oder das infizierte Makro an den Systemadministrator übergeben. Das Hilfesystem enthält Informationen, die Ihnen bei dieser Entscheidung von Nutzen sein können.

13.5. Protokoll der Arbeitsergebnisse

Mit Hilfe von Kaspersky® Report Viewer können Sie das Protokoll über die Arbeitsergebnisse des Programms einsehen. Dazu klicken Sie im Hauptfenster auf die Schaltfläche **Report**.

Das Arbeitsprotokoll enthält:

- *den Zeitpunkt, zu dem das Makro einen verdächtigen Befehl auszuführen versuchte.*
- *den verdächtigen Befehl*
- *die von Kaspersky® Office Guard ausgeführte Aktion:*
    - Freigeben – wenn die verdächtige Aktion erlaubt wurde.
    - Ablehnen – wenn die verdächtige Aktion übersprungen wurde.
    - Abbrechen – wenn das Makro abgebrochen wurde.

Die Statistik der Arbeitsergebnisse befindet sich im Hauptfenster von Kaspersky® Office Guard auf der Registerkarte **Statistik** (s. Bild 102).

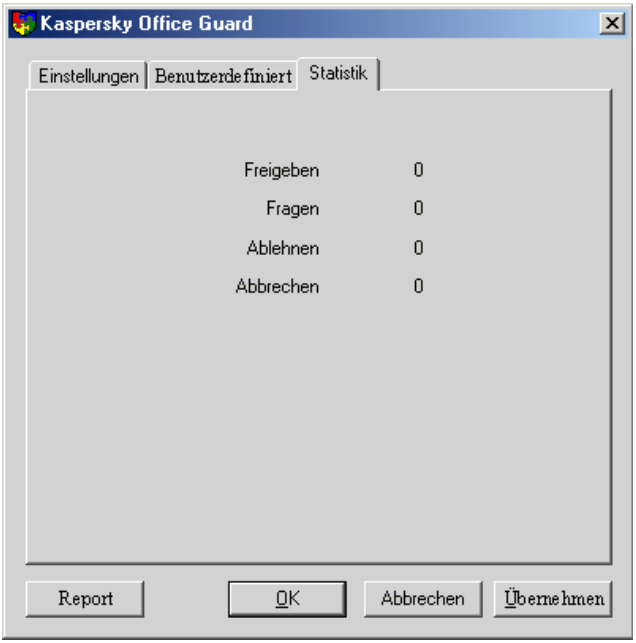


Bild 102. Registerkarte **Statistik**

KAPITEL 14. KASPERSKY® INSPECTOR

Kaspersky® Inspector ist ein Antiviren-Programm zur Überwachung von Laufwerken, das für die Betriebssysteme Microsoft Windows 95 OSR2/98/ME® und Microsoft Windows NT/2000® bestimmt ist.

Kaspersky® Inspector untersucht Laufwerke auf Veränderungen von Datei- und Ordnerinhalten. Das Programm kann sowohl als zusätzlicher Antiviren-Schutz, als auch zur Kontrolle von Laufwerkmodifikationen eingesetzt werden.

Mit diesem Programm können Sie die für die Untersuchung von Laufwerken mit dem Kaspersky Anti-Virus® Scanner benötigte Zeit erheblich verkürzen, da Kaspersky® Inspector nach Abschluss der Laufwerküberprüfung nur noch neue und geänderte Dateien an den Kaspersky AV Scanner zum Scannen weiterleitet.

Die Funktion von Kaspersky® Inspector basiert auf der Speicherung von Basisdaten über ein Laufwerk in einer Tabelle. Diese Tabelle enthält ein Muster des Master-Bootsektor und der Bootsektoren, eine Liste der Nummern von fehlerhaften Clustern, die Struktur des Stammverzeichnisses sowie Informationen über alle zu kontrollierenden Dateien.

Kaspersky® Inspector greift über den IOS (Input-Output Supervisor) unmittelbar auf die Laufwerksektoren zu und verwendet nicht die konventionellen Methoden (Interrupts von INT 21h und INT 13h). Dadurch können aktiv getarnte Viren erfolgreich aufgespürt werden, die sich im Arbeitsspeicher befinden und die Bearbeitung dieser (für einen Computer) lebenswichtigen Interrupts übernommen haben.

Ferner speichert Kaspersky® Inspector die verfügbare DOS-Kapazität des Arbeitsspeichers und überprüft bei jedem Neustart, ob diese sich verändert hat (was meistens bei einer Infektion durch Bootviren der Fall ist), sowie die Anzahl der installierten Laufwerke.

Kaspersky® Inspector bietet folgende Spezialfunktionen:

- Direkter Zugriff auf Laufwerke über den IOS-Treiber (Eingabe/Ausgabe-Supervisor), wobei DOS-residente Viren (darunter Bootviren, die beim Start des Computers den 13h-Interrupt übernommen haben) umgangen werden.

- Möglichkeit zur Wiederherstellung der Bootsektoren von Laufwerken.
- Möglichkeit zur Überprüfung komprimierter Laufwerke.
- Möglichkeit zur Überprüfung von Dateisystemen (FAT12, FAT16, VFAT32, NTFS) ohne Aufruf von Betriebssystemsfunktionen, die zum Verwalten von Dateien verwendet werden.
- Analyse von veränderten Dateien hinsichtlich der Länge.
- Arbeit mit OLE2-Dokumenten (Word-Dokumente, Excel-Arbeitsmappen und Access-Datenbanken).
- Möglichkeit zur Wiederherstellung der ausführbaren Dateien von DOS und Windows 95 OSR2/98/NT mit Hilfe des Reparaturmoduls KAVI Cure Module.
- Möglichkeit zur Suche nach aktiven Stealth-Viren.

14.1. Besonderheiten des Einsatzes von Kaspersky® Inspector in MS Windows NT

Auf Grund der besonderen Architektur von Microsoft Windows NT® werden folgende Elemente nicht von Kaspersky® Inspector überprüft:

- *Debug-Register*
- *Umfang des verfügbaren DOS-Speichers*

Alle anderen Programmfunktionen stehen beim Einsatz unter Microsoft Windows in vollem Umfang zur Verfügung.

14.2. Funktionsweise von Kaspersky® Inspector

Antiviren-Revisoren verfügen über einen einheitlichen Suchalgorithmus für Veränderungen. Bei der Überprüfung führen sie folgende Operationen aus:

- *Berechnung von Kontrollsummen (CRC-Summen) für Laufwerksektoren und Dateien.*
- *Speichern von CRC-Summen in einer speziellen Datenbank (Tabelle).*
- *Bei nachfolgenden Überprüfungen werden die tatsächlichen (neuen) CRC-Summen mit den früheren, in der Datenbank gespeicherten Werten verglichen.*

In der Datenbank werden außerdem zusätzliche Angaben über Dateien gespeichert – deren Längen, Zeitpunkt der Erstellung und letzten Änderung, Attribute und Daten, die zur Wiederherstellung veränderter (infizierter) Dateien erforderlich sind. Zudem werden in der Datenbank Muster Festplatten-Bootsektoren (Master-Boot und Boot), eine Liste der Nummern von fehlerhaften Clustern, die Struktur des Stammverzeichnisses sowie weitere Informationen über alle Kontrollobjekte gespeichert.

Ferner speichert Kaspersky® Inspector Informationen über das Betriebssystem und die installierte Hardware, wie z.B. Kapazität des Arbeitsspeichers (Überprüfung auf Infektion durch Bootviren) und Anzahl der installierten Festplatten, um diese Daten bei jedem Neustart zu prüfen.

Während der Überprüfung greift Kaspersky® Inspector über den IOS unmittelbar auf die Laufwerksektoren zu und verwendet nicht die konventionellen Methoden (Interrupts von INT 21h und INT 13h). Dank dieser Sonderfunktion kann Kaspersky® Inspector sogenannte Stealth-Viren (unsichtbare Viren) (siehe Pkt. 14.2.3) erfolgreich erkennen und entfernen.

14.2.1. Untersuchungen, die von Kaspersky® Inspector vorgenommen werden

Beim ersten Start speichert Kaspersky AV die Kapazität des DOS-Arbeitsspeichers, die Adresse der INT 13h-Routine und erstellt Tabellen für die zu überprüfenden Laufwerke.

Bei jedem folgenden Neustart überprüft Kaspersky® Inspector folgende Elemente:

- *Kapazität des DOS-Arbeitsspeichers und Adresse der INT 13h-Routine.*
- *Bootsektoren (Master-Boot und Boot). Der Master-Bootsektor wird bei Überprüfung aller logischen Laufwerke untersucht. Wird eine Differenz zwischen der gespeicherten Kopie und den ermittelten Daten festgestellt, besteht die Möglichkeit, den modifizierten Sektor wiederherzustellen. Außerdem können Sie mit dem integrierten Viewer die Daten vor und nach der Überprüfung vergleichen.*
- *Liste der Nummern fehlerhafter Cluster. Bestimmte Viren markieren gute Cluster als beschädigt und legen in diesen ihren Code und Daten ab. Bei Auftauchen eines neuen fehlerhaften Cluster werden Sie von Kaspersky® Inspector darüber informiert.*
- *Verzeichnistabelle des Datenträgers. Es wird nach neuen und gelöschten Ordnern gesucht.*
- *Dateistruktur der Laufwerke. Es wird nach neuen, gelöschten, umbenannten, verschobenen und geänderten Dateien gesucht. Geprüft wird auch, ob Länge, Erstellungsdatum und Erstellungszeit der Dateien sowie deren Kontrollsummen geändert wurden.*

Die bei der Überprüfung festgestellten Veränderungen werden analysiert. Weisen die Veränderungen nicht auf die Existenz eines Virus hin (z.B. die Änderungen der Dateilänge entsprechen der Änderung von Datum und Uhrzeit des Speicherns), dann informiert Kaspersky® Inspector lediglich über alle festgestellten Modifikationen. Bei "verdächtigen" Veränderungen (die auf Virusaktivitäten hinweisen), warnt Kaspersky® Inspector vor einer möglichen Virus-Infektion.

14.2.2. Analyse von Laufwerkmodifikationen

Alle registrierten Veränderungen von Dateien und Sektoren auf Laufwerken werden analysiert und in zwei Kategorien unterteilt: "harmlose" und "verdächtige". Zu den "harmlosen" zählen beispielsweise Veränderungen von Datei-Inhalten, wenn dabei Datum und Uhrzeit der Dateierstellung geändert wurden.

In jedem Fall stellt Kaspersky® Inspector ausführliche Informationen über alle Modifikationen bereit. Die Informationen werden in einem Dialogfenster angezeigt. Zudem speichert er eine Liste der Laufwerkveränderungen als Textdatei. Treten "verdächtige" Veränderungen auf, werden Sie von Kaspersky® Inspector vor einer möglichen Virus-Infektion gewarnt.

Zu den "**verdächtigen**" Veränderungen gehören:

- *Veränderung des Inhalts einer Datei ohne Änderung des Datums und der Uhrzeit der letzten Modifikation (typisch für die meisten Datei-Viren).*
- *Veränderung der Dateilängen verschiedener Dateien um einen ähnlichen Wert.*
- *falsches Datum oder Uhrzeit der letzten Dateimodifikation: Tag liegt über 31, Monat über 12 oder Jahr über dem laufenden, Minuten liegen über 59, Stunden über 23 oder Sekunden über 59 (mit diesen Techniken "markieren" einige Viren infizierte Dateien).*
- *Veränderung einer Datei, deren Name in der Liste als schreibgeschützt angegeben ist.*
- *für Viren charakteristische Veränderungen, die den DOS-Kern infizieren (Dateien IO.SYS, IBMBIO.BIN…).*

Lassen Sie Meldungen von Kaspersky® Inspector über Laufwerkveränderungen niemals unbeachtet (insbesondere Hinweise auf "verdächtige" Modifikationen). Ist der Grund von Änderungen unbekannt, dann versuchen Sie ihn festzustellen.

Sollten die Meldungen des Programms technische Informationen beinhalten, die Ihnen unverständlich sind, wenden Sie sich bitte an einen Fachmann oder an den technischen Kundenservice von Kaspersky Lab, aber lassen Sie solche Meldungen niemals unbeachtet.

Werden diese Empfehlungen nicht beachtet, kann es zu einer Infektion Ihres Rechners kommen, was die Wahrscheinlichkeit eines Datenverlustes auf dem betroffenen Laufwerk erhöht.

14.2.3. Suche nach aktiven Stealth-Viren

Mit dem Begriff "Stealth" (stealth – unsichtbar) werden Viren bezeichnet, die auf bestimmte Art und Weise ihre Anwesenheit im System tarnen. Hierzu fangen sie System-Interrupts ab, bearbeiten Zugriffe auf infizierte Objekte und verändern so obligatorische Datenblöcke, damit die Dateien und Sektoren des infizierten Systems wie virusfrei aussehen. Es gibt Viren, die verschiedene Techniken verwenden, um sich im System zu verstecken, wobei diese Methoden oft recht kompliziert sein können. Hierbei ist anzumerken, dass es Stealth-Viren aller Art gibt: Datei-, Boot- und sogar Makroviren können Stealth-Funktionen enthalten. Ausführliche Informationen über Stealth-Viren finden Sie in der "Virenenzyklopädie" (http://www.viruslist.com).

Verwendet ein Virus verschiedene Techniken, um seinen Code zu tarnen, ist es unmöglich, ihn mit gewöhnlichen Methoden zu erkennen: Beim Öffnen oder Lesen einer infizierten Datei werden nur normale Daten gelesen, wobei der Viruscode unbemerkt bleibt. Um solche Viren zu finden, verwenden Antiviren-Programme verschiedene Anti-Stealth-Techniken (z.B. direktes Lesen der Daten vom Laufwerk).

Kaspersky® Inspector setzt die zuverlässigsten Methoden ein, mit denen sowohl bekannte als auch neue Stealth-Viren sicher erkannt werden können.

Es ist anzumerken, dass die Fähigkeit zur Tarnung zugleich einen Schwachstelle der Stealth-Viren darstellt, auf deren Grund sich die Existenz von Viren im Computer mit einem komplizierten, aber praktisch störungsfreien Verfahren feststellen lässt. Um einen Stealth-Virus im System zu finden, reicht es aus, den Inhalt des Bootsektors und/oder der verdächtigen Dateien mit zwei verschiedenen Methoden zu lesen und danach die Resultate zu vergleichen.

Der erste Lesevorgang erfolgt mit den für das jeweilige Betriebssystem üblichen Methoden. Beim zweiten Lesevorgang wird "direkt" gelesen, wobei das Betriebssystem umgangen wird.

Hält sich ein Stealth-Virus im System auf, so werden sich die mit der ersten Methode über ein infiziertes Objekt eingelesenen Informationen von den Ergebnissen beim Lesen mit dem zweiten Verfahren unterscheiden, da ein Stealth-Virus standardmäßige Zugriffe abfängt und virusfreie Daten vortäuscht. Auf dieser Tatsache beruht der Vergleichsalgorithmus, der in Kaspersky®

Inspector realisiert wurde. Zur Aktivierung der Suche nach aktiven Stealth-Viren s. Pkt. 14.5.2.5.

14.2.4. Löschen von Viren mit dem Reparaturmodul (KAVI Cure Module®)

KAVI Cure Module® (KAVIC) ist ein in KAVI integriertes Programmmodul (*cure.dll*), mit dem Computerviren ohne Verwendung von Antiviren-Datenbanken gelöscht werden können.

KAVIC unterscheidet sich prinzipiell dadurch von Antiviren-Scannern (KAV®), dass es über bestimmte Informationen einer zu schützenden Datei verfügt und keine Kenntnisse von konkreten Viren besitzt. Interne Tests bei Kaspersky Labs haben gezeigt, dass KAVIC in 96 % der Fälle Dateien wiederherstellt (diese Statistik kann nicht als Axiom betrachtet werden, da die Ergebnisse der Wiederherstellung von einer Vielzahl externer Faktoren abhängig sind). So wird Ihnen KAVIC helfen, die meisten Viren zu entfernen, unabhängig davon, ob diese bekannt sind oder nicht.

Kaspersky® Inspector teilt während seiner Arbeit dem KAVIC-Modul mit, welche Dateien verändert wurden und ob seit dem letzten Start Dateien angelegt oder gelöscht wurden. KAVIC sammelt seinerseits die notwendigen Informationen zur Dateiwiederherstellung.

Die aktuelle Version von KAVIC unterstützt die Option zur Wiederherstellung (Desinfektion) von DOS- und Windows-Dateien (Dateien mit den Erweiterungen EXE, COM, SYS, PRG, DLL, SCR, OCX…).

14.2.5. Überprüfung der Einstellungen des Betriebssystems bei dessen Start (Treiber *KAVIBOOT.VXD*)

Der ***Treiber KAVIBOOT.VXD*** dient der Überprüfung von bestimmter charakteristischer Eigenschaften des Betriebssystems (Windows 95 OSR2/98), wenn dieses geladen wird. Dieser Treiber prüft:

- *die verfügbare DOS-Speicherkapazität*
- *Master-Bootsektor (MBR)*
- *Adressen der INT 13h-Routine (Lesen/Schreiben auf die Festplatte)*

Dadurch kann eine Infektion durch Bootviren erkannt werden.

Bei allen Lese-Operationen der Sektoren wird unmittelbar auf das BIOS zugegriffen. DOS-Routinen werden dabei umgangen. Außerdem ist in dem Treiber ein Mechanismus zum Schutz der vom Laufwerk gelesenen Daten vor Virenangriffen integriert.

Das im Treiber verwendete System zum Schutz vor Virenangriffen kann in sehr seltenen Fällen während des Lesevorgangs zum Absturz des Treibers führen. Um solche Situationen auszuschließen, wird beim ersten Start des Treibers automatisch ein Absturz-Test durchgeführt.

Sollte Ihr Rechner beim ersten Start nach der Programminstallation abstürzen, genügt es, den Computer einfach neu zu starten. In diesem Fall wird der Treiber feststellen, das nach nicht ordnungsgemäßem Herunterfahren ein Neustart vorgenommen wurde, und im weiteren diese Prozeduren nicht mehr verwenden.

14.3. Benutzeroberfläche von Kaspersky® Inspector

14.3.1. Hauptfenster

Wird Kaspersky® Inspector ohne Befehlszeilenparameter gestartet (s. Pkt.14.4.), dann erscheint das Programm-Hauptfenster auf dem Bildschirm (s. Bild 103).

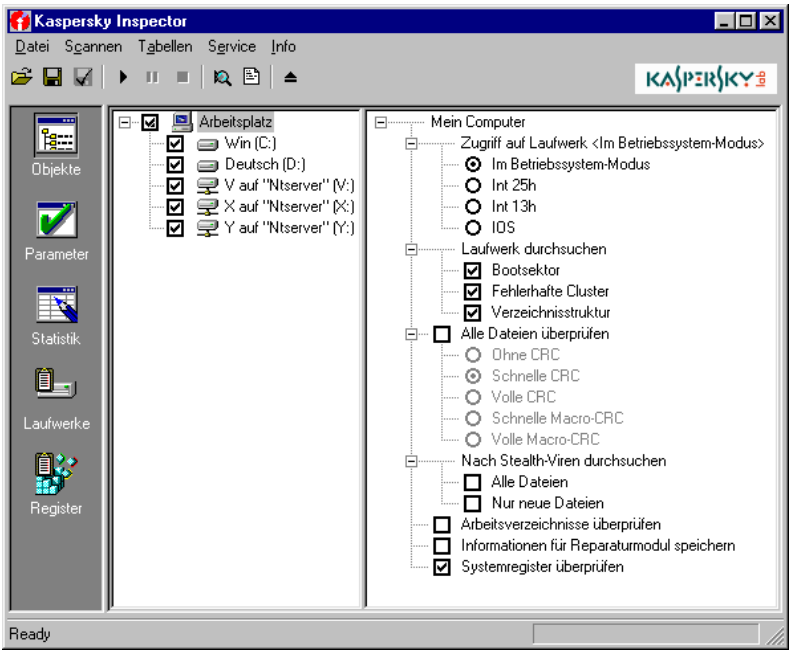


Bild 103. Hauptfenster des Programms Kaspersky® Inspector

Das Hauptfenster enthält folgende Elemente: Menüzeile (s. Pkt. 14.3.2), Symbolleiste (s. Pkt. 14.3.3), Kategorienleiste (s. Pkt. 14.3.4), Arbeitsbereich (s. Pkt. 14.3.5) und Statuszeile (s. Pkt. 14.3.6).

14.3.2. Menü

Direkt unter der Titelzeile des Hauptfensters befindet sich die Menüleiste (siehe Bild 104).

Bild 104. Menüleiste

Alle während der Arbeit mit Kaspersky® Inspector verfügbaren Befehle können durch Auswahl des entsprechenden Menüpunktes aufgerufen werden. Die Menübefehle werden in Tabelle 1 beschrieben.

Tabelle 1. Menübefehle

Menü	Menübefehl	Beschreibung
Datei	**Profil als Standard speichern**	Speichert das aktuelle Profil als Standard.
	Profil laden	Lädt ein früher gespeichertes Profil (s. Pkt. 14.5.3).
	Profil speichern	Speichert die gewählten Einstellungen als Profil (s. Pkt. 14.5.3).
	Profil speichern unter	Speichert das aktuelle Profil unter einem neuen Namen.
	Beenden	Beendet das Programm.
Scannen	**Beginnen**	Startet den Überprüfungsvorgang (s. Pkt. 14.4.4).
	Beenden	Bricht den Überprüfungsvorgang ab.
	Anhalten	Hält den Überprüfungsvorgang vorübergehend an.
Tabellen	**Registrierungstabelle erstellen**	Erstellt neue Registrierungstabelle (s. Pkt. 14.4.4.2).
	Laufwerktabellen erstellen	Erstellt neue Laufwerktabelle (s. Pkt. 14.4.4.2).
Service	**Bericht zeigen**	Auf dem Bildschirm erscheint das Protokoll der letzten Überprüfung.
Info	**Inhalt**	Öffnet das Hilfesystem.
	Über das Programm	Öffnet das Fenster mit Angaben zu Hersteller, Versionsnummer des Programms und Ihren Registrierungsdaten.

14.3.3. Symbolleiste

Unter der Menüleiste befindet sich die Symbolleiste (s. Bild 105). Diese enthält Schaltflächen für bei der Arbeit mit dem Programm häufig gebrauchte Befehle.

Bild 105. Symbolleiste

Die meisten Schaltflächen der Symbolleiste sind auch als Menüpunkte vorhanden (s. Pkt. 14.3.2). Wenn Sie den Mauszeiger auf ein Symbol führen, erscheint ein Infotext mit der Bezeichnung der Schalfläche.

Eine Beschreibung der Menüpunkte finden Sie in Tabelle 2.

Tabelle 2. Schaltflächen der Symbolleiste

Schaltfläche und Bezeichnung	**Menübefehl**	**Funktion**
 Profil laden	Befehl **Profil laden** (Menü **Datei**)	Lädt ein früher gespeichertes Profil (s. Pkt. 14.5.3).
 Profil speichern	Befehl **Profil speichern** (Menü **Datei**)	Speichert die gewählten Einstellungen als Profil (s. Pkt. 14.5.3)
 Profil als Standard speichern	Befehl **Profil als Standard speichern** (Menü **Datei**)	Speichert das aktuelle Profil als Standard

Schaltfläche und Bezeichnung	Menübefehl	Funktion
 Scanvorgang beginnen	Befehl **Scanvorgang beginnen** (Menü **Scannen**)	Startet den Überprüfungsvorgang (s. Pkt. 14.4.4)
 Anhalten	Befehl **Anhalten** (Menü **Scannen**)	Hält den Überprüfungsvorgang an
 Beenden	Befehl **Beenden** (Menü **Scannen**)	Bricht den Überprüfungsvorgang ab
 Scan-Vorschau		Zeigt die aktuellen Einstellungen für die Objektüberprüfung an
 Bericht zeigen	Befehl **Bericht zeigen** (Menü **Service**)	Startet Kaspersky® Report Viewer, der zum Lieferumfang des Softwarepakets gehört
 Beenden	Befehl **Beenden** (Menü **Datei**)	Beendet das Programm

14.3.4. Kategorienleiste

Auf der linken Seite des Hauptfensters befindet sich die Kategorienleiste.

Diese enthält fünf Schaltflächen, von denen jede einer bestimmten Parameterkategorie entspricht (s. Tabelle 3.). Um zu einer gewünschten Kategorie zu gelangen, klicken Sie auf die entsprechende Schaltfläche.

Durch Rechtsklick auf eine beliebige Stelle der Kategorienleiste kann das Kontextmenü dieser Leiste geöffnet werden, das zwei Punkte enthält:

- ***Kleine Symbole*** – *Kleine Kategoriensymbole anzeigen.*
- ***Große Symbole*** – *Große Kategoriensymbole anzeigen.*

Tabelle 3. Kategorien

Kategorie	Beschreibung
	Hier werden Scanbereich, zu scannende Objekte und Regeln für die Behandlung von infizierten Objekten festgelegt. Alle Einstellungen sind in dem speziellen Bedienungselement, dem *Konfigurationsbaum der Objekthierarchie* organisiert (s. Pkt. 14.5.2)
	Hier werden generelle Untersuchungseinstellungen vorgenommen, die für alle zu überprüfenden Objekte gelten, sowie Einstellungen für die Kooperation von Kaspersky® Inspector mit anderen zum Paket Kaspersky Anti-Virus® Personal Pro gehörenden Modulen (KAVI Cure Module und KAV32). Außerdem können hier die Einstellungen für das Protokoll festgelegt werden (s. Pkt. 14.5.1).
	Hier werden die Suchergebnisse in Tabellenform dargestellt (s. Pkt. 14.6.1).
	Hier werden die vollständigen Ergebnisse der Objektuntersuchung angezeigt und notwendige Änderungen vorgenommen (s. Pkt. 14.6.2–14.6.5).
	Hier werden die vollständigen Ergebnisse der Registrierungsüberprüfung angezeigt und notwendige Änderungen vorgenommen (s. Pkt. 14.6.6).

14.3.5. Arbeitsbereich

Den größten Teil des Hauptfensters nimmt der Arbeitsbereich ein. Das Aussehen des Arbeitsbereichs hängt von der gewählten Kategorie ab.

14.3.6. Statuszeile

Im unteren Bereich des Hauptfensters befindet sich die Statuszeile.

In der Statuszeile wird der aktuelle Status des Programms angezeigt. Während des Untersuchungsvorgangs erscheinen hier die Namen der überprüften Dateien.

14.4. Start von Kaspersky® Inspector

14.4.1. Start aus dem Start-Menü von MS Windows

Kaspersky® Inspector kann aus dem **Start**-Menü von MS Windows gestartet werden. Dazu werden nach Klick auf die Schaltfläche **Start** nacheinander folgende Punkte gewählt:

Programme→Kaspersky Anti-Virus→Kaspersky Inspector.

14.4.2. Start von Kaspersky® Inspector aus Kaspersky AV Control Centre

Wie alle zum Softwarepaket Kaspersky Anti-Virus® Personal Pro gehörenden Anwendungen kann auch Kaspersky® Inspector von Kaspersky Anti-Virus® Control Centre aus gestartet werden. In Control Centre kann für Kaspersky® Inspector der automatische Start täglich zu einem bestimmten Zeitpunkt oder in bestimmten Zeitabständen festgelegt werden.

14.4.3. Erster Start des Programms

Beim ersten Start bietet Kaspersky® Inspector an, für alle zu überprüfenden Objekte (s. Pkt. 14.5.2) Tabellen zu erstellen (s. Bild 106). Diese Tabellen sind für die Arbeit von Kaspersky® Inspector erforderlich. Werden keine Tabellen angelegt, kann Kaspersky® Inspector die Laufwerke nicht auf Veränderungen überprüfen.

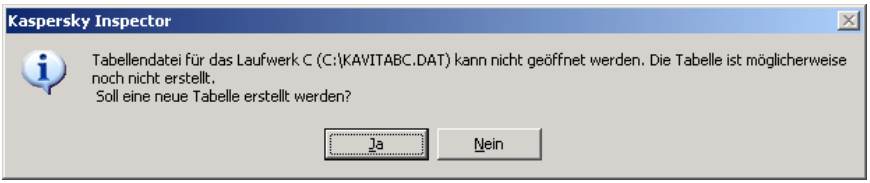


Bild 106. Anfrage auf Tabellenerstellung

Klicken Sie auf **Ja**, damit Kaspersky® Inspector die Tabellen automatisch erstellt. Danach ist Kaspersky® Inspector bei jedem weiteren Neustart in vollem Umfang einsatzbereit.

14.4.4. Start der Untersuchung auf Laufwerkveränderungen

14.4.4.1. Untersuchung eines Laufwerks auf Veränderungen

Wurde beim Starten von Kaspersky® Inspector aus Kaspersky AV Control Centre angegeben, das Programm ein Mal täglich zu starten, oder wird das Programm mit einem entsprechenden Parameter aus der Befehlszeile gestartet, so wird Kaspersky® Inspector jeden Tag beim ersten Start des Betriebssystems automatisch gestartet und überprüft die Laufwerke auf Veränderungen (s. Pkt. 14.2.1).

Sollte zu einem anderen Zeitpunkt eine Überprüfung von Laufwerken erforderlich sein, klicken Sie in der Symbolleiste des Hauptfensters auf die Schaltfläche  .

Dadurch wird die Überprüfung der Objekte gestartet, die in den entsprechenden Einstellungen angegeben wurden (s. Pkt. 14.5.2).

14.4.4.2. Erstellen neuer Tabellen

In bestimmten Fällen (z.B. wenn auf dem Rechner ein neues Laufwerk installiert wurde oder bereits angelegte Laufwerktabellen aus irgendeinem Grund beschädigt oder gelöscht wurden) ist das Erstellen neuer Tabellen notwendig.

Um neue Tabellen für ein bzw. mehrere Laufwerke zu erstellen, markieren Sie zunächst das gewünschte Laufwerk bzw. die Laufwerke (durch Klick mit der linken Maustaste auf das entsprechende Piktogramm) (s. Pkt. 14.5.2) und wählen dann einen der folgenden Punkte aus dem Menü **Tabellen**:

Registrierungstabelle erstellen – Zum Erstellen neuer Registrierungstabellen. Dabei erscheint auf dem Bildschirm ein Dialogfenster (s. Bild 107). Klicken Sie auf **Ja**, um das Erstellen neuer Tabellen zu bestätigen. Danach werden neue Registrierungstabellen erstellt.

Laufwerktabellen erstellen – Zum Erstellen neuer Laufwerktabellen. Dabei erscheint auf dem Bildschirm ein Dialogfenster (s. Bild 108). Klicken Sie auf **Ja**, um das Erstellen einer neuen Tabelle zu bestätigen. Danach wird die Prozedur zum Erstellen der neuen Tabelle gestartet. Dies nimmt einige Zeit in Anspruch.

Bild 107. Abfrage auf Erstellen einer neuen Registrierungstabelle

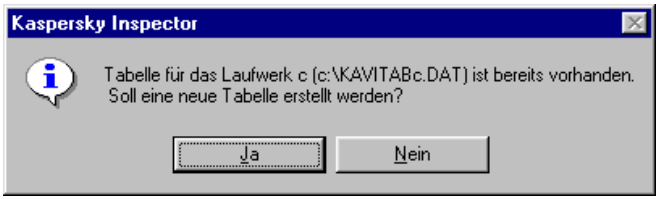


Bild 108. Abfrage auf Erstellen einer neuen Laufwerktabelle

14.4.5. Start der Suche nach Stealth-Viren

Um die Suche nach Stealth-Viren für ein oder mehrere Objekte zu starten (s. Pkt. 14.5.2), aktivieren Sie das gewünschte Kontrollkästchen im entsprechenden Konfigurationsabschnitt (s. Pkt. 14.5.2.5) und klicken Sie in der Symbolleiste des Programmhauptfensters auf die Schaltfläche  .

Beim Scannen eines Laufwerks untersucht Kaspersky® Inspector die Bootsektoren (Master-Bootsektor und Bootsektoren logischer Laufwerke) und vergleicht die Längen und Kontrollsummen der Dateien, die vom Betriebssystem ermittelt werden mit deren Ist-Werten, die auf Basis der Ergebnisse des Direktzugriffs auf das Laufwerk berechnet werden. Stimmen die Leseergebnisse nicht überein, bricht Kaspersky® Inspector den Scanvorgang sofort ab, damit ein Virus keine anderen Dateien und Sektoren infizieren kann, und auf dem Bildschirm erscheint eine Warnmeldung.

14.5. Konfiguration der Programmparameter

14.5.1. Generelle Untersuchungseinstellungen

Um für Kaspersky® Inspector generelle Einstellungen vorzunehmen, klicken Sie in der Kategorienleiste (s. Pkt. 14.3.4) auf das Symbol 

. Im Arbeitsbereich des Programmfensters erscheint dann der Baum für generelle Einstellungen (s. Bild 109).

Bild 109. Baum für generelle Einstellungen von Kaspersky® Inspector

Zur bequemen Konfiguration ist das Programm mit einem Assistenten für die generellen Einstellungen ausgestattet. Mit Hilfe des Assistenten können nur die Grundeinstellungen der Programmfunktionen festgelegt werden. Die übrigen Einstellungen werden unmittelbar im Arbeitsbereich des Programmfensters vorgenommen.

Um das Programm mit Hilfe des Assistenten zu konfigurieren,

1. Klicken Sie auf die Schaltfläche **Assistent**, die sich in der oberen rechten Ecke des Programmfensters befindet.

2. Auf dem Bildschirm erscheint das Dialogfenster **Suchmodus** (s. Bild 110). Hier wird der Überprüfungsmodus festgelegt. Klicken Sie nach der Auswahl auf die Schaltfläche **Weiter**.

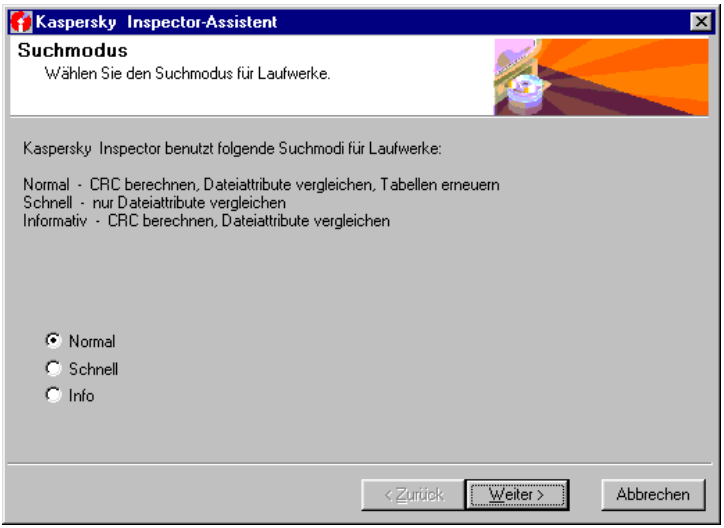


Bild 110. Dialogfenster **Suchmodus**

3. Auf dem Bildschirm erscheint das Dialogfenster **Dateitypen** (s. Bild 111), das der Überprüfung und Redaktion einer Liste mit den Erweiterungen der von KAV Inspector zu kontrollierenden Dateien dient.

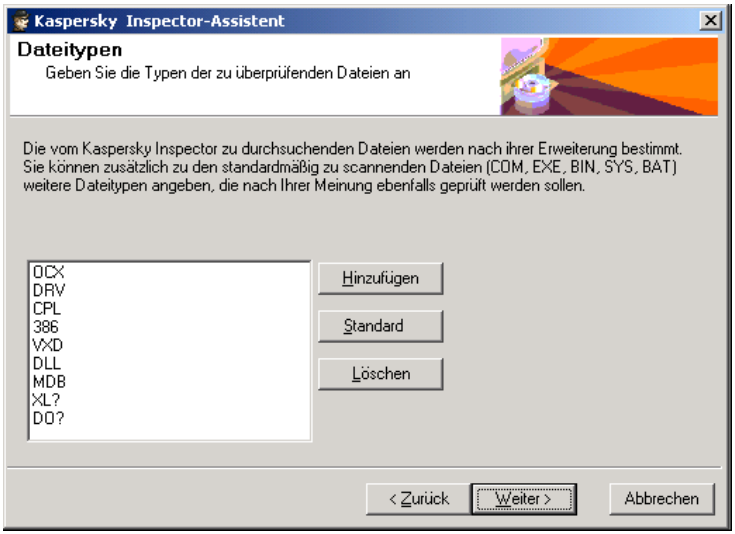


Bild 111. Dialogfenster **Dateitypen**

- *Um der Liste einen neuen Wert hinzuzufügen, klicken Sie auf **Hinzufügen**. Danach erscheint auf dem Bildschirm das Dialogfenster **Erweiterung hinzufügen** (s. Bild 112). Geben Sie im Feld **Erweiterung** den gewünschten Wert ein, wählen Sie im Feld **CRC-Typ** aus der Dropdown-Liste einen Algorithmus zur Berechnung der Kontrollsumme für die betreffende Erweiterung aus und klicken Sie auf **Hinzufügen**.*

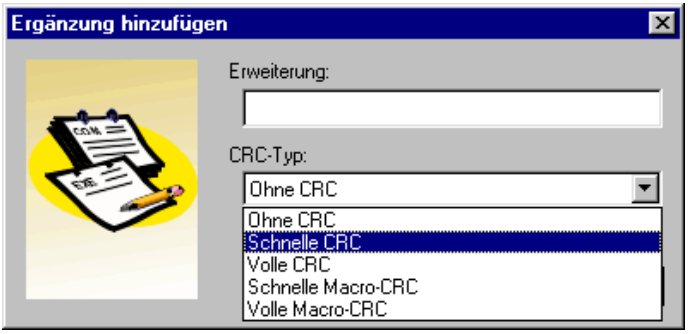


Bild 112. Dialogfenster **Erweiterung hinzufügen**

Bei Eingabe der Erweiterung können Sie den Platzhalter **?** verwenden. Geben Sie z.B. die Erweiterung **OV?** ein, werden alle Dateien überprüft, deren Erweiterung mit OV beginnt (OVL, OVR, …).

- *Zum Löschen von bereits angegebenen Erweiterungen markieren Sie diese per Mausklick in der Liste und klicken auf **Löschen**.*

4. Klicken Sie auf **Weiter**. Danach erscheint auf dem Bildschirm das Dialogfenster **Interaktion mit Kaspersky AV Scanner** (s. Bild 113), in das die Informationen eingegeben werden, die Kaspersky® Inspector für die Kooperation mit dem Antiviren-Scanner benötigt. In diesem Fenster befinden sich folgende Eingabefelder:

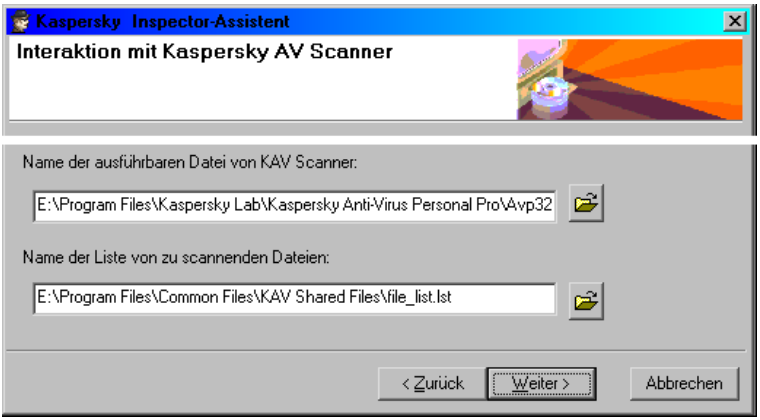


Bild 113. Dialogfenster **Interaktion mit KAV Scanner**

- **Name der ausführbaren Datei von KAV Scanner** – Geben Sie hier den Pfad der ausführbaren Datei KAV32 an. Klicken Sie dazu auf die Schaltfläche rechts des Feldes und geben Sie im folgenden Dialogfenster den Pfad dieser Datei an.

- **Name der Liste von zu scannenden Dateien** – Geben Sie hier den Pfad der Datei an, in der KAV Inspector die Liste der gefundenen veränderten Dateien speichern soll. Klicken Sie hierzu auf die Schaltfläche rechts des Feldes und geben Sie im folgenden Dialogfenster den Pfad der Datei an.

5. Klicken Sie auf **Weiter**. Auf dem Bildschirm erscheint das Dialogfenster **Report** (s. Bild 114). Geben Sie in diesem Dialogfenster in der Zeile **Name der Reportdatei** den Pfad der Datei an, in der die Berichte über die Scanergebnisse gespeichert werden sollen. Klicken Sie hierzu auf die Schaltfläche rechts des Feldes und geben Sie im folgenden Dialogfenster den Pfad dieser Datei an.

6. Klicken Sie nach dem Abschluss der Konfiguration auf die Schaltfläche **Fertig**.

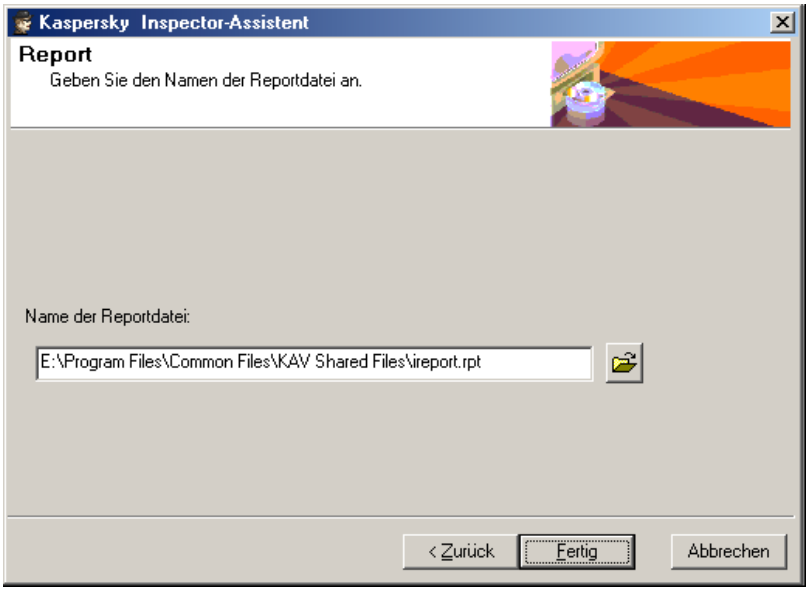


Bild 114. Dialogfenster **Report**

14.5.2. Einstellungen für die Überprüfung von Objekten

14.5.2.1. Einstellungen für die Überprüfung von Festplatten und logischen Laufwerken

Zur Konfiguration der Parameter für die Laufwerküberprüfung klicken Sie in der Kategorienleiste (s. Pkt. 14.3.4) auf das Symbol 

. Daraufhin teilt sich das Programmfenster in zwei Hälften (s. Bild 115).

Auf der linken Seite wird die Liste der überprüfbaren Laufwerke angezeigt. Auf der rechten Seite befindet sich ein Konfigurationsbaum.

Wird das Kontrollkästchen ☑ neben dem jeweiligen Laufwerk aktiviert, so wird dieses Laufwerk von Kaspersky® Inspector überprüft.

Für jedes Laufwerk können individuelle Einstellungen vorgenommen werden.

Welche Einstellungen verfügbar sind, hängt vom jeweiligen Objekttyp ab. Objekte, die verschiedenen Hierarchieebenen angehören, besitzen unterschiedliche Einstellungsmöglichkeiten.

Der Konfigurationsbaum des Objekts **Arbeitsplatz** verfügt über die meisten Einstellungsmöglichkeiten (s. Pkt. 14.5.2.2–14.5.2.6).

Für die Festplatten Ihres Rechners sind fast alle vorhandenen Einstellungen zur Verfügung, außer der Überprüfung der Registrierungsdateien (s. Pkt. 14.5.2.6).

Für logische Laufwerke kann die Art des Laufwerkzugriffs von Kaspersky® Inspector nicht gewählt werden (s. Pkt. 14.5.2.2) und die Einstellungen der zu überprüfenden Laufwerkkomponenten stehen nicht zur Verfügung (nur Veränderungen in der Verzeichnisstruktur können überprüft werden) (s. Pkt. 14.5.2.3).

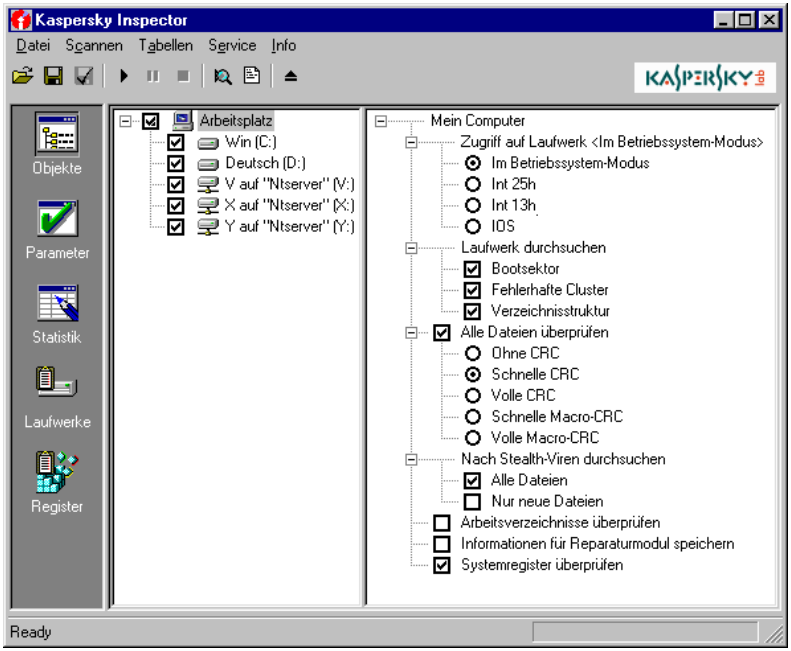


Bild 115. Einstellungen für die Laufwerküberprüfung

14.5.2.2. Art des Laufwerkzugriffs

Zugriff auf Laufwerk – Art des Zugriffs auf das Laufwerk:

- **Im Betriebssystem-Modus** – Kaspersky® Inspector greift unter Verwendung des Betriebssystems auf das Laufwerk zu. Wurde für ein Laufwerk diese Zugriffsart gewählt, kann keine Suche nach Stealth-Viren und keine Überprüfung von Bootsektoren und fehlerhaften Cluster erfolgen.
- **Int 25h** – Zugriff unter Verwendung von Laufwerktreibern (INT 25h). In diesem Fall erfolgen Lesen und Dateisuche durch direktes Lesen der Laufwerksektoren ohne DOS-Zugriff, d.h. mit dem 25h-Interrupt (absolutes Lesen des Laufwerks). Dieser Modus kann bei der Überprüfung von komprimierten Laufwerken (z.B. mit Programmen wie Stacker Ver. 4.x, DriveSpace) gewählt werden. Die o.g. Programme zur Laufwerkkomprimierung werden von Kaspersky® Inspector unterstützt und solche Laufwerke werden durch ein spezielles Symbol repräsentiert. Sollten Sie andere Komprimierungsprogramme verwenden, die von Kaspersky® Inspector nicht unterstützt werden, müssen Sie den Zugriffsmodus auf das komprimierte Laufwerk - INT 25h - selbst festlegen.
- **Int 13h** – Zugriff über INT 13h. In diesem Fall erfolgt das Auslesen der Laufwerksektoren durch direktes Lesen über das BIOS (13h-Interrupt). Dieser Modus kann verwendet werden, wenn **nur** physische Laufwerke, d.h. Festplattenpartitionen überprüft werden.
- **IOS** – Zugriff über IOS (IO Supervisor). In diesem Fall erfolgt der Zugriff auf das Laufwerk nach folgenden Regeln: Bei 32-Bit-Zugriff auf Laufwerke (Verwendung von VFAT-Laufwerken ("Dragon")), bei Einsatz von Protected Mode Programmen zur Laufwerkkomprimierung (DriveSpace), oder Zugriff auf das Laufwerk über Real Mode Mapper wird der Treiber für den 32-Bit-Zugriff (IOS) auf Laufwerke direkt aufgerufen. Andernfalls erfolgt der Zugriff auf die Laufwerke über INT 13h bzw. über den Laufwerktreiber. In anderen Worten, der Zugriff erfolgt fast immer über den IO Supervisor. Diese Option ist nur für Windows 9x verfügbar.

14.5.2.3. Zu überprüfende Laufwerkkomponenten

Laufwerk durchsuchen – zu überprüfende Laufwerkkomponenten:

- ☑ **Bootsektor** – Hier kann die Überprüfung des Bootsektors für ein Laufwerk ausgeschaltet werden. Dies kann beispielsweise für Laufwerke erforderlich sein, die mit dem Programm Stacker (Programm zur Komprimierung von

Laufwerken) angelegt wurden, da dieses Programm den Inhalt des Bootsektors ständig modifiziert.

☑ **Fehlerhafte Cluster** – Hier kann die Kontrolle über das Auftauchen neuer fehlerhafter Cluster auf einem Laufwerk ein- oder ausgeschaltet werden.

☑ **Verzeichnisstruktur** – Hier kann die Kontrolle von Veränderungen in der Struktur des Verzeichnisbaums eines Laufwerks (Suche nach neuen und gelöschten Verzeichnissen) ein- oder ausgeschaltet werden.

14.5.2.4. Methode zur Berechnung der Kontrollsummen für die Dateien eines Laufwerks

☑ **Alle Dateien überprüfen** – Prüfung aller Dateien unabhängig von den generellen Einstellungen für die Dateiüberprüfung. In diesem Fall wird Kaspersky® Inspector alle Dateien auf dem angegebenen Laufwerk überprüfen.

Hier lässt sich außerdem der gewünschte Algorithmus zur Berechnung von Kontrollsummen einstellen:

⊙ **Ohne CRC** – Für Dateien mit den gewählten Erweiterungen werden keine Kontrollsummen berechnet. In den Tabellen werden nur Dateilängen, Erstellungszeit und Erstellungsdatum gespeichert.

⊙ **Schnelle CRC** – Dieser Kontrollsummentyp ist abhängig von der internen Struktur ausführbarer DOS- und Windows-Dateien. Dabei lässt mit geringem Zeitaufwand die Integrität dieser Dateien zuverlässig kontrollieren. Diese Option wird ausdrücklich für Dateien mit den Erweiterungen COM, EXE, VXD, DLL, 386, CPL, SCR und sonstige ausführbare Dateien empfohlen.

⊙ **Volle CRC** – CRC-Berechnung in der gesamten Datei. Sichert die volle Kontrolle über die Datei-Integrität, wobei die Überprüfung jedoch wesentlich mehr Zeit benötigt. Empfehlenswert für BAT- und SYS-Dateien.

⊙ **Schnelle Makro-CRC** – Dieser Kontrollsummentyp ist abhängig von der internen Struktur von Makrodokumenten (Dokumente von Microsoft Word®, Microsoft Excel® und Microsoft Access®) und erlaubt eine zuverlässige Kontrolle der Integrität von OLE2-Dokumenten. Empfehlenswert für Dateien mit den Erweiterungen DOC, DOT (DO?), XLS, XLA, (XL?), MDB.

⊙ **Volle Makro-CRC** – Berechnung von CRC in allen Makros. Sichert die maximale Kontrolle der Integrität von OLE2-Dokumenten.

Makro-CRC sollte nur für Dateien aktiviert werden, die OLE2-Makros enthalten. Im Moment werden folgende Anwendungen unterstützt: Microsoft Word®, Microsoft Excel® und Microsoft Access®.

14.5.2.5. Suche nach Stealth-Viren

Nach Stealth-Viren durchsuchen – Laufwerk wird nach Stealth-Viren durchsucht:

☑ **Alle Dateien** – alle Dateien.

☑ **Nur neue Dateien** – nur neue Dateien.

Ist bei der Überprüfung des Computers die Option **Alle Dateien** aktiviert, so wird nur nach Stealth-Viren gesucht.

Laufwerke auf die über das Betriebssystem zugegriffen wird (Zugriffstyp **Im Betriebssystem-Modus**) werden nicht auf Stealth-Viren überprüft.

14.5.2.6. Zusätzliche Einstellungen

☑ **Arbeitsverzeichnisse überprüfen** – Aktiviert für das gewählte Laufwerk die Überprüfung von Arbeitsverzeichnissen.

☑ **Informationen für Reparaturmodul speichern** – Aktiviert die Desinfektion für das gewählte Laufwerk.

☑ **Systemregistrierung überprüfen** – Aktiviert die Überprüfung der Registrierungsdateien.

14.5.3. Speichern von Einstellungen auf der Festplatte und Laden von Einstellungen von der Festplatte

Alle Einstellungen (s. Pkt. 14.5.1 u. 14.5.2) können in einer speziellen Datei mit der Erweiterung *.klr gespeichert werden.

Um vorgenommene Einstellungen auf der Festplatte zu speichern,

1. Wählen Sie im Menü **Datei** den Punkt **Profil speichern unter**.
2. Geben Sie im folgenden Windows-Dialogfenster Pfad und Namen der Datei an, in der die gewählten Einstellungen gespeichert werden sollen.
3. Klicken Sie auf **Speichern**.

Zum Laden von gespeicherten Einstellungen aus einer Datei:

1. Wählen Sie im Menü **Datei** den Punkt **Profil laden**.
2. Geben Sie im folgenden Windows-Dialogfenster Pfad und Namen der Datei ein, aus der die Einstellungen geladen werden sollen.
3. Klicken Sie auf **Öffnen**.

14.6. Ansicht der Überprüfungsergebnisse

14.6.1. Ansicht von Informationen über die Aktivitäten von Kaspersky® Inspector

Zur Ansicht von Informationen über die Aktivitäten von Kaspersky® Inspector

1. Klicken Sie nach dem Start des Überprüfungsvorgangs auf das Symbol der Kategorie 

.

2. Auf dem Bildschirm erscheint das Programmfenster (s. Bild 116), in dem allgemeine Informationen über den Überprüfungsvorgang angezeigt werden.

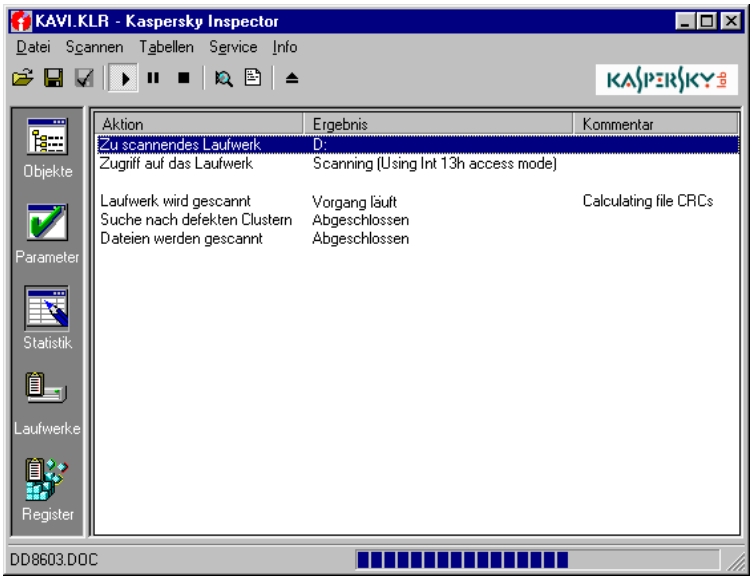


Bild 116. Dialogfenster mit allgemeinen Infos über den Überprüfungsvorgang

14.6.2. Ansicht von Informationen über Modifikationen

Nach Abschluss des Überprüfungsvorgangs erscheint auf dem Bildschirm ein Dialogfenster, in dem Sie die Anzeige der Überprüfungsergebnisse aufrufen können (s. Bild 117).

Um das Arbeitsfenster mit einer Übersicht der Veränderungen zu öffnen, klicken Sie auf **Ja**.

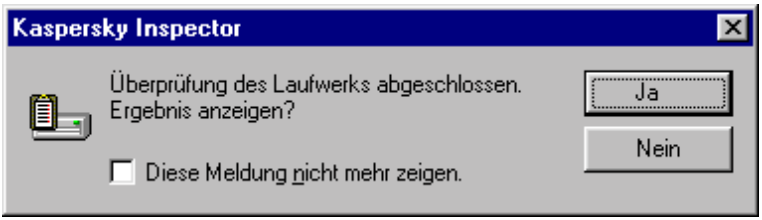


Bild 117. Dialogfenster zum Öffnen einer Übersicht der Modifikationen

Danach erscheint im Programmfenster eine Liste aller von Kaspersky® Inspector bei der Überprüfung festgestellten Modifikationen mit Angabe der Anzahl jedes Veränderungstyps (s. Bild 118).

Wurden verdächtige Modifikationen festgestellt, die auf Virenaktivitäten hinweisen könnten, zeigt Kaspersky® Inspector eine Warnung mit einer Liste aller verdächtigen Veränderungen an, bevor das Fenster mit den Ergebnissen der Überprüfung geöffnet wird.

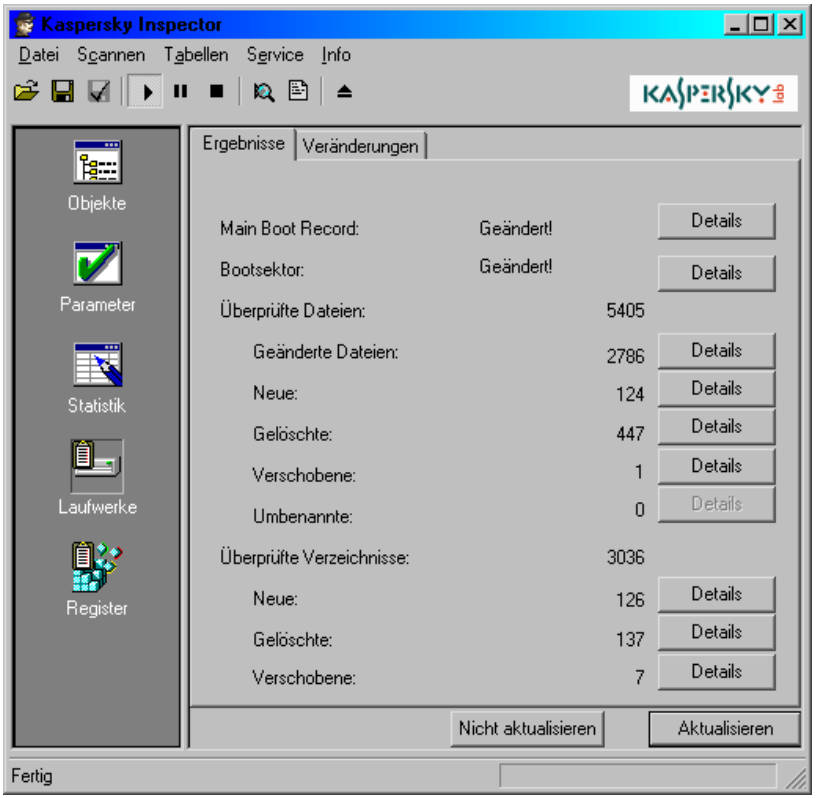


Bild 118. Liste der festgestellten Veränderungen

In dieser Liste werden Informationen über alle Veränderungen angezeigt, die seit der letzten Laufwerküberprüfung erfolgt sind: Anzahl der geänderten, gelöschten, umbenannten, verschobenen und neuen Dateien, Anzahl der neuen und gelöschten Verzeichnisse, sowie Veränderungen im Master-Bootsektor und Bootsektor. Wünschen Sie ausführlichere Informationen zu den jeweiligen Objekten, klicken Sie auf **Details**.

Auf Wunsch können Sie alle festgestellten Veränderungen als hierarchische Liste anzeigen lassen. Wechseln Sie hierzu auf die Registerkarte **Veränderungen** (s. Bild 119).

Mit Hilfe des Kontextmenüs dieser hierarchischen Liste können Sie alle veränderten Ordner und Dateien mit den in Kaspersky® Inspector verfügbaren Operationen bearbeiten. (s. Pkt. 14.6.3).

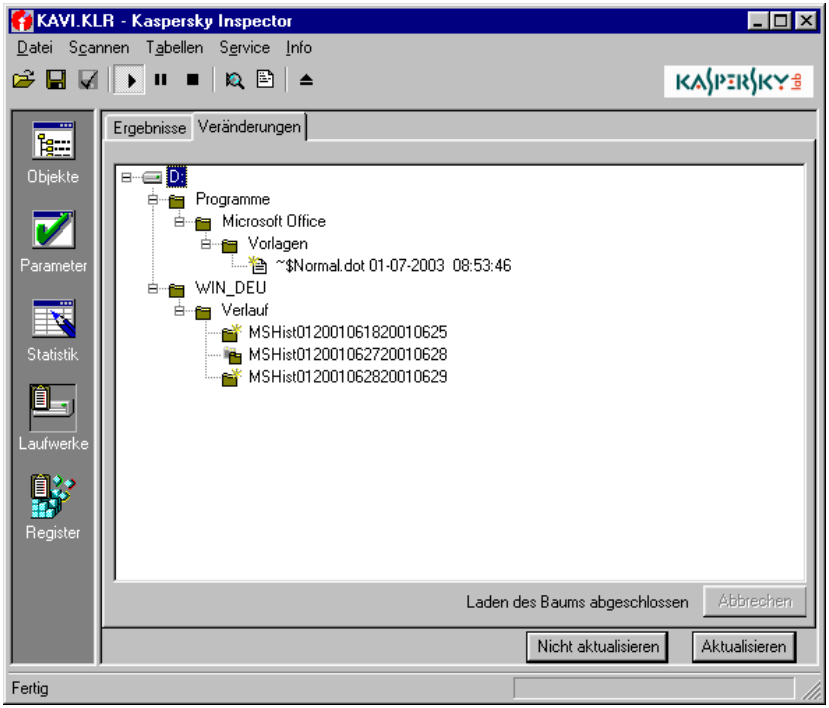


Bild 119. "Ergebnisbaum"

14.6.3. Mögliche Operationen für modifizierte Ordner und Dateien

Um ausführliche Informationen über veränderte Ordner und Dateien zu erhalten, klicken Sie neben der Bezeichnung der jeweiligen Änderungsart auf die Schaltfläche **Details**.

Auf dem Bildschirm erscheint ein Dialogfenster mit detaillierten Angaben aller festgestellten Veränderungen (s. Bild 120).

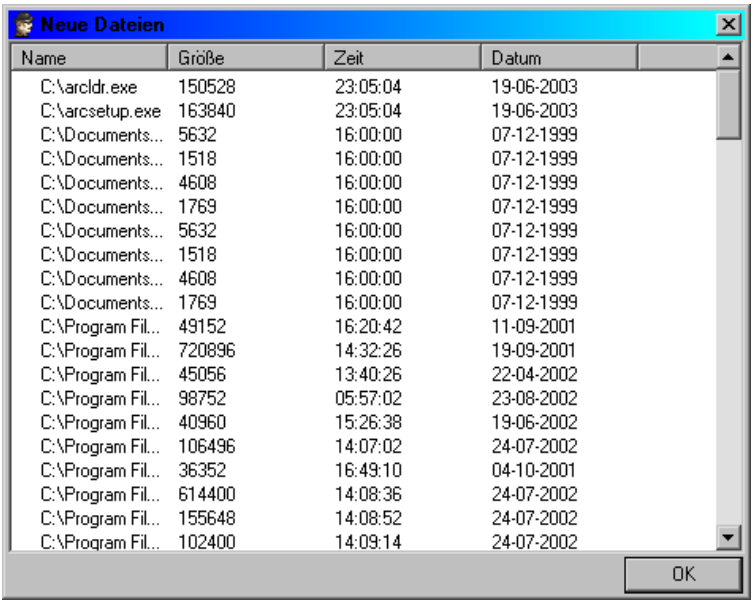


Bild 120. Liste der Veränderungen (neue Verzeichnisse)

Mit folgenden Arten veränderter Objekte kann bei Bedarf einer Reihe von Operationen durchgeführt werden, die in Kaspersky® Inspector vorgesehen sind:

- *mit veränderten Dateien – Zeile **Geänderte Dateien** (Gruppe **Überprüfte Dateien**)*
- *mit neuen Dateien – Zeile **Neue** (Gruppe **Überprüfte Dateien**)*
- *mit verschobenen Dateien – Zeile **Verschobene** (Gruppe **Überprüfte Dateien**)*
- *umbenannten Dateien – Zeile **Umbenannte** (Gruppe **Überprüfte Dateien**)*
- *neuen Verzeichnissen – Zeile **Neue** (Gruppe **Überprüfte Verzeichnisse**)*

Die übrigen Typen gefundener Modifikationen können nicht geändert werden.

Alle vorgesehenen Programmoperationen für geänderte Objekte werden über das Kontextmenü aufgerufen.

Für **geänderte** und **neue Dateien** stehen folgende Befehle zur Verfügung:

- ***Löschen*** *– Datei löschen.*
- ***Zur Liste der ausgeschlossenen Dateien hinzufügen*** *– Gewählte Datei in die Liste der nicht zu überprüfenden Dateien aufnehmen.*
- ***Zur Liste der unveränderbaren Dateien hinzufügen*** *– Gewählte Datei in die Liste schreibgeschützter Dateien aufnehmen.*
- ***Mit KAV überprüfen*** *– Gewählte Datei mit dem Antiviren-Scanner untersuchen.*
- ***Alle Dateien mit KAV überprüfen*** *– Alle Dateien aus dieser Liste mit dem Antiviren-Scanner untersuchen.*

Umbenannte und verschobene Dateien können nur gelöscht werden. Dazu dient der Befehl **Löschen** im Kontextmenü.

Bei der Ansicht der Liste **neuer Verzeichnisse** haben Sie die Wahl zwischen zwei Kontextmenü-Befehlen:

- ***Mit KAV überprüfen*** *– Ausgewähltes Verzeichnis mit dem Antiviren-Scanner untersuchen.*
- ***Alle Dateien mit KAV überprüfen*** *– Alle Verzeichnisse aus dieser Liste mit dem Antiviren-Scanner untersuchen.*

14.6.4. Dialogfenster zur Ansicht des Master-Bootsektors

Hat Kaspersky® Inspector im Master-Bootsektor des Rechners Veränderungen vorgefunden, erscheint auf dem Bildschirm eine Warnmeldung über die festgestellten Modifikationen.

Zur Anzeige ausführlicher Informationen zu diesen Veränderungen dient die Schaltfläche **Details** in der Zeile **Master Boot Record**.

Nach dem Klick auf diese Schaltfläche erscheint das Dialogfenster **Master Boot Record** (s. Bild 121).

In diesem Fenster können Sie sehen, welche Felder der Partitionstabelle modifiziert wurden. Bei den meisten Virusinfektionen bleibt die Partitionstabelle unberührt, und nur das Ladeprogramm wird geändert. Es gibt aber Viren, welche die Anfangsadresse der aktiven Partition verändern, wobei das Ladeprogramm unverändert bleibt. Das Ladeprogramm wird auch beim Wechsel des Betriebssystems (oder der Version des Betriebssystems) geändert.

Prüfen Sie sorgfältig mögliche Ursachen für Veränderungen im MBR!

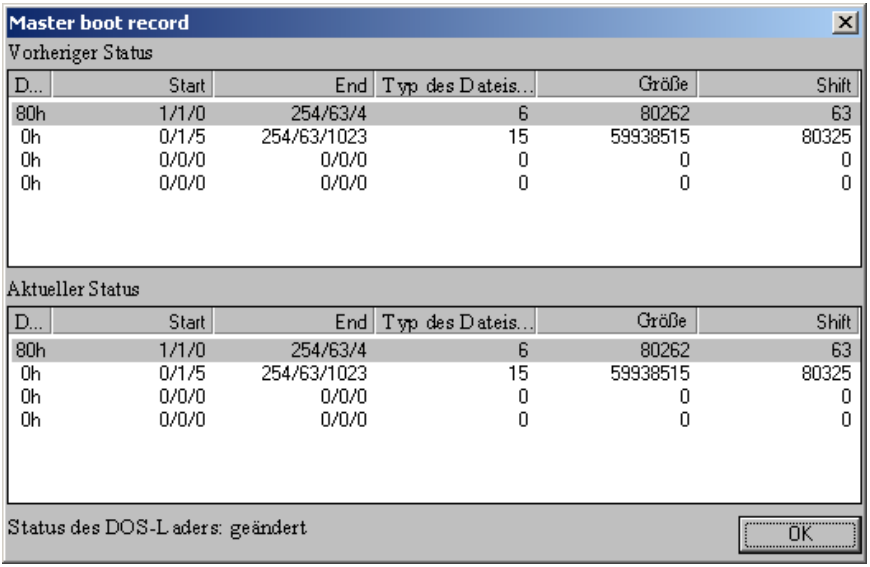


Bild 121. Dialogfenster **Master Boot Record**

14.6.5. Dialogfenster zur Ansicht des Bootsektors

Hat Kaspersky® Inspector im Bootsektor des Rechners Veränderungen vorgefunden, erscheint auf dem Bildschirm eine Warnmeldung über die festgestellten Modifikationen.

Zur Anzeige ausführlicher Informationen dient die Schaltfläche **Details** in der Zeile **Bootsektor**.

Nach Klick auf diese Schaltfläche erscheint das Dialogfenster **Boot Record** (s. Bild 122).

In diesem Dialogfenster können Sie sehen, welche Felder des BIOS-Parameter-Blocks (BPB) modifiziert wurden. Gewöhnlich bleibt bei einer Virusinfektion der BPB unangetastet, und nur das Ladeprogramm wird geändert (häufig werden der Sprung zum Ladeprogramm (JMP to loader) und der Name des Betriebssystemherstellers verändert). Das Ladeprogramm wird auch beim Wechsel des Betriebssystems (oder der Version des Betriebssystems) geändert.

Prüfen Sie sorgfältig mögliche Ursachen für Veränderungen im BR!

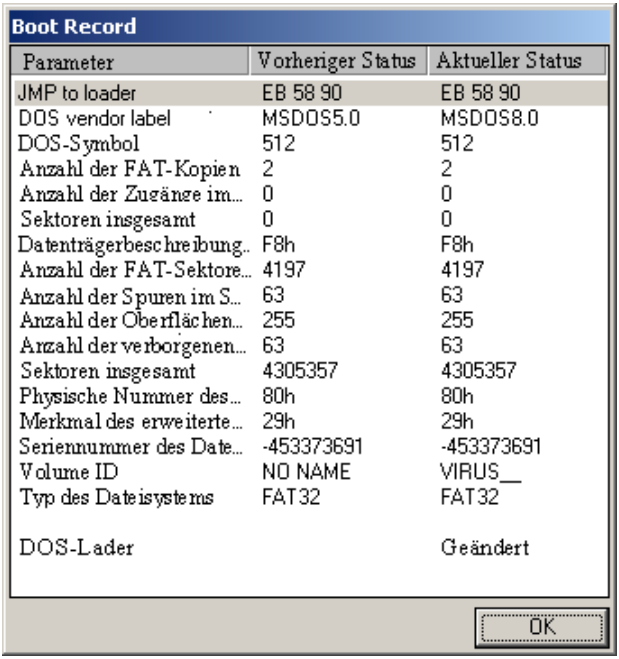


Bild 122. Dialogfenster **Boot Record**

14.6.6. Ansicht der Veränderungen in Registrierungsdateien

Wurde in den Programmeinstellungen die Überprüfung der Registrierungsdateien des Rechners aktiviert (s. Pkt. 14.5.2.6), dann kann durch Klick auf das Symbol 

in der Kategorienleiste die Liste der von Kaspersky® Inspector festgestellten Veränderungen geöffnet werden. Im Programmfenster erscheint eine Gesamtübersicht aller Veränderungen (s. Bild 123).

Auf Wunsch können Sie alle festgestellten Veränderungen als hierarchische Liste anzeigen lassen. Wechseln Sie hierzu auf die Registerkarte **Veränderungen** (s. Bild 124).

Zur Ansicht detaillierter Informationen über die Registrierungsschlüssel, die seit der letzten Überprüfung verändert, neue erstellt oder gelöscht wurden, klicken Sie neben der Bezeichnung der jeweiligen Änderungsart auf die Schaltfläche **Details**. Danach erscheint auf dem Bildschirm ein Dialogfenster mit der ausführlichen Beschreibung aller festgestellten Modifikationen (s. Bild 125).

Kaspersky® Inspector untersucht nicht alle Registrierungsschlüssel des Rechners auf Veränderungen, sondern nur diejenigen, die den automatischen Start von Programmen übernehmen. Nachfolgend finden werden die wichtigsten von ihnen genannt:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Internet Settings\Zones

HKEY_CURRENT_USER\Software\Microsoft\Office\8.0

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Runonce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Runonceex

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Runservices
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Runservicesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio
n\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio
n\Runonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio
n\Runonceex

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio
n\Runservices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio
n\Runservicesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion

HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps
```

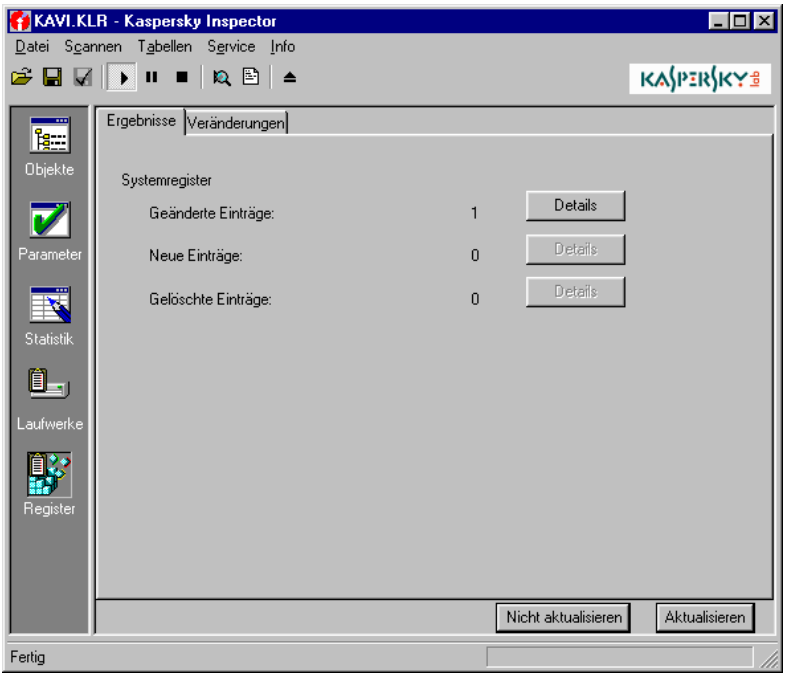


Bild 123. Liste der festgestellten Veränderungen in der Registrierung

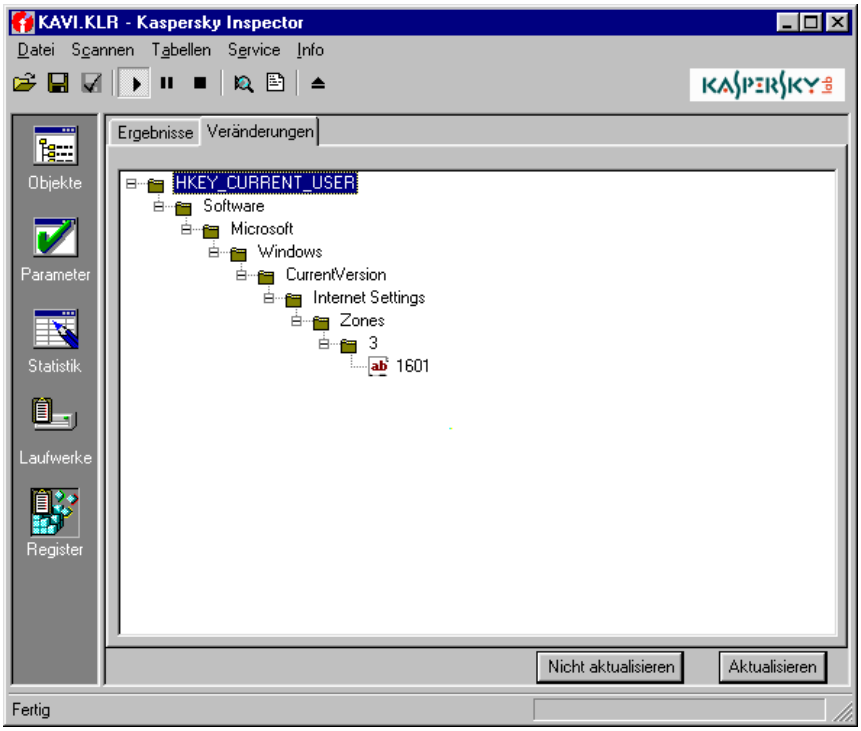


Bild 124. "Ergebnisbaum" der Veränderungen in Registrierungsdateien

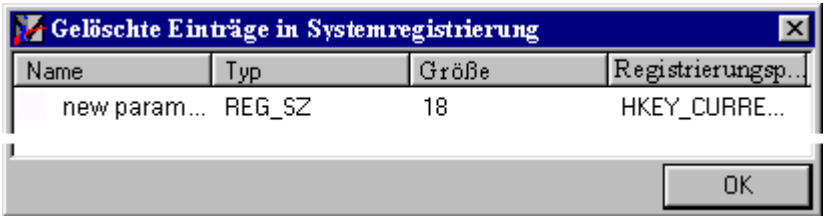


Bild 125. Liste der gelöschten Registierungsschlüssel

14.6.7. Übernehmen/Ablehnen von Tabellenänderungen

Um Veränderungen in Dateien, Verzeichnissen und Registrierung, die bei der Überprüfung festgestellt wurden, in die Tabellen von Kaspersky® Inspector aufzunehmen, klicken Sie auf die Schaltfläche **Aktualisieren** (s. Bild 118 u. Bild 123). Daraufhin werden alle Änderungen in den Tabellen gespeichert. Bei den folgenden Überprüfungen wird Kaspersky® Inspector den aktuellen Zustand der Laufwerke mit diesen Daten vergleichen.

Möchten Sie die Veränderungen aus irgendeinem Grund nicht in die Tabellen aufnehmen, klicken Sie auf **Nicht aktualisieren**. Kaspersky® Inspector wird dann bei der nächsten Überprüfung diese Veränderungen erneut registrieren.

ANHANG A. ZUSÄTZLICHE SUCHFUNKTIONEN

A.1. Heuristisches Scannen

Die heuristische Suchmaschine (Code Analyzer) untersucht die Codes von Dateien und Sektoren mit Hilfe unterschiedlicher Algorithmen von Kaspersky Anti-Virus® auf virenähnliche Befehle. Findet die heuristische Suchmaschine eine Befehlskombination (z.B. Datei öffnen, in einer Datei speichern, Interrupt-Vektoren abfangen usw.), so gilt die betreffende Datei als *verdächtig* und eine entsprechende Meldung erscheint:

```
Verdacht: <TYP>
```

wobei: <TYP> einer der folgenden Zeilen entspricht:

- ***Com*** *– Datei könnte einen unbekannten Virus enthalten, der COM-Dateien infiziert.*
- ***Exe*** *– Datei könnte einen unbekannten Virus enthalten, der EXE-Dateien infiziert.*
- ***ComExe*** *– Datei könnte einen unbekannten Virus enthalten, der Dateien der Formate COM und EXE infiziert.*
- ***ComTSR***, ***ExeTSR***, ***SysTSR***, ***ComExeTSR*** *– Datei könnte einen unbekannten residenten Virus enthalten, der Dateien der Formate COM, EXE und SYS infiziert.*
- ***Boot*** *– Datei könnte durch einen unbekannten Bootvirus oder ein Bootvirus-Installationsprogramm infiziert sein.*
- ***Trojan*** *– Datei besitzt Ähnlichkeit mit einem Trojanischen Programm.*
- ***Trivial*** *– Datei könnte einen unbekannten Virus enthalten, der ausführbare Dateien im aktuellen Verzeichnis durch sich ersetzt (die Größe eines solchen Virus liegt normalerweise unter 300 Byte).*

- ***HLL*** *– Datei könnte einen unbekannten Virus enthalten, der ausführbare Dateien infiziert und in Programmiersprachen mit hohem Niveau geschrieben wurde (C, Pascal).*

- ***Win32*** *– Datei könnte einen unbekannten Windows-Virus enthalten.*

- ***Formula*** *– Excel-Datei enthält verdächtige Befehle.*

- ***Macro.Word97.Fs*** *– Verdacht auf einen Virus der Familie Macro.Word97.Fs.*

- ***RemoteTemplate*** *– Dokument enthält einen Verweis auf eine Vorlage, die beim Öffnen der Datei automatisch geladen wird.*

- ***HTML.SecurityBreach.2*** *– HTML-Datei oder E-Mail im HTML–Format enthält einen Verweis auf ein verdächtiges Objekt.*

- ***IRC-Worm.generic*** *– Datei könnte einem unbekannten Wurm enthalten, der sich über IRC-Kanäle versendet.*

- ***BAT*** *– Datei könnte einen unbekannten Virus enthalten, der Dateien im BAT-Format infiziert.*

- ***VBS.I-Worm*** *– Datei könnte von einem unbekannten Wurm infiziert sein, der sich per E-Mail versendet.*

Diese Suchmaschine kann natürlich wie jeder heuristischer Algorithmus Fehlalarm auslösen. Sie wurde aber mit einer sehr großen Anzahl von Dateien getestet, wobei kein tatsächlicher Fehlalarm ausgelöst wurde. Sollten Sie bei virusfreien Dateien Fehlalarme beobachten, senden Sie bitte Kopien dieser Dateien zur Analyse an Kaspersky Labs Ltd.

Die heuristische Suchmaschine überprüft beim Scannen eine Vielzahl von Programmalgorithmen (einschließlich mehrerer Unterstufen). Mit diesem Mechanismus können mehr als 92% der Viren (einschließlich vieler verschlüsselter Viren) aus der Virensammlung von Kaspersky Labs Ltd. erkannt werden. Deshalb schätzen wir, dass mit derselben Wahrscheinlichkeit auch neue unbekannte Viren erkannt werden.

A.2. Redundantes Scannen

In den meisten Fällen trägt sich ein Virus an einen Einsprungspunkt der Datei ein und verweist auf seinen Körper, der gewöhnlich an das Ende der Datei angefügt wird. Zur Desinfektion eines solchen Virus ist das normale Scannen völlig ausreichend, d.h. das Löschen des Viruscodes aus dem Einsprungspunkt und des eigentlichen Virus-Körpers, auf den die Ausgangsadresse verweist.

In bestimmten Fällen schreibt der Virus seinen Körper aber nicht als einheitlichen Block, sondern "verteilt" ihn auf freie Dateiabschnitte. In diesem Fall wird durch normales Scannen der Virus unschädlich gemacht (seine Anfangsadresse wird aus dem Einsprungspunkt und der Hauptteil des Virus-Körpers wird entfernt), aber einige Teile des Virus verbleiben in der Datei.

Gerade zum Auffinden solcher Reste wurde die Funktion zum *redundanten Scannen* entwickelt, bei dem nicht nur die Einsprungspunkte, sondern die gesamte Datei ausführlich untersucht wird.

Die redundante Scan-Funktion sollte nur für einzelne Dateien und Verzeichnisse verwendet werden und nur dann, wenn beim gewöhnlichen Scannen kein Virus gefunden wurde, das System sich aber weiterhin "merkwürdig" verhält (häufige "selbständige" Neustarts, verlangsamter Betrieb bestimmter Programme usw.). In anderen Fällen ist die Verwendung des redundanten Scan-Modus nicht empfehlenswert, weil dabei die Scangeschwindigkeit erheblich verlangsamt wird und sich die Wahrscheinlichkeit von Fehlalarmen beim Scannen virusfreier Dateien erhöht.

ANHANG B. GLOSSAR

Antiviren-Datenbanken – Datenbanken mit Virusdefinitionen und Methoden zur Virusdesinfektion. Kaspersky Labs aktualisiert die Antiviren-Datenbanken täglich mit Informationen über neue Viren und stellt im Internet Updates bereit, von wo diese mit Hilfe des Aktualisierungsprogramms heruntergeladen werden können.

Antiviren-Revisor – s. "Programm zur Laufwerküberprüfung".

Antiviren-Scanner – Ein Programm, das den Rechner auf verdächtige Objekte durchsucht (siehe auch "Kaspersky Anti-Virus® Scanner").

Antiviren-Programm – Software, die den Rechner vor Eindringen und Ausbreitung von Viren schützt.

Bootvirus – Infiziert den Bootsektor einer Diskette oder den Bootsektor oder Master-Bootsektor (MBR) einer Festplatte. Bei einem Neustart "zwingt" der Virus das System statt des ursprünglichen Bootcode den Viruscode zu in den Arbeitsspeicher zu laden und diesem die Systemverwaltung zu übergeben. D.h. die Infektion erfolgt beim Booten von einer infizierten Quelle.

Fehlalarm – Eine Situation, in der ein virusfreies Objekt von einem Antiviren-Programm als infiziert eingestuft wird.

Heuristische Suchmaschine/Code Analyzer – Analyse der Befehlabfolge in einem untersuchten Objekt, Vergleich mit einer vorhandenen Statistik und Entscheidung darüber, ob das Objekt **möglicherweise infiziert** oder **nicht infiziert** ist. Wird zur Suche nach unbekannten Viren verwendet.

Interfaceteil einer Paketkomponente von Kaspersky Anti-Virus® – Teil eines Programms, der zur Kommunikation zwischen dem Serviceteil des Programms und dem Benutzer dient.

Kaspersky Anti-Virus® Control Centre – Ein Programm mit der Funktion einer Kontrollzentrale. Es dient zur automatischen Zeitsteuerung des Taskstarts und zur Ergebniskontrolle der Taskausführung.

Kaspersky Anti-Virus® Mail Checker – Ein Programm zum Antiviren-Schutz für Personalcomputer, die zum Senden und Empfang von E-Mails Software verwenden, die mit Microsoft Exchange Client kompatibel ist.

Kaspersky Anti-Virus® Monitor (Monitor) – Residenter Antiviren-Monitor. Wird von Monitor ein Virus gefunden, sperrt er den Zugriff auf das verdächtige Objekt und benachrichtigt den Benutzer.

Kaspersky Anti-Virus® Rescue Disk – Ein Programm zum Erstellen von Rettungsdisketten.

Kaspersky Anti-Virus® Scanner (Scanner) – Ein Programm, mit dem nach Vorgaben des Benutzers der Rechner auf Viren untersucht und gefundene Viren gelöscht werden können.

Kaspersky Anti-Virus® Script Checker – Ein Programm, das Ihren Rechner vor Skript-Viren und Würmern schützt, die unmittelbar im Hauptspeicher ausgeführt werden.

Kaspersky Anti-Virus® Updater – Ein Programm zur automatischen Aktualisierung von Antiviren-Datenbanken und Paketkomponenten.

Kaspersky® Inspector (Inspector) – Ein Programm zur Überprüfung von Laufwerken. Kaspersky® Inspector überprüft Laufwerke auf Veränderungen von Datei- und Verzeichnisinhalten und benachrichtigt den Benutzer, sobald er verdächtige Modifikationen feststellt. Dieses Programm kann als zusätzliches Antiviren-Programm oder zur Kontrolle von Laufwerkveränderungen eingesetzt werden. Es beschleunigt den Suchvorgang, da nur neue und modifizierte Dateien an den Scanner übergeben werden.

Kaspersky® Office Guard – Ein Programm zum Schutz von Microsoft Office 2000 Dokumenten vor bekannten und unbekannten Makroviren.

Kaspersky® Report Viewer – Ein Programm zur Ansicht und Verwaltung von Protokollen, die von den Komponenten des Softwarepakets Kaspersky Anti-Virus® erstellt werden.

Kategorie – Mit diesem Begriff wird eine Gruppe von ähnlichen Einstellungen bezeichnet. Die Schaltflächen zur Auswahl der einzelnen Kategorien befinden sich in einem gesonderten Bereich (gewöhnlich auf der linken Seite des Dialogfensters).

Konfigurationsbaum – Ein Element der Benutzeroberfläche, in dem alle Daten in Form eines Baums dargestellt werden. Die Gabelungen des Baums bilden Standardbedienungselemente (Schaltflächen, Listen, Kontrollkästchen usw.).

Konfigurationsdatei (*Profil*) – Datei, in der die wichtigsten Programmeinstellungen gespeichert werden. Einstellungen kann man in eine Datei exportieren (speichern) oder aus einer Datei importieren (laden). Beim

Programmstart werden die Einstellungen aus der **Standard-Konfigurationsdatei** benutzt.

Laufwerktabelle – Eine von Kaspersky® Inspector erstellte Datei, in der Angaben über den Inhalt logischer Laufwerke eines Rechners gespeichert werden (CRC-Dateien, Verzeichnisstruktur).

Makrovirus – Ein Virus, der in einer Makrosprache geschrieben wurde. Solche Viren werden bei Ausführung eines Makros aktiv. Dabei werden auch andere Dateien infiziert, die Makros enthalten können (Word-Dokumente, Excel-Arbeitsmappen u.a.).

Polymorpher Virus – Ein Virus, der spezielle Methoden verwendet, um seine Entdeckung und Analyse zu erschweren. Solche Viren besitzen keine Signaturen, d.h. sie enthalten keine unveränderbaren Codeteile.

Programm zur Laufwerküberprüfung – Ein Programm, das Laufwerke auf Modifikationen untersucht (siehe auch "Kaspersky® Inspector").

Quarantäne – Spezielles Verzeichnis, in dem verschlüsselte Kopien verdächtiger Dateien abgelegt werden. Diese Dateien lassen sich später mit Hilfe von Kaspersky Anti-Virus® Control Centre wiederherstellen, falls sie versehentlich gelöscht wurden, oder sie können zur Analyse an Kaspersky Labs gesendet werden.

Registrierungstabelle – Eine von Kaspersky® Inspector erstellte Datei, in der Angaben über kritische Registrierungsschlüssel (Ladevorgang beim Start, Schlüsseldateien) gespeichert werden.

Residenter Antiviren-Monitor – Ein Programm, das sich ständig im Arbeitsspeicher befindet und den gesamten Datenfluss (geöffnete Dokumente, gespeicherte Dateien usw.) kontrolliert.

Rettungsdisketten – Ein Diskettensatz, mit dem der Computer in Notfällen gestartet und auf Viren durchsucht werden kann. Mit Rettungsdisketten kann die Funktionsfähigkeit des Rechners nach einem Virenangriff wiederherstellt werden. Rettungsdisketten enthalten ein Betriebssystem, ein Antiviren-Programm und die Antiviren-Datenbanken. Sie können mit Hilfe des Programms Kaspersky Anti-Virus® Rescue Disk erstellt werden.

Scannen/Scanvorgang – Virus-Suche in dem zu überprüfenden Bereich, um vorhandene Viren (Scanner) oder verdächtige Objekte (Inspector) zu entdecken. Als Scanbereich können Hauptspeicher, Laufwerke, Verzeichnisse u.a. gelten.

Skript-Virus – Ein Virus, der in einer Skriptsprache geschrieben wurde. Gewöhnlich werden solche Viren in eine Webseite eingebettet und bei der Anzeige der Seite gestartet. Ein Skript-Virus kann sich auch in einer im HTML-Format geschriebenen E-Mail befinden.

Smart-Maske – Um die Arbeit der Antiviren-Programme (z.B. Kaspersky Anti-Virus® Scanner) zu beschleunigen, können jene Dateien von der Untersuchung ausgeschlossen werden, die nicht infiziert werden können. Dazu wird die Untersuchung nach Smart-Maske aktiviert (Punkt **Alle infizierbaren**). Eine Liste der infizierbaren Dateien ist in den Antiviren-Datenbanken gespeichert und wird zusammen mit diesen aktualisiert.

Serviceteil einer Paketkomponente von Kaspersky Anti-Virus® – Teil eines Programms, der sich ständig im Arbeitsspeicher befindet. Von ihm werden die wichtigsten Aufgaben ausgeführt (Scannen, Systemüberwachung).

Stealth-Virus – Ein Virus, der sich durch bestimmte Methoden im System unsichtbar macht. Viren aller Art können Stealth-Funktionen besitzen.

Systemeinbruch – Unbefugter Zugriff (Crack, Hack) auf Daten/Ressourcen eines Systems. Dazu wird oft Malware verwendet.

"Trojanisches" Pferd (Trojaner) – Ein Programm (Teil eines Programms), das destruktive oder unerwünschte Aktionen ausführt. Die Hauptfunktionen der Trojaner sind Remote-Administration, Diebstahl von Informationen, Zugriffs-überwachung usw.

Update-Server – Ein Server, auf dem sich neue Antiviren-Datenbanken oder Programmmodule befinden.

Verdächtiger Makrobefehl – Ein Makrobefehl, dessen Ausführung gefährliche Folgen für das System verursachen kann (z.B. das Löschen einer Datei). Mi®t Kaspersky® Office Guard können Sie die Vorgehensweise zum Auffinden solcher Makrobefehle festlegen.

Verdächtiges Objekt – Objekt, dessen Aktionen/Inhalte Ähnlichkeit mit Aktionen/Inhalten eines Virus aufweisen. Ein solches Objekt kann sich im Arbeitsspeicher, in einer Datei, einem Makro usw. befinden.

Virenangriff – Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

Virus – Ein charakteristisches Kennzeichen von Viren ist deren Fähigkeit, sich zu verdoppeln (wobei die Kopien nicht unbedingt mit dem Original übereinstimmen) und die Kopien über Netzwerke und/oder Dateien, Systembereiche eines

Computers und andere ausführbare Objekte zu verbreiten. Dabei behalten die Kopien die Fähigkeit zur Weiterverbreitung.

Warnmeldung – Eine E-Mail, die von einer Kaspersky Anti-Virus® Komponente automatisch an die angegebene Adresse gesendet wird, sobald ein bestimmtes Ereignis eintritt (Virusfund, Programmstörung usw.).

Windows-Virus – Ein Virus, der die Besonderheiten des Betriebssystems Microsoft Windows ausnutzt.

Wurm – Ein Virus, der sich über Netzwerke ausbreitet. Nachdem sich ein Wurm in einem Rechner eingenistet hat, ermittelt er die Netzwerkadressen anderer Computer und sendet seine Kopien an diese Adressen. Solche Viren legen manchmal auf Systemlaufwerken Arbeitsdateien an oder greifen mit Ausnahme des Arbeitsspeichers überhaupt nicht auf die Ressourcen des infizierten Rechners zu.

ANHANG C. KASPERSKY LABS LTD.

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

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

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

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

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

Wir bieten eine breite Palette an Zusatzdienstleistungen an, die ein reibungsloses Funktionieren und die problemlose Anpassung unserer Produkte an die speziellen Bedürfnisse Ihres Unternehmens gewährleisten. Unser Service reicht von der Projektierung bis hin zur Implementierung und Produktbegleitung für komplexe Virenschutzsysteme in Ihrem Unternehmen. Unsere Virendatenbanken werden zweimal täglich aktualisiert. Für unsere Kunden garantieren wir mehrsprachigen technischen Service rund um die Uhr.

C.1. Andere Produkte von Kaspersky Labs

Kaspersky Anti-Virus® Lite

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

Das Programmpaket von Kaspersky Anti-Virus® Lite umfasst:

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

Kaspersky Anti-Virus® Personal

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

Kaspersky Anti-Virus® Personal gewährleistet:

- ***die Virenprüfung*** *der lokalen Laufwerke auf Anfrage durch den Anwender;*

- ***die automatische Virenprüfung in Echtzeit*** *für sämtliche benutzten Dateien;*

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

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

Kaspersky Anti-Virus® Personal Pro

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

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

Kaspersky® Anti-Hacker

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

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

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

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

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

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

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeichern, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- ***einen Virenscanner**, der eine Überprüfung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;*

- ***den Antivirus-Monitor**, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.*

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz[5] vor Viren für:

- Computerarbeitsplätze *unter Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.*
- Dateiserver *unter Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD u OpenBSD, Linux.*
- Mailsysteme *vom Typ Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.*

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

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite bietet Rundumschutz[6] vor Viren für:

- Computerarbeitsplätze *unter Windows 98/Me, Windows 2000/NT/XP Workstation und Linux.*
- Dateiserver *unter Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD u Linux.*

[5] Je nach Lieferumfang
[6] Je nach Lieferumfang

- Mailsysteme *vom Typ Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.*

- Datenströme, die über Firewalls ein- und ausgehen.

- Handheld-PCs.

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

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

Kaspersky® Anti-Spam

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

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts.

C.2. Kontaktinformationen

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

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

ANHANG D. ENDBENUTZER-LIZENZVERTRAG FÜR KASPERSKY ANTI-VIRUS

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

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

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

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

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

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden.
- Sie sind berechtigt, die installierte SOFTWARE ein Jahr lang zu verwenden (Lizenzdauer).

2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering),

zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet.

• Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

• Supportleistungen. Nach Kauf der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:

– tägliches Update der Antiviren-Datenbank

– kostenloses Update der Software

– kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit Hot-Line-Service

• Viren-Entdeckung und heilende Updates auf Anfrage innerhalb von 48 Stunden.

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

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

5. GEWÄHRLEISTUNG. KASPERSKY LABS gewährleistet, dass:

• die SOFTWARE den Spezifikationen im wesentlichen entspricht.

• der Originaldatenträger frei von Material- und Herstellungsfehlern ist.

• das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation (sämtliche Informationen enthält, die KASPERSKY LABS für die Benutzung der Software für erforderlich hält).

• die SOFTWARE binnen 6 Monaten ab der ersten Installation oder dem ersten Download, falls richtig behandelt, vollfunktionsfähig ist, der in der beiliegenden Dokumentation bestimmten Funktionalität entsprechend.

Die Gewährleistungsfrist beträgt 6 Monate ab der ersten Installation oder dem ersten Download der Software den beiliegenden Dokumentationen von Kaspersky Labs entsprechend. Gewährleistungspflichtige Mängel werden von KASPERSKY LABS oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Labs nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls

eine Mangelrüge rechtzeitig an Kaspersky Labs oder dessen Lieferanten gerichtet wurde. KASPERSKY LABS oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

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

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

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