Dr Solomon's
Anti-Virus Toolkit
für Workstation

Dr Solomon's Software Ltd.
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK
Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777
E-Mail: support@drsolomon.com

Dr Solomon's Software, Inc.
1 New England Executive Park, Burlington, MA 01803, USA
Tel: +1 781 273 7400 Fax: +1 781 273 7474
E-Mail: support@us.drsolomon.com

Dr Solomon's Software GmbH
Luisenweg 40, 20537 Hamburg, Deutschland
Tel: Unterstützung +49 (0)1805 237678
E-Mail: support@de.drsolomon.com

Dr Solomon's Software Australasia Pty Ltd.
96-98 Market Street, South Melbourne, Victoria 3205, Australia
Tel: +61 3 9690 0455 Fax: +61 3 9690 7349
E-Mail: support@au.drsolomon.com

CompuServe: GO DRSOLOMON
World Wide Web: www.drsolomon.com

Copyright

Haftungsausschluß

Warenzeichen

Software-Version

In diesem Handbuch wird Version 7.78 von Dr Solomon's Anti-Virus Toolkit beschrieben.

Handbuchausgabe

Ausgabe 1.0
November 1997

Inhalt

Vorwort vii
Konventionen viii
Bildschirmauszüge ix
Verwandte Produkte x
Das Virenlexikon x
Andere Versionen des Anti-Virus Toolkit x
Windows NT-Version für Server x
Novell NetWare x
SCO UNIX x
Macintosh-Betriebssysteme x
Registrierung und Aktualisierungen xi
Falls Sie Hilfe benötigen xii
Deutschland xii
Großbritannien xiii
USA xiii
Australien xiii
Weltweit xiv

1. Installation des Toolkit 1
1.1 Erste Überprüfung auf Viren 1
SOS-Diskette 1
Standardüberprüfung 1
Besonderes Überprüfungsverfahren 2
1.2 README-Dateien 5
1.3 Windows 3.x 6
Systemvoraussetzungen 6
Installation des Toolkit 7
Vermeiden von Konflikten mit anderer Anti-Virus-Software 7
Installation von CD-ROM 7
Erweiterte Installationsoption 10
Installation von Diskette 15
Deinstallation des Toolkit 19
1.4 Windows 95 21
Systemvoraussetzungen 21
Installation des Toolkit 21
Vermeiden von Konflikten mit anderer Anti-Virus-Software 21
Installation von CD-ROM 21
Schnellinstallation 22
Erweiterte Installationsoption 25
Installation von Diskette 31
Deinstallation des Toolkit 38

1.5 Windows NT 39
Systemvoraussetzungen 39
Hardwarevoraussetzungen 39
Softwarevoraussetzungen 39
Installation des Toolkit 40
Vermeiden von Konflikten mit anderer Anti-Virus-Software 40
Installation von CD-ROM 40
Installation von Diskette 47
Deinstallation des Toolkit (Windows NT Version 4) 50
Deinstallation des Toolkit (Windows NT Version 3.51) 50
1.6 OS/2 51
Systemvoraussetzungen 51
Installation des Toolkit 51
Installation von CD-ROM 51
Installation von Diskette 52
Deinstallation des Toolkit 54
1.7 DOS 55
Systemvoraussetzungen 55
Installation des Toolkit 55
Installation von CD-ROM 55
Installation von Diskette 60
Deinstallation des Toolkit 63

2. Aktualisierung des Toolkit 65
2.1 Windows 3.x 65
Aktualisierung von CD-ROM 65
Schnellinstallation 65
Aktualisierung von Diskette 66
2.2 Windows 95 67
Aktualisierung von CD-ROM 67
Schnellinstallation 67
Aktualisierung von Diskette 67
2.3 Windows NT 68
Aktualisierung von CD-ROM 68
Schnellinstallation 68
Aktualisierung von Diskette 69
2.4 OS/2 70
Aktualisierung von CD-ROM 70
Aktualisierung von Diskette 71
2.5 DOS 72
Aktualisierung von CD-ROM 72
Aktualisierung von Diskette 73

3. Überprüfung auf Viren 75
3.1 Überprüfungsprogramme, die bei Bedarf ausgeführt werden 75
FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS 75
Überprüfung auf Viren 75
ViVerify für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS 77
3.2 Automatische Überprüfungsprogramme (Zugriffsscanner) 77
WinGuard für Windows 3.x, Windows 95 und Windows NT 77
WinGuard im täglichen Gebrauch 78
VirusGuard für Windows 3.x, Windows 95 und DOS 79
So starten Sie VirusGuard 79
Falls VirusGuard einen Virus findet 81

4. Weitere Einstellungen für die Virensuche 83
4.1 Erweiterte Virensuche mit FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS 83
Benutzerdefinierte Virensuche 83
4.2 Erweiterte Virensuche mit ViVerify für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS 86
Viverify 86
Reparaturdatenbank 87
Von der Überprüfung ausgeschlossene Dateien 87
Suche nach geänderten Dateien 88
Berechnen von Prüfsummen 88
Überprüfen von Dateien 90
4.3 Erweiterte Virensuche mit VirusGuard für Windows 3.x, Windows 95 und DOS ...92
Testen von VirusGuard 92
4.4 Erweiterte Virensuche mit WinGuard für Windows 3.x und Windows 95 93
Testen von WinGuard 93
Ändern der Konfiguration von WinGuard 94
Allgemeine Hinweise 94
Ändern der Konfiguration für die Überprüfung 95
Übersicht über die Überprüfungseinstellungen 97
Ändern der Warnmeldungen 101
Berichterstellung 103
Aktivierung 103
Dateiansicht 104
Falls WinGuard einen Virus findet 105
4.5 Erweiterte Virensuche mit WinGuard für Windows NT 107
Falls WinGuard einen Virus findet - „Entfernen“ nicht aktiviert 107
Falls WinGuard einen Virus findet - „Entfernen“ aktiviert 108
Das Warndialogfeld - Bisher-Liste 110
Das Warndialogfeld - Benutzerdefinierte Meldung 111
Ändern der Einstellungen 112

5. Verwendung des Zeitplaners in Windows 3.x, Windows 95 und Windows NT 123
5.1 Zeitplan-Editor - Übersicht und Aufrufen 123
Erstellen neuer Ereignisse 124
Registerkarte „Ereignis“ 124
Registerkarte „Intervall“ 127
Registerkarte „Einstellungen für Virensuche“ 128
Registerkarte „Einstellungen für Überprüfung“ 134
5.2 Ausführung des Zeitplaners 138
5.3 Ereignisverwaltung 140
Bearbeiten von Ereignissen 140
Löschen von Ereignissen 141
Deaktivieren von Ereignissen 141
Aktivieren von Ereignissen 141
Ausschneiden und Einfügen von Ereignissen 142
Kopieren und Einfügen von Ereignissen 143
Gültigkeitsprüfung von Ereignissen (nur für Windows 3.x verfügbar) 143
5.4 Protokolldatei des Zeitplaners 144
Ansicht der Protokolldatei 144
Umbenennen der Protokolldatei 145
5.5 Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“ 145
5.6 Allgemeine Umgebungseinstellungen 149

6. Entfernung von Viren 151
6.1 Entfernung von Viren aus Laufwerken 151
6.2 Ersetzen von Bootsektoren 154

7. Online-Dokumentation 157
7.1 Windows 3.x 158
Installation von Adobe Acrobat Reader 158
Kopieren des Handbuchs 159
7.2 Windows 95 160
Installation von Adobe Acrobat Reader 160
Kopieren des Handbuchs 161
7.3 Windows NT 162
Installation von Adobe Acrobat Reader 162
Kopieren des Handbuchs 163
7.4 OS/2 165
Installation von Adobe Acrobat Reader 165
Kopieren des Handbuchs 166
7.5 Gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs 168

8. Überblick über Computerviren 169
8.1 Was ist ein Virus? 169
8.2 Verbreitung von Viren 170
8.3 Weitere mögliche Probleme 171
Softwarefehler 171
Konflikte durch hardwarenahe Software 172
Trojanische Pferde 173
Zeitbomben und logische Bomben 173
Scherzprogramme 173
Benutzerfehler 174
8.4 Vorkehrungen 174
Datensicherungen 175
Softwarekauf 175
Disketten und andere Datenträger 175
Vermeiden von Verschlüsselung und Kennwortschutz 176
Kooperation der Mitarbeiter 176
Das Anti-Virus Toolkit 177
WinGuard 177
VirusGuard 177
FindVirus 178
ViVerify 178
SOS-Diskette 178
Zeitplaner 178
Virenlexikon 178

9. Fehlerbehebung und erweiterte Einstellungen 179
9.1 Fehlerbehebung 179
Meldung über fehlerhafte Datei MESSAGES.DRV 179
Deinstallation ohne ein Deinstallationsprogramm 179
Durch die Installation des Toolkit kann Windows 95 nicht mehr ausgeführt werden Meldung „Legen Sie eine Diskette mit \COMMAND.COM ein.“ 180
9.2 Erweiterte Installationsoptionen 181
9.3 Zusätzliche Dienstprogramme 181
CleanBoot 182
Disketten mit geändertem Format 184
CleanPart 184
TKUTIL 185
Angabe des Laufwerks 187
Angabe des freien Speicherplatzes 187
Angabe des Hauptprozessortyps 187
Angabe des Arbeitsspeichertyps 188
Angabe der speicherresidenten Programme des Toolkit 188
Angabe des letzten Tastenanschlags 188
Angabe der Ausführung einer Stapeldatei 189
Erstellung eines neuen Verzeichnisses 189

Aktualisierung von Dateien 190
Synchronisierung von .INI-Dateien 191
Hinzufügen von Text in einer Datei 191
Starten von WinGuard beim Systemstart 193
Löschen von Text aus einer Datei 193
Deaktivierung des automatischen Starts von WinGuard beim Systemstart 194
Textsuche 194
Überprüfung, ob VirusGuard installiert ist 195
Überprüfung, ob RingFence installiert ist 195
Bestimmung des Wochentages 196
Bestimmung des Monatstages 196
Sperren des Computers 196
Ausgabe von Warnsignalen 197
Abspielen einer Melodie 197
Entfernung anderer Anti-Virus-Produkte 197
Senden eines Formularvorschubzeichens an den Drucker 198
Neustart von VirusGuard 198
Neustart von speicherresidenten Programmen 198
Angabe technischer Informationen 199
WTKUTIL 199
Hinzufügen von WinGuard 199
Entfernung von WinGuard 200
Überprüfung, ob WinGuard läuft 200
Speichern der Einstellungen 200
Wiederherstellung von Einstellungen 201
Vergleichen von Einstellungen 201
Zusammenfassung aller Befehle 201
9.4 FindVirus-Fehlerebenen 202
Erweiterte Fehlerebenen von FindVirus 202

Glossar 205

Index 211

Vorwort

Dr Solomon's Anti-Virus Toolkit bietet alle Funktionen, die Sie benötigen, um Virusinfektionen auf Ihrem Computer festzustellen, vorhandene Viren zu entfernen und zukünftigen Virusinfektionen vorzubeugen.

Um Ihnen bei der möglichst effizienten Nutzung des Toolkit zu helfen, ist dieses Handbuch in folgende Abschnitte unterteilt:

Kapitel 1: **„Installation des Toolkit“**. In diesem Kapitel finden Sie schrittweise Anleitungen für die Installation des Toolkit.

Kapitel 2: **„Aktualisierung des Toolkit“**. In diesem Kapitel wird erläutert, wie Sie das Toolkit von Diskette und CD-ROM aktualisieren.

Kapitel 3: **„Überprüfung auf Viren“**. In diesem Kapitel werden die Dr Solomon's-Produkte für die automatische Virensuche und die Überprüfung bei Bedarf erläutert. Darüber hinaus enthält das Kapitel die Grundlagen der Überprüfung auf Viren.

Kapitel 4: **„Weitere Einstellungen für die Virensuche“**. In diesem Kapitel finden Sie detaillierte Anleitungen zur Verwendung und Konfiguration von Dr Solomon's Anti-Virus-Programmen.

Kapitel 5: **„Verwendung des Zeitplaners in Windows 3.x, Windows 95 und Windows NT“**. In diesem Kapitel wird die Verwendung des Zeitplaners Dr Solomon's Scheduler erläutert.

Kapitel 6: **„Entfernung von Viren“**. In diesem Kapitel wird erläutert, wie Viren aus Dateien, Bootsektoren und Partitionssektoren entfernt werden.

Kapitel 7: **„Online-Dokumentation“**. In diesem Kapitel wird erläutert, wie Sie Adobe Acrobat Reader von der CD-ROM installieren und das Online-Handbuch mit Hilfe von Adobe Acrobat Reader anzeigen.

Kapitel 8: **„Überblick über Computerviren“**. In diesem Kapitel wird erläutert, was Computerviren sind. Außerdem finden Sie Ratschläge zu einfachen Maßnahmen, die Sie zum Schutz des Systems vor Viren ergreifen können.

Kapitel 9: **„Fehlerbehebung und erweiterte Einstellungen“**. In diesem Kapitel werden einige allgemeine Probleme behandelt, zu denen die Benutzer möglicherweise Fragen haben. Außerdem werden erweiterte Toolkit-Optionen erläutert.

Am Ende des Handbuchs finden Sie ein Glossar, das unter anderem die wichtigsten im Handbuch verwendeten Begriffe enthält. Das Handbuch hat außerdem einen umfangreichen Index.

Konventionen

In diesem Handbuch werden bestimmte Konventionen verwendet.

Zur einfachen Referenz sind Seiten, die Informationen über ein bestimmtes Betriebssystem enthalten, mit dem Namen des Betriebssystems gekennzeichnet.

Von Ihnen einzugebende Informationen sind in der Schriftart `Courier` dargestellt. Beispiel:

```
D:\SETUP
```

Variablen werden in der Schriftart Courier *`kursiv`* gedruckt und innerhalb spitzer Klammern angezeigt. Beispiel: Installationsanleitungen für das OS/2-Toolkit:

„Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von
<*SPRACHE*>\PRODUCTS\OS/2
und drücken Sie die <Eingabetaste>.“

In diesem Fall ersetzen Sie <*SPRACHE*> durch den Namen der Sprache der zu installierenden Software. Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie zum Beispiel auf einem englischen System arbeiten, aber ein deutsches OS/2-Toolkit installieren möchten, ist der Name des Verzeichnisses „Deutsch“, nicht „German“.

Maustasten, mit denen Sie klicken und Optionen, die Sie auswählen müssen, sind **fettgedruckt** dargestellt.

Tasten, die Sie drücken müssen, stehen in spitzen Klammern. Beispiele:

<Eingabetaste> bezeichnet die Eingabetaste.

<Esc> bezeichnet die Esc-Taste.

Im Text finden Sie am Rand Symbole, mit denen bestimmte Punkte hervorgehoben werden. Diese Symbole haben folgende Bedeutungen:

Warnung 	Warnung, die Sie sorgfältig lesen sollten.
Tip 	Hinweis auf wichtige Informationen bzw. Tips, die Sie besonders beachten sollten.
Hilfe 	Hinweis auf zusätzliche Informationen.

Bildschirmauszüge

In den allgemeinen Abschnitten stammen die meisten Bildschirmauszüge aus der Windows 95-Version des Anti-Virus Toolkit. Bildschirmauszüge von anderen Betriebssystemen sind als solche gekennzeichnet.

Verwandte Produkte

Das Virenlexikon

Das Toolkit enthält das Virenlexikon, das Hintergrundinformationen über Viren bietet und ausführlich über die Viren informiert, die vom Toolkit erkannt werden. Sie sind im Lexikon in verschiedene Kategorien aufgeteilt. Ihre Auswirkungen werden beschrieben, und es werden alle zusätzlichen Namen aufgeführt, unter denen ein Virus bekannt ist.

Das Toolkit enthält auch eine Online-Fassung des Virenlexikons. Neue Viren werden jeweils in die aktuelle Version aufgenommen. Die Online-Fassung des Lexikons ist im Gegensatz zur gedruckten Ausgabe stets auf dem neuesten Stand.

Andere Versionen des Anti-Virus Toolkit

Windows NT-Version für Server

Die Windows NT-Version für Server bietet Hilfsprogramme für die Installation, Konfiguration, Aktualisierung, Deinstallation und Verwaltung von Anwendungen des Dr Solomon's Anti-Virus Toolkit auf Netzwerkcomputern in einem Windows NT-Netzwerk.

Novell NetWare

Die NetWare-Version des Anti-Virus Toolkit bietet Hilfsprogramme für den Schutz von NetWare-Servern gegen Viren. Um einen umfassenden Schutz zu gewährleisten, enthält das Paket auch die Toolkit-Versionen für DOS und Windows.

SCO UNIX

Die SCO UNIX-Version des Anti-Virus Toolkit bietet Virenerkennung, Virenentfernung und Schutz vor Viren für Computer, auf denen SCO UNIX ausgeführt wird. Das Paket enthält auch die DOS-Version des Toolkit.

Macintosh-Betriebssysteme

Die Macintosh-Version des Anti-Virus Toolkit bietet Virenerkennung, Virenentfernung und Schutz vor Viren für Macintosh-Betriebssysteme.

Registrierung und Aktualisierungen

Die Virenforscher von Dr Solomon's erhalten monatlich zwischen 300 und 400 neue Viren zur Untersuchung, und das Toolkit wird jeden Monat aktualisiert, um wirkungsvollen Schutz vor diesen neuen Viren zu bieten. Zu Ihrer eigenen Sicherheit sollten Sie den regelmäßigen Software-Aktualisierungsdienst nutzen. Für viele Benutzer ist bereits eine vierteljährliche Aktualisierung ausreichend. Wenn Ihr System jedoch besonders gefährdet oder Sicherheit von besonderer Wichtigkeit ist, können Sie Ihren Virenschutz auch monatlich aktualisieren.

Sie haben möglicherweise ein Toolkit erworben, zu dem Sie ein Jahr lang kostenlose Aktualisierungen beziehen können. In diesem Fall erhalten Sie nach der Registrierung automatisch 12 Monate ab dem Datum auf der Registrierkarte entweder monatliche oder vierteljährliche Aktualisierungen.

Warnung

Wenn Sie die Registrierkarte nicht einsenden, erhalten Sie keine Aktualisierungen, obwohl Sie sie bereits bezahlt haben.

Wenn Sie kein Toolkit-Paket mit kostenlosen Aktualisierungen erworben haben, rufen Sie bei Dr Solomon's an, um Aktualisierungen zu bestellen. Weitere Informationen finden Sie auf der Karte selbst.

Dem Toolkit-Paket liegt eine Registrierkarte bei. Bitte füllen Sie diese aus, und senden Sie sie an Dr Solomon's oder die Dr Solomon's-Vertretung in Ihrem Land.

Warnung

Wenn Sie das von Ihnen erworbene Produkt nicht registrieren lassen, erhalten Sie keine Aktualisierungen für das Toolkit.

Falls die Registrierkarte in Ihrem Paket fehlt, rufen Sie Dr Solomon's oder die Dr Solomon's-Vertretung in Ihrem Land an.

Tip Senden Sie Ihre Registrierkarte ein.

Falls Sie Hilfe benötigen

Falls bei der Installation oder Verwendung des Toolkit Probleme auftreten, haben Sie mehrere Möglichkeiten, Hilfe zu erhalten.

Lesen Sie die Dokumentation, einschließlich der README-Dateien auf der CD-ROM bzw. den Disketten, sowie das Handbuch und die Hilfetexte. Überprüfen Sie, ob die Software richtig installiert ist. Wenden Sie sich gegebenenfalls an Ihren Fachhändler.

Wenn Sie ein Problem nicht selbst beheben können, sind Ihnen die Mitarbeiter der technischen Unterstützung von Dr Solomon's gern behilflich. Die Unterstützung ist kostenlos.

Sie können Dr Solomon's Software wie folgt erreichen:

Deutschland

Telefon:	Technische Unterstützung 01805 237678
Fax:	Verkauf 01805 237677
E-Mail:	support@de.drsolomon.com
Adresse:	Dr Solomon's Software GmbH Luisenweg 40 D-20537 Hamburg

Großbritannien

Telefon:	+44 (0)1296 318700
Fax:	+44 (0)1296 318734
E-Mail:	support@drsolomon.com
BBS:	+44 (0)1296 318810
Adresse:	Dr Solomon's Software Ltd. Alton House Gatehouse Way Aylesbury Buckinghamshire HP19 3XU Großbritannien

Tip

Falls Sie außerhalb der normalen Arbeitszeiten anrufen, hören Sie sich den gesamten Text des Anrufbeantworters an, und folgen Sie den Anleitungen.

USA

Telefon:	+1 781 273 7400
Fax:	+1 781 273 7474
E-Mail:	support@us.drsolomon.com
BBS:	+1 781 229 8804
Adresse:	Dr Solomon's Software, Inc. 1 New England Executive Park Burlington MA 01803, USA

Australien

Telefon:	+61 3 9690 0455
Fax:	+61 3 9690 7349
E-Mail:	support@au.drsolomon.com
Adresse:	Dr Solomon's Software Australasia Pty Ltd. 96-98 Market Street South Melbourne Victoria 3205 Australien

Weltweit

CompuServe:	GO DRSOLOMON
World Wide Web:	www.drsolomon.com

Wenn Sie sich mit Dr Solomon's in Verbindung setzen, sollten Sie folgendes bereithalten:

- Die Seriennummer. Sie finden sie auf der Registrierkarte.
- Die Version von Windows 3.x, Windows 95, Windows NT, OS/2 oder DOS, die Sie benutzen.
- Die Versionsnummer des Toolkit, das Sie benutzen. Diese Nummer finden Sie auf der Toolkit-CD oder auf den Etiketten der Installationsdisketten.
- Die Versionsnummer des Toolkit-Handbuchs, das Sie benutzen. Diese Nummer finden Sie auf der Copyright-Seite des Handbuchs.
- Die SOS-Diskette oder eine saubere (d. h. virenfreie), schreibgeschützte DOS Systemdiskette oder einen sauberen, schreibgeschützten Satz OS/2-Systemdisketten.
- Die angezeigten Fehlermeldungen, falls es sich um einen Anwendungsfehler handelt.

Wenn möglich, sollten Sie sich bei einem Anruf an dem infizierten Computer befinden. Wir benötigen unter Umständen weitere Informationen, oder wir bitten Sie gegebenenfalls, einige Diagnosetests durchzuführen.

1. Installation des Toolkit

In diesem Kapitel wird erläutert, wie Sie eine erste Überprüfung auf Viren durchführen und das Toolkit installieren und deinstallieren. Anleitungen zur Aktualisierung des Toolkit finden Sie im Abschnitt „Aktualisierung des Toolkit“ auf Seite 65.

1.1 Erste Überprüfung auf Viren

Sie müssen sicherstellen, daß Ihr Computer virenfrei ist, bevor Sie die Dr Solomon’s-Software installieren. Dr Solomon’s bietet zwei Möglichkeiten für die Überprüfung des Computers.

Tip

Wenn Sie mit Windows NT oder OS/2 arbeiten, fahren Sie bitte direkt mit den Installationsanleitungen für diese Betriebssysteme fort. Die Installationsanleitungen für Windows NT finden Sie im Abschnitt „Windows NT“ auf Seite 39, die Installationsanleitungen für OS/2 im Abschnitt „OS/2“ auf Seite 51.

SOS-Diskette

Standardüberprüfung

Warnung

Falls Sie ein komprimiertes Laufwerk oder besondere Hardware haben, können Sie den Computer möglicherweise nicht vollständig mit der SOS-Diskette überprüfen.

Sie können die SOS-Diskette nicht verwenden, um ein Netzwerk auf Viren zu überprüfen, oder wenn Sie mit Windows NT oder OS/2 arbeiten. Wenn Sie die SOS-Diskette nicht verwenden können, finden Sie weitere Informationen unter „Besonderes Überprüfungsverfahren“ auf Seite 2.

1. Schalten Sie den Computer aus.

2. Legen Sie die SOS-Diskette in Laufwerk A: ein, und schalten Sie den Computer wieder ein.

   [*Hinweis: Sie sehen kurz die Meldung „Die SOS-Diskette wird gestartet...“, anschließend wird die Benutzeroberfläche der SOS-Diskette angezeigt.*]

3. Mit <F2> starten Sie die Überprüfung aller ausführbaren Dateien auf der (den) lokalen Festplatte(n).

4. Wenn der Bericht anzeigt, daß der Computer virenfrei ist, beenden Sie die SOS-Diskette durch Drücken von <Esc>; nehmen Sie dann die Diskette aus dem Laufwerk, und starten Sie den Computer neu. Fahren Sie mit Schritt 5 fort, falls ein Virus gefunden wird.

5. Drücken Sie <F4> auf der Benutzeroberfläche der SOS-Diskette, um den Computer auf Viren zu überprüfen und bekannte Viren zu entfernen, bevor Sie mit der Installation fortfahren. Wenn der Bericht anzeigt, daß der Computer virenfrei ist, beenden Sie die SOS-Diskette durch Drücken von <Esc>; nehmen Sie dann die Diskette aus dem Laufwerk, und starten Sie den Computer neu.

Besonderes Überprüfungsverfahren

Falls Sie ein komprimiertes Laufwerk oder besondere Hardware haben, müssen Sie die folgenden Schritte ausführen.

Warnung

Sie können dieses Verfahren nicht anwenden, um ein Netzwerk auf Viren zu überprüfen, oder wenn Sie mit Windows NT oder OS/2 arbeiten.

1. Legen Sie eine saubere (d. h. virenfreie), schreibgeschützte DOS-Systemdiskette in Laufwerk A: ein. Diese Systemdiskette sollte dieselbe DOS-Version wie die Festplatte haben. Die Diskette muß alle Treiber haben, die für von Ihnen verwendete Dienstprogramme zur Festplattenkomprimierung und für besondere Hardware benötigt werden.

Um eine saubere Systemdiskette zu erstellen, müssen Sie eine Diskette als Systemdiskette formatieren. Falls Sie mit besonderen Treibern auf die Festplatte zugreifen, kopieren Sie diese ebenfalls auf die Diskette, und erstellen Sie eine entsprechende CONFIG.SYS-Datei.

Warnung Denken Sie daran, daß durch Formatieren einer Diskette alle auf ihr gespeicherten Daten verlorengehen.

Wenn Sie zum Beispiel Stacker oder SuperStore verwenden (d. h. Komprimierungsprogramme, die nicht Teil des Betriebssystems sind), müssen Sie eine Systemdiskette erstellen, die saubere Kopien der Komprimierungstreiber sowie eine CONFIG.SYS-Datei enthält, die diese Treiber lädt. Durch diese saubere Systemdiskette kann das Betriebssystem die Festplatte lesen, und FindVirus kann die Dateien auf der Festplatte überprüfen.

Wenn Sie beispielsweise das Microsoft-Dienstprogramm DriveSpace in MS-DOS 6.22 verwenden, formatieren Sie die saubere Systemdiskette mit folgendem Befehl (wenn die Diskette in Laufwerk A: eingelegt ist):

```
FORMAT A: /U /S
```

Mit Hilfe dieser Diskette können Sie den Computer starten und auf das komprimierte Laufwerk zugreifen.

Wenn eine Festplatte mit den Microsoft-Programmen DoubleSpace oder DriveSpace komprimiert ist, wird ein „Host“-Laufwerk erstellt. Diesem Laufwerk wird im allgemeinen der Buchstabe H zugewiesen. Das Laufwerk enthält die Datei COMMAND.COM und folgende versteckte Dateien:

```
IO.SYS
MSDOS.SYS
DRVSPACE.BIN
DRVSPACE.000
```

DRVSPACE.INI

Wenn der Computer normal gestartet wird, werden die Systemdateien von Laufwerk H: (dem „Host“-Laufwerk) geladen, das mit Hilfe von DRVSPACE.BIN die Datei DRVSPACE.000 als Laufwerk C: aufsetzt.

Eine wie beschrieben formatierte Diskette enthält die normalen Systemdateien sowie die Datei DRVSPACE.BIN, durch die sowohl auf das „Host“-Laufwerk (H:) als auch auf das komprimierte Laufwerk (C:) normal zugegriffen werden kann.

Falls Sie ein anderes Dienstprogramm zur Festplattenkomprimierung verwenden, sind die in diesem Handbuch angegebenen Dateinamen möglicherweise anders.

2. Schalten Sie den Computer ein. Entfernen Sie die DOS-Systemdiskette, wenn die Eingabeaufforderung A:\ angezeigt wird. Wir empfehlen Ihnen, an diesem Punkt zu überprüfen, ob Sie auf alle normalen Laufwerke zugreifen können. Falls Sie nicht auf alle normalen Laufwerke zugreifen können, liegt gegebenenfalls ein Konfigurationsproblem vor.

3. Legen Sie die SOS-Diskette ein. Geben Sie folgendes ein:

   MB_MENU <Eingabetaste>

4. Drücken Sie <F2>, wenn die Benutzeroberfläche der SOS-Diskette angezeigt wird, um mit der Überprüfung aller ausführbaren Dateien auf der (den) lokalen Festplatte(n) zu beginnen.

5. Wenn der Bericht anzeigt, daß der Computer virenfrei ist, beenden Sie die SOS-Diskette durch Drücken von <Esc>; nehmen Sie dann die Diskette aus dem Laufwerk, und starten Sie den Computer neu. Fahren Sie mit Schritt 6 fort, falls ein Virus gefunden wird.

6. Drücken Sie F4 auf der Benutzeroberfläche der SOS-Diskette, um den Computer auf Viren zu überprüfen und bekannte Viren zu entfernen, bevor Sie mit der Installation fortfahren. Wenn der Bericht anzeigt, daß der Computer virenfrei ist, beenden Sie die SOS-Diskette durch Drücken von <Esc>; nehmen Sie dann die Diskette aus dem Laufwerk, und starten Sie den Computer neu.

1.2 README-Dateien

Als Teil der Installation wird eine README-Datei in den Toolkit-Ordner kopiert. Diese Datei enthält Ergänzungen zu den Handbüchern sowie Informationen über die neuesten Toolkit-Entwicklungen; wir empfehlen daher, diese Datei genau durchzulesen.

Sie werden während der Toolkit-Installation gefragt, ob Sie die README-Datei lesen möchten. Sie können die Datei auch zu einem späteren Zeitpunkt in einem Texteditor anzeigen lassen, wie z. B. dem Editor von Microsoft.

1.3 Windows 3.x

Systemvoraussetzungen

Dr Solomon's Anti-Virus Toolkit läuft auf jedem IBM- oder IBM-kompatiblen Computer, auf dem Windows 3.x ausgeführt wird. Das System sollte über folgendes verfügen:

- DOS 3.3 oder höher; geben Sie folgendes ein, um zu überprüfen, welche DOS-Version ausgeführt wird:

  `VER` <Eingabetaste>

  Diese Eingabe erfolgt an der DOS-Eingabeaufforderung.

Für die Installation benötigen Sie:

- 5 MB Festplattenspeicher für das Windows- und DOS Toolkit.

So überprüfen Sie, ob Sie genügend Festplattenspeicher haben:

Gehen Sie zur DOS-Eingabeaufforderung. Geben Sie den Buchstaben des Laufwerks ein, auf dem Sie das Toolkit installieren möchten, und drücken Sie dann die Eingabetaste. Beispiel: Geben Sie

`C:\` <Eingabetaste>

ein. Wenn die Eingabeaufforderung C: angezeigt wird, geben Sie

`DIR` <Eingabetaste>

ein. Sie sehen eine Verzeichnisliste des Laufwerks, gefolgt von der Anzeige, wieviel Festplattenspeicher benutzt wird und wie viele Byte frei sind. Für die Installation des Windows- und DOS-Toolkit müssen mindestens 5.000.000 Byte frei sein.

VirusGuard, das in DOS residente Überprüfungsprogramm, läuft schneller, wenn Ihr System über folgendes verfügt:

- XMS-Speicher;
- EMS-Speicher;
- ein RAM-Laufwerk.

Falls Sie das Toolkit in einem Netzwerk oder auf mehreren Computern gleichzeitig ausführen möchten, sollten Sie sich bei Dr Solomon's oder Ihrem Händler nach einer Unternehmslizenz erkundigen.

Installation des Toolkit

Vor der Installation von Dr Solomon's Anti-Virus Toolkit sollten Sie alle laufenden Windows-Anwendungen schließen.

Vermeiden von Konflikten mit anderer Anti-Virus-Software

Um Konflikte zu vermeiden, empfehlen wir, vor der Installation des Toolkit alle anderen Anti-Virus-Programme zu deinstallieren.

Warnung

Insbesondere müssen Sie vor der Installation von WinGuard alle anderen automatischen Überprüfungsprogramme (Zugriffsscanner) bzw. speicherresidenten Virensuchprogramme deinstallieren, wie zum Beispiel Scanshield von McAfee.

Installation von CD-ROM

Schnellinstallation

Tip

In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Durch die Aktualisierung des Toolkit können Sie bestehende Toolkit-Konfigurationen der vorigen Toolkit-Version beibehalten. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 10.

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.

2. Wählen Sie **Ausführen** aus dem Menü **Datei**.

3. Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

   ```
   \SETUP
   ```

   ein, und wählen Sie **OK**. Beispiel:

   ```
   D:\SETUP
   ```

4. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.

5. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon's Anti-Virus Toolkit für Windows 3.x zu bestätigen. Klicken Sie auf **Installieren**.

6. Das Dialogfeld für die Überprüfung des Datenträgers mit der SOS-Diskette wird angezeigt. Klicken Sie auf **OK**, wenn Sie den Computer bereits mit der SOS-Diskette von Dr Solomon's überprüft haben. Wenn Sie den Computer noch nicht überprüft haben, lesen Sie den Abschnitt „Erste Überprüfung auf Viren“ auf Seite 1.

7. Das Dialogfeld **Zielverzeichnis auswählen** wird angezeigt. Wenn Sie das Toolkit in einem anderen Verzeichnis als dem angegebenen installieren möchten, klicken Sie auf **Durchsuchen** und wählen dann das Laufwerk und/oder Verzeichnis aus, wo das Toolkit installiert werden soll. Klicken Sie auf **Weiter**.

   Sie können die Installation durch Klicken auf **Abbrechen** beenden.

8. Klicken Sie auf **Ja**, um die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen.

Tip

Wir empfehlen Ihnen, die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen. Wenn Sie sich entscheiden, diese nicht zu aktivieren, können Sie dies später tun. Informationen zur Aktivierung von VirusGuard finden Sie im Thema „VirusGuard“ der Online-Hilfe zum Toolkit. Informationen zur Aktivierung von WinGuard finden Sie im Abschnitt „Ändern der Konfiguration von WinGuard“ auf Seite 94.

9. Klicken Sie auf **Ja**, um die Aktivierung des Zeitplaners Dr Solomon's Scheduler zu bestätigen. Wenn Sie auf **Nein** klicken, können Sie den Zeitplaner auch später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Anschnitt „Ausführung des Zeitplaners“ auf Seite 138.

   Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

10. Klicken Sie auf **Ja**, um die README-Datei zu lesen, und schließen Sie nach dem Lesen die Datei, um zur Installation zurückzukehren.

11. Klicken Sie auf **OK**, um eine Überprüfung des Computers auf Viren zu starten. FindVirus wird sofort ausgeführt. Falls ein Virus gefunden wird, finden Sie Informationen zur Beseitigung der Infektion im Abschnitt „Entfernung von Viren aus Laufwerken“ auf Seite 151.

12. Klicken Sie im Dialogfeld **Alles in Ordnung** auf **OK** und anschließend auf **Beenden**, um das FindVirus-Fenster zu schließen. Falls eine Diskette im Diskettenlaufwerk ist, entfernen Sie diese.

Tip

Wir empfehlen, den Computer jetzt neu zu starten, damit VirusGuard und WinGuard, die automatischen Virensuchprogramme (Zugriffsscanner) von Dr Solomon's aktiviert werden.

13. Wählen Sie eine der Optionen im Dialogfeld **Installation abgeschlossen**, und klicken Sie auf **Weiter**.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Erweiterte Installationsoption

Tip

Über diese Option wird eine vollständige Version des Toolkit installiert, durch die das bereits vorhandene Toolkit mit allen dafür festgelegten Konfigurationen überschrieben wird.

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Workstation CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.

2. Wählen Sie **Ausführen** aus dem Menü **Datei**.

3. Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

   ```
   \SETUP
   ```

   ein, und klicken Sie auf **OK**. Beispiel:

   ```
   D:\SETUP
   ```

4. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Erweiterte Installationsoptionen**, und klicken Sie auf **Weiter**.

5. Wählen Sie im nächsten Dialogfeld **Dr Solomon's Anti-Virus Toolkit installieren**, und klicken Sie auf **Weiter**.

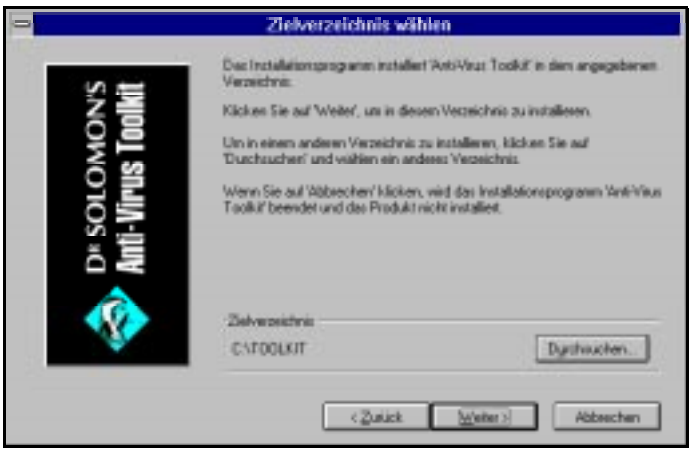
6. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon's Anti-Virus Toolkit für Windows 3.x zu bestätigen. Klicken Sie auf **Installieren**.

7. Das folgende Dialogfeld wird angezeigt:

   Klicken Sie auf **OK**, wenn Sie den Computer bereits mit der SOS-Diskette von Dr Solomon's überprüft haben. Wenn Sie den Computer noch nicht überprüft haben, lesen Sie den Abschnitt „Erste Überprüfung auf Viren" auf Seite 1.

8. Im Dialogfeld **Zielverzeichnis auswählen** können Sie Laufwerk und Verzeichnis für die Installation des Toolkit festlegen. Wenn Sie das Toolkit in einem anderen Verzeichnis als dem vorgegebenen installieren möchten, klicken Sie auf **Durchsuchen** und wählen dann das Laufwerk und/oder Verzeichnis aus, wo das Toolkit installiert werden soll. Klicken

Sie auf **Weiter**, wenn Sie einen Installationspfad für das Toolkit festgelegt haben.



Sie können die Installation durch Klicken auf **Abbrechen** beenden.

9. Klicken Sie auf **Ja**, um die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen.

.

Tip

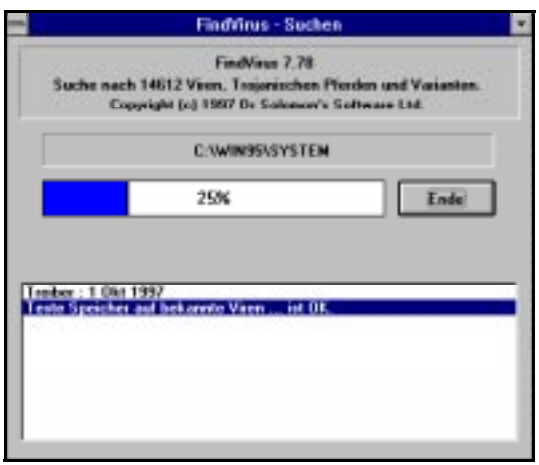
Wir empfehlen Ihnen, die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen. Wenn Sie sich entscheiden, diese nicht zu aktivieren, können Sie dies später tun. Informationen zur Aktivierung von VirusGuard finden Sie im Thema „VirusGuard“ der Online-Hilfe zum Toolkit. Informationen zur Aktivierung von WinGuard finden Sie im Abschnitt „Ändern der Konfiguration von WinGuard“ auf Seite 94.

10. Klicken Sie auf **Ja**, um die Aktivierung des Zeitplaners Dr Solomon's Scheduler zu bestätigen. Wenn Sie auf **Nein** klicken, können Sie den Zeitplaner auch später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Anschnitt „Ausführung des Zeitplaners“ auf Seite 138.

Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

11. Klicken Sie auf **Ja**, um die README-Datei zu lesen, und schließen Sie nach dem Lesen die Datei, um zur Installation zurückzukehren.

12. Klicken Sie auf **OK**, um eine Überprüfung des Computers auf Viren zu starten. FindVirus wird sofort ausgeführt.



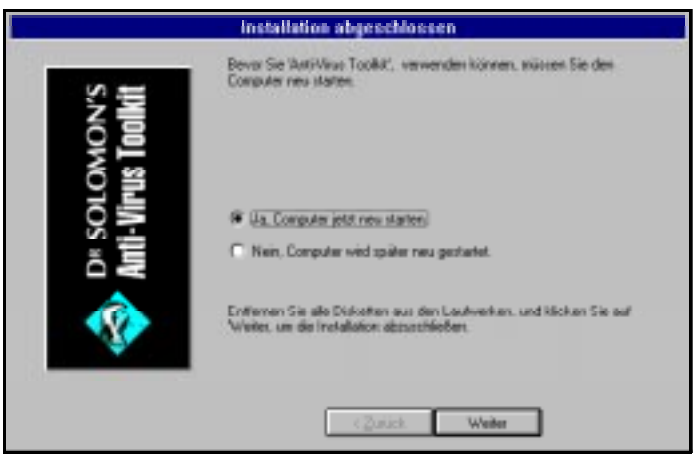
Falls ein Virus gefunden wird, finden Sie Informationen zur Beseitigung der Infektion im Abschnitt „Entfernung von Viren aus Laufwerken“ auf Seite 151.

13. Klicken Sie im Dialogfeld **Alles in Ordnung** auf **OK** und anschließend auf **Beenden**, um das FindVirus-Fenster zu schließen. Falls eine Diskette im Diskettenlaufwerk ist, entfernen Sie diese.

Tip

Wir empfehlen, den Computer jetzt neu zu starten, damit VirusGuard und WinGuard, die automatischen Virensuchprogramme (Zugriffsscanner) von Dr Solomon’s aktiviert werden.

14. Wähle Sie eine der Optionen im Dialogfeld **Installation abgeschlossen**, und klicken Sie auf **Beenden**.



Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

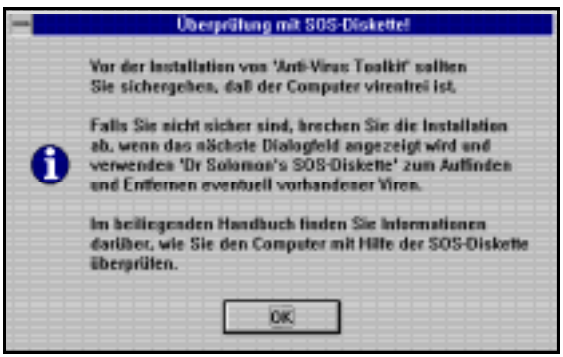
Installation von Diskette

1. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **Windows 3.X**) in das Diskettenlaufwerk ein.

2. Wählen Sie **Ausführen** aus dem Menü **Datei** des Programm-Managers.

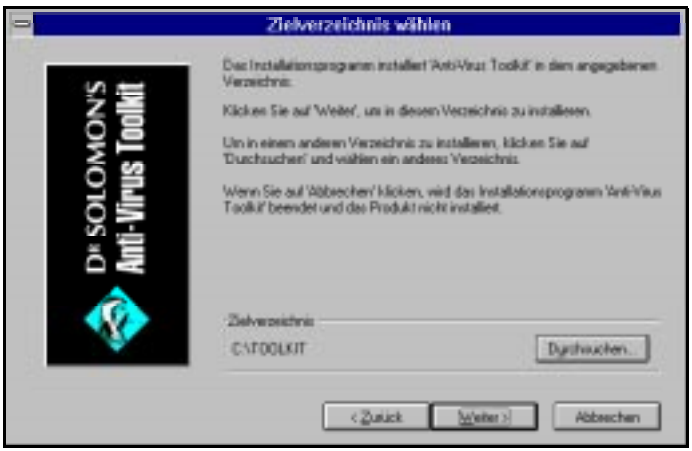
3. Geben Sie `A:\Setup` ein, und klicken Sie auf **OK**.

4. Das Dialogfeld für die Überprüfung des Datenträgers mit der SOS-Diskette wird angezeigt. Klicken Sie auf **OK**, wenn Sie den Computer bereits mit der SOS-Diskette von Dr Solomon's überprüft haben. Wenn Sie den Computer noch nicht überprüft haben, lesen Sie den Abschnitt „Erste Überprüfung auf Viren“ auf Seite 1.



5. Im Dialogfeld **Zielverzeichnis auswählen** können Sie Laufwerk und Verzeichnis für die Installation des Toolkit festlegen. Wenn Sie das Toolkit in einem anderen Verzeichnis als dem vorgegebenen installieren möchten, klicken Sie auf **Durchsuchen** und wählen dann das Laufwerk und/oder

Verzeichnis aus, wo das Toolkit installiert werden soll. Klicken Sie auf **Weiter**, wenn Sie einen Installationspfad für das Toolkit festgelegt haben.



6. Legen Sie weitere Installationsdisketten ein, wenn Sie dazu aufgefordert werden, und klicken Sie danach jeweils auf **OK**.

   Sie können die Installation durch Klicken auf **Abbrechen** beenden.

7. Klicken Sie auf **Ja**, um die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen.

Tip

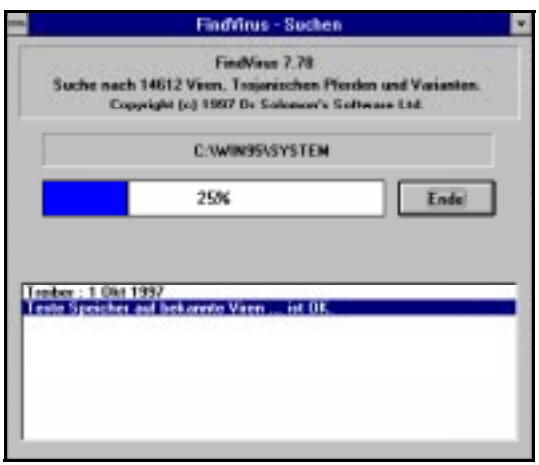
Wir empfehlen Ihnen, die Aktivierung der automatischen Überprüfung (der Zugriffsscanner) zu bestätigen. Wenn Sie sich entscheiden, diese nicht zu aktivieren, können Sie dies später tun. Informationen zur Aktivierung von VirusGuard finden Sie im Thema „VirusGuard“ der Online-Hilfe zum Toolkit. Informationen zur Aktivierung von WinGuard finden Sie im Abschnitt „Ändern der Konfiguration von WinGuard“ auf Seite 94.

8. Klicken Sie auf **Ja**, um die Aktivierung des Zeitplaners Dr Solomon's Scheduler zu bestätigen. Wenn Sie auf **Nein** klicken, können Sie den Zeitplaner auch später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Anschnitt „Ausführung des Zeitplaners“ auf Seite 138.

Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

9. Klicken Sie auf **Ja**, um die README-Datei zu lesen, und schließen Sie nach dem Lesen die Datei, um zur Installation zurückzukehren.

10. Klicken Sie auf **OK**, um eine Überprüfung des Computers auf Viren zu starten. FindVirus wird sofort ausgeführt.



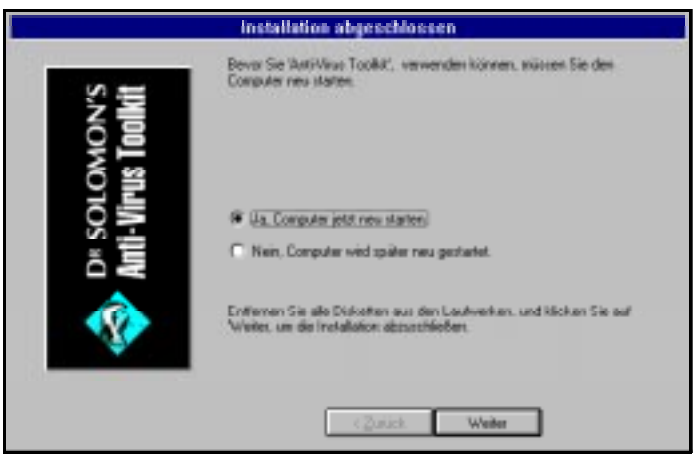
Falls ein Virus gefunden wird, finden Sie Informationen zur Beseitigung der Infektion im Abschnitt „Entfernung von Viren aus Laufwerken“ auf Seite 151.

11. Klicken Sie im Dialogfeld **Alles in Ordnung** auf **OK** und anschließend auf **Beenden**, um das FindVirus-Fenster zu schließen. Falls eine Diskette im Diskettenlaufwerk ist, entfernen Sie diese.

Tip

Wir empfehlen, den Computer jetzt neu zu starten, damit VirusGuard und WinGuard, die automatischen Virensuchprogramme (Zugriffsscanner) von Dr Solomon’s aktiviert werden.

12. Wähle Sie eine der Optionen im Dialogfeld **Installation abgeschlossen**, und klicken Sie auf **Weiter**.



Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Deinstallation des Toolkit

Warnung

Wenn Sie Ihr System von Windows 3.x auf Windows 95 aufrüsten, müssen Sie zunächst WinGuard deaktivieren. Die Windows 3.x-Version von WinGuard ist mit Windows 95 nicht kompatibel.

Tip

Wenn Sie ein Windows 3.x-Toolkit in der Version 7.75 oder früher deinstallieren, müssen Sie die Deinstallation des Toolkit manuell vornehmen. Anleitungen zur manuellen Deinstallation des Windows 3.x-Toolkit finden Sie im Abschnitt „Deinstallation ohne ein Deinstallationsprogramm“ auf Seite 179.

So deinstallieren Sie Dr Solomon’s Anti-Virus Toolkit für Windows 3.x:

1. Doppelklicken Sie in Windows auf die Programmgruppe **Dr Solomon’s AVTK**.

2. Doppelklicken Sie auf **Dr Solomon’s AVTK deinstallieren**.

3. Klicken Sie in dem angezeigten Warndialogfeld auf **Ja.**

4. Falls WinGuard läuft, muß das Deinstallationsprogramm den Computer neu starten, um WinGuard zu deaktivieren. Sie werden in einem Dialogfeld gefragt, ob das Deinstallationsprogramm den Computer neu starten soll. Klicken Sie auf **Ja**. Wenn Sie **Nein** wählen, wird die Deinstallation abgebrochen.

   Der Bildschirm wird schwarz, Windows wird neu gestartet und die Deinstallation von Dr Solomon’s Anti-Virus Toolkit fortgesetzt.

5. An diesem Punkt fragt Sie das Deinstallationsprogramm möglicherweise, ob einige Dateien gelöscht oder verschoben werden sollen, zum Beispiel Protokoll- oder Zeitplanerdateien. In diesem Dialogfeld können Sie folgende Möglichkeiten wählen:

- **Löschen**: Es wird nur die angezeigte Datei gelöscht.
- **Alle löschen**: Die angezeigte Datei und alle anderen Dateien in diesem Verzeichnis werden ohne weitere Bestätigungsaufforderungen gelöscht.
- **Verschieben**: Es wird nur die angezeigte Datei verschoben. Das Dialogfeld **Speichern unter** wird angezeigt. Wählen Sie ein neues Verzeichnis und / oder einen neuen Dateinamen für die Datei.
- **Alle verschieben**: Die angezeigte Datei und alle anderen Dateien in diesem Verzeichnis werden ohne weitere Bestätigungsaufforderungen verschoben. Das Dialogfeld **Zielverzeichnis auswählen** wird angezeigt. Wählen Sie ein neues Verzeichnis aus.

   Entscheiden Sie sich für eine dieser Möglichkeiten.

6. Klicken Sie im nächsten Dialogfeld auf **Fertig**, um die Deinstallation von Dr Solomon's Toolkit abzuschließen.

1.4 Windows 95

Systemvoraussetzungen

Das Anti-Virus Toolkit für Windows 95 läuft auf jedem Computer, auf dem Windows 95 ausgeführt wird.

Es werden etwa 5 MB Festplattenspeicher benötigt.

Falls Sie das Toolkit auf mehreren Computern gleichzeitig installieren möchten, sollten Sie sich bei Dr Solomon's oder Ihrem Händler nach einer Unternehmslizenz erkundigen.

Installation des Toolkit

Vermeiden von Konflikten mit anderer Anti-Virus-Software

Um Konflikte zu vermeiden, empfehlen wir, vor der Installation des Toolkit alle anderen Anti-Virus-Programme zu deinstallieren.

Warnung

Insbesondere müssen Sie vor der Installation von WinGuard alle anderen automatischen Überprüfungsprogramme (Zugriffsscanner) bzw. speicherresidenten Virensuchprogramme deinstallieren, wie zum Beispiel Scanshield von McAfee.

Installation von CD-ROM

Warnung

Falls Sie ein Windows 3.x-Toolkit installiert haben, müssen Sie dieses vor der Installation des Windows 95-Toolkit entfernen. Anleitungen zur Entfernung des Windows 3.x-Toolkit finden Sie im Abschnitt „Deinstallation des Toolkit“ auf Seite 19.

Schnellinstallation

Tip

In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Durch die Aktualisierung des Toolkit können Sie bestehende Toolkit-Konfigurationen der vorigen Toolkit-Version beibehalten. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 25.

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.

2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.

3. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon’s Anti-Virus Toolkit für Windows 95 zu bestätigen. Klicken Sie auf **Installieren**.

4. In einem weiteren Dialogfeld werden Sie aufgefordert, die Installation fortzusetzen oder abzubrechen. Klicken Sie auf **Weiter**.

5. Im nächsten Dialogfeld werden Sie gefragt, wo das Toolkit installiert werden soll. Geben Sie den gewünschten Installationspfad ein, falls Sie das vorgegebene Verzeichnis nicht übernehmen möchten. Klicken Sie danach auf **OK**.

   Durch Klicken auf **Abbrechen** können Sie die Installation beenden.

6. Sie werden gefragt, welche Einstellungen WinGuard haben soll.

Tip

Wir empfehlen die Auswahl von **WinGuard automatisch ausführen**. WinGuard läuft dann ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77.

7. Sie werden gefragt, welche Einstellungen VirusGuard haben soll. VirusGuard ist das DOS-Gegenstück zu WinGuard. Das Programm bietet Virenschutz, wenn Windows 95 nicht aktiv ist. VirusGuard kann so konfiguriert werden, daß bei verschiedenen Operationen eine Überprüfung auf Viren stattfindet (beim Kopieren von Dateien, der Ausführung von Programmdateien usw.).

Hilfe

Einzelheiten über die VirusGuard-Optionen finden Sie im Überblick über die Parameter des Themas „VirusGuard“ in der Online-Hilfe zum Toolkit.

Tip

Wir empfehlen die Auswahl einer der Optionen unter **VirusGuard installieren**..... . Wenn Sie **Standardsicherheit** wählen, werden Dateien bei jedem Kopierversuch überprüft, während bei Auswahl der Option **Minimale Sicherheit** lediglich Dateien überprüft werden, die von Disketten kopiert werden sollen.

8. Wenn Sie sich für die Installation von VirusGuard entscheiden, wird Ihnen in einem Dialogfeld mitgeteilt, daß die Datei AUTOEXEC.BAT dahingehend geändert wurde, daß VirusGuard gestartet wird, und daß die ursprüngliche Datei AUTOEXEC.BAT als AUTOEXEC.DRS gespeichert wurde. Klicken Sie auf **OK**, um fortzufahren.

9. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon’s Scheduler gefragt. Wenn Sie **Ja** wählen, wird der Zeitplaner dem Autostart-Ordner hinzugefügt. Wenn Sie **Nein** wählen, müssen Sie den Zeitplaner manuell aufrufen, wenn Sie ihn ausführen möchten. Anleitungen zum Starten des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

   Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

10. Sie werden gefragt, ob Sie das 16-Bit DOS-Dienstprogramm „CLEANBOO“ installieren möchten. Dieses Dienstprogramm kann hilfreich sein, und wir empfehlen seine Installation. Weitere Informationen über das Dienstprogramm finden Sie im Abschnitt „CleanBoot“ auf Seite 182 oder unter dem Thema „CleanBoot“ in der Online-Hilfe zum Toolkit.

11. Wenn die Dateien auf die Festplatte kopiert worden sind, wird ein Meldungsfeld angezeigt, in dem Ihnen mitgeteilt wird, daß eine FindVirus-Überprüfung gestartet wird. Klicken Sie auf **OK**, um fortzufahren.

    In einem Dialogfeld wird der Fortschritt angezeigt. Sie können auf **Beenden** klicken, um die Überprüfung abzubrechen. Es wird empfohlen, dies nicht zu tun, da dann möglicherweise unentdeckte Viren auf der Festplatte bleiben. Wenn Sie diese Überprüfung abbrechen, sollten Sie so bald wie möglich nach Abschluß der Installation eine vollständige FindVirus-Überprüfung durchführen.

    Wenn die Überprüfung abgeschlossen ist, werden die Ergebnisse in einem Meldungsfeld angezeigt. Klicken Sie auf **OK**, um fortzufahren.

    Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.

12. Klicken Sie auf **Beenden.**

13. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon’s Anti-Virus Toolkit für Windows 95 einsehen möchten. Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

14. Sie werden gefragt, ob Sie den Computer neu starten möchten. Wenn Sie **Nein** wählen, werden der Zeitplaner, VirusGuard und WinGuard erst beim nächsten Neustart des Computers aktiv.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Erweiterte Installationsoption

Warnung

Falls Sie ein Windows 3.x-Toolkit installiert haben, müssen Sie dieses vor der Installation des Windows 95-Toolkit entfernen. Anleitungen zur Entfernung des Windows 3.x-Toolkit finden Sie im Abschnitt „Deinstallation des Toolkit“ auf Seite 19.

Tip

Über diese Option wird eine vollständige Version des Toolkit installiert, durch die das bereits vorhandene Toolkit mit allen dafür festgelegten Konfigurationen überschrieben wird.

Tip

Dr Solomon’s Anti-Virus Toolkit für Windows 95 kann über SMS installiert werden. Installationsoptionen finden Sie in der mit Ihrem Toolkit gelieferten Microsoft SMS PDF-Datei.

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.

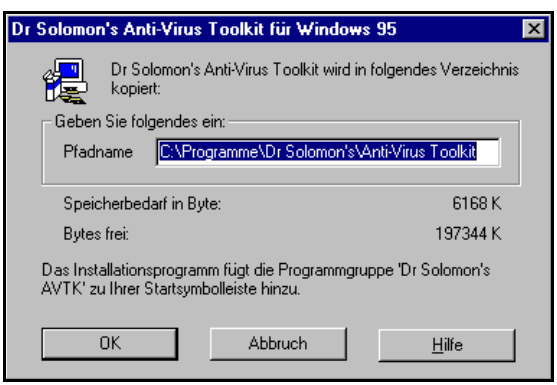
2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Erweiterte Installationsoptionen**, und klicken Sie auf **Weiter**.

3. Wählen Sie im nächsten Dialogfeld **Dr Solomon’s Anti-Virus Toolkit installieren**, und klicken Sie auf **Weiter**.

4. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon's Anti-Virus Toolkit für Windows 95 zu bestätigen. Klicken Sie auf **Installieren**.

5. In einem weiteren Dialogfeld werden Sie aufgefordert, die Installation fortzusetzen oder abzubrechen. Klicken Sie auf **Weiter**.

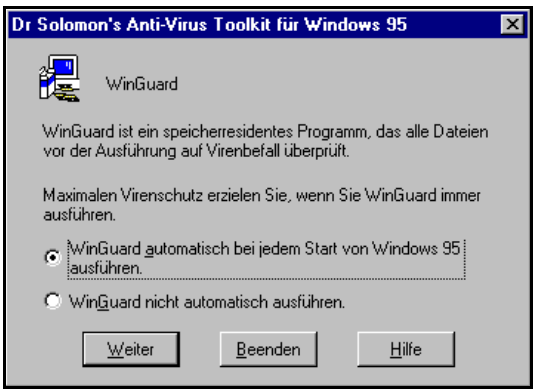
Im nächsten Dialogfeld werden Sie gefragt, wo das Toolkit installiert werden soll.



6. Geben Sie den gewünschten Installationspfad ein, falls Sie das vorgegebene Verzeichnis nicht übernehmen möchten, und klicken Sie danach auf **OK**.

   Durch Klicken auf **Abbrechen** können Sie die Installation beenden.

7. Sie werden nach den Einstellungen für die Ausführung von WinGuard gefragt.



Tip

Wir empfehlen die Auswahl von **WinGuard automatisch ausführen**. WinGuard läuft dann ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77.

8. Sie werden nach den Einstellungen für die Ausführung von VirusGuard gefragt.

VirusGuard ist das DOS-Gegenstück zu WinGuard. Das Programm bietet Virenschutz, wenn Windows 95 nicht aktiv ist. VirusGuard kann so konfiguriert werden, daß bei verschiedenen Operationen eine Überprüfung auf Viren stattfindet (beim Kopieren von Dateien, der Ausführung von Programmdateien usw.)

Hilfe

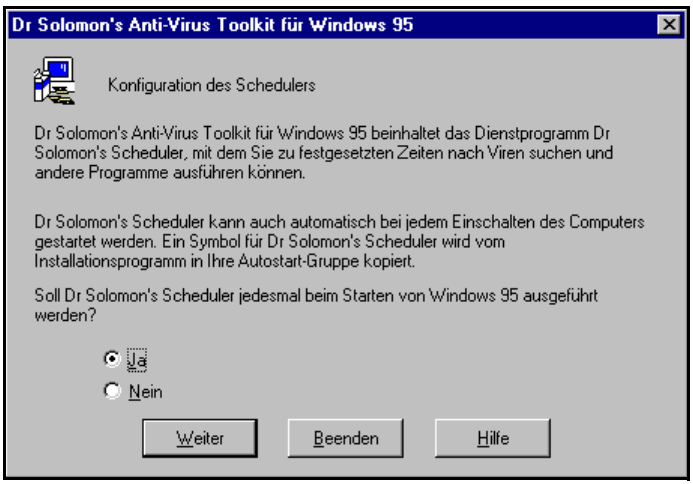
Einzelheiten über die VirusGuard-Optionen finden Sie im Überblick über die Parameter des Themas „VirusGuard“ in der Online-Hilfe zum Toolkit.

Tip

Wir empfehlen die Auswahl einer der Optionen unter **VirusGuard installieren**..... . Wenn Sie **Standardsicherheit** wählen, werden Dateien bei jedem Kopierversuch überprüft, während bei Auswahl der Option **Minimale Sicherheit** lediglich Dateien überprüft werden, die von Disketten kopiert werden sollen.

9. Wenn Sie sich für die Installation von VirusGuard entscheiden, wird Ihnen in einem Dialogfeld mitgeteilt, daß die Datei AUTOEXEC.BAT dahingehend geändert wurde, daß VirusGuard gestartet wird, und daß die ursprüngliche Datei AUTOEXEC.BAT als AUTOEXEC.DRS gespeichert wurde. Klicken Sie auf **OK**, um fortzufahren.

10. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon's Scheduler gefragt.



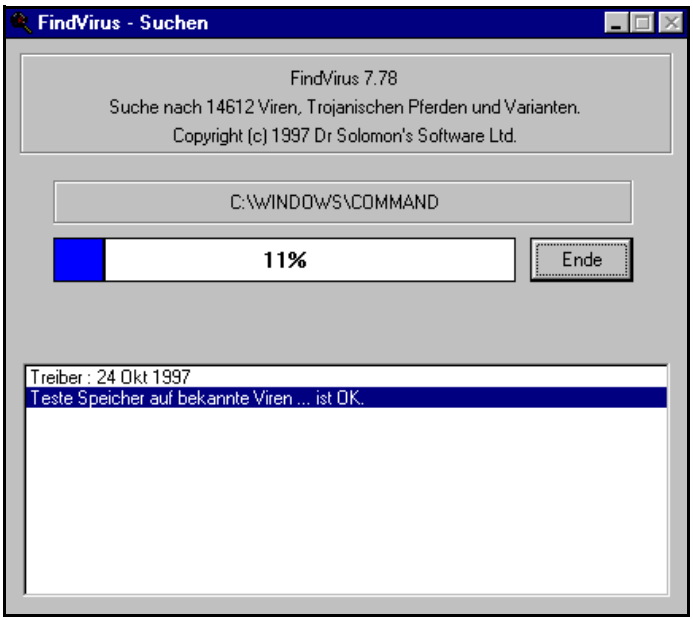
Wenn Sie **Ja** wählen, wird der Zeitplaner dem Autostart-Ordner hinzugefügt. Wenn Sie **Nein** wählen, müssen Sie den Zeitplaner manuell aufrufen, wenn Sie ihn ausführen möchten. Anleitungen zum Starten des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

11. Sie werden gefragt, ob Sie das 16-Bit DOS-Dienstprogramm „CLEANBOO“ installieren möchten. Dieses Dienstprogramm kann hilfreich sein, und wir empfehlen seine Installation. Weitere Informationen über das Dienstprogramm finden Sie im Abschnitt „CleanBoot“ auf Seite 182 oder unter dem Thema „Cleanboot“ in der Online-Hilfe zum Toolkit.

12. Wenn die Dateien auf die Festplatte kopiert worden sind, wird ein Meldungsfeld angezeigt, in dem Ihnen mitgeteilt wird, daß eine FindVirus-Überprüfung gestartet wird. Klicken Sie auf **OK**, um fortzufahren.

In einem Dialogfeld wird der Fortschritt angezeigt:



Sie können auf **Beenden** klicken, um die Überprüfung abzubrechen. Es wird empfohlen, dies nicht zu tun, da dann möglicherweise unentdeckte Viren auf der Festplatte bleiben. Wenn Sie diese Überprüfung abbrechen, sollten Sie so bald wie möglich nach Abschluß der Installation eine vollständige FindVirus-Überprüfung durchführen.

13. Wenn die Überprüfung abgeschlossen ist, werden die Ergebnisse in einem Meldungsfeld angezeigt. Klicken Sie auf **OK**, um fortzufahren.

    Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.

14. Klicken Sie auf **Beenden.**

15. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon’s Anti-Virus Toolkit für Windows 95 einsehen möchten.

    Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei

fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

16. Sie werden gefragt, ob Sie den Computer neu starten möchten.

Wenn Sie **Nein** wählen, werden der Zeitplaner, VirusGuard und WinGuard erst beim nächsten Neustart des Computers aktiv.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Installation von Diskette

Warnung

Falls Sie ein Windows 3.x-Toolkit installiert haben, müssen Sie dieses vor der Installation des Windows 95-Toolkit entfernen. Anleitungen zur Entfernung des Windows 3.x-Toolkit finden Sie im Abschnitt „Deinstallation des Toolkit“ auf Seite 19.

Wenn Sie wissen, daß der Computer virenfrei ist und Sie das Windows 3.x-Toolkit deinstalliert haben, können Sie das Windows 95-Toolkit installieren.

1. Starten Sie Windows 95, und legen Sie Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **Windows 95**) in das Diskettenlaufwerk ein.

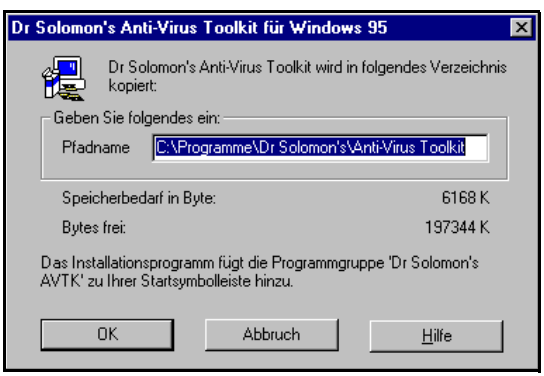
2. Klicken Sie auf **Start** und anschließend auf **Ausführen**. Geben Sie im Dialogfeld **Öffnen** folgendes ein:

   A:\SETUP

3. Klicken Sie auf **OK**.

4. In einem Dialogfeld werden Sie aufgefordert, die Installation fortzusetzen oder abzubrechen. Klicken Sie auf **Weiter**.

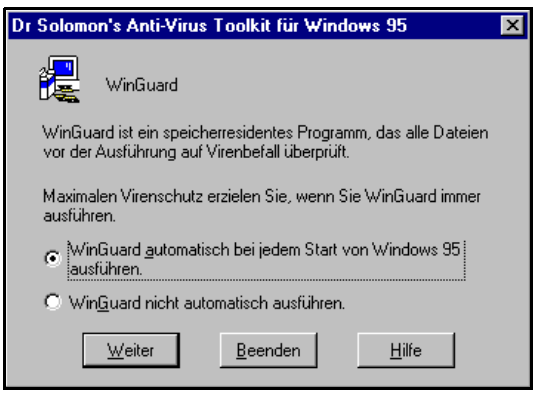
Im nächsten Dialogfeld werden Sie gefragt, wo das Toolkit installiert werden soll.



5. Geben Sie den gewünschten Installationspfad ein, falls Sie das vorgegebene Verzeichnis nicht übernehmen möchten. Klicken Sie danach auf **OK**.

6. Folgen Sie den Aufforderungen, weitere Disketten einzulegen. Durch Klicken auf **Abbrechen** können Sie die Installation beenden.

7. Sie werden nach den Einstellungen für die Ausführung von WinGuard gefragt.



Tip

Wir empfehlen die Auswahl von **WinGuard automatisch ausführen**. WinGuard läuft dann ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77.

8. Sie werden nach den Einstellungen für die Ausführung von VirusGuard gefragt.

VirusGuard ist das DOS-Gegenstück zu WinGuard. Das Programm bietet Virenschutz, wenn Windows 95 nicht aktiv ist. VirusGuard kann so konfiguriert werden, daß bei verschiedenen Operationen eine Überprüfung auf Viren stattfindet (beim Kopieren von Dateien, der Ausführung von Programmdateien usw.)

Hilfe

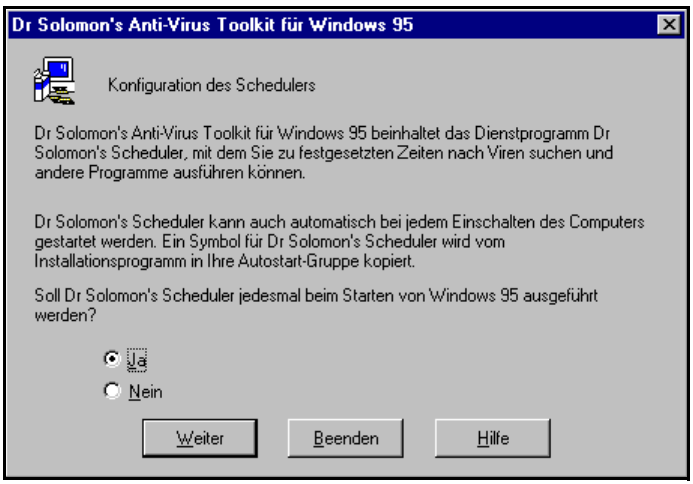
Einzelheiten über die VirusGuard-Optionen finden Sie im Überblick über die Parameter des Themas „VirusGuard“ in der Online-Hilfe zum Toolkit.

Tip

Wir empfehlen die Auswahl einer der Optionen unter **VirusGuard installieren**..... . Wenn Sie **Standardsicherheit** wählen, werden Dateien bei jedem Kopierversuch überprüft, während bei Auswahl der Option **Minimale Sicherheit** lediglich Dateien überprüft werden, die von Disketten kopiert werden sollen.

9. Wenn Sie sich für die Installation von VirusGuard entscheiden, wird Ihnen in einem Dialogfeld mitgeteilt, daß die Datei AUTOEXEC.BAT dahingehend geändert wurde, daß VirusGuard gestartet wird, und daß die ursprüngliche Datei AUTOEXEC.BAT als AUTOEXEC.DRS gespeichert wurde. Klicken Sie auf **OK**, um fortzufahren.

10. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon's Scheduler gefragt.



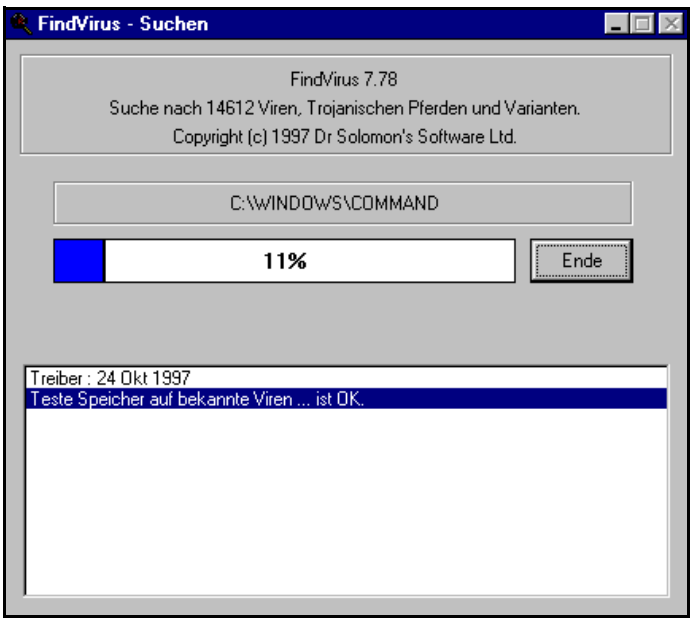
Wenn Sie **Ja** wählen, wird der Zeitplaner dem Autostart-Ordner hinzugefügt. Wenn Sie **Nein** wählen, müssen Sie den Zeitplaner manuell aufrufen, wenn Sie ihn ausführen möchten. Anleitungen zum Starten des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

11. Sie werden gefragt, ob Sie das 16-Bit DOS-Dienstprogramm „CLEANBOO“ installieren möchten. Dieses Dienstprogramm kann hilfreich sein, und wir empfehlen seine Installation. Weitere Informationen über das Dienstprogramm finden Sie im Abschnitt „CleanBoot“ auf Seite 182 oder unter dem Thema „CleanBoot“ in der Online-Hilfe zum Toolkit.

12. Wenn die Dateien auf die Festplatte kopiert worden sind, wird ein Meldungsfeld angezeigt, in dem Ihnen mitgeteilt wird, daß eine FindVirus-Überprüfung gestartet wird. Klicken Sie auf **OK**, um fortzufahren.

    In einem Dialogfeld wird der Fortschritt angezeigt:



    Sie können auf **Beenden** klicken, um die Überprüfung abzubrechen. Es wird empfohlen, dies nicht zu tun, da dann möglicherweise unentdeckte Viren auf der Festplatte bleiben. Wenn Sie diese Überprüfung abbrechen, sollten Sie so bald wie möglich nach Abschluß der Installation eine vollständige FindVirus-Überprüfung durchführen.

13. Wenn die Überprüfung abgeschlossen ist, werden die Ergebnisse in einem Meldungsfeld angezeigt. Klicken Sie auf **OK**, um fortzufahren.

    Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.

14. Klicken Sie auf **Beenden.**

15. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon's Anti-Virus Toolkit für Windows 95 einsehen möchten.

    Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

16. Sie werden gefragt, ob Sie den Computer neu starten möchten.

    Wenn Sie **Nein** wählen, werden der Zeitplaner, VirusGuard und WinGuard erst beim nächsten Neustart des Computers aktiv.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben, und lesen Sie auch den Abschnitt zur Fehlerbehebung unter „Fehlerbehebung und erweiterte Einstellungen“ auf Seite 179. Falls Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon's. Adressen und Telefon- und Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Deinstallation des Toolkit

Tip

Falls Dr Solomon's Anti-Virus Toolkit nicht auf der Registerkarte **Installieren/Deinstallieren** des Dialogfelds **Eigenschaften von Software** in der **Systemsteuerung** aufgeführt ist, müssen Sie das Toolkit manuell deinstallieren. Anleitung zur manuellen Deinstallation des Toolkit finden Sie im Abschnitt „Deinstallation ohne ein Deinstallationsprogramm“ auf Seite 179.

So deinstallieren Sie das Toolkit:

1. Klicken Sie auf **Start** und anschließend auf **Einstellungen** und auf **Systemsteuerung**.
2. Klicken Sie in der **Systemsteuerung** auf das Symbol **Software**.
3. Wählen Sie **Dr Solomon's Anti-Virus Toolkit** aus der Liste.
4. Klicken Sie auf **Hinzufügen/Entfernen**.
5. Bestätigen Sie die Entfernung des Programms, wenn Sie dazu aufgefordert werden.
6. Reagieren Sie auf die Aufforderung, dem Toolkit-Verzeichnis seit der Installation hinzugefügte Dateien (wie z. B. Berichtdateien) zu verschieben oder zu löschen.

1.5 Windows NT

Tip

Dr Solomon's Anti-Virus Toolkit für Windows NT kann über SMS installiert werden. Installationsoptionen finden Sie in der mit Ihrem Toolkit gelieferten Microsoft SMS PDF-Datei.

Systemvoraussetzungen

Hardwarevoraussetzungen

Das Anti-Virus Toolkit für Windows NT läuft auf Computern, auf denen Windows NT Workstation oder Server ausgeführt wird. Für das Programm wird ein Intel-Prozessor benötigt, und es läuft auf keiner anderen Windows NT-Hardwareplattform.

Es werden etwa 5 MB Festplattenspeicher benötigt.

WinGuard NT für Digital Alpha-Computer ist ebenfalls erhältlich. Weitere Informationen erhalten Sie von Dr Solomon's Software oder Ihrem Händler.

Softwarevoraussetzungen

Für die Ausführung des Anti-Virus Toolkit für Windows NT wird Windows NT Version 3.51 oder höher benötigt.

Wir empfehlen, daß Sie das jeweils neueste Service Pack von Microsoft für Windows NT verwenden.

Falls Sie das Toolkit in einem Netzwerk oder auf mehreren Computern gleichzeitig ausführen möchten, sollten Sie sich bei Dr Solomon's oder Ihrem Händler nach einer unternehmensweiten Lizenz erkundigen.

Dr Solomon's hat auch eine Anti-Virus Toolkit Management Edition für Windows NT Server entwickelt. Dieses Management Edition Toolkit verfügt über Funktionen zur Verteilung von Software und Konfiguration von Netzwerkcomputern.

Installation des Toolkit

Vermeiden von Konflikten mit anderer Anti-Virus-Software

Um Konflikte zu vermeiden, empfehlen wir, vor der Installation des Toolkit alle anderen Anti-Virus-Programme zu deinstallieren.

Warnung

Insbesondere müssen Sie vor der Installation von WinGuard NT alle anderen automatischen Überprüfungsprogramme (Zugriffsscanner) bzw. speicherresidenten Virensuchprogramme deinstallieren, wie zum Beispiel Scanshield von McAfee.

Installation von CD-ROM

Schnellinstallation

Tip

In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 43.

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

2. Wenn Sie Windows NT Version 4 ausführen, wird ein Toolkit-CD-Startbildschirm angezeigt.

Für Benutzer von Windows NT Version 3.51:
Wählen Sie nach dem Einlegen der Toolkit-CD in das CD-ROM-Laufwerk **Ausführen** aus dem Menü **Datei**.

Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

```
\SETUP
```

ein, und wählen Sie **OK**. Beispiel:

```
D:\SETUP
```

Der Toolkit-CD-Startbildschirm wird angezeigt.

3. Wählen Sie in dem angezeigten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.

4. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon's Anti-Virus Toolkit für Windows NT zu bestätigen. Klicken Sie auf **Installieren**.

5. Sie werden aufgefordert, das Installationsverzeichnis zu bestätigen. Geben Sie einen anderen Verzeichnispfad ein, wenn Sie die angezeigte Vorgabe nicht übernehmen möchten, und klicken Sie auf **Weiter**. Der Installationsprozeß wird gestartet.

   Durch Klicken auf **Abbrechen** können Sie die Installation jederzeit beenden. Wenn Sie das Programm später neu installieren möchten, sollten Sie alle im Toolkit-Verzeichnis vorhandenen Dateien löschen, die während der ersten Installation erstellt wurden.

6. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon's Scheduler gefragt. Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

   Wählen Sie **Ja**, um zu bestätigen, daß der Zeitplaner aktiviert werden soll. Wenn Sie **Nein** wählen, können Sie den Zeitplaner später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

7. Sie werden nach den Einstellungen für die Ausführung von WinGuard NT gefragt.
   WinGuard NT läuft ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77. Wir empfehlen Ihnen, **Ja** zu wählen.

8. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon's Anti-Virus Toolkit für Windows NT einsehen möchten. Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

9. FindVirus wird automatisch ausgeführt, um die lokalen Festplatten auf Viren zu überprüfen. Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.

Warnung

Geraten Sie nicht in Panik, falls FindVirus einen Virus auf dem Computer findet! Informationen über Vorgehensweisen bei Virenbefall des Computers finden Sie in Kapitel 6, „Entfernung von Viren“.

An dieser Stelle werden Sie möglicherweise aufgefordert, den Computer neu zu starten.

Die Installation ist jetzt abgeschlossen, und der Computer ist auf Viren überprüft worden. Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon's. Adressen und Telefon- und Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Erweiterte Installationsoption

Tip 	Über diese Option wird eine vollständige Version des Toolkit installiert. Durch die in Kürze erhältliche Software für die Aktualisierung können Sie das Schnellinstallationsverfahren für die Aktualisierung eines bereits vorhandenen Toolkit verwenden.

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

2. Wenn Sie Windows NT Version 4 ausführen, wird ein Toolkit-CD-Startbildschirm angezeigt.

Für Benutzer von Windows NT Version 3.51:
Wählen Sie nach dem Einlegen der Toolkit-CD in das CD-ROM-Laufwerk **Ausführen** aus dem Menü **Datei**.

Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

```
\SETUP
```

ein, und wählen Sie **OK**. Beispiel:

```
D:\SETUP
```

Der Toolkit-CD-Startbildschirm wird angezeigt.

3. Wählen Sie in dem angezeigten Dialogfeld **Erweiterte Installationsoptionen**, und klicken Sie auf **Weiter**.

4. Wählen Sie im nächsten Dialogfeld **Dr Solomon's Anti-Virus Toolkit installieren**, und klicken Sie auf **Weiter**.

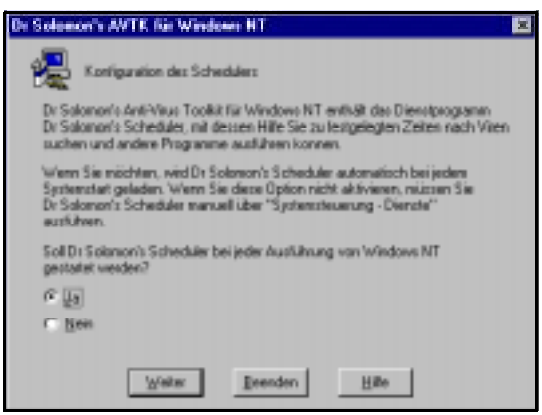
5. Im nächsten Dialogfeld werden Sie aufgefordert, die Installation von Dr Solomon's Anti-Virus Toolkit für Windows NT zu bestätigen. Klicken Sie auf **Installieren**.

6. Sie werden aufgefordert, das Installationsverzeichnis zu bestätigen:

7. Geben Sie einen anderen Verzeichnispfad ein, wenn Sie die angezeigte Vorgabe nicht übernehmen möchten, und klicken Sie auf **Weiter**. Der Installationsprozeß wird gestartet.

   Durch Klicken auf **Abbrechen** können Sie die Installation jederzeit beenden. Wenn Sie das Programm später neu installieren möchten, sollten Sie alle im Toolkit-Verzeichnis vorhandenen Dateien löschen, die während der ersten Installation erstellt wurden.

8. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon's Scheduler gefragt.



Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

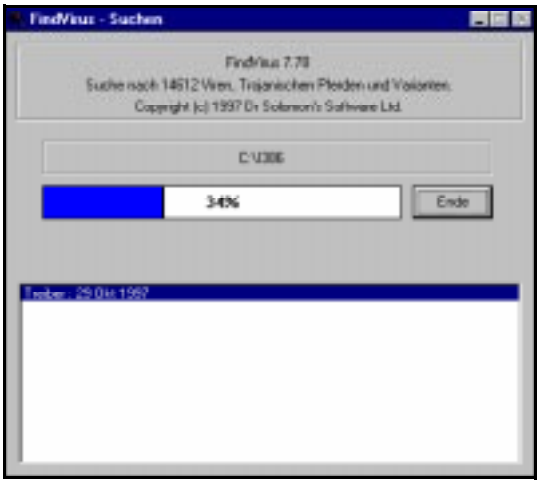
Wählen Sie **Ja**, um zu bestätigen, daß der Zeitplaner aktiviert werden soll. Wenn Sie **Nein** wählen, können Sie den Zeitplaner später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

9. Sie werden nach den Einstellungen für die Ausführung von WinGuard NT gefragt.

WinGuard NT läuft ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77. Wir empfehlen Ihnen, **Ja** zu wählen.

10. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon’s Anti-Virus Toolkit für Windows NT einsehen möchten. Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

11. FindVirus wird automatisch ausgeführt, um die lokalen Festplatten auf Viren zu überprüfen. Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.



Warnung

Geraten Sie nicht in Panik, falls FindVirus einen Virus auf dem Computer findet! Informationen über Vorgehensweisen bei Virenbefall des Computers finden Sie in Kapitel 6, „Entfernung von Viren“.

An dieser Stelle werden Sie möglicherweise aufgefordert, den Computer neu zu starten.

Die Installation ist jetzt abgeschlossen, und der Computer ist auf Viren überprüft worden. Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Installation von Diskette

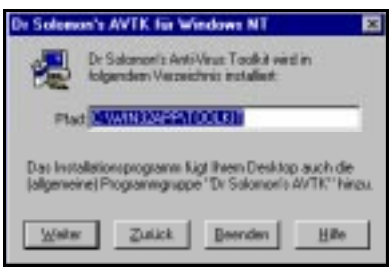
1. Starten Sie den Computer wie gewohnt. Melden Sie sich mit einem Benutzernamen an, der zur Administratorgruppe gehört.

2. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **Windows NT**) in das Diskettenlaufwerk ein.

3. Wählen Sie **Ausführen** aus dem Menü **Datei** des Programm-Managers oder aus dem Menü **Start**.

4. Geben Sie an der Eingabeaufforderung `A:\SETUP` ein, und drücken Sie die <Eingabetaste>. Folgen Sie den angezeigten Anweisungen.

5. Sie werden aufgefordert, das Installationsverzeichnis zu bestätigen:



6. Geben Sie einen anderen Verzeichnispfad ein, wenn Sie die angezeigte Vorgabe nicht übernehmen möchten, und klicken Sie auf **Weiter**. Der Installationsprozeß wird gestartet.

7. Legen Sie weitere Disketten ein, wenn Sie dazu aufgefordert werden. Durch Klicken auf **Abbrechen** können Sie die Installation jederzeit abbrechen. Wenn Sie das Programm später neu installieren möchten, sollten Sie alle im Toolkit-Verzeichnis vorhandenen Dateien löschen, die während der ersten Installation erstellt wurden.

8. Sie werden nach den Einstellungen für die Ausführung des Zeitplaners Dr Solomon's Scheduler gefragt.

Der Zeitplaner ermöglicht Ihnen die Ausführung von Ereignissen zu vorher festgelegten Zeiten. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können nur einmal oder in regelmäßigen Abständen ausgeführt werden.

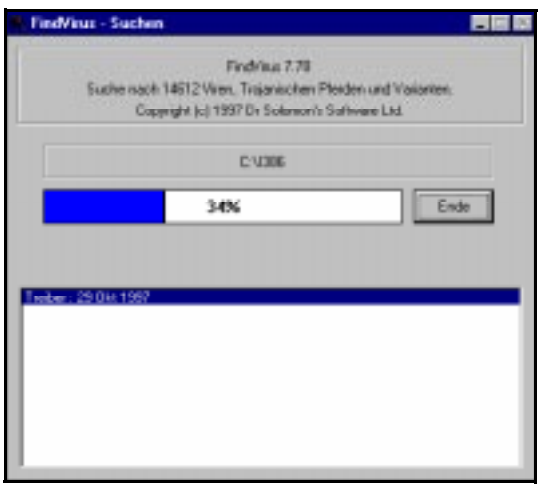
Wählen Sie **Ja**, um zu bestätigen, daß der Zeitplaner aktiviert werden soll. Wenn Sie **Nein** wählen, können Sie den Zeitplaner später aktivieren. Anleitungen zur Ausführung des Zeitplaners nach der Installation des Toolkit finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

9. Sie werden nach den Einstellungen für die Ausführung von WinGuard NT gefragt.

WinGuard NT läuft ständig im Hintergrund. Das Programm überprüft, ob Dateien virenfrei sind, bevor Sie auf sie zugreifen können. Ausführliche Informationen hierzu finden Sie im Abschnitt „WinGuard für Windows 3.x, Windows 95 und Windows NT“ auf Seite 77. Wir empfehlen Ihnen, **Ja** zu wählen.

10. Sie werden gefragt, ob Sie die neuesten Änderungen an Dr Solomon's Anti-Virus Toolkit für Windows NT einsehen möchten. Klicken Sie auf **Ja**, um die README-Datei anzusehen. Wenn Sie **Nein** wählen, wird die Installation ohne Anzeige der README-Datei fortgesetzt. Wir empfehlen Ihnen, die Datei zu lesen, da sie Informationen über neue Funktionen und Änderungen an der Software enthält.

11. FindVirus wird automatisch ausgeführt, um die lokalen Festplatten auf Viren zu überprüfen. Weitere Informationen über FindVirus finden Sie im Abschnitt „FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 75.



Warnung

Geraten Sie nicht in Panik, falls FindVirus einen Virus auf dem Computer findet! Informationen über Vorgehensweisen bei Virenbefall des Computers finden Sie in Kapitel 6, „Entfernung von Viren“.

An dieser Stelle werden Sie möglicherweise aufgefordert, den Computer neu zu starten.

Die Installation ist jetzt abgeschlossen, und der Computer ist auf Viren überprüft worden. Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon's. Adressen und Telefon- und Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Deinstallation des Toolkit (Windows NT Version 4)

1. Wählen Sie **Einstellungen** und anschließend **Systemsteuerung** aus dem Menü **Start**.
2. Klicken Sie in der **Systemsteuerung** auf das Symbol **Software**.
3. Wählen Sie **Dr Solomon's Anti-Virus Toolkit** aus der Liste.
4. Klicken Sie auf **Hinzufügen/Entfernen**.
5. Bestätigen Sie die Entfernung des Programms, wenn Sie dazu aufgefordert werden.
6. Reagieren Sie auf die Aufforderung, dem Toolkit-Verzeichnis seit der Installation hinzugefügte Dateien (wie z. B. Berichtdateien) zu verschieben oder zu löschen.

Deinstallation des Toolkit (Windows NT Version 3.51)

1. Wählen Sie aus der Programmgruppe **Dr Solomon's AVTK** das Symbol **Deinstallation**.
2. Bestätigen Sie die Entfernung des Programms, wenn Sie dazu aufgefordert werden.
3. Reagieren Sie auf die Aufforderung, dem Toolkit-Verzeichnis seit der Installation hinzugefügte Dateien (wie z. B. Berichtdateien) zu verschieben oder zu löschen.

1.6 OS/2

Systemvoraussetzungen

Das Anti-Virus Toolkit für OS/2 läuft auf jedem Computer, auf dem OS/2 Version 2 oder höher ausgeführt wird.

Es werden etwa 2,5 MB Festplattenspeicher benötigt.

Wenn Sie das Toolkit auf mehreren Computern gleichzeitig installieren möchten, sollten Sie sich bei Dr Solomon's Software oder Ihrem Händler nach einer Unternehmenslizenz erkundigen.

Installation des Toolkit

Installation von CD-ROM

1. Starten Sie den Computer. Legen Sie die CD-ROM in das CD-ROM-Laufwerk ein, wenn der Präsentationsmanager angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

   Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `D:` <Eingabetaste>

   Geben Sie dann folgendes ein:

   `CD <`*`SPRACHE`*`>\PRODUCTS\OS2\AVTK` <Eingabetaste>

   Wenn Sie zum Beispiel das englische OS/2-Toolkit installieren, geben Sie folgendes ein:

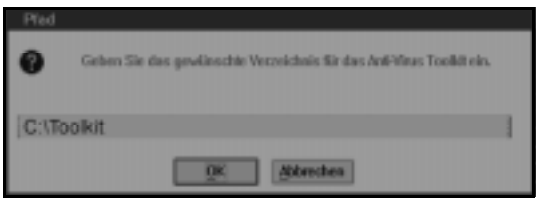
   `CD ENGLISH\PRODUCTS\OS2\AVTK` <Eingabetaste>

   Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber ein deutsches OS/2-Toolkit installieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

Geben Sie an der neuen Eingabeaufforderung folgendes ein:

SETUP <Eingabetaste>

3. In einem Dialogfeld werden Sie nach dem Installationsverzeichnis für das Toolkit gefragt. Geben Sie einen anderen Pfad ein, wenn Sie die Vorgabe nicht übernehmen möchten. Klicken Sie auf **OK**.



Sie können die Installation durch Klicken auf **Pause** unterbrechen und durch Klicken auf **OK** wieder aufnehmen. Durch Klicken auf **Beenden** können Sie die Installation jederzeit abbrechen.

Falls Sie die Installation abbrechen und später fortsetzen möchten, müssen Sie zunächst alle bereits installierten Dateien löschen. Anleitungen zum Löschen eines teilweise installierten Toolkit finden Sie im Abschnitt „Deinstallation des Toolkit“ auf Seite 54.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Installation von Diskette

1. Starten Sie den Computer. Legen Sie die Dr Solomon’s Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **OS/2**) in das Diskettenlaufwerk ein, wenn der Desktop des Präsentationsmanagers angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

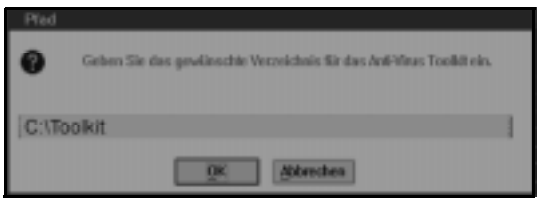
Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

```
A:  <Eingabetaste>
```

Geben Sie an der neuen Eingabeaufforderung folgendes ein:

```
SETUP  <Eingabetaste>
```

3. In einem Dialogfeld werden Sie nach dem Installationsverzeichnis für das Toolkit gefragt. Geben Sie einen andere Pfad ein, wenn Sie die Vorgabe nicht übernehmen möchten. Klicken Sie auf **OK**.



Sie können die Installation durch Klicken auf **Pause** unterbrechen und durch Klicken auf **OK** wieder aufnehmen. Durch Klicken auf **Beenden** können Sie die Installation jederzeit abbrechen.

Falls Sie die Installation abbrechen und später fortsetzen möchten, müssen Sie zunächst alle bereits installierten Dateien löschen. Anleitungen zum Löschen eines teilweise installierten Toolkit finden Sie im folgenden Abschnitt, „Deinstallation des Toolkit“.

Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Deinstallation des Toolkit

So deinstallieren Sie das Toolkit:

1. Öffnen Sie eine OS/2-Befehlssitzung.
2. Wechseln Sie zu dem Laufwerk und Verzeichnis, wo die Toolkit-Dateien installiert sind.
3. Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `DEL TOOLKIT` <Eingabetaste>

   Sie werden aufgefordert, das Löschen des Toolkit-Verzeichnisses zu bestätigen. Geben Sie folgendes ein:

   `J` <Eingabetaste>
4. Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `RD TOOLKIT` <Eingabetaste>
5. Kehren Sie zum Desktop zurück. Klicken Sie mit der rechten Maustaste auf das Toolkit-Symbol, und wählen Sie **Löschen** aus dem angezeigten Menü. Bestätigen Sie in den folgenden Dialogfeldern, daß Sie das Toolkit-Symbol vom Desktop löschen möchten.

1.7 DOS

Systemvoraussetzungen

Dr Solomon's Anti-Virus Toolkit läuft auf jedem IBM- bzw. IBM-kompatiblen Computer. Das System sollte über folgendes verfügen:

- DOS 3.3 oder höher; geben Sie folgendes ein, um zu überprüfen, welche DOS-Version ausgeführt wird:

  VER <Eingabetaste>

  Diese Eingabe erfolgt an der DOS-Eingabeaufforderung.

Für die Installation benötigen Sie:

- 2,5 MB Festplattenspeicher für das DOS-Toolkit.

VirusGuard, das DOS-residente Überprüfungsprogramm, läuft schneller, wenn Ihr System über folgendes verfügt:

- XMS-Speicher;
- EMS-Speicher;
- ein RAM-Laufwerk.

Falls Sie das Toolkit in einem Netzwerk oder auf mehreren Computern gleichzeitig ausführen möchten, sollten Sie sich bei Dr Solomon's oder Ihrem Händler nach einer Unternehmenslizenz erkundigen.

Installation des Toolkit

Installation von CD-ROM

1. Starten Sie den Computer, und vergewissern Sie sich, daß Sie an einer DOS-Eingabeaufforderung sind. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie die <Eingabetaste>. Beispiel:

`D:` <Eingabetaste>

Geben Sie dann folgendes ein:

`CD <`*`SPRACHE`*`>\PRODUCTS\DOS\AVTK` <Eingabetaste>

Wenn Sie zum Beispiel das englische DOS-Toolkit installieren, geben Sie folgendes ein:

`CD ENGLISH\PRODUCTS\DOS\AVTK` <Eingabetaste>

Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber ein deutsches DOS-Toolkit installieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

Geben Sie an der neuen Eingabeaufforderung folgendes ein:

`INSTALL` <Eingabetaste>

2. Im ersten angezeigten Bildschirm werden Sie nach dem Laufwerk gefragt, auf dem das Toolkit installiert werden soll. Wählen Sie mit Hilfe der Pfeiltasten nach links und rechts ein Laufwerk aus, und drücken Sie die <Eingabetaste>, um Ihre Auswahl zu bestätigen. Auf diesem Bildschirm wird außerdem angezeigt, wieviel freien Festplattenspeicher das System hat, wieviel Speicherplatz das Toolkit in Anspruch nimmt,

und wieviel Speicherplatz nach der Installation des Toolkit verbleibt.

Drücken Sie <Esc>, wenn Sie die Installation abbrechen möchten.

3. Im folgenden Bildschirm werden Sie aufgefordert, das Verzeichnis zu bestätigen, in dem das Toolkit installiert werden soll. Geben Sie ein anderes Verzeichnis ein, wenn Sie die Vorgabe nicht übernehmen möchten. Drücken Sie die <Eingabetaste>, um die Installation fortzusetzen.

Drücken Sie <Esc>, wenn Sie die Installation abbrechen möchten.

4. Im nächsten Bildschirm wird der Fortschritt der Installation angezeigt. Danach werden Sie gefragt, ob Sie VirusGuard aktivieren möchten.

Geben Sie **J** ein, um VirusGuard zu aktivieren.

Tip

Wir empfehlen die Aktivierung von VirusGuard. Wenn Sie das Programm nicht aktivieren möchten, können Sie dies später nachholen.

Wenn Sie sich für die Installation von VirusGuard entscheiden, werden Sie in einem weiteren Bildschirm aufgefordert, zu bestätigen, daß das Programm Änderungen an den Dateien AUTOEXEC.BAT und CONFIG.SYS vornehmen soll. Wenn das Programm Änderungen vornimmt, werden Sicherungskopien dieser Dateien im Stammverzeichnis des Laufwerks gespeichert, das die Dateien enthält. Geben Sie **J** ein, um fortzufahren.

5. Im nächsten Bildschirm werden Sie aufgefordert, die Sicherheitseinstellung für VirusGuard auszuwählen. Wählen Sie die Einstellung mit Hilfe der Pfeiltasten nach oben und unten aus, und

drücken Sie die <Eingabetaste>, um die gewählte Einstellung zu bestätigen.

6. Ein Bildschirm wird angezeigt, auf dem alle Informationen zusammengefaßt sind. Im nächsten Bildschirm teilt Ihnen das Installationsprogramm den Namen der AUTOEXEC.BAT-Sicherungsdatei mit.

7. Der letzte Bildschirm bestätigt, daß die Installation abgeschlossen und FindVirus jetzt die lokale(n) Festplatte(n) überprüft.

   Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon's. Adressen und Telefon- und Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Tip

Wir empfehlen eine weitere vollständige Überprüfung auf Viren nach Abschluß der Installation.

Installation von Diskette

1. Starten Sie den Computer, und vergewissern Sie sich, daß Sie an einer DOS-Eingabeaufforderung sind.

2. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **DOS**) in das Diskettenlaufwerk ein.

3. Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie die <Eingabetaste>. Beispiel:

   `A:` <Eingabetaste>

4. Geben Sie `INSTALL` an der Eingabeaufforderung `A:` ein, und drücken Sie die <Eingabetaste>.

5. Im ersten angezeigten Bildschirm werden Sie nach dem Laufwerk gefragt, auf dem das Toolkit installiert werden soll. Wählen Sie mit Hilfe der Pfeiltasten nach links und rechts ein Laufwerk aus, und drücken Sie die <Eingabetaste>, um Ihre Auswahl zu bestätigen. Auf diesem Bildschirm wird außerdem angezeigt, wieviel freien Festplattenspeicher das System hat, wieviel Speicherplatz das Toolkit in Anspruch nimmt, und wieviel Speicherplatz nach der Installation des Toolkit verbleibt.

.

Drücken Sie <Esc>, wenn Sie die Installation abbrechen möchten.

6. Im folgenden Bildschirm werden Sie aufgefordert, das Verzeichnis zu bestätigen, in dem das Toolkit installiert werden soll. Geben Sie ein anderes Verzeichnis ein, wenn Sie die Vorgabe nicht übernehmen möchten. Drücken Sie die <Eingabetaste>, um die Installation fortzusetzen.

   Drücken Sie <Esc>, wenn Sie die Installation abbrechen möchten.

7. Im nächsten Bildschirm wird der Fortschritt der Installation angezeigt. Danach werden Sie gefragt, ob Sie VirusGuard aktivieren möchten. Geben Sie **J** ein, um VirusGuard zu aktivieren.

Tip

Wir empfehlen die Aktivierung von VirusGuard. Wenn Sie das Programm nicht aktivieren möchten, können Sie dies später nachholen.

Wenn Sie sich für die Installation von VirusGuard entscheiden, werden Sie in einem weiteren Bildschirm aufgefordert, zu bestätigen, daß das Programm Änderungen an den Dateien AUTOEXEC.BAT und CONFIG.SYS vornehmen soll. Wenn das Programm Änderungen vornimmt, werden Sicherungskopien dieser Dateien im Stammverzeichnis des Laufwerks gespeichert, das die Dateien enthält. Geben Sie **J** ein, um fortzufahren.

8. Im nächsten Bildschirm werden Sie aufgefordert, die Sicherheitseinstellung für VirusGuard auszuwählen. Wählen Sie die Einstellung mit Hilfe der Pfeiltasten nach oben und unten aus, und drücken Sie die <Eingabetaste>, um die gewählte Einstellung zu bestätigen.

9. Ein Bildschirm wird angezeigt, auf dem alle Informationen zusammengefaßt sind. Im nächsten Bildschirm teilt Ihnen das Installationsprogramm den Namen der AUTOEXEC.BAT-Sicherungsdatei mit.

10. Der letzte Bildschirm bestätigt, daß die Installation abgeschlossen ist und FindVirus jetzt die lokale(n) Festplatte(n) überprüft.

    Falls Sie Probleme bei der Installation des Toolkit haben, vergewissern Sie sich, daß Sie die in diesem Handbuch aufgeführten Schritte richtig befolgt haben. Wenn Sie das Problem nicht lösen können, wenden Sie sich an die technische Unterstützung von Dr Solomon's. Adressen und Telefon- und

Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Tip 

Wir empfehlen eine weitere vollständige Überprüfung auf Viren nach Abschluß der Installation.

Deinstallation des Toolkit

1. Wechseln Sie zu dem Laufwerk und/oder Verzeichnis, wo die Toolkit-Dateien installiert sind.

2. Löschen Sie alle Toolkit-Dateien aus dem Toolkit-Verzeichnis. Falls Sie beispielsweise das Toolkit im Vorgabeverzeichnis C:\TOOLKIT installiert haben, löschen Sie die Toolkit-Dateien wie in den folgenden Anleitungen beschrieben. Geben Sie an der Eingabeaufforderung C:\

   `CD TOOLKIT` <Eingabetaste>

   ein, um in das Toolkit-Verzeichnis zu wechseln. Geben Sie an der Eingabeaufforderung C:\Toolkit folgendes ein:

   `DEL *.*` <Eingabetaste>

   Sie werden aufgefordert, zu bestätigen, daß Sie die Toolkit-Dateien löschen möchten. Geben Sie folgendes ein:

   `J` <Eingabetaste>

3. Löschen Sie das Toolkit, indem Sie folgendes eingeben:

   `DEL TOOLKIT` <Eingabetaste>

   Sie werden aufgefordert, zu bestätigen, daß Sie das Toolkit-Verzeichnis löschen möchten. Geben Sie folgendes ein:

   `J` <Eingabetaste>

4. Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   ```
   RD TOOLKIT <Eingabetaste>
   ```

5. Öffnen Sie die Datei AUTOEXEC.BAT, und löschen Sie die Zeile, die den Befehl **VirusGuard** enthält. Die VirusGuard-Datei heißt GUARD.COM. Wenn Sie VirusGuard im Verzeichnis C:\TOOLKIT installiert hatten, heißt die zu löschende Zeile

   ```
   C:\TOOLKIT\GUARD.COM
   ```

6. Starten Sie den Computer neu.

2. Aktualisierung des Toolkit

Das Toolkit wird monatlich aktualisiert, um neue Viren erkennen zu können, und Aktualisierungen sind vierteljährlich oder monatlich erhältlich. Dr Solomon's empfiehlt ein Abonnement des Aktualisierungsservices, damit Sie sicher sein können, jederzeit vor Viren geschützt zu sein. Weitere Informationen finden Sie im Abschnitt „Registrierung und Aktualisierungen“ auf Seite xi.

2.1 Windows 3.x

Aktualisierung von CD-ROM

Schnellinstallation

Tip

In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Durch die Aktualisierung des Toolkit können Sie bestehende Toolkit-Konfigurationen der vorigen Toolkit-Version beibehalten. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 10.

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.
2. Wählen Sie **Ausführen** aus dem Menü **Datei**.
3. Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

   ```
   \SETUP
   ```

   ein, und klicken Sie auf **OK**. Beispiel:

   ```
   D:\SETUP
   ```

4. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.

5. Im nächsten Dialogfeld werden Sie aufgefordert, die Aktualisierung von Dr Solomon's Anti-Virus Toolkit für Windows 3.x zu bestätigen. Klicken Sie auf **Aktualisieren**.

6. Folgen Sie den angezeigten Anweisungen.

Aktualisierung von Diskette

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **Windows 3.X**) in das Diskettenlaufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.

2. Wählen Sie **Ausführen** aus dem Menü **Datei** des Datei-Manangers.

3. Geben Sie `A:\SETUP` im Dialogfeld **Öffnen** ein, und klicken Sie auf **OK**.

4. Folgen Sie den angezeigten Anweisungen.

2.2 Windows 95

Aktualisierung von CD-ROM

Schnellinstallation

Tip

In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Durch die Aktualisierung des Toolkit können Sie bestehende Toolkit-Konfigurationen der vorigen Toolkit-Version beibehalten. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 25.

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.
2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie im nächsten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.
3. Im nächsten Dialogfeld werden Sie aufgefordert, die Aktualisierung von Dr Solomon’s Anti-Virus Toolkit für Windows 95 zu bestätigen. Klicken Sie auf **Aktualisieren**.
4. Folgen Sie den angezeigten Anweisungen.

Aktualisierung von Diskette

1. Starten Sie den Computer. Legen Sie die Installationsdiskette 1 (mit der Aufschrift **WINDOWS 95**) in das Diskettenlaufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.
2. Klicken Sie auf **Start** und anschließend auf **Ausführen**.
3. Geben Sie `A:\SETUP` im Dialogfeld **Öffnen** ein, und klicken Sie auf **OK**.
4. Folgen Sie den angezeigten Anweisungen.

2.3 Windows NT

Aktualisierung von CD-ROM

Schnellinstallation

Tip 	In Kürze wird Software für die schrittweise Aktualisierung erhältlich sein, durch die Sie das Verfahren zur Schnellinstallation verwenden können, um Ihr Toolkit zu aktualisieren. Anleitungen für die vollständige Installation des Toolkit finden Sie im Abschnitt „Erweiterte Installationsoption“ auf Seite 43.

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

2. Wenn Sie Windows NT Version 4 ausführen, wird ein Toolkit-CD-Startbildschirm angezeigt.

Für Benutzer von Windows NT Version 3.51:
Wählen Sie nach dem Einlegen der Toolkit-CD in das CD-ROM-Laufwerk **Ausführen** aus dem Menü **Datei**.

Geben Sie in das angezeigte Eingabefeld den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt. Geben Sie anschließend

```
\SETUP
```

ein, und klicken Sie auf **OK**. Beispiel:

```
D:\SETUP
```

Ein Toolkit-CD-Startbildschirm wird angezeigt.

3. Wählen Sie in dem angezeigten Dialogfeld **Schnellinstallation**, und klicken Sie auf **Weiter**.

4. Im nächsten Dialogfeld werden Sie aufgefordert, die Aktualisierung von Dr Solomon's Anti-Virus Toolkit für Windows NT zu bestätigen. Klicken Sie auf **Aktualisieren**.

5. Folgen Sie den angezeigten Anweisungen.

Aktualisierung von Diskette

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **Windows NT**) in das Diskettenlaufwerk ein.

2. Wählen Sie **Ausführen** aus dem Menü **Datei** des Programm-Managers oder aus dem Menü **Start**.

3. Geben Sie `A:\SETUP` an der Eingabeaufforderung ein, und drücken Sie die <Eingabetaste>.

4. Folgen Sie den angezeigten Anweisungen.

2.4 OS/2

Aktualisierung von CD-ROM

1. Starten Sie den Computer. Legen Sie die CD-ROM in das CD-ROM-Laufwerk ein, wenn der Präsentationsmanager angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

   Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `D:` <Eingabetaste>

   Geben Sie dann folgendes ein:

   `CD <`*`SPRACHE`*`>\PRODUCTS\OS2\AVTK` <Eingabetaste>

   Wenn Sie zum Beispiel das englische OS/2-Toolkit aktualisieren, geben Sie folgendes ein:

   `CD ENGLISH\PRODUCTS\OS2\AVTK` <Eingabetaste>

   Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber das deutsche OS/2-Toolkit aktualisieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

   Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `SETUP` <Eingabetaste>

3. Folgen Sie den angezeigten Anweisungen.

Aktualisierung von Diskette

1. Starten Sie den Computer. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **OS/2**) in das Diskettenlaufwerk ein, wenn der Präsentationsmanager angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

   Geben Sie den Buchstaben des Diskettenlaufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `A:` <Eingabetaste>

   Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `SETUP` <Eingabetaste>

3. Folgen Sie den angezeigten Anweisungen.

2.5 DOS

Aktualisierung von CD-ROM

1. Starten Sie den Computer, und vergewissern Sie sich, daß Sie an einer DOS-Eingabeaufforderung sind. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

   Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `D:` <Eingabetaste>

   Geben Sie dann folgendes ein:

   `CD <`*`SPRACHE`*`>\PRODUCTS\DOS\AVTK` <Eingabetaste>

   Wenn Sie zum Beispiel das englische DOS-Toolkit aktualisieren, geben Sie folgendes ein:

   `CD ENGLISH\PRODUCTS\DOS\AVTK` <Eingabetaste>

   Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber das deutsche DOS-Toolkit aktualisieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

   Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `INSTALL` <Eingabetaste>

2. Folgen Sie den angezeigten Anweisungen.

Aktualisierung von Diskette

1. Starten Sie den Computer, und vergewissern Sie sich, daß Sie an einer DOS-Eingabeaufforderung sind. Legen Sie die Dr Solomon's Anti-Virus Toolkit Installationsdiskette 1 (mit der Aufschrift **DOS**) in das Diskettenlaufwerk ein.

2. Geben Sie den Buchstaben des Diskettenlaufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `A:` <Eingabetaste>

3. Geben Sie `INSTALL` an der Eingabeaufforderung `A:` ein, und drücken Sie die <Eingabetaste>.

4. Folgen Sie den angezeigten Anweisungen.

3. Überprüfung auf Viren

3.1 Überprüfungsprogramme, die bei Bedarf ausgeführt werden

Dr Solomon's Toolkit enthält zwei Virensuchprogramme, die Sie bei Bedarf ausführen können: FindVirus und Viverify.

FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS

Wenn ein neuer Virus entdeckt wird, wird er analysiert, um seine Eigenschaften festzustellen. Sobald diese bekannt sind, können sie in ein Suchprogramm einprogrammiert werden, das den Virus dann auf Computern identifizieren kann.

Bei dem Dr Solomon's-Programm für die Virensuche handelt es sich um das Überprüfungsprogramm „FindVirus". FindVirus wird ständig mit den Informationen über neu entdeckte Viren aktualisiert.

FindVirus kann auch Viren aus Dateien, Boot und Partitionssektoren entfernen. Wenn ein Virus im Boot- oder Partitionssektor einer Festplatte gefunden wird, wird eine Meldung über die Infektion angezeigt, die Überprüfung aber gleichzeitig abgebrochen, was für zusätzliche Sicherheit sorgt. Sie sollten die Entfernungsfunktion ausführen und die Festplatte danach erneut überprüfen. Infizierte Dateien können auch in Bilddateien von Bootsektoren gefunden werden.

Die Vorgabeeinstellungen für FindVirus sind so gewählt worden, daß sie für die meisten Situationen angemessen sind und die Dateien überprüft werden, die für Virusinfektionen am anfälligsten sind. Sie können eine Überprüfung mit diesen Vorgabeeinstellungen ausführen, oder Sie können die Optionen an Ihre Anforderungen anpassen.

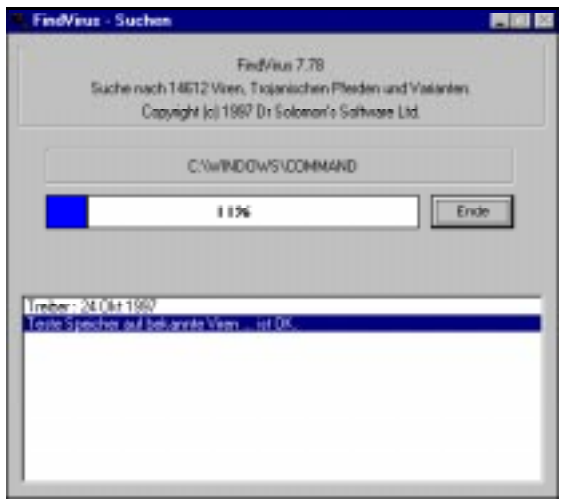
Überprüfung auf Viren

Verwenden Sie den Hauptbildschirm, um mit den ursprünglichen Einstellungen bzw. den zuletzt im Menü **Prüfen** vorgenommenen Einstellungen nach Viren zu suchen:

1. Wählen Sie im Feld **Laufwerke** das (die) zu überprüfende(n) Laufwerk(e) aus.

2. Klicken Sie auf die Schaltfläche **Suchen**.

3. Ein Dialogfeld wird angezeigt, das zunächst den Fortschritt der Überprüfung und anschließend das Ergebnis anzeigt.



Durch Klicken auf **Beenden** können Sie die Überprüfung jederzeit abbrechen. Der Bericht führt alle Viren auf, die bis zum Abbruch der Überprüfung gefunden wurden. Wenn während dieser Zeit keine Viren gefunden wurden, wird das Dialogfeld **Viren suchen** wieder angezeigt.

4. Sehen Sie sich die Ergebnisse an, wenn die Überprüfung abgeschlossen ist, und klicken Sie dann auf **Beenden**, um zum Dialogfeld **Viren suchen** zurückzukehren.

Warnung

Für Benutzer von Windows NT: Wenn Ihr Benutzername (d. h. der Name, mit dem Sie sich angemeldet haben) nicht in der Administratorgruppe zu finden ist, kann FindVirus den Partitionssektor und den Bootsektor der Festplatte nicht überprüfen. In diesem Fall werden die Meldungen „Partitionssektor kann nicht gelesen werden“ und „Bootsektor kann nicht gelesen werden“ angezeigt. Wenden Sie sich an den Systemadministrator, wenn Sie diese Sektoren überprüfen müssen.

Wenn eine Virusinfektion gefunden wird, entfernen Sie diese über das FindVirus-Menü **Entfernen**; weitere Informationen finden Sie im Abschnitt „Entfernung von Viren aus Laufwerken“ auf Seite 151 oder in den Erläuterungen zur Verwendung des Toolkit in der Online-Hilfe.

Hilfe

Informationen über die Ausführung von FindVirus von einer Befehlszeile finden Sie unter dem Thema „FindVirus“ in der Online-Hilfe zum Toolkit.

ViVerify für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS

ViVerify ist das erweiterte Suchprogramm von Dr Solomon’s, das Sie bei Bedarf ausführen können. Informationen über ViVerify finden Sie im Abschnitt „Erweiterte Virensuche mit ViVerify für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS“ auf Seite 86.

3.2 Automatische Überprüfungsprogramme (Zugriffsscanner)

Die Dr Solomon’s Toolkits für Windows 3.x, Windows 95 und Windows NT enthalten jeweils das automatische Überprüfungsprogramm WinGuard, das beim Zugriff auf Dateien bzw. Boot- und Partitionssektoren ausgeführt wird und daher auch als Zugriffsscanner bezeichnet wird. Der Zugriffsscanner für DOS heißt VirusGuard.

WinGuard für Windows 3.x, Windows 95 und Windows NT

WinGuard läuft ständig im Hintergrund und überwacht den Computer.

WinGuard wird zusammen mit Windows gestartet. Wenn Sie einen Vorgang ausführen, durch den ein Virus verbreitet werden könnte, kann WinGuard die betreffende Datei bzw. den Boot- oder Partitionssektor überprüfen. Falls das Programm einen Virus findet, wird der Vorgang blockiert und eine Warnmeldung angezeigt. Sie können aber auch festlegen, daß Viren automatisch entfernt werden.

Sie können die Funktionsweise von WinGuard ändern. Die ursprünglichen Einstellungen (die Vorgabeeinstellungen bei Installation) sind so gewählt worden, daß sie für die meisten Situationen angemessen sind. Sie können diese Einstellungen jedoch ändern und an Ihre persönlichen Anforderungen anpassen.

Sie können zum Beispiel festlegen, durch welche Vorgänge eine Überprüfung ausgelöst wird und welche Dateiformate überprüft werden. Weitere Informationen über die Änderung der Vorgabekonfiguration von WinGuard finden Sie im Abschnitt „Erweiterte Virensuche mit WinGuard für Windows 3.x und Windows 95“ auf Seite 93 bzw. „Erweiterte Virensuche mit WinGuard für Windows NT“ auf Seite 107.

Tip

In Windows NT können nur Administratoren die WinGuard-Einstellungen ändern.

WinGuard im täglichen Gebrauch

WinGuard wird bei jedem Start von Windows mit aufgerufen. Um anzugeben, daß das Programm aktiviert ist, wird in Windows 3.x und Windows NT (Version 3.51) auf dem Desktop und in Windows 95 und Windows NT (Version 4) in der Task-Leiste ein Symbol angezeigt.

Wenn Sie dieses Symbol nicht sehen, haben Sie WinGuard möglicherweise bei der Installation des Toolkit nicht installiert, oder WinGuard ist deaktiviert worden; weitere Informationen finden Sie im Abschnitt „Übersicht über die Überprüfungseinstellungen“ auf Seite 97.

Wenn WinGuard einmal aktiviert ist, läuft es automatisch. Der einzige Hinweis, daß das Programm aktiv ist, ist das Symbol; Sie bemerken WinGuard nur, falls ein Virus gefunden wird.

VirusGuard für Windows 3.x, Windows 95 und DOS

VirusGuard ist das DOS-Gegenstück zu WinGuard. Wenn Sie sich bei der Installation des Toolkit entscheiden, VirusGuard zu aktivieren (siehe Kapitel 1), bietet VirusGuard unter DOS automatischen Schutz. Wenn Windows gestartet wird, übernimmt WinGuard diese Funktion.

Ohne VirusGuard kann unter DOS eine Virusinfektion auftreten. Diese Infektion würde zwar bei der nächsten Windows-Sitzung von WinGuard erkannt werden (falls Sie auf die infizierte Datei zugreifen und es sich um einen Dateivirus handelt), der Virus kann unter Umständen jedoch schon vorher ausgelöst werden und Schäden verursachen.

Dr Solomon's Software empfiehlt, daß Sie, wenn Sie mit Windows 3.x oder Windows 95 arbeiten, sowohl WinGuard als auch VirusGuard ständig ausführen, um den bestmöglichen Schutz vor Viren zu gewährleisten.

Tip

VirusGuard unterstützt keine Extratreiberdateien.

So starten Sie VirusGuard

Tip

Falls Sie sich bei der Installation des Toolkit entschieden haben, VirusGuard nicht zu aktivieren, können Sie es mit Hilfe der in diesem Abschnitt und in der Online-Hilfe zum Toolkit beschriebenen Befehle auch später aktivieren.

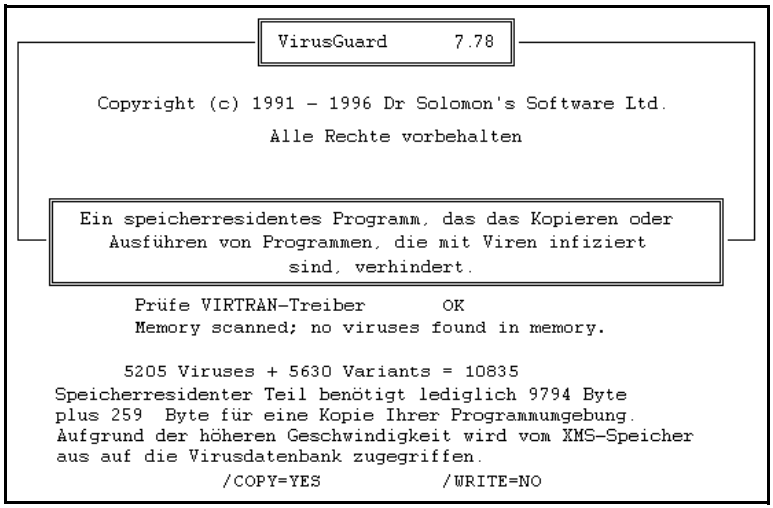
Geben Sie an der DOS-Eingabeaufforderung den Befehl zum Starten von VirusGuard ein. Der Befehl hat folgende Syntax:

```
GUARD [/Parameter]...
```

Hilfe

Informationen über die Parameter finden Sie im Abschnitt „Überblick über die Parameter“ des Themas „VirusGuard“ in der Online-Hilfe zum Toolkit.

Beim Starten von VirusGuard wird kurz folgender Bildschirm angezeigt:



Tip

VirusGuard kann nach dem Starten nicht mehr abgebrochen werden.

Falls VirusGuard einen Virus findet

Falls VirusGuard einen Virus findet, wird folgendes ausgelöst:

- Der aktuelle Vorgang wird unterbrochen.
- Ein Alarmsignal ertönt.
- Im Bildschirm-Vordergrund wird eine Warnmeldung angezeigt.

Drücken Sie die Taste <Strg>, und entfernen Sie die Infektion sofort mit Hilfe von FindVirus. Verwenden Sie dazu entweder die Benutzeroberfläche oder die SOS-Diskette (siehe Seite 1).

4. Weitere Einstellungen für die Virensuche

4.1 Erweiterte Virensuche mit FindVirus für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS

Tip Nicht alle in diesem Kapitel beschriebenen Einstellungen sind für alle Betriebssysteme verfügbar.

Mit Hilfe des Menüs **Prüfen** können Sie die Virensuche starten. Das Menü bietet Optionen, über die Sie die Art der Suche ändern können.

Benutzerdefinierte Virensuche

1. Wenn Sie Ihre eigenen Einstellungen für die Virensuche festlegen möchten, wählen Sie **Viren suchen** aus dem Menü **Prüfen**.

   Das Dialogfeld **Viren suchen** wird angezeigt.

2. Wählen Sie im Feld **Laufwerke** das (die) zu überprüfende(n) Laufwerk(e) aus.

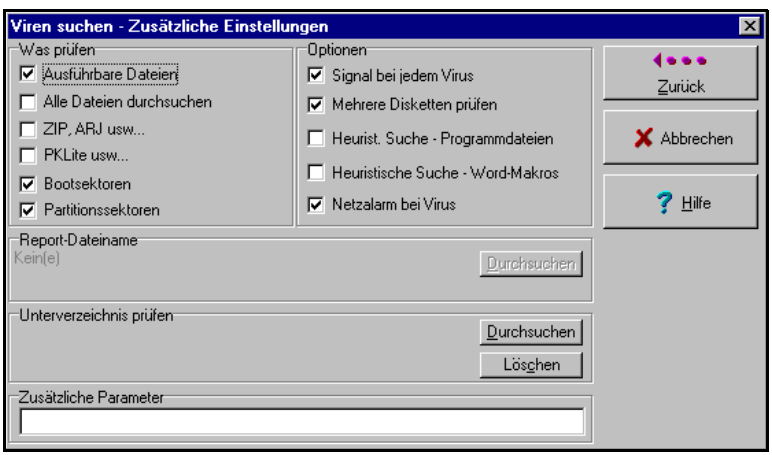
3. Wählen Sie im Feld **Bericht** die gewünschte Option: **Bericht in Datei** oder **Bericht auf Drucker**.

Tip

Die Optionen in diesem Dialogfeld gelten auch für Suchvorgänge, bei denen Viren entfernt werden, wenn diese Suchvorgänge über die Option **Viren von Laufwerk entfernen** aus dem Menü **Entfernen** oder über die Schaltfläche **Entfernen** gestartet werden.

4. Durch Klicken auf die Schaltfläche **Erweitert** können Sie die Einstellungen für den Suchvorgang an Ihre Anforderungen anpassen.

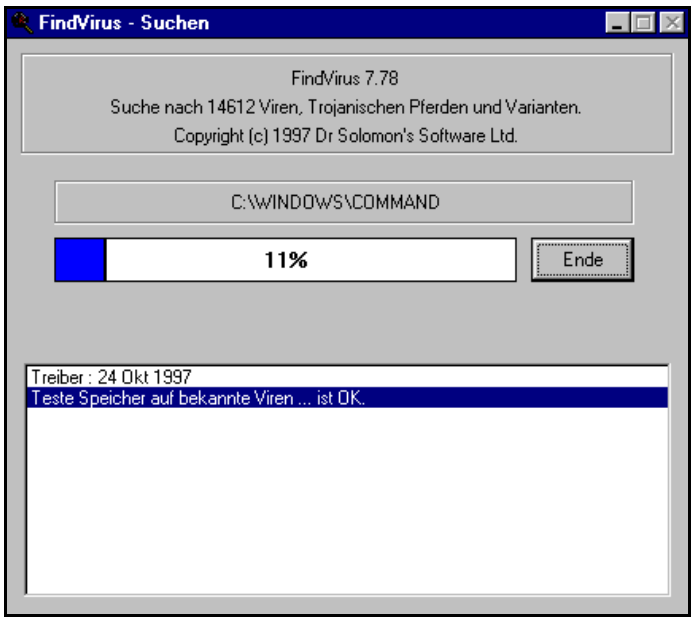
   Das Dialogfeld **Viren suchen - Zusätzliche Einstellungen** wird angezeigt.



   Klicken Sie nach dem Festlegen der Einstellungen auf die Schaltfläche **Zurück**, um zum Dialogfeld **Viren suchen** zurückzukehren.

5. Klicken Sie auf die Schaltfläche **Suchen**.

6. Ein Dialogfeld wird angezeigt, in dem zunächst der Fortschritt und dann die Ergebnisse des Suchvorgangs angezeigt werden.



Durch Klicken auf **Beenden** können Sie die Überprüfung jederzeit abbrechen. Der Bericht führt alle Viren auf, die bis zum Abbruch der Überprüfung gefunden wurden. Wenn während dieser Zeit keine Viren gefunden wurden, wird das Dialogfeld **Viren suchen** angezeigt.

7. Sehen Sie sich die Ergebnisse an, wenn die Überprüfung abgeschlossen ist, und klicken Sie dann auf **Beenden**, um zum Dialogfeld **Viren suchen** zurückzukehren.

Warnung

Für Benutzer von Windows NT: Wenn Ihr Benutzername (d. h. der Name, mit dem Sie sich angemeldet haben) nicht in der Administratorgruppe zu finden ist, kann FindVirus den Partitionssektor und den Bootsektor der Festplatte nicht überprüfen. In diesem Fall werden die Meldungen „Partitionssektor kann nicht gelesen werden“ und „Bootsektor kann nicht gelesen werden“ angezeigt. Wenden Sie sich an den Systemadministrator, wenn Sie diese Sektoren überprüfen müssen.

Wenn eine Virusinfektion gefunden wird, beseitigen Sie diese mit Hilfe der FindVirus-Option **Entfernen**; weitere Informationen finden Sie in der Erläuterung der Verwendung des Toolkit in der Online-Hilfe.

4.2 Erweiterte Virensuche mit ViVerify für Windows 3.x, Windows 95, Windows NT, OS/2 und DOS

Tip 

Nicht alle in diesem Kapitel beschriebenen Einstellungen sind für alle Betriebssysteme verfügbar.

Viverify

Ausführbare Dateien ändern sich im allgemeinen nicht; wenn sich eine ausführbare Datei geändert hat, ist sie möglicherweise mit einem Virus infiziert. Durch Ausführen eines Überprüfungsvorgangs, bei dem mitgeteilt wird, welche Dateien sich geändert haben, erfährt der Benutzer, welche Dateien gegebenenfalls infiziert sind.

Das Dr Solomon's-Programm, das nach geänderten Dateien sucht, heißt ViVerify. ViVerify überprüft auch, ob sich Boot- und Partitionssektoren geändert haben.

Um eine Datei zu überprüfen, erstellt ViVerify eine neue Prüfsumme für die Datei und vergleicht diese mit der bereits berechneten und gespeicherten Prüfsumme. Wenn die Datei sich geändert hat, stimmen die Prüfsummen nicht überein.

Sie müssen Prüfsummen nur berechnen, wenn Sie das Toolkit neu installieren und wenn Sie neue Software installieren. Sobald die Prüfsummen berechnet sind, können Sie sie regelmäßig auf Änderungen prüfen.

Die Dateien, die gespeicherte Prüfsummen enthalten, werden codiert, um sie vor Viren zu schützen. Sie geben diesen Code ein, wenn Sie die Prüfsummen berechnen lassen.

Sie können ViVerify über die Benutzeroberfläche oder von der Befehlszeile aus aufrufen.

Sie können die Funktionsweise von ViVerify ändern und folgendes festlegen:

- ob Sie nach Änderungen suchen oder Prüfsummen berechnen lassen möchten;
- welche Laufwerke überprüft werden sollen.

Es stehen auch erweiterte Optionen zur Verfügung, die Sie nur benötigen, wenn Sie die Suche an Ihre Anforderungen anpassen möchten. Die Vorgabeeinstellungen dieser erweiterten Optionen sind für die meisten Situationen ausreichend.

Reparaturdatenbank

ViVerify verfügt über eine sogenannte „Reparaturdatenbank“. Diese Datenbank wird gleichzeitig mit einer Prüfsummendatei erstellt und ist mit dieser Datei verknüpft. Die Reparaturdatenbank enthält eine Kopie der Abschnitte einer Datei, die für eine Virusinfektion am anfälligsten sind.

Der Bericht am Ende der Überprüfung auf Änderungen enthält eine Aufforderung zur Reparatur geänderter Dateien. Wenn Sie diese Option auswählen, werden die Abschnitte der Datei aus der Reparaturdatenbank wieder in die Datei zurückkopiert, so daß der Ausgangszustand wiederhergestellt wird.

Von der Überprüfung ausgeschlossene Dateien

ViVerify sucht nur in ausführbaren Dateien nach Änderungen. Obwohl sich die meisten ausführbaren Dateien nicht ändern, gibt es Ausnahmen, die von der Überprüfung durch ViVerify ausgeschlossen sind. Es handelt sich um folgende Dateien:

```
CONFIG.SYS
WPQUE.SYS
WPSYSD.SYS
BOOTCONF.SYS
TELIX.FON
```

Es wird empfohlen, diese Dateien von Zeit zu Zeit mit FindVirus zu überprüfen. ViVerify überprüft nicht den Papierkorb.

Suche nach geänderten Dateien

Anders als Datendateien ändern sich die meisten ausführbaren Dateien nicht von einem Tag zum andern. Wenn eine ausführbare Datei sich geändert hat, ist sie möglicherweise mit einem Virus infiziert.

Berechnen von Prüfsummen

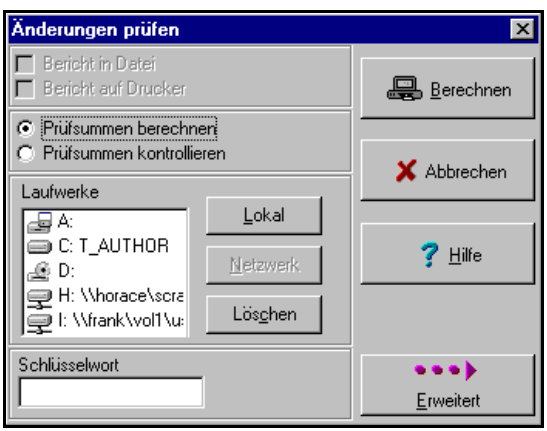
Bevor Sie Dateien auf Änderungen überprüfen können, müssen Sie sogenannte „Prüfsummen“ erzeugen. Bei einer Prüfsumme handelt es sich um die Aufzeichnung des Status einer Datei; eine Änderung der Prüfsumme deutet auf eine Änderung der Datei hin.

Wenn Sie eine neue Softwareanwendung installieren, sollten Sie Prüfsummen neu berechnen, damit die neuen Dateien aufgezeichnete Prüfsummen haben.

1. Wählen Sie **Änderungen prüfen** im Menü **Prüfen**. Das Dialogfeld **Änderungen prüfen** wird angezeigt.

2. Wählen Sie **Prüfsummen berechnen**.

   Das Dialogfeld sieht jetzt folgendermaßen aus:



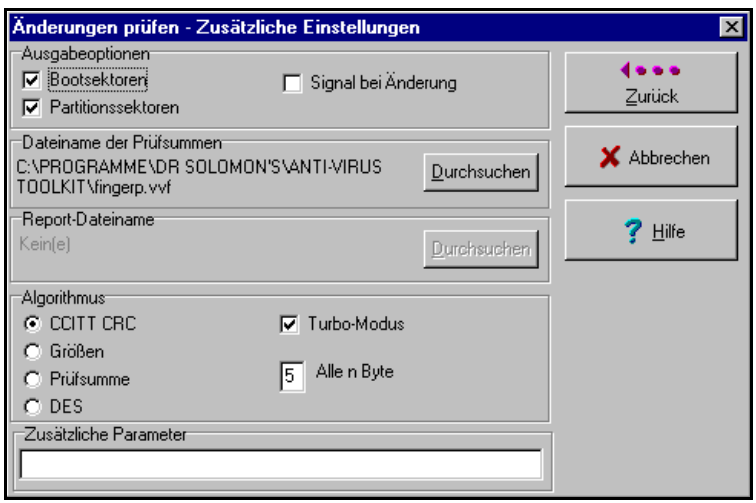
3. Wählen Sie die Laufwerke aus, die auf Änderungen überprüft werden sollen.

4. Geben Sie mindestens acht alphanumerische Zeichen in das Feld **Schlüsselwort** ein. Dieses Schlüsselwort wird verwendet, um die Prüfsummendatei zu verschlüsseln und so vor Schäden durch Viren zu schützen. Das Schlüsselwort ist kein Kennwort.

5. Wenn Sie für die Art der Prüfsummenberechnung keine besonderen Wünsche haben, können Sie jetzt die Prüfsummen auf der Grundlage der aktuellen Einstellungen berechnen lassen (im allgemeinen sind die Vorgabeeinstellungen ausreichend). Fahren Sie mit Schritt 8. fort. Wenn Sie besondere Wünsche für die Art des Überprüfungsvorgangs haben, fahren Sie mit dem nächsten Schritt fort.

6. Klicken Sie auf **Erweitert**, wenn Sie besondere Anforderungen für die Art der Berechnung der Prüfsummen haben.

   Das Dialogfeld **Änderungen prüfen - Zusätzliche Einstellungen** wird angezeigt.



Hilfe

Informationen über die Optionen in diesem Dialogfeld finden Sie unter dem Thema „Dialogfeld **Änderungen prüfen - Zusätzliche Einstellungen**“ in der Online-Hilfe zum Toolkit.

Tip

Mit Hilfe dieses Dialogfelds können Sie mehrere Prüfsummendateien mit Namen Ihrer Wahl erstellen, und so jede Prüfsummendatei an eine bestimmte Laufwerksauswahl anpassen.

7. Klicken Sie nach dem Festlegen der Einstellungen auf **Zurück**, um zum Dialogfeld **Änderungen prüfen** zurückzukehren.

8. Klicken Sie auf **Berechnen**, oder drücken Sie die <Eingabetaste>.

9. Möglicherweise wird ein Dialogfeld mit der Meldung „Prüfsummendatei existiert bereits. Überschreiben?“ angezeigt. Wenn Sie die Prüfsummendatei nicht überschreiben möchten, können Sie mit Hilfe der zusätzlichen Einstellungen eine andere Datei angeben; siehe Schritt 6.

10. In einem Dialogfeld wird der Fortschritt der Prüfsummenberechnung und anschließend die Meldung angezeigt, daß die Prüfsummen berechnet worden sind. Klicken Sie auf **Beenden**, um zum Dialogfeld **Änderungen prüfen** zurückzukehren.

Sie können die Dateien jetzt auf Änderungen überprüfen. Dabei werden nur die Dateien überprüft, die eine Prüfsumme haben.

Überprüfen von Dateien

Sobald Sie die Prüfsummen berechnet haben, können Sie sie verwenden, um Dateien auf Änderungen zu überprüfen:

1. Aktivieren Sie im Dialogfeld **Änderungen prüfen** die Option **Prüfsummen kontrollieren**.

2. Wählen Sie die zu überprüfenden Laufwerke aus.

3. Geben Sie das bei der Berechnung der Prüfsummen verwendete Schlüsselwort in das Feld Schlüsselwort ein; siehe Schritt 4 auf Seite 88.

4. Klicken Sie auf die Schaltfläche **Kontrollieren**, oder drücken Sie die <Eingabetaste>.

5. In einem Dialogfeld wird der Fortschritt der Überprüfung angezeigt. Sie können jederzeit auf **Abbrechen** klicken. Wenn Sie den Vorgang abbrechen, werden Sie aufgefordert, dies zu bestätigen. Anschließend wird ein Meldungsdialogfeld mit den Ergebnissen der Überprüfung bis zum Abbruch des Vorgangs angezeigt.

6. Wenn die Überprüfung abgeschlossen ist, werden die Ergebnisse in einem Dialogfeld angezeigt. In diesem Dialogfeld werden die Dateien in drei Kategorien aufgelistet:

- **Dateien, die sich verändert haben, jedoch reparabel sind**;
- **Dateien, die sich verändert haben, jedoch nicht reparabel sind**;
- **Neue Dateien** (hierbei handelt es sich um Dateien, die gefunden wurden, aber in der Prüfsummendatei keine Prüfsumme haben).

7. Wenn ViVerify angibt, daß sich eine Datei geändert hat, bedeutet dies nicht unbedingt, daß sie infiziert ist. Überprüfen Sie die Datei mit FindVirus, und aktivieren Sie für die Überprüfung die Option **Heuristische Suche**.

8. Falls geänderte Dateien gefunden wurden, klicken Sie auf eine der Dateien. Die Schaltfläche **Aktualisieren** wird aktiviert (d. h. sie ist nicht mehr grau unterlegt). Bei reparablen Dateien wird auch die Schaltfläche **Reparieren** aktiviert.

9. Klicken Sie auf **Aktualisieren**, um die Prüfsummendatei mit einer neu berechneten Prüfsumme für die geänderte Datei zu aktualisieren, damit die Datei bei der nächsten Überprüfung nicht als geändert aufgeführt wird. Klicken Sie auf **Reparieren**, damit die Datei repariert wird. Informationen darüber, wie Dateien repariert werden, finden Sie im Abschnitt „Reparaturdatenbank“ auf Seite 87.

10. Falls neue Dateien gefunden wurden, sollten Sie diese mit FindVirus überprüfen. Wenn Sie sicher sind, daß diese Dateien virenfrei sind, klicken Sie auf eine der Dateien. Die Schaltfläche **Aktualisieren** wird aktiviert (d. h. sie ist nicht mehr grau unterlegt). Dateien werden möglicherweise als „Neu“ aufgeführt, wenn Sie ein anderes Laufwerk ausgewählt haben als das, auf dem die Prüfsummen berechnet wurden, oder weil Dateien nach der Berechnung der Prüfsummen auf das Laufwerk kopiert wurden.

11. Klicken Sie auf **Aktualisieren**, um die Prüfsummendatei mit einer neu berechneten Prüfsumme für die neue Datei zu aktualisieren, damit die Datei bei der nächsten Überprüfung nicht als neu aufgeführt wird.

4.3 Erweiterte Virensuche mit VirusGuard für Windows 3.x, Windows 95 und DOS

Testen von VirusGuard

In den Anleitungen dieses Abschnitts wird beschrieben, wie Sie VirusGuard testen, indem Sie eine VirusGuard-Warnung auslösen. Sie lösen diese Warnung aus, indem Sie eine Datei erstellen, die für VirusGuard wie ein Virus aussieht. Sie können diesen Vorgang verwenden, um die Funktion von VirusGuard zu testen und zu sehen, was bei einer Warnung passiert. Durch den Test wird VirusGuard mit der Vorgabeeinstellung für Sicherheit ausgelöst.

So lösen Sie eine VirusGuard-Warnung aus:

1. Fahren Sie den Computer herunter, und starten Sie ihn erneut im DOS-Modus.

2. Geben Sie folgendes ein:

   `COPY CON TRYGUARD.COM` <Eingabetaste>

   Geben Sie anschließend folgende Zeichenfolge ein:

   `ZQZXJVBVT` <Eingabetaste>

   Sie müssen Großbuchstaben eingeben.

Geben Sie dann folgendes ein:

`CTRL Z` <Eingabetaste>

3. Benennen Sie die soeben erstellte Datei TRYGUARD.COM um. VirusGuard gibt jetzt eine Warnung aus; weitere Informationen finden Sie im Abschnitt „Falls VirusGuard einen Virus findet“ auf Seite 81.

Löschen Sie nach dem Test die Datei TRYGUARD.COM, um weitere Warnungen zu vermeiden.

4.4 Erweiterte Virensuche mit WinGuard für Windows 3.x und Windows 95

Testen von WinGuard

Sie können eine WinGuard-Warnung auslösen, um WinGuard zu testen und zu sehen, was bei einer Warnung passiert.

So lösen Sie eine WinGuard-Warnung aus:

1. Öffnen Sie eine neue Datei in einem Texteditor, wie zum Beispiel dem Editor von Microsoft Windows.

2. Geben Sie die Zeichenfolge `ZQZXJVBVT` ein. Sie müssen Großbuchstaben eingeben.

3. Speichern Sie diese Zeichenfolge auf einer Diskette. Sie können einen beliebigen Dateinamen mit einer Erweiterung für eine ausführbare Datei verwenden. Nennen Sie Datei beispielsweise `TRYGUARD.COM` oder `TRYGUARD.EXE`.

4. Wenn die Option **Überprüfen beim Schreiben** aktiviert ist (siehe Seite 98), gibt WinGuard jetzt eine Warnung aus; siehe „Falls WinGuard einen Virus findet“ auf Seite 105. WinGuard kann den Virus nicht aus dieser Testdatei entfernen, die Warnung ist daher dieselbe, die ausgegeben würde, wenn **Automatische Entfernung** deaktiviert wäre (siehe Seite 99), wobei gleichgültig ist, ob diese Option tatsächlich deaktiviert ist.

5. Wenn WinGuard noch keine Warnung ausgegeben hat, benennen Sie die Datei um und geben ihr eine andere Erweiterung für eine ausführbare Datei. Wenn Sie die Datei beispielsweise `TRYGUARD.COM` genannt haben, ändern Sie dies zu `TRYGUARD.EXE`. WinGuard wird jetzt eine Warnung ausgeben.

6. Löschen Sie nach dem Test die Datei, falls WinGuard erlaubt hat, sie zu speichern, um weitere Warnungen zu vermeiden.

Ändern der Konfiguration von WinGuard

Sie können die Funktionsweise von WinGuard ändern. Die von Dr Solomon's festgelegten Vorgabeeinstellungen sind für die meisten Benutzer ausreichend, möglicherweise möchten Sie diese Einstellungen aber ändern, um sie an Ihre persönlichen Anforderungen anzupassen.

Sie können die WinGuard-Einstellungen mit Hilfe des WinGuard-Konfigurationsprogramms ändern.

Sie können die WinGuard-Konfiguration für die Überprüfung und den Text ändern, der in der Warnmeldung angezeigt wird, wenn ein Virus gefunden wird. Um weitere Änderungen durch andere Benutzer zu blockieren, können Sie auch ein Kennwort festlegen.

Allgemeine Hinweise

Wie bereits erwähnt, ist die Vorgabekonfiguration von WinGuard für die meisten Situationen ausreichend.

Die häufigsten Ausnahmen sind:

- Sie arbeiten mit Dateien, die eingebettete OLE-Objekte enthalten (z. B. Microsoft Word-Dokumente). In diesem Fall empfehlen wir die Aktivierung der Option **Alle OLE-Dateien überprüfen** (siehe Seite 98).

- Sie laden Dateien entweder aus dem Internet oder von verschiedenen BBS, oder Sie arbeiten mit komprimierten Dateien. In diesem Fall empfehlen wir die Aktivierung der Option **Überprüfen beim Schreiben** (siehe Seite 98).

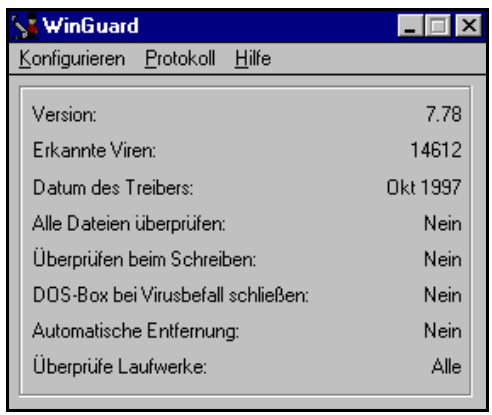
Ändern der Konfiguration für die Überprüfung

So ändern Sie die WinGuard-Einstellungen für die Überprüfung:

1. Öffnen Sie WinGuard durch Doppelklicken auf das WinGuard-Symbol auf dem Desktop (Windows 3.x) oder Klicken auf das WinGuard-Symbol in der Task-Leiste (Windows 95):

Falls WinGuard deaktiviert ist, wird das Symbol nicht angezeigt. In diesem Fall müssen Sie das Programm von der Programmgruppe **Anti-Virus Toolkit** (Windows 3.x) oder **Dr Solomon's AVTK** (Windows 95) aus starten.

Das folgende Dialogfeld wird angezeigt:



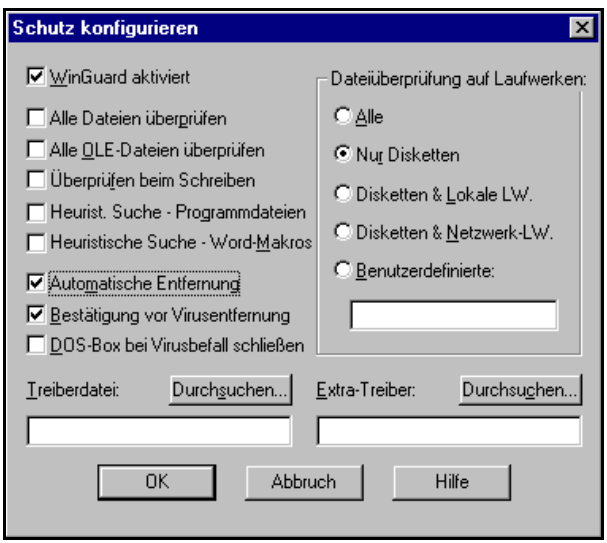
Überprüfen Sie die Konfiguration, und entscheiden Sie sich, ob Sie sie ändern möchten. Falls WinGuard nicht aktiviert ist, wird die Meldung „WinGuard ist NICHT geladen" angezeigt.

2. Wenn Sie die Konfiguration ändern oder WinGuard aktivieren möchten, wählen Sie **Schutz** aus dem Menü **Konfigurieren**.

3. Geben Sie das Kennwort ein, falls Sie dazu aufgefordert werden.

Wenn kein Kennwort vorhanden ist, können Sie eins festlegen. Wenn Sie das Kennwort kennen, können Sie es ändern. Weitere Informationen finden Sie auf Seite 102.

Das folgende Dialogfeld wird angezeigt:

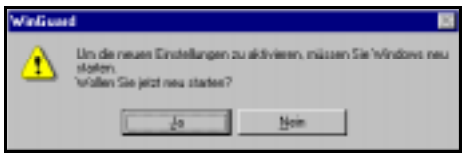


4. Nehmen Sie die Änderungen an der Konfiguration vor.

5. Klicken Sie auf **OK**, wenn Sie fertig sind. Eine Bestätigungsaufforderung wird angezeigt:

6. Klicken Sie auf **OK**, um die Änderungen zu bestätigen. Durch Klicken auf **Abbrechen** ignorieren Sie die vorgenommenen Änderungen. Wenn Sie

auf **OK** klicken, werden Sie aufgefordert, Windows neu zu starten, damit die Änderungen wirksam werden:



7. Klicken Sie auf **Ja**, um Windows neu zu starten. Kicken Sie auf **Abbrechen**, wenn Sie Windows nicht neu starten möchten. Wenn Sie jetzt nicht neu starten, werden die Änderungen beim nächsten Starten des Computers wirksam.

Übersicht über die Überprüfungseinstellungen

Das WinGuard-Konfigurationsdialogfeld ist auf Seite 96 abgebildet.

Es enthält folgende Optionen:

- **WinGuard aktiviert**: Wenn dieses Kontrollkästchen aktiviert ist, läuft WinGuard im Hintergrund. Wenn Sie diese Option deaktivieren, läuft WinGuard nicht automatisch.

Warnung Wenn Sie WinGuard deaktivieren, ist das System anfällig für Virusinfektionen.

Alle Dateien überprüfen: Aktivieren Sie dieses Kontrollkästchen, um alle Dateien auf Viren zu überprüfen.

Wenn diese Option nicht aktiviert ist, werden nur die Dateien überprüft, die für Virusinfektionen am anfälligsten sind. Diese Dateien werden aufgrund ihrer Erweiterung ausgewählt, und zwar auf der Grundlage, daß nur Dateien mit ausführbarem Code infiziert werden können. Typische Beispiele für diese Dateiformate sind Programmdateien mit der Erweiterung .EXE oder .COM, oder Dateien, die Makros enthalten. Dateien, die keinen ausführbaren Code enthalten, wie zum Beispiel die Datendateien, in denen die Ergebnisse Ihrer Arbeit auf dem Computer gespeichert sind, können nicht infiziert werden.

Wenn **Alle Dateien überprüfen** deaktiviert ist, werden nur Dateien mit folgenden Erweiterungen überprüft:

APP	DOC	OVR	XLB
BIN	DOT	SCR	XLS
COM	EXE	SYS	XTP
DLL	OVL	XLA	

Die Überprüfung aller Dateien dauert länger; wählen Sie diese Option daher nur, wenn Sie beispielsweise ausführbare Dateien haben, deren Erweiterung aufgrund einer Umbenennung nicht in der Liste aufgeführt ist.

Durch die Aktivierung dieser Option wird automatisch auch das Kontrollkästchen **Alle OLE-Dateien überprüfen** aktiviert.

- **Alle OLE-Dateien überprüfen**: Aktivieren Sie dieses Kontrollkästchen, um sicherzugehen, daß alle Dateien, die OLE-Objekte enthalten (Object Linking and Embedding = Objekte verknüpfen und einbetten), überprüft werden.

  Diese Option wird automatisch aktiviert, wenn **Alle Dateien überprüfen** aktiviert ist.

  Diese OLE-Option ist vorhanden, weil Datendateien, wie z. B. Microsoft Word-Dokumente, infiziert werden können, wenn Sie ausführbaren Code in Form von Makros enthalten.

  Sie haben auch ohne die Aktivierung dieser Option einen gewissen Schutz, weil die Liste mit Erweiterungen, aufgrund derer Dateien für die Überprüfung ausgewählt werden, wenn **Alle Dateien überprüfen** deaktiviert ist (wie weiter oben gezeigt) die Microsoft Word-Erweiterungen .DOC und .DOT sowie die Excel-Erweiterungen .XL? enthält. Die Option **Alle OLE-Dateien überprüfen** bietet jedoch dann Schutz, wenn Sie Dateien mit anderen Erweiterungen haben, die OLE-Objekte enthalten.

- **Überprüfen beim Schreiben**: Aktivieren Sie dieses Kontrollkästchen, damit Dateien sofort nach dem Schreiben auf den Datenträger überprüft werden.

Dadurch ist Ihr System geschützt, wenn Sie z. B. Dateien aus dem Internet laden.

Tip

Sie sollten diese Option aktivieren, wenn Sie Dateikomprimierung oder Archivdienstprogramme wie PKZIP verwenden. Wenn **Überprüfen beim Schreiben** aktiviert ist, werden Dateien sofort nach der Entkomprimierung überprüft.

- **Heurist. Suche - Programmdateien**: Aktivieren Sie diese Option, wenn bei der Überprüfung nach möglichem neuem (d. h. bisher unentdecktem) Viruscode in Programmdateien gesucht werden soll. Durch diese Option wird die Sicherheit erhöht, aber auch die Überprüfungszeit verlängert.

- **Heuristische Suche - Word-Makros**: Aktivieren Sie diese Option, wenn bei der Überprüfung nach möglichem neuem (d. h. bisher unentdecktem) Viruscode in Word-Makros gesucht werden soll. Durch diese Option wird die Sicherheit erhöht, aber auch die Überprüfungszeit verlängert.

- **Automatische Entfernung**: Aktivieren Sie diese Option, damit WinGuard infizierende Viren automatisch entfernt, sobald sie entdeckt werden. Weitere Informationen finden Sie im Abschnitt „Falls WinGuard einen Virus findet“ auf Seite 105.

- **Bestätigung vor Virusentfernung**: Aktivieren Sie diese Option, damit WinGuard Sie auffordert, zu bestätigen, daß der Virus automatisch entfernt werden soll. Diese Option ist deaktiviert, d. h. grau unterlegt, wenn **Automatische Entfernung** deaktiviert ist.

- **DOS-Box bei Virusbefall schließen**: Aktivieren Sie diese Option, damit die von WinGuard ausgeführten Maßnahmen bei einer Viruswarnung das Schließen von DOS beinhalten, wenn Sie in DOS arbeiten. Wenn diese Option deaktiviert ist, wird DOS lediglich zum Symbol verkleinert.

- **Treiberdatei**: Treiberdateien enthalten die Information über bekannte Viren, aufgrund derer diese Viren entdeckt werden. WinGuard verwendet vorgabemäßig die Treiberdatei FINDVIRU.DRV.

  Falls Sie diese Option benutzen müssen, sollten Sie sich auf jeden Fall an die technische Unterstützung von Dr Solomon’s wenden.

- **Extratreiber**: Dr Solomon's gibt von Zeit zu Zeit Extratreiberdateien heraus. Sie enthalten Informationen über neue Viren, die nicht in der Standard-Treiberdatei enthalten sind, und ergänzen daher die Liste der Viren, die gefunden werden können.

  Falls Sie diese Option benutzen müssen, um den Namen der Extratreiberdatei anzugeben, sollten Sie sich auf jeden Fall an die technische Unterstützung von Dr Solomon's wenden. Sie müssen den vollständigen Pfad der Extratreiberdatei angeben.

Tip

Wenn die Extratreiberdatei den Namen EXTRA.DRV hat und im Toolkit-Verzeichnis gespeichert ist, braucht sie nicht gesondert angegeben zu werden, da sie dann automatisch verwendet wird.

Tip

Sie können Extratreiberdateien Ihre eigenen Anmerkungen hinzufügen, um sie leichter zu identifizieren und auseinanderzuhalten. Verwenden Sie einen Texteditor, wie z. B. den Editor von Microsoft Windows, um Ihre Anmerkungen hinzuzufügen und anzeigen zu lassen. Jede Anmerkungszeile muß mit einem Semikolon (;) beginnen.

- **Dateiüberprüfung auf Laufwerken**: Lokale Laufwerke sind die Festplatten, die lokal auf dem Computer installiert sind, im allgemeinen Laufwerk C: und möglicherweise weitere Laufwerke. Auf Netzlaufwerke wird über ein Netzwerk zugegriffen.

Tip

Es wird empfohlen, **Alle** auszuwählen, da durch diese Option Viren gefunden werden, wenn auf einer lokalen Festplatte auf sie zugegriffen wird, und der Computer außerdem vor einer Virusinfektion durch externe Quellen geschützt ist.

Falls Sie **Benutzerdefinierte** wählen, müssen Sie die Buchstaben der zu überprüfenden Laufwerke in das Feld eingeben; die Buchstaben brauchen nicht durch Leerzeichen oder Interpunktionszeichen getrennt zu werden.

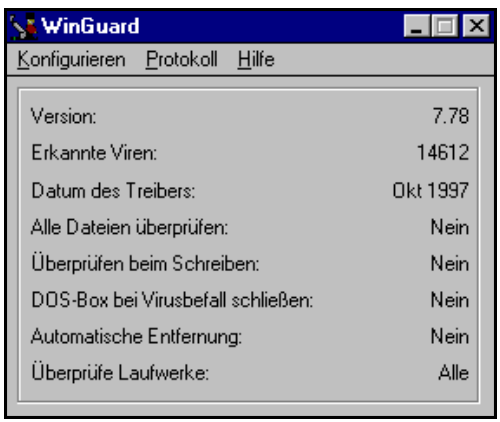
Ändern der Warnmeldungen

So ändern Sie den Text der WinGuard-Meldungen:

1. Öffnen Sie WinGuard durch Doppelklicken auf das WinGuard-Symbol auf dem Desktop (Windows 3.x) oder Klicken auf das WinGuard-Symbol in der Task-Leiste (Windows 95):

Falls WinGuard deaktiviert ist, wird das Symbol nicht angezeigt. In diesem Fall müssen Sie WinGuard zunächst aktivieren; Informationen dazu finden Sie im Abschnitt „Ändern der Konfiguration für die Überprüfung“ auf Seite 95.

Das folgende Dialogfeld wird angezeigt:



2. Wählen Sie **Warnung** aus dem Menü **Konfigurieren**.

3. Geben Sie das Kennwort ein, falls Sie dazu aufgefordert werden.

Das folgende Dialogfeld wird angezeigt:

Das Dialogfeld enthält die Warnungen, die angezeigt werden, wenn ein Virus gefunden wird. Je nachdem, ob es sich um einen Dateivirus oder einen Boot- oder Partitionssektorvirus handelt, wird jeweils eine andere Meldung angezeigt. Die Netzwerkmeldung wird zusätzlich zur lokalen Warnmeldung über das Netzwerk gesendet.

4. Geben Sie den gewünschten Text ein. Sie können alles außer <diesem Text> ändern. Der Text in spitzen Klammern wird durch die entsprechenden Datei- bzw. Virusnamen ersetzt, wenn die Meldung angezeigt wird.

5. Wenn Sie ein neues Kennwort festlegen oder das Kennwort ändern möchten, geben Sie es in das Feld **Kennwort** ein. Bestätigen Sie das Kennwort, indem Sie es erneut in das Feld **Kennwort wiederholen** eingeben.

   Durch das Kennwort sind beide Optionen des Menüs **Konfigurieren** geschützt.

Berichterstellung

WinGuard kann seine Aktivitäten in einer Protokolldatei aufzeichnen. Es werden nur die Überprüfungen protokolliert, bei denen ein Virus gefunden wurde. Bei dem Protokoll handelt es sich um eine Textdatei. Diese Datei wird vorgabemäßig im Toolkit-Verzeichnis gespeichert.

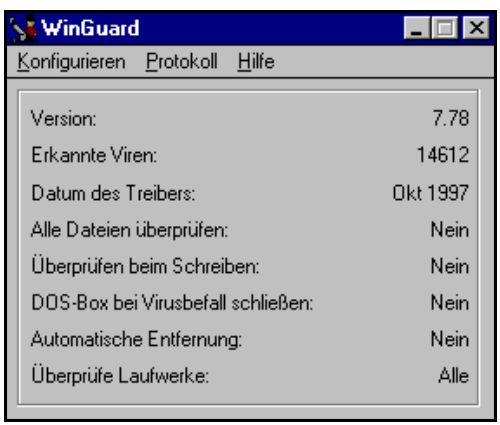
Aktivierung

So aktivieren Sie die Berichterstellung:

1. Öffnen Sie WinGuard durch Doppelklicken auf das WinGuard-Symbol auf dem Desktop (Windows 3.x) oder Klicken auf das WinGuard-Symbol in der Task-Leiste (Windows 95):

   Falls WinGuard deaktiviert ist, wird das Symbol nicht angezeigt. In diesem Fall müssen Sie WinGuard zunächst aktivieren; Informationen dazu finden Sie im Abschnitt „Ändern der Konfiguration für die Überprüfung“ auf Seite 95.

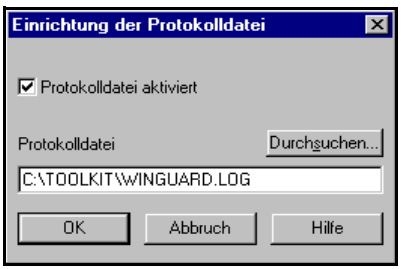
2. Das folgende Dialogfeld wird angezeigt:



3. Wählen Sie **Optionen** aus dem Menü **Protokoll**.

4. Geben Sie das Kennwort ein, falls Sie dazu aufgefordert werden.

Das folgende Dialogfeld wird angezeigt:



5. Aktivieren Sie das Kontrollkästchen **Protokolldatei aktiviert**.

6. Wenn Sie möchten, können Sie den Vorgabenamen der Protokolldatei ändern. Sie können ein anderes Verzeichnis für die Datei festlegen, indem Sie den Pfad direkt eingeben, oder indem Sie auf die Schaltfläche **Durchsuchen** klicken und den Pfad aus dem angezeigten Dialogfeld auswählen.

7. Klicken Sie auf **OK**.

Dateiansicht

Die Protokolldatei hat ein Standard-Textformat. Sie können sie in einem Texteditor ansehen.

Sie können auch das WinGuard-Konfigurationsprogramm verwenden:

1. Öffnen Sie WinGuard durch Doppelklicken auf das WinGuard-Symbol auf dem Desktop (Windows 3.x) oder Klicken auf das WinGuard-Symbol in der Task-Leiste (Windows 95):

Falls WinGuard deaktiviert ist, wird das Symbol nicht angezeigt. In diesem Fall müssen Sie WinGuard zunächst aktivieren; Informationen dazu finden Sie im Abschnitt „Ändern der Konfiguration für die Überprüfung“ auf Seite 95.

2. Wählen Sie **Ansicht** aus dem Menü **Protokoll**.

   Die Protokolldatei wird im Editor von Microsoft Windows angezeigt.

Falls WinGuard einen Virus findet

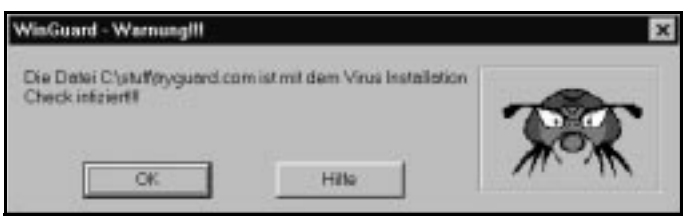
Was passiert, wenn WinGuard einen Virus findet, hängt davon ab, ob die Option **Automatische Entfernung** aktiviert oder deaktiviert ist.

Tip

Automatische Entfernung ist vorgabemäßig deaktiviert; Sie müssen diese Option manuell aktivieren (siehe Seite 99).

Falls WinGuard einen Virus findet und **Automatische Entfernung** nicht aktiviert ist:

- Wenn die Überprüfung nicht beim Schreiben in eine Datei stattfindet (siehe **Überprüfen beim Schreiben** auf Seite 98), wird der Vorgang abgebrochen.
- Im Bildschirmvordergrund wird eine Warnung angezeigt:



- Je nachdem, welche Optionen Sie festgelegt haben (siehe „Ändern der Warnmeldungen“ auf Seite 101), wird entweder ein Bericht über den Virus in einer Protokolldatei gespeichert oder eine Netzwerkmeldung weitergeleitet.
- Wenn die Überprüfung nicht beim Schreiben in eine Datei stattfindet, erhalten Sie wahrscheinlich auch von Ihrer Anwendung die Meldung,

daß nicht auf die angegebene Datei bzw. den angegebenen Datenträger zugegriffen werden kann.

Sie sollten auf **OK** klicken und die Infektion sofort beseitigen. Sie haben folgende Möglichkeiten für die Entfernung von Viren:

- Aktivieren Sie die WinGuard-Option **Automatische Entfernung** (Sie müssen nach Aktivierung von **Automatische Entfernung** den Computer neu starten, damit diese Einstellung wirksam wird), und wiederholen Sie dann den Vorgang;
- Führen Sie FindVirus aus, entweder von der Benutzeroberfläche oder von der SOS-Diskette (siehe „SOS-Diskette“ auf Seite 1).

Falls WinGuard einen Virus findet, **Automatische Entfernung** aktiviert und die Entfernung erfolgreich ist, wird eine Meldung angezeigt, z. B.:

Klicken Sie auf **OK**, um fortzufahren.

Falls der Virus nicht entfernt werden kann, passiert das gleiche wie bei Deaktivierung von **Automatische Entfernung**. Wenden Sie sich in diesem Fall an die technische Unterstützung von Dr Solomon’s.

Warnung

Für Benutzer von Windows 95: Falls WinGuard einen Dateivirus nicht entfernen kann, sollten Sie die Datei löschen. Nach dem Löschen der Datei müssen Sie den Papierkorb auf dem Desktop leeren, um sicherzustellen, daß die infizierte Datei nicht auf dem Computer bleibt.

4.5 Erweiterte Virensuche mit WinGuard für Windows NT

Entfernen ist eine der Optionen, die Sie für während eines Lesezugriffs gefundene infizierte Dateien auswählen, und (unabhängig davon) als den Vorgang festlegen können, der ausgeführt wird, wenn bei einem Schreibzugriff infizierte Dateien gefunden werden. Als Vorgabe ist **Nichts unternehmen** festgelegt; wenn WinGuard den Virus automatisch entfernen soll, müssen Sie die Option **Entfernen** aktivieren. Sie nehmen die Auswahl auf der Registerkarte **Operation** vor; siehe Seite 114.

Falls WinGuard einen Virus findet - „Entfernen“ nicht aktiviert

Die Option **Entfernen** bezieht sich nicht auf die Boot- und Partitionssektoren von Festplatten. Falls WinGuard einen Virus in einem dieser Sektoren findet, werden immer die in diesem Abschnitt beschriebenen Vorgänge ausgeführt.

Falls WinGuard einen Virus findet und **Entfernen** für die Zugriffsart nicht aktiviert ist:

- Der ausgeführte Vorgang wird abgebrochen.
- Das Warndialogfeld (in einer seiner beiden Formen) wird im Bildschirmvordergrund angezeigt. Dieses Dialogfeld ist auf den Seiten 110 und 111 abgebildet.
- Je nach den festgelegten Optionen werden Berichte über den Virus als Warnmeldungen weitergegeben oder im Ereignisprotokoll aufgezeichnet. Weitere Informationen finden Sie im Abschnitt „Registerkarte „Ausgabe““ auf Seite 117.
- Je nachdem, welche Maßnahmen für welche Zugriffsart festgelegt wurden (siehe „Registerkarte „Operation““ auf Seite 114), unternimmt WinGuard gar nichts, die Datei wird gelöscht oder in ein Quarantäneverzeichnis verschoben.
- Sie erhalten wahrscheinlich auch eine Warnung von der ausgeführten Anwendung, daß auf die angegebene Datei / den angegebenen Datenträger nicht zugegriffen werden kann.
- Alle anderen Aktivitäten des Systems werden wie gewohnt fortgesetzt.

Führen Sie die folgenden Schritte aus:

1. Wenn Sie als Warndialogfeld die Bisher-Liste verwenden, können Sie durch Klicken auf die Schaltfläche **FindVirus ausführen** die Infektionen schnell entfernen. Sie müssen dazu allerdings die Option **Entfernen** auf der Registerkarte **FindVirus** aktiviert haben. Es wird empfohlen, auch die nächsten Schritte auszuführen.

2. Notieren Sie sich die Einzelheiten der infizierten Dateien aus dem Warndialogfeld, und schließen Sie das Dialogfeld.

3. Beenden Sie das Programm wie gewohnt, und speichern Sie alle Dateien, an denen Sie gearbeitet haben.

4. Versuchen Sie, eine weitere Verbreitung des Virus zu verhindern; beenden Sie alle nicht unbedingt notwendigen Anwendungen auf dem Computer.

Warnung

Beenden Sie ohne die entsprechende Vorbereitung keine Anwendungen, die für die Ausführung der Netzwerkfunktionen benötigt werden.

5. Sie sollten den Virus so bald wie möglich mit Hilfe von FindVirus entfernen; weitere Informationen finden Sie im Abschnitt „Entfernung von Viren aus Laufwerken“ auf Seite 151. Sie können auch die Option **Entfernen** aktivieren und den Vorgang wiederholen.

Falls WinGuard einen Virus findet - „Entfernen“ aktiviert

Die Option **Entfernen** bezieht sich nicht auf die Boot- und Partitionssektoren von Festplatten. Falls WinGuard einen Virus in einem dieser Sektoren findet, werden immer die auf Seite 107 beschriebenen Vorgänge ausgeführt.

Falls WinGuard einen Virus in einer Datei oder im Bootsektor einer Diskette findet und **Entfernen** für die entsprechende Zugriffsart aktiviert ist, wird automatisch versucht, den Virus zu entfernen.

Wenn der Virus erfolgreich entfernt werden kann, können Sie normal weiterarbeiten. Wenn die Option **Warndialogfeld bei erfolgreicher Entfernung nicht anzeigen** auf der Registerkarte **Entfernung** deaktiviert ist (siehe Seite 116), wird das Dialogfeld angezeigt, um Sie zu informieren, daß der Virus entfernt worden ist. Wenn **Warndialogfeld bei erfolgreicher Entfernung nicht anzeigen** aktiviert ist, wird das Warndialogfeld nicht angezeigt.

Wenn WinGuard erfolglos versucht, einen Virus aus dem Bootsektor einer Diskette zu entfernen, verhält sich das Programm so, als wäre **Entfernen** nicht aktiviert, wie auf Seite 107 beschrieben.

Was passiert, wenn WinGuard erfolglos versucht, einen Virus aus einer Datei zu entfernen, hängt davon ab, welche Option im Feld **Falls der Dateivirus nicht entfernt werden kann** auf der Registerkarte **Entfernung** ausgewählt ist (siehe Seite 116).

- Wenn **Nichts unternehmen** ausgewählt ist, zeigt WinGuard nur das Warndialogfeld an.
- Wenn **Löschen** ausgewählt ist, löscht WinGuard zusätzlich zur Anzeige des Warndialogfelds die Datei.
- Wenn **In Quarantäneverzeichnis verschieben** ausgewählt ist, verschiebt WinGuard zusätzlich zur Anzeige des Warndialogfelds die Datei in das auf der Registerkarte **Operation** angegebene Quarantäneverzeichnis.

Auf Seite 107 finden Sie eine Beschreibung der ausgeführten Vorgänge, wenn WinGuard einen Virus findet und **Entfernen** für die aktuelle Zugriffsart nicht aktiviert ist.

Das Warndialogfeld - Bisher-Liste

Sie können WinGuard so konfigurieren, daß eins von zwei unterschiedlichen Warndialogfeldern angezeigt wird; in diesem Abschnitt wird die sogenannte „Bisher-Liste“ beschrieben. Informationen über benutzerdefinierte Meldungen finden Sie im nächsten Abschnitt.

Die Bisher-Liste sieht folgendermaßen aus:

Schließt das Warndialogfeld, ohne die Berichte zu löschen.

Löscht die Berichte, ohne das Warndialog-feld zu schließen

Führt eine FindVirus-Überprüfung auf allen Laufwerken aus, auf denen sich eine in einem Infektionsbericht aufgeführte Datei befindet.

Diese Schaltfläche ist grau unterlegt, wenn FindVirus nicht installiert ist.

Ruft das Hauptdialogfeld von Dr Solomon's Anti-Virus Toolkit auf.

Diese Schaltfläche ist grau unterlegt, wenn das Anti-Virus Toolkit nicht installiert ist.

In dem Dialogfeld werden Berichte über Virusinfektionen aufgeführt.

Wenn die Option **Warndialogfeld bei erfolgreicher Entfernung nicht anzeigen** auf der Registerkarte **Entfernung** (siehe Seite 116) deaktiviert ist, enthält das Dialogfeld auch Berichte über erfolgreiche Virusentfernungen.

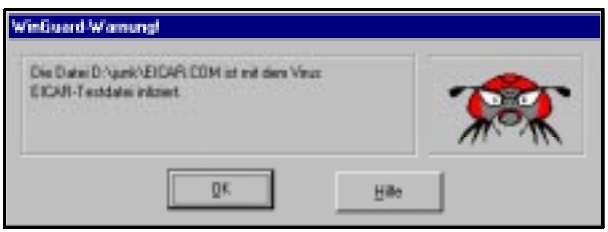
Das Dialogfeld bietet Ihnen die Möglichkeit, FindVirus oder das Toolkit auszuführen (vorausgesetzt, sie sind installiert).

Die Berichte enthalten Datum und Zeit und den Namen der infizierten Datei bzw. der Datei, aus der ein Virus entfernt wurde. Neue Berichte werden an das Ende der Liste angehängt; die Berichte werden gespeichert, bis Sie auf **Löschen** klicken.

Das Warndialogfeld - Benutzerdefinierte Meldung

Sie können WinGuard so konfigurieren, daß eins von zwei unterschiedlichen Warndialogfeldern angezeigt wird; in diesem Abschnitt wird die benutzerdefinierte Warnmeldung beschrieben. Informationen über die Bisher-Liste finden Sie im vorigen Abschnitt.

Das Dialogfeld mit der benutzerdefinierten Warnmeldung sieht folgendermaßen aus:



Das Dialogfeld zeigt folgendes an:

- Virusinfektionen;
- erfolglose Versuche, Viren zu entfernen;
- erfolgreiche Entfernungen von Viren (aber nur, wenn die Option **Warndialogfeld bei erfolgreicher Entfernung nicht anzeigen** auf der Registerkarte **Entfernung** (siehe Seite 116) deaktiviert ist).

Auf der Registerkarte **Meldung** (siehe Seite 118) können Sie Ihren eigenen Text für die Meldungen eingeben, die bei Infektionen von Dateien, Boot- und Partitionssektoren angezeigt werden.

Ändern der Einstellungen

Die Vorgabeeinstellungen von WinGuard, mit denen das Programm installiert wird, sind für die meisten Situationen ausreichend. Sie können die Einstellungen jedoch ändern, um sie an Ihre Anforderungen anzupassen.

Ausführliche Informationen über die Vorgabeeinstellungen finden Sie in der Übersichtstabelle unter dem Thema „Konfiguration“ in der WinGuard-Hilfe.

Starten des Konfigurationsdienstprogramms

Sie ändern die Einstellungen über das Konfigurationsdienstprogramm in der Systemsteuerung.

Tip

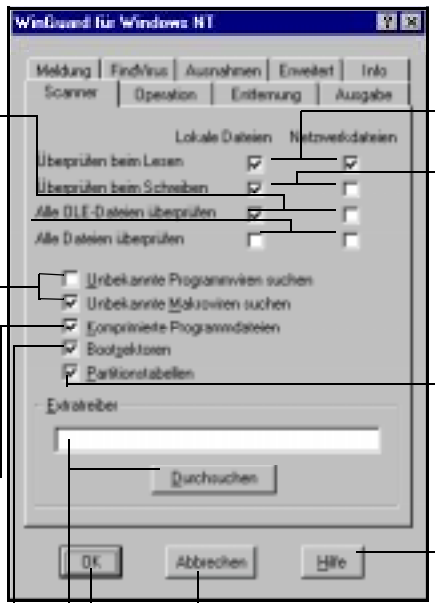
Nur Administratoren können die Konfiguration der Einstellungen ändern.

Ein Dialogfeld mit mehreren Registerkarten wird angezeigt. Durch Klicken auf eine Registerkarte wird diese im Vordergrund angezeigt.

In den folgenden Abschnitten werden die Optionen auf den Registerkarten im einzelnen aufgeführt.

Registerkarte „Scanner“

Auf dieser Registerkarte legen Sie fest, was überprüft wird, und wann Dateien überprüft werden. Außerdem geben Sie an, ob ein Extratreiber verwendet werden soll.



Alle Dateien mit OLE-Objekten auf Netzlaufwerken und/oder lokalen Laufwerken werden überprüft. Hierbei werden auch Makroviren gefunden.

Alle Datendateien und ausführbaren Dateien auf lokalen und/oder Netzlaufwerken werden überprüft.

Es wird nach neuen bzw. unentdeckten Viren gesucht (heuristische Suche). Die Sicherheit wird erhöht, die Überprüfungszeit verlängert.

Dateien, die mit Programmen wie PKLite oder LZExe komprimiert sind, werden überprüft.

Die Bootsektoren von lokalen Festplatten (NTFS oder DOS FAT) werden beim Systemstart bzw. bei jedem Neustart von WinGuard überprüft. Auch Bootsektoren von Disketten werden beim Zugriff überprüft.

Überprüfung von Dateien bei Lesezugriff auf lokalen Festplatten und/oder Netzlaufwerken.

Überprüfung von Dateien sofort nach dem Schreiben auf lokale Festplatten und/oder Netzlaufwerke.

Überprüfung der Partitionstabellen von lokalen Festplatten bei jedem Systemstart bzw. Neustart von WinGuard.

Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Ignorieren aller Änderungen.

Übernahme von Änderungen. Falls ein Extratreiber hinzugefügt wird, muß Windows NT neu gestartet werden, damit die Änderungen

Geben Sie den Dateinamen des Extratreibers hier ein, oder klicken Sie auf **Durchsuchen**, um ihn aus dem angezeigten Dialogfeld auszuwählen.

Verwenden Sie diese Option nur unter Anleitung von Dr Solomon’s, z. B. wenn ein neuer Extratreiber für einen plötzlichen Virusnotfall herausgegeben wird.

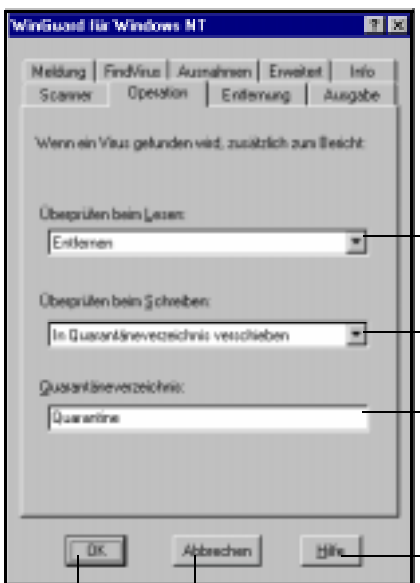
Registerkarte „Operation“

Auf dieser Registerkarte legen Sie fest, welche Schritte WinGuard zusätzlich zur Anzeige des Warndialogfelds und dem Senden einer Netzwerknachricht (falls aktiviert) ausführt, wenn ein Virus gefunden wird.

Klicken Sie für die Optionen **Überprüfen beim Lesen u**nd **Überprüfen beim Schreiben** auf den Pfeil nach unten , und wählen Sie die gewünschte Einstellung aus dem Dropdown-Menü.

Tip

Keine der Einstellungen, die Sie auf dieser Registerkarte festlegen, gelten für Lese- oder Schreibzugriffe auf Netzlaufwerke; für diese Laufwerke gilt immer die Einstellung **Nichts unternehmen**.



Bestimmt, was mit einer infizierten Datei passiert, wenn diese gelesen wird. Wählen Sie **Entfernen**, um den Virus automatisch zu entfernen, **In Quarantäneverzeichnis verschieben**, um die infizierte Datei in das unter **Quarantäne-verzeichnis** festgelegte Verzeichnis zu verschieben, und **Nichts unternehmen**, damit lediglich ein Bericht erstellt wird.

Bestimmt, was mit einer infizierten Datei passiert, wenn diese auf einen Datenträger geschrieben wird: **Entfernen**, **In Quarantäneverzeichnis verschieben**, **Nichts unternehmen** oder **Löschen**, um die infizierte Datei zu entfernen.

Erstellen des Verzeichnisses, in das infizierte Dateien verschoben werden, wenn für **Überprüfen beim Lesen** oder **Überprüfen beim Schreiben** die Option **In Quarantäneverzeichnis verschieben** ausgewählt ist. Geben Sie den Verzeichnisnamen und/oder Pfad ein, aber keinen Laufwerksbuchstaben.

Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Ignorieren aller Änderungen.

Übernahme von Änderungen.

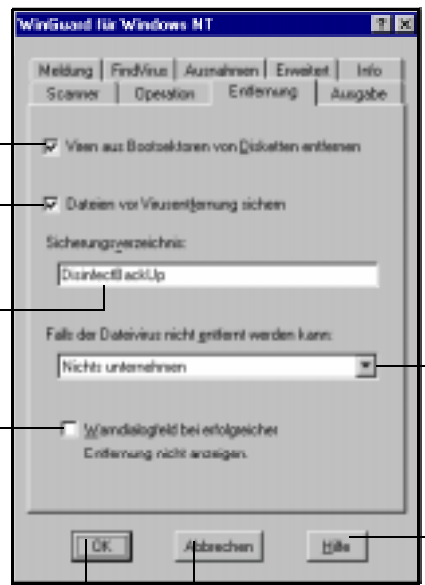
Wenn eine Datei in ein Quarantäneverzeichnis verschoben wird, das bereits eine Datei mit demselben Namen enthält, wird die Dateierweiterung geändert. Die neue Erweiterung besteht aus dem „alten“ ersten Zeichen und einer Zahl. Beispiel: Die Datei AFILE.COM wird umbenannt zu AFILE.C01; bei der nächsten Verschiebung wird AFILE.C02 aus AFILE.COM usw.

Warnung

Wenn Sie für **Überprüfen beim Schreiben** die Option **Löschen** wählen, gehen möglicherweise Dateien verloren. Beispiel: Auf einem nicht geschützten Computer wird ein MS Word-Dokument auf einem gemeinsam benutzten Computer in einem Netzwerk geöffnet. Der Computer, auf dem die Datei ursprünglich gespeichert war, ist geschützt. Die Datei wird mit einem Makro-Virus infiziert und dann gespeichert. Wenn auf dem geschützten Computer **Überprüfen beim Schreiben** aktiviert ist, wird die Datei sofort nach dem Speichern überprüft. Die Infektion wird festgestellt und die Datei gelöscht; das Dokument geht verloren.

Registerkarte „Entfernung“

Auf dieser Registerkarte legen Sie fest, welche Maßnahmen WinGuard ergreift, wenn für **Überprüfen beim Lesen** oder **Überprüfen beim Schreiben** auf der Registerkarte **Operation** (siehe Seite 114) die Option **Entfernen** aktiviert ist. Außerdem legen Sie fest, ob Viren automatisch aus dem Bootsektor von Disketten entfernt werden sollen (aus den Bootsektoren von Festplatten werden Viren nicht automatisch entfernt).



Automatische Entfernung von Viren aus den Bootsektoren von Disketten.

Sicherung der Dateien im angegebenen Sicherungsverzeichnis vor der automatischen Entfernung.

Name des Verzeichnisses, in das die Sicherungsdateien kopiert werden.

Warndialogfeld bei Entfernung von Dateiviren nicht anzeigen.

Festlegen der zu ergreifenden Maßnahmen, falls ein Dateivirus nicht automatisch entfernt werden kann.
Nichts unternehmen: Es wird ein Bericht über die Infektion ausgegeben, so als wäre die Option **Entfernen** nicht aktiviert.
In Quarantäneverzeichnis verschieben: Die infizierte Datei wird in das im Feld **Quarantäneverzeichnis** auf der Registerkarte **Operation** angegebene Verzeichnis kopiert.
Löschen: Die infizierte Datei wird gelöscht.

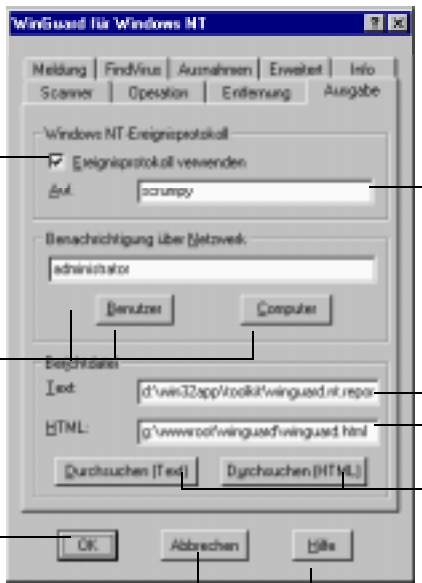
Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Ignorieren aller Änderungen.

Übernahme von Änderungen.

Registerkarte „Ausgabe“

Auf dieser Registerkarte legen Sie fest, welche Berichte WinGuard ausgibt, wenn ein Virus gefunden wird. WinGuard erstellt die Berichte zusätzlich zur Anzeige des Warndialogfelds.



Kopieren der Namen der Datei und des infizierenden Virus in das NT-Ereignis-protokoll.

Geben Sie den Namen eines Benutzers oder Computers ein, oder klicken Sie auf **Benutzer** oder **Computer**, und wählen Sie einen Namen aus der Liste, um über den Windows NT-Mel-dungsdienst Berichte an den ausgewählten Benutzer oder Computer zu senden.

Übernahme von Änderungen.

Ignorieren aller Änderungen.

Aufrufen der Online-Hilfe-datei für dieses Dialogfeld.

Geben Sie den Namen des Computers ein, in dessen Ereignisprotokoll der Bericht angezeigt werden soll. Hinweis: Sie müssen die entsprechenden Zugriffs-rechte haben. Die Rechte können manuell konfigu-riert werden. Siehe Online-Hilfethema „Konfiguration eines Fernrechners für die Aufzeichnung von Ereignisprotokollen“.

Geben Sie einen Datei-namen in das entspre-chende Feld ein, oder wählen Sie über die Schaltfläche **Durch-suchen** eine bestehende Berichtdatei aus, um ein ständiges Protokoll von Virusinfektionen zu erstellen.

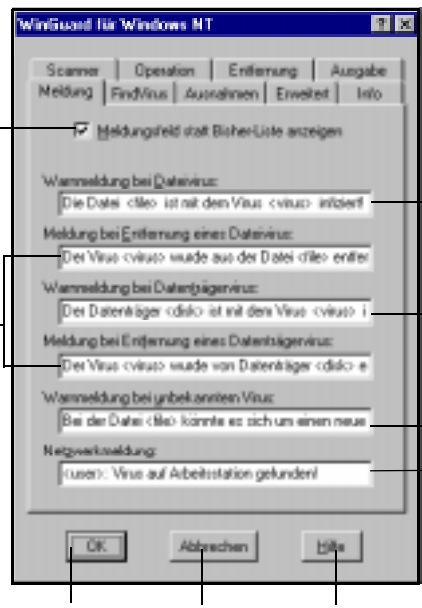
Datum und Zeit der Entdeckung der Infektion sowie der Dateiname, der Virustyp und der Name des Benutzers, der auf die Datei zugreifen wollte, werden aufgezeichnet. Neue Berichte werden an das Ende der bestehen-den Datei angehängt.

Registerkarte „Meldung“

Auf dieser Registerkarte geben Sie den Text der Meldungen ein, die im benutzerdefinierten Warndialogfeld angezeigt werden (siehe Seite 111).

Aktivieren Sie dieses Kontrollkästchen, damit im Warndialogfeld die auf dieser Registerkarte festgelegte Warnmeldung angezeigt wird. Wenn diese Option nicht aktiviert ist, zeigt das Warndialogfeld eine Liste aller seit dem letzten Löschen der Liste gefundenen Virusinfektionen an.

Geben Sie den Text ein, der bei erfolgreicher Entfernung eines Virus im Warndialogfeld angezeigt werden soll. Es müssen folgende Informationen enthalten sein: <virus>, um den Namen des infizierenden Virus anzuzeigen; <file>, um den Namen der infizierten Datei anzuzeigen; <disk>, um den Buchstaben des infizierten Laufwerks anzuzeigen.



Übernahme von Änderungen.

Ignorieren aller Änderungen.

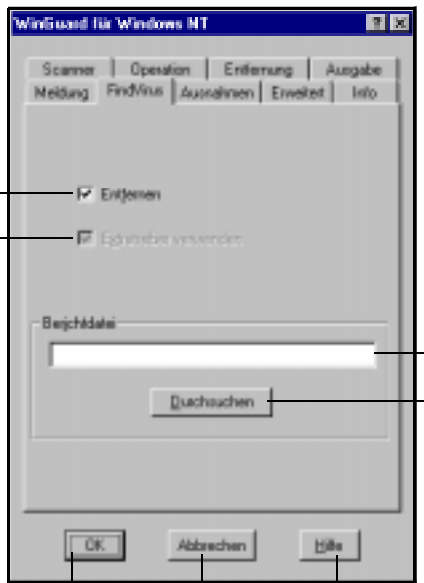
Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Geben Sie den Text ein, der im Warndialogfeld angezeigt wird, wenn ein Virus gefunden wird. Folgende Informationen müssen enthalten sein: <virus>, um den Namen des infizierenden Virus anzuzeigen; <file>, um den Namen der infizierten Datei anzuzeigen; <disk>, um den Buchstaben des infizierten Laufwerks anzuzeigen.

Geben Sie den Text für die Meldung ein, die in das auf der Registerkarte **Ausgabe** unter **Benachrichtigung über Netzwerk** angegebene Ziel gesendet werden soll, falls ein Virus gefunden wird. Folgende Informationen müssen enthalten sein: <user>, um den Namen des angemeldeten Benutzers anzuzeigen; <virus>, um den Namen des infizierenden Virus anzuzeigen; <file>, um den Namen der infizierten Datei anzuzeigen.

Registerkarte „FindVirus“

Wenn FindVirus installiert ist, haben Sie im Dialogfeld mit der Bisher-Liste die Möglichkeit, FindVirus zu starten. Auf der Registerkarte **FindVirus** legen Sie die von FindVirus verwendeten Einstellungen fest.



FindVirus entfernt Viren bei Ausführung.

Wenn diese Option aktiviert ist, verwendet FindVirus bei Ausführung den auf der Registerkarte **Scanner** angegebenen Extratreiber. Extratreiber werden manchmal zwischen regulären Aktualisierungen herausgegeben, um Schutz vor plötzlich auftretenden Virusnotfällen zu bieten.
Es handelt sich hier um eine unabhängige Funktion, die sich nicht auf die im FindVirus-Hauptdialogfeld des Toolkit vorgenommenen Einstellungen auswirkt.

Geben Sie den Dateinamen oder vollständigen Pfad einer Datei ein, oder wählen Sie über die Schaltfläche **Durchsuchen** eine Datei aus, in die Berichte von FindVirus-Überprüfungen kopiert werden sollen.
Es handelt sich hier um eine unabhängige Funktion, die sich nicht auf die im FindVirus-Hauptdialogfeld des Toolkit vorgenommenen Einstellungen auswirkt.

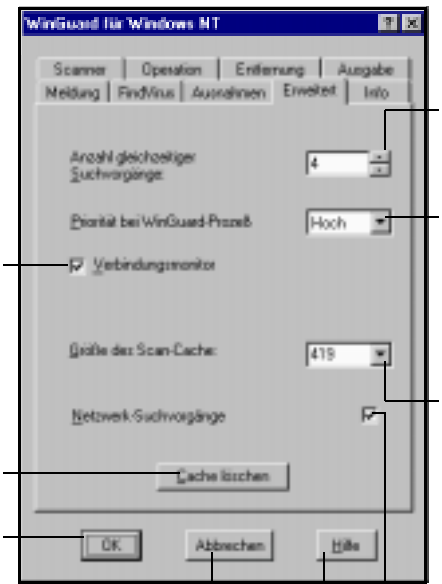
Übernahme von Änderungen.

Ignorieren aller Änderungen.

Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Registerkarte „Erweitert“

Über diese Registerkarte erfolgt die Feinabstimmung der internen Funktionsweise von WinGuard. Die Vorgabeeinstellungen auf dieser Registerkarte sind für die meisten Benutzer ausreichend. Sollten Sie dennoch Änderungen vornehmen wollen, gehen Sie äußerst vorsichtig vor, und seien Sie sich der Konsequenzen bewußt.



WinGuard wird in das NetWare-Toolkit integriert, das auf einem Server läuft. Das NetWare-Toolkit überprüft, ob WinGuard auch auf der Arbeitsstation läuft, bevor eine Anmeldung im Netzwerk zugelassen wird.

Löschen aller Einträge aus dem Scan-Cache.

Übernahme von Änderungen.

Ignorieren aller Änderungen.

Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Anzahl der Dateien (höchstens 64), die mit Hilfe von Windows NT-Multithreading gleichzeitig gelesen werden können.

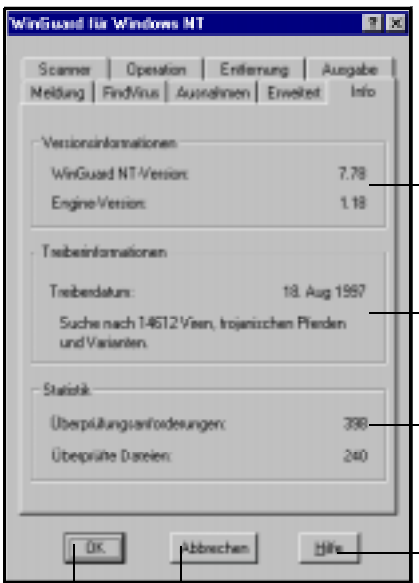
WinGuard-Prozeßpriorität. Wenn **Hoch** ausgewählt ist, überprüft WinGuard Dateien so schnell wie möglich. Dies wirkt sich nicht auf andere Anwendungen aus, da WinGuard nur bei einer Überprüfung Prozessorzeit beansprucht.

Festlegen der Größe des Scan-Cache. Im Scan-Cache sind die Dateien gespeichert, auf die seit der letzten Überprüfung kein Schreibzugriff mehr erfolgt ist. Da Dateien nur durch Schreibzugriff geändert werden können, werden diese Dateien nicht untersucht, wodurch die Überprüfungszeit reduziert wird.

Auf einem Netzwerkcomputer gelesene Dateien werden in den Scan-Cache aufgenommen. Diese Option kann gefahrlos verwendet werden, wenn auf allen vernetzten Computern WinGuard NT ausgeführt wird. Wenn nicht, seien Sie VORSICHTIG, da eine Datei nicht aus dem Scan-Cache entfernt wird, wenn auf einem anderen Computer in sie geschrieben wird.

Registerkarte „Info“

Auf dieser Registerkarte wird die Statistik des Überprüfungsvorgangs angezeigt. Es handelt sich herbei nicht um eine Registerkarte mit konfigurierbaren Einstellungen.



Anzeige der WinGuard-Versionsnummer und der Versionsnummer des Überprüfungsengine (mit FindVirus gemeinsam benutzt).

Anzeige des Datums der Treiberdatei und der Anzahl von Viren, trojanischen Pferden und Varianten, deren eindeutige Prüfsumme WinGuard überprüft. Diese Informationen werden mit jeder neuen Version aktualisiert.

Anzahl der seit dem Starten von WinGuard NT aufgerufenen Dateien und durchgeführten Überprüfungsvorgänge.

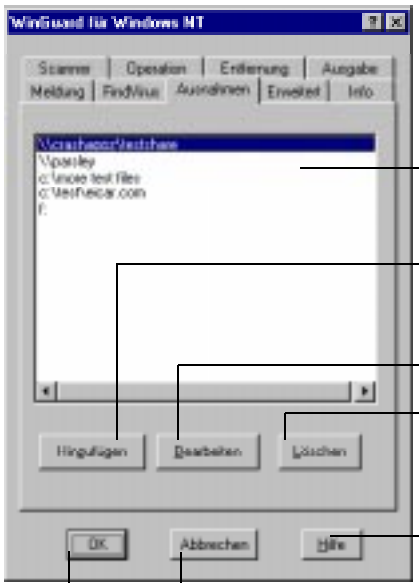
Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Ignorieren aller Änderungen.

Übernahme von Änderungen.

Registerkarte „Ausnahmen“

Auf dieser Registerkarte legen Sie Dateien oder Pfade fest, die nicht überprüft werden sollen.



Zeigt eine Liste mit Dateien bzw. Pfaden an, die von der Überprüfung ausgenommen werden.

Über diese Schaltfläche fügen Sie der Liste einen Eintrag hinzu. Sie können Dateien aus dem Datei-Manager oder Explorer ziehen und im Listenfeld ablegen.

Bearbeiten eines Eintrags in der Ausnahmenliste.

Entfernen eines Eintrags aus der Ausnahmenliste.

Aufrufen der Online-Hilfedatei für dieses Dialogfeld.

Ignorieren aller Änderungen.

Übernahme von Änderungen.

5. Verwendung des Zeitplaners in Windows 3.x, Windows 95 und Windows NT

Mit Hilfe des Zeitplaner-Editors erstellen Sie Ereignisse, die zu festgesetzten Zeiten ausgeführt werden. Bei den Ereignissen kann es sich um Überprüfungen auf Viren, Dateiprüfungen oder die Ausführung einer beliebigen Anwendung handeln. Ereignisse können lediglich einmal oder in regelmäßigen Zeitabständen ausgeführt werden.

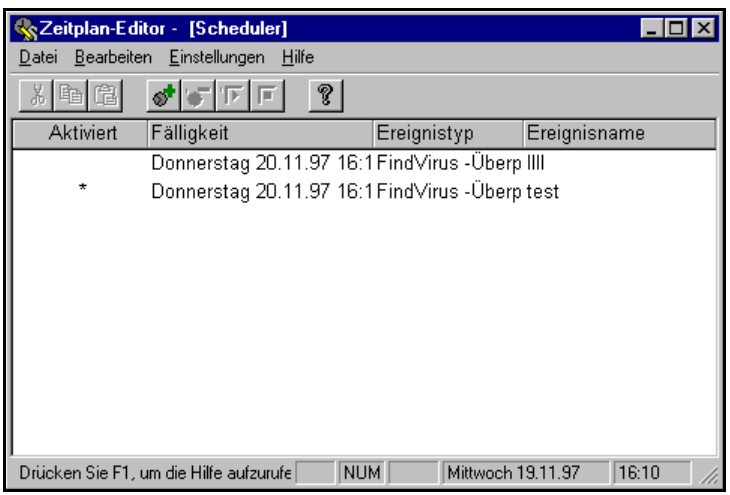
Wenn die Ereignisse erstellt sind, sorgt der speicherresidente Zeitplaner dafür, daß sie zu ihren festgesetzten Zeiten ausgeführt werden.

Die Ergebnisse von Ereignissen können in eine Protokolldatei geschrieben werden, so daß Sie sie später einsehen können.

5.1 Zeitplan-Editor - Übersicht und Aufrufen

Sie können den Zeitplan-Editor über das entsprechende Symbol in der Programmgruppe **Dr Solomon's AVTK** aufrufen.

Der Zeitplan-Editor sieht folgendermaßen aus:



Auf dem Bildschirm werden bereits erstellte Ereignisse zusammengefaßt, jeweils ein Ereignis pro Zeile.

Wenn Sie auf die Ränder der Überschriftenfelder klicken und mit gedrückter linker Maustaste ziehen, können Sie die Größe der Spalten ändern.

Klicken Sie auf ein bestehendes Ereignis, um es auszuwählen und zu bearbeiten.

Sie können eine Symbolleiste anzeigen lassen (siehe Seite 149), die Symbole für Elemente des Menüs **Bearbeiten** enthält. Wenn Sie mit dem Mauszeiger auf ein Symbol zeigen, werden Kurzinformationen über die Funktionsweise des Symbols angezeigt (siehe Seite 149).

Erstellen neuer Ereignisse

Tip

Wenn Sie wie in diesem Abschnitt beschrieben ein neues Ereignis erstellt haben, müssen Sie darauf achten, daß der Zeitplaner läuft, damit das Ereignis ausgeführt werden kann. Weitere Informationen finden Sie im Abschnitt „Ausführung des Zeitplaners“ auf Seite 138.

Registerkarte „Ereignis“

So erstellen Sie ein neues Ereignis:

1. Klicken Sie auf das Symbol **Neues Ereignis**, oder wählen Sie **Ereignis hinzufügen** aus dem Menü **Ereignis**. Das Dialogfeld **Neues Ereignis** wird angezeigt:

2. Geben Sie in das Feld **Name** einen eindeutigen Namen für das Ereignis ein.

3. Wählen Sie im Feld **Typ** einen Ereignistyp aus dem Dropdown-Menü aus. Folgende Möglichkeiten stehen zur Verfügung:

- **Virensuche - FindVirus ausführen**. Wenn Sie diese Option auswählen, wird dem Dialogfeld die Registerkarte **Einstellungen für Virensuche** hinzugefügt.

- **Änderungen prüfen - ViVerify ausführen**. Wenn Sie diese Option auswählen, wird dem Dialogfeld die Registerkarte **Einstellungen für Überprüfung** hinzugefügt.

- **Anwendung ausführen**. In Windows NT steht diese Option nur Administratoren zur Verfügung. Wenn Sie diese Option auswählen, wird am unteren Rand des Dialogfelds das Feld **Programm** hinzugefügt, in das Sie Informationen eingeben müssen.

- **Nachricht senden (nur für Windows 3.x und Windows NT)**. Wenn Sie diese Option auswählen, wird am unteren Rand des Dialogfelds das Feld **Nachricht** hinzugefügt, in das Sie Informationen eingeben müssen.

4. Wählen Sie das Format der Fensteranzeige aus dem Dropdown-Menü aus. Dadurch wird festgelegt, wie das Fenster für das Ereignis während der Ausführung angezeigt wird.

5. Aktivieren Sie im Feld **Schreiben in Protokolldatei des Zeitplaners** eins der runden Optionsfelder. In der Protokolldatei werden die Einzelheiten jedes ausgelösten Ereignisses aufgezeichnet, unter anderem die festgelegte Zeit und das Datum des Ereignisses und ob es erfolgreich ausgelöst wurde. Folgende Optionen stehen für das Schreiben in die Protokolldatei zur Verfügung:

- **Immer**.

- **Nur bei Fehler**. Ein Fehler liegt beispielsweise dann vor, wenn das Ereignis nicht ausgeführt werden kann oder die ausführbare Datei einer Anwendung nicht gefunden wird.

- **Nie**.

6. Gehen Sie zur Registerkarte **Intervall**, und legen Sie die gewünschten Einstellungen fest wie im Abschnitt „Registerkarte „Intervall““ auf Seite 127 beschrieben.

7. Wenn Sie **Virensuche - FindVirus ausführen** als Ereignistyp gewählt haben, gehen Sie zur Registerkarte **Einstellungen für Virensuche** und legen die gewünschten Einstellungen fest wie im Abschnitt „Registerkarte „Einstellungen für Virensuche““ auf Seite 128 beschrieben.

8. Wenn Sie **Änderungen prüfen - ViVerify ausführen** als Ereignistyp gewählt haben, gehen Sie zur Registerkarte **Einstellungen für Überprüfung** und legen die gewünschten Einstellungen fest wie im Abschnitt „Registerkarte „Einstellungen für Überprüfung““ auf Seite 134 beschrieben.

9. Wenn Sie **Anwendung ausführen** gewählt haben, füllen Sie die Eingabefelder im Feld **Programm** aus, das am unteren Rand des Dialogfelds angezeigt wird. Machen Sie folgende Angaben:

- In das Feld **Beschreibung** können Sie Text direkt eingeben. Sie können auch auf den Pfeil nach unten neben dem Eingabefeld klicken, um eine Dropdown-Liste anzuzeigen. In der Liste sind Beschreibungen von Programmen aufgeführt, die auf der Registerkarte **Listenfelder** im Dialogfeld **Vorgabeeinstellungen für Dr Solomon's Scheduler** festgelegt wurden (siehe Schritt 11 auf Seite 148). Klicken Sie auf eine dieser Beschreibungen, um das entsprechende Programm auszuwählen.

- Geben Sie die Befehlszeile direkt in das Feld **Befehlszeile** ein, oder suchen Sie die ausführbare Datei über die Schaltfläche **Durchsuchen**. Das Feld wird automatisch ausgefüllt, wenn Sie die Beschreibung des Programms über die Dropdown-Liste des Feldes **Beschreibung** auswählen.

- Geben Sie das Ausgangsverzeichnis des Programms in das Feld **Anfangsverzeichnis** ein.

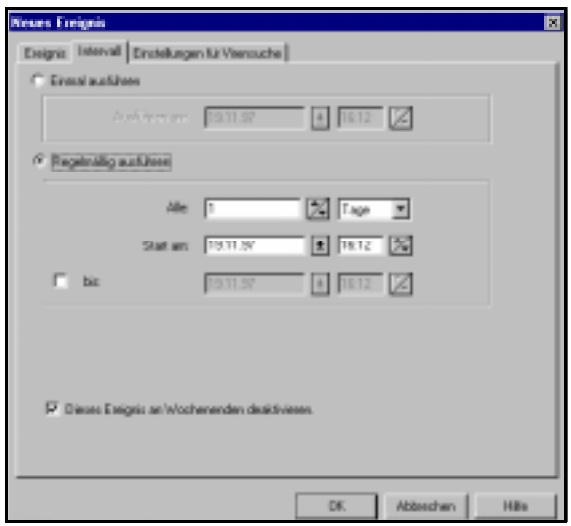
- Klicken Sie auf **OK**.

10. **Nur für Benutzer von Windows 3.x und Windows NT**: Wenn Sie **Nachricht senden** ausgewählt haben, geben Sie den Text der Nachricht in das Feld **Nachricht** und die Anmelde-ID des Zielbenutzers in das Feld **Senden an** ein. Klicken Sie auf **OK**. Den Text der Nachricht geben Sie im Dialogfeld **Vorgabeeinstellungen für Dr Solomon's Scheduler** ein (siehe Seite 145).

11. Wenn Sie die Konfiguration des Ereignisses abgeschlossen haben und möchten, daß der Zeitplaner ausgeführt wird, klicken Sie auf **OK**. Das Dialogfeld **Speichern** wird angezeigt. Wählen Sie die gewünschte Option, und klicken Sie auf **OK**.

Registerkarte „Intervall“

In Schritt 6 der Beschreibungen im Abschnitt „Erstellen neuer Ereignisse“ (siehe Seite 126) gehen Sie zu dieser Registerkarte. Fahren Sie mit Schritt 7 der Beschreibung fort, wenn Sie die Einstellungen festgelegt haben.



Erläuterungen zu den Elementen der Registerkarte **Intervall**:

- Das Format für Datum und Uhrzeit ist das in Windows festgelegte Format.

- Sie können kein Datum und keine Uhrzeit nach 23:59 Uhr am 31. Dezember 2038 wählen.

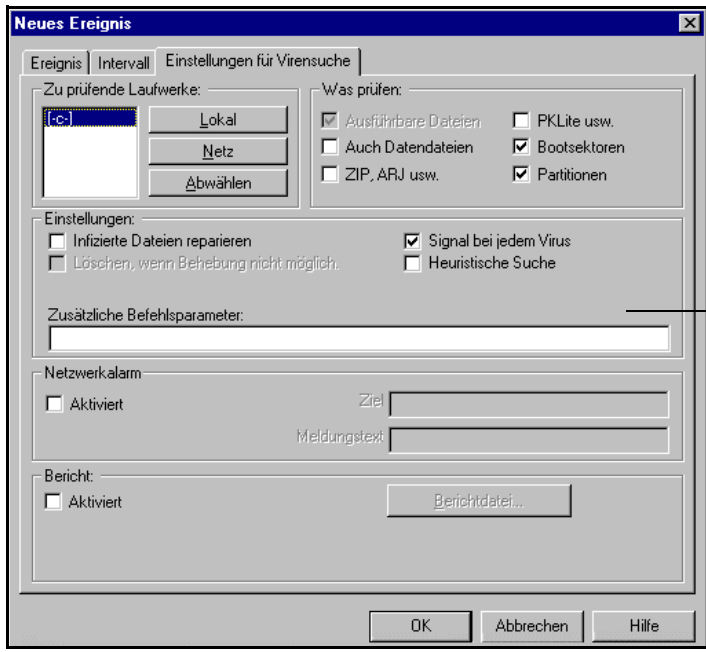
- Sie können kein Datum und keine Zeit aus der Vergangenheit wählen.
- Anmerkung für die Option **Dieses Ereignis an Wochenenden deaktivieren**: Wochenenden beginnen Freitags um Mitternacht und enden Sonntags um Mitternacht.
- Wenn Sie ein monatliches Intervall und als Startdatum den letzten Tag eines Monats wählen, werden Sie gefragt, ob das Ereignis am letzten Tag jedes Monats oder an dem tatsächlich angegebenen Tag ausgeführt werden soll.
- Sie können Datum und Uhrzeit jeweils direkt eingeben oder mit Hilfe der Pfeilschaltflächen einstellen.
- Um ein Datum einzugeben, klicken Sie auf den Pfeil nach unten neben dem Eingabefeld und wählen ein Datum aus dem daraufhin angezeigten Kalender aus.
- Die Einstellungen im Abschnitt **Regelmäßig ausführen** sind die auf der Registerkarte **Allgemein** des Dialogfelds **Vorgabeeinstellungen für Dr Solomon's Scheduler** festgelegten Einstellungen (siehe Schritte 4 bis 7 auf Seite 147). Sie sollten diese Funktion verwenden, wenn Sie häufig dieselben Einstellungen benutzen.

Registerkarte „Einstellungen für Virensuche“

In Schritt 7 der Beschreibungen im Abschnitt „Erstellen neuer Ereignisse“ (siehe Seite 126) gehen Sie zu dieser Registerkarte. Klicken Sie auf **OK**, wenn Sie die gewünschten Einstellungen festgelegt haben. Die Ereigniskonfiguration ist damit abgeschlossen.

Tip

Die Anfangseinstellungen auf dieser Registerkarte werden auf der Registerkarte **Einstellungen für Virensuche** des Dialogfelds **Vorgabeeinstellungen für Dr Solomon's Scheduler** festgelegt; siehe Schritt 9 auf Seite 147. Sie sollten diese Funktion verwenden, wenn Sie häufig dieselben Einstellungen benutzen.



Windows NT enthält eine weitere Option, **Bericht in NT-Ereignisprotokoll**: Aktivieren Sie diese Option, um dem NT-Ereignisprotokoll bei jeder Ausführung eines Ereignisses einen Eintrag hinzuzufügen.

Für FindVirus gibt es folgende Optionen und Einstellungen:

Funktion	Beschreibung
Zu prüfende Laufwerke:	Klicken Sie auf ein nicht markiertes Laufwerk, um es auszuwählen. Klicken Sie auf ein markiertes Laufwerk, um die Auswahl aufzuheben. Klicken Sie auf die Schaltfläche **Lokal**, um zusätzlich zu allen bereits ausgewählten Laufwerken alle lokalen Laufwerke zu markieren. Klicken Sie auf die Schaltfläche **Netz**, um zusätzlich zu allen bereits ausgewählten Laufwerken alle Netzlaufwerke zu markieren. UNC-Pfadnamen werden unterstützt.
Was prüfen:	
Ausführbare Dateien	Diese Option ist grau unterlegt, weil ausführbare Dateien immer überprüft werden. FindVirus verwendet die Erweiterung einer Datei, um sie zu identifizieren und so festzustellen, ob sie überprüft werden muß. Wenn Sie ausführbare Dateien mit nicht standardmäßigen Erweiterungen haben, sollten Sie **Alle Dateien** wählen.
Alle Dateien	Aktivieren Sie diese Option, um alle Dateien zu überprüfen, nicht nur solche mit der Erweiterung einer ausführbaren Datei. Dadurch wird die Sicherheit erhöht, aber auch die Überprüfungszeit verlängert. Sie sollten diese Option auf Quarantänecomputern aktivieren, wenn Sie nach einer Infektion das gesamte System säubern möchten, oder wenn Sie ausführbare Dateien mit nicht standardmäßigen Erweiterungen haben.

Funktion	Beschreibung
ZIP, ARJ usw.	Aktivieren Sie diese Option, damit komprimierte Dateien zeitweise entkomprimiert werden und die in ihnen enthaltenen Dateien überprüft werden können. Die Funktion kann für komprimierte Dateien in den folgenden Formaten angewendet werden: ARC, PKZip, PKLite, LZExe, ARJ, ICE, LZH, Diet (Version 1.0) und CryptCom-Dienstprogramme. Die komprimierten Mutterdateien selbst (z. B. Archivdateien mit der Erweiterung .ZIP) werden überprüft, wenn **Alle Dateien** aktiviert ist.
PKLite usw.	Aktivieren Sie diese Option, damit komprimierte Dateien zeitweise entkomprimiert werden und die in ihnen enthaltenen Dateien überprüft werden können. Die Funktion kann für komprimierte Dateien in den folgenden Formaten angewendet werden: PKLite, LZExe, ICE, Diet (Version 1.0) und CryptCom. Die komprimierten Mutterdateien selbst (z. B. Archivdateien mit der Erweiterung .ZIP) werden überprüft, wenn **Alle Dateien** aktiviert ist.
Bootsektoren	Sie sollten diese Option nur dann deaktivieren, wenn sie ein besonderes Problem verursacht, z. B. wenn Sie ein Netzlaufwerk überprüfen, das keinen Bootsektor hat.
Partitionen	Sie sollten diese Option nur dann deaktivieren, wenn sie ein besonderes Problem verursacht.

Funktion	Beschreibung
Einstellungen:	
Viren aus infizierten Dateien entfernen	Aktivieren Sie diese Option, damit Viren aus infizierten Dateien entfernt werden. Wenn nicht durch **Zusätzliche Befehlsparameter** anders angegeben, werden infizierte Dateien, aus denen der Virus nicht entfernt werden kann, umbenannt; der erste Buchstabe der Dateierweiterung wird zu „V“.
Löschen, wenn Viren-entfernung nicht möglich	Wenn diese Option ausgewählt ist und FindVirus den Virus nicht aus einer Datei entfernen kann, wird die Datei gelöscht.
Signal bei jedem Virus	Gibt bei jedem gefundenen Virus einen Signalton aus.
Heuristische Suche	Bei der heuristischen Analyse handelt es sich um eine Technik zur Identifizierung möglichen neuen Viruscodes (auch in Makros). Durch die Aktivierung dieser Option wird die Sicherheit erhöht, aber auch die Überprüfungszeit verlängert.
Zusätzliche Befehls-parameter	Sie können die Suche noch weiter anpassen, indem Sie FindVirus-Parameter in dieses Feld eingeben; weitere Informationen finden Sie unter dem Thema „FindVirus“ in der Online-Hilfe zum Toolkit. Die meisten der verfügbaren Parameter brauchen Sie nicht anzugeben, da es für sie Einstellungen auf der Registerkarte gibt, die Sie statt dessen verwenden. Für einige Parameter gibt es jedoch keine entsprechenden Optionen auf der Registerkarte. Wenn Sie ihre Funktionen benötigen, müssen Sie den entsprechenden Parameter angeben.

Funktion	Beschreibung
Netzwerkalarm:	
Aktiviert	Aktivieren Sie diese Option, damit im gesamten Netzwerk eine Viruswarnung ausgelöst wird.
Ziel	Gibt die Anmelde-ID des Zielbenutzers an.
Meldungstext	Gibt den Text der Netzwerkmeldung an.
Bericht:	
Aktiviert	Aktivieren Sie diese Option, wenn die Ergebnisse der Überprüfung zusätzlich zur Anzeige auf dem Bildschirm in eine ASCII-DAtei kopiert werden sollen. Der Name der Berichtdatei muß über die Schaltfläche **Berichtdatei** angegeben werden.
Berichtdatei	Durch Klicken auf diese Schaltfläche wird ein Dialogfeld geöffnet, in dem Sie eine bereits vorhandene Datei öffnen oder den Namen einer neuen Datei angeben können. Vorhandene Dateien werden überschrieben, neue Dateien erstellt. Das Kontrollkästchen **Aktiviert** muß markiert sein.

Hilfe

Wenn Sie eine Einstellung festlegen möchten, die im Dialogfeld **Viren suchen** oder **Viren suchen - Zusätzliche Einstellungen** ist, aber auf dieser Registerkarte nicht angezeigt wird, können Sie den entsprechenden Befehlsparameter für diese Einstellung im Feld **Zusätzliche Befehlsparameter** eingeben. Weitere Informationen finden Sie unter dem Thema „FindVirus“ in der Online-Hilfe zum Toolkit.

Warnung

Obwohl bei FindVirus-Überprüfungen zu festgelegten Zeiten Boot- und Partitionssektorviren auf Festplatten gefunden werden können, kann FindVirus diese Viren nicht automatisch entfernen. Wenn FindVirus bei einer Zeitplaner-Überprüfung einen Boot- oder Partitionssektorvirus feststellt, müssen Sie die Viren anschließend unter Verwendung der SOS-Diskette von dem entsprechenden Laufwerk entfernen. Informationen über die SOS-Diskette finden Sie im Abschnitt „SOS-Diskette“ auf Seite 1.

Wenn Sie mit Windows NT arbeiten und FindVirus einen Boot- oder Partitionssektorvirus auf einer Festplatte findet, sollten Sie sich an die technische Unterstützung von Dr Solomon’s wenden. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

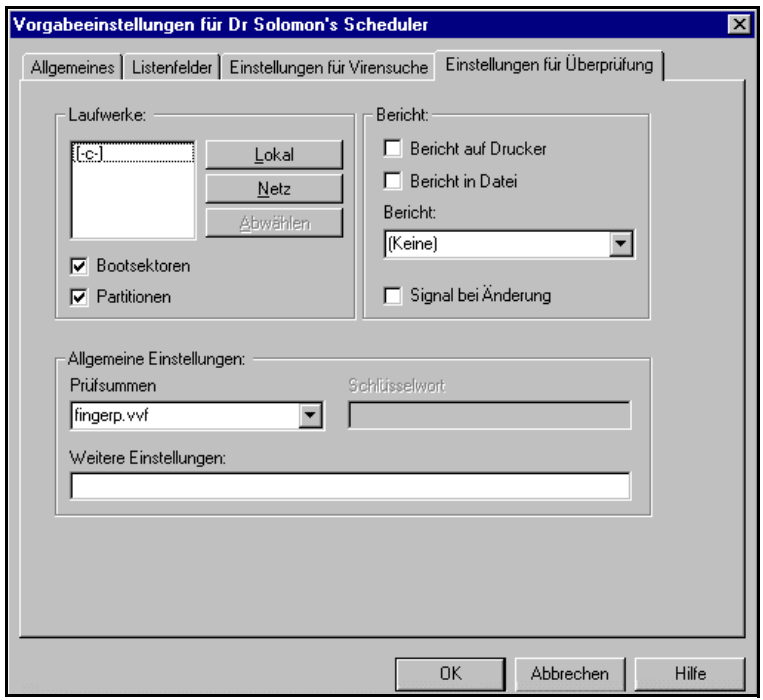
Registerkarte „Einstellungen für Überprüfung“

In Schritt 8 der Beschreibung im Abschnitt „Erstellen neuer Ereignisse“ (siehe Seite 126) gehen Sie zu dieser Registerkarte. Klicken Sie auf **OK**, wenn Sie die gewünschten Einstellungen festgelegt haben. Die Ereigniskonfiguration ist damit abgeschlossen.

Tip

Die Anfangseinstellungen auf dieser Registerkarte werden auf der Registerkarte **Einstellungen für Überprüfung** des Dialogfelds **Vorgabeeinstellungen für Dr Solomon’s Scheduler** festgelegt; siehe Schritt 10 auf Seite 148. Sie sollten diese Funktion verwenden, wenn Sie häufig dieselben Einstellungen benutzen.

Bei der Überprüfung wird nach Änderungen in den Prüfsummendateien gesucht, die bereits manuell erstellt wurden.



Für ViVerify gibt es folgende Optionen und Einstellungen:

Funktion	Beschreibung
Laufwerke:	Klicken Sie auf ein nicht markiertes Laufwerk, um es auszuwählen. Klicken Sie auf ein markiertes Laufwerk, um die Auswahl aufzuheben. Klicken Sie auf die Schaltfläche **Lokal**, um zusätzlich zu allen bereits ausgewählten Laufwerken alle lokalen Laufwerke zu markieren. Klicken Sie auf die Schaltfläche **Netz**, um zusätzlich zu allen bereits ausgewählten Laufwerken alle Netzlaufwerke zu markieren. UNC-Pfadnamen werden unterstützt.

Funktion	Beschreibung
Bootsektoren	Bootsektoren werden überprüft.
Partitionen	Partitionssektoren werden überprüft.
Bericht:	
Bericht auf Drucker	Aktivieren Sie diese Option, wenn die Ergebnisse der Überprüfung zusätzlich zur Anzeige auf dem Bildschirm auch auf dem Standarddrucker ausgegeben werden sollen.
Bericht in Datei	Aktivieren Sie diese Option, wenn die Ergebnisse der Überprüfung zusätzlich zur Anzeige auf dem Bildschirm auch in eine ASCII-Datei kopiert werden sollen. Der Vorgabename der Berichtdatei ist VIVERIFY.REP im Toolkit-Verzeichnis; über das Eingabefeld **Bericht** können Sie den Namen ändern.
Bericht:	Über dieses Eingabefeld können Sie eine andere Berichtdatei festlegen, indem Sie einen neuen Pfad und / oder Dateinamen eingeben, oder indem Sie eine Datei aus der Dropdown-Liste auswählen. Die Liste enthält die letzten vorgenommenen Einträge.
Signal bei Änderung	Es wird jedesmal ein Signalton ausgegeben, wenn eine Änderung festgestellt wird.

Funktion	Beschreibung
Allgemeine Einstellungen:	
Prüfsummen	In diesem Feld geben Sie die Prüfsummendatei an, indem Sie einen neuen Pfad und / oder Dateinamen eingeben, oder indem Sie eine Datei aus der Dropdown-Liste auswählen. Die Liste enthält die letzten vorgenommenen Einträge. Nur solche Dateien, für die ein Eintrag in der Prüfsummendatei besteht, können auf Änderungen geprüft werden. Jede Datei, die ViVerify zu überprüfen versucht, aber keinen Eintrag hat, wird als „neue“ Datei gemeldet. Sie können dies umgehen, indem Sie bei der Überprüfung auf Änderungen mit einer bestimmten Laufwerksauswahl die Prüfsummendatei verwenden, die mit derselben Laufwerkskombination erstellt wurde.
Schlüsselwort	Prüfsummendateien werden unter Verwendung des von Ihnen eingegebenen Schlüsselworts verschlüsselt, um sie vor Virenbefall zu schützen. Geben Sie das bei der Berechnung der Prüfsummendatei verwendete Schlüsselwort ein.

Funktion	Beschreibung
Weitere Einstellungen	Sie können die Suche noch weiter anpassen, indem Sie ViVerify-Parameter in dieses Feld eingeben; weitere Informationen finden Sie unter dem Thema „ViVerify“ in der Online-Hilfe zum Toolkit. Die meisten der verfügbaren Parameter brauchen Sie nicht anzugeben, da es für sie Einstellungen auf der Registerkarte gibt, die Sie statt dessen verwenden. Für einige Parameter gibt es jedoch keine entsprechenden Optionen auf der Registerkarte. Wenn Sie ihre Funktionen benötigen, müssen Sie den entsprechenden Parameter angeben.

Tip

Die meisten dieser Optionen werden auch im Dialogfeld **Änderungen prüfen** (siehe Seite 88) oder **Änderungen prüfen - Zusätzliche Einstellungen** (siehe Seite 89) der Toolkit-Benutzeroberfläche angezeigt. Wenn Sie eine Einstellung festlegen möchten, die in einem dieser Dialogfelder ist, aber auf dieser Registerkarte nicht angezeigt wird, können Sie den entsprechenden Befehlsparameter für diese Einstellung im Feld **Weitere Einstellungen** angeben.

5.2 Ausführung des Zeitplaners

Wenn Sie regelmäßige Ereignisse eingerichtet haben, müssen Sie darauf achten, daß der Zeitplaner läuft. Wenn dies der Fall ist, wird sein Symbol angezeigt.

Wenn Sie während der Installation festgelegt haben, daß der Zeitplaner nicht aktiviert sein soll, können Sie ihn später aktivieren.

Für Benutzer von Windows 3.x:

1. Klicken Sie in der Programmgruppe **Anti-Virus Toolkit** auf das Symbol des Zeitplaners, und halten Sie die Maustaste gedrückt.

2. Ziehen Sie den Zeitplaner in die Programmgruppe **Autostart**.

3. Starten Sie Windows neu. Der Zeitplaner ist jetzt aktiviert, und das Symbol wird am unteren Rand des Bildschirms angezeigt.

Für Benutzer von Windows 95:

Falls der Zeitplaner nicht läuft, starten Sie ihn von der Programmgruppe **Dr Solomon's AVTK** im Startmenü aus.

Für Benutzer von Windows NT:

1. Klicken Sie auf **Start**, und wählen Sie **Einstellungen** und anschließend **Systemsteuerung**.

2. Doppelklicken Sie in der Systemsteuerung auf das Symbol **Dienste**.

3. Blättern Sie in dem angezeigten Dialogfeld durch die Liste der Dienste, und wählen Sie **Dr Solomon's Scheduler**. Klicken Sie auf **Start**.

Konfiguration des Zeitplaner-Dienstes in Windows NT

Möglicherweise möchten Sie das Konto ändern, das der Zeitplaner-Dienst für die Anmeldung verwendet. Vorgabemäßig wird das Konto **System** verwendet.

Tip Sie sollten ein Konto nur für den Zeitplaner einrichten.

Sie können mit Hilfe des Zeitplaners FindVirus-Überprüfungen festlegen, bei denen gemeinsame benutzte Netzlaufwerke durchsucht oder Berichte auf andere gemeinsam benutzte Computer im Netzwerk kopiert werden. In diesem Fall müssen Sie darauf achten, daß sich der Zeitplaner-Dienst mit einem Konto anmeldet, das die entsprechenden Rechte für die gemeinsam benutzten Computer hat.

Damit bei FindVirus-Überprüfungen per Zeitplaner andere im Netzwerk gemeinsam benutzte Computer durchsucht werden können, muß sich der Zeitplaner-Dienst über ein Konto anmelden, das Lesezugriff auf die gemeinsam benutzten Computer hat.

Damit bei FindVirus-Überprüfungen per Zeitplaner Berichte auf andere im Netzwerk gemeinsam benutzte Computer kopiert werden können, muß sich der Zeitplaner-Dienst über ein Konto anmelden, das Schreibzugriff auf die gemeinsam benutzten Computer hat.

5.3 Ereignisverwaltung

Bearbeiten von Ereignissen

So bearbeiten Sie ein bestehendes Ereignis:

1. Rufen Sie den Zeitplan-Editor auf.
2. Markieren Sie das zu bearbeitende Ereignis, und wählen Sie **Ereignis bearbeiten** aus dem Menü **Bearbeiten**. Sie können auch auf das Ereignis doppelklicken.

   Das Dialogfeld **Ereignis bearbeiten** wird angezeigt. Dieses Dialogfeld ist identisch mit dem Dialogfeld **Neues Ereignis**. Der einzige Unterschied besteht darin, daß es mit den zuletzt für das zu bearbeitende Ereignis gespeicherten Einstellungen angezeigt wird und nicht wie durch das Dialogfeld **Vorgabeeinstellungen** festgelegt.
3. Wiederholen Sie die im Abschnitt „Erstellen neuer Ereignisse“ auf Seite 124 aufgeführten Schritte, und ändern Sie die bestehenden Einstellungen nach Ihren Wünschen. Klicken Sie auf **OK**, wenn Sie die Eingabe der Änderungen abgeschlossen haben.
4. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.
5. Klicken Sie auf **OK**.

Löschen von Ereignissen

1. Rufen Sie den Zeitplan-Editor auf.
2. Markieren Sie das gewünschte Ereignis.
3. Klicken Sie auf das Symbol **Ereignis löschen**, oder wählen Sie **Ereignis löschen** aus dem Menü **Bearbeiten**.
4. Klicken Sie auf **Ja**.
5. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.
6. Klicken Sie auf **OK**.

Deaktivieren von Ereignissen

Ereignisse sind vorgabemäßig aktiviert. Dies wird durch ein Symbol in der Spalte **Aktiviert** angezeigt.

1. Rufen Sie den Zeitplan-Editor auf.
2. Markieren Sie das gewünschte Ereignis.
3. Klicken Sie auf das Symbol **Ereignis deaktivieren**, oder wählen Sie **Ereignis deaktivieren** aus dem Menü **Bearbeiten**.
4. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.
5. Klicken Sie auf **OK**.

Aktivieren von Ereignissen

Ein aktiviertes Ereignis wird durch ein Symbol in der Spalte **Aktiviert** angezeigt.

1. Rufen Sie den Zeitplan-Editor auf.
2. Markieren Sie das gewünschte Ereignis.
3. Klicken Sie auf das Symbol **Ereignis aktivieren**, oder wählen Sie **Ereignis aktivieren** aus dem Menü **Bearbeiten**.

4. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.

5. Klicken Sie auf **OK**.

Ausschneiden und Einfügen von Ereignissen

Wenn Sie ein Ereignis ausschneiden, wird das ursprüngliche Ereignis aus dem Dialogfeld Zeitplan-Editor entfernt, aber seine Einstellungen können in ein neues Ereignis eingefügt werden.

1. Rufen Sie den Zeitplan-Editor auf.

2. Markieren Sie das gewünschte Ereignis.

3. Klicken Sie auf das Symbol **Ausschneiden**, oder wählen Sie **Ausschneiden** aus dem Menü **Bearbeiten**.

4. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf das Symbol **Einfügen**, oder wählen Sie **Einfügen** aus dem Menü **Bearbeiten**.

7. Machen Sie die entsprechenden Angaben, und klicken Sie auf **OK**.

8. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.

9. Klicken Sie auf **OK**.

Kopieren und Einfügen von Ereignissen

Wenn Sie ein Ereignis kopieren, bleibt das ursprüngliche Ereignis unangetastet, aber die Einstellungen können in ein neues Ereignis eingefügt werden. Wenn ein Ereignis kopiert worden ist, muß es einen neuen Namen erhalten.

1. Rufen Sie den Zeitplan-Editor auf.
2. Markieren Sie das gewünschte Ereignis.
3. Klicken Sie auf das Symbol **Kopieren**, oder wählen Sie **Kopieren** aus dem Menü **Bearbeiten**.
4. Klicken Sie auf das Symbol **Einfügen**, oder wählen Sie **Einfügen** aus dem Menü **Bearbeiten**.

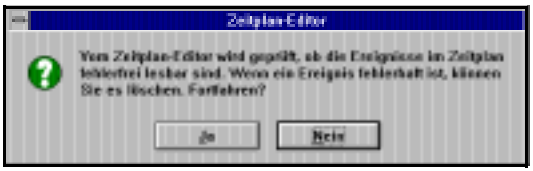
5. Machen Sie die entsprechenden Angaben, und klicken Sie auf **OK**.
6. Wählen Sie die gewünschte Option im Dialogfeld **Speichern**.
7. Klicken Sie auf **OK**.

Gültigkeitsprüfung von Ereignissen (nur für Windows 3.x verfügbar)

Sie können die Gültigkeit von Ereignissen prüfen. Ereignisse, bei denen Dateien beschädigt worden sind, werden gelöscht.

1. Rufen Sie den Zeitplan-Editor auf.

2. Wählen Sie **Zeitplan prüfen** aus dem Menü **Datei**.



3. Wählen Sie **Ja**. Wenn keine fehlerhaften Ereignisse vorhanden sind, wird eine Meldung angezeigt, daß die Gültigkeitsprüfung abgeschlossen ist.

4. Klicken Sie auf **OK**.

Falls Ereignisse fehlerhaft sind, werden sie gelöscht.

5.4 Protokolldatei des Zeitplaners

In der Protokolldatei des Zeitplaners können Einzelheiten über die Auslösung von Ereignissen aufgezeichnet werden, unter anderem die festgesetzte Uhrzeit und das festgelegte Datum für das Ereignis und ob die Auslösung erfolgreich war.

Weitere Informationen über die Einstellungen für das Schreiben in die Protokolldatei des Zeitplaners finden Sie in Schritt 5 auf Seite 125.

Ansicht der Protokolldatei

1. Rufen Sie den Zeitplan-Editor auf.
2. Wählen Sie **Protokolldatei des Zeitplaners** aus dem Menü **Datei**.
3. Wählen Sie **Anzeigen**.

   Die Protokolldatei wird im Windows-Editor geöffnet.

Umbenennen der Protokolldatei

Der Vorgabename für die Protokolldatei ist TK_SCHED.LOG im Toolkit-Verzeichnis. So ändern Sie den Namen:

1. Rufen Sie den Zeitplan-Editor auf.
2. Wählen Sie **Protokolldatei des Zeitplaners** aus dem Menü **Datei** und anschließend **Namen ändern**.

   Das Dialogfeld **Protokolldatei des Zeitplaners umbenennen** wird angezeigt.
3. In diesem Dialogfeld können Sie eine neue Datei erstellen oder eine bereits bestehende Datei auswählen, um sie zu überschreiben.

5.5 Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“

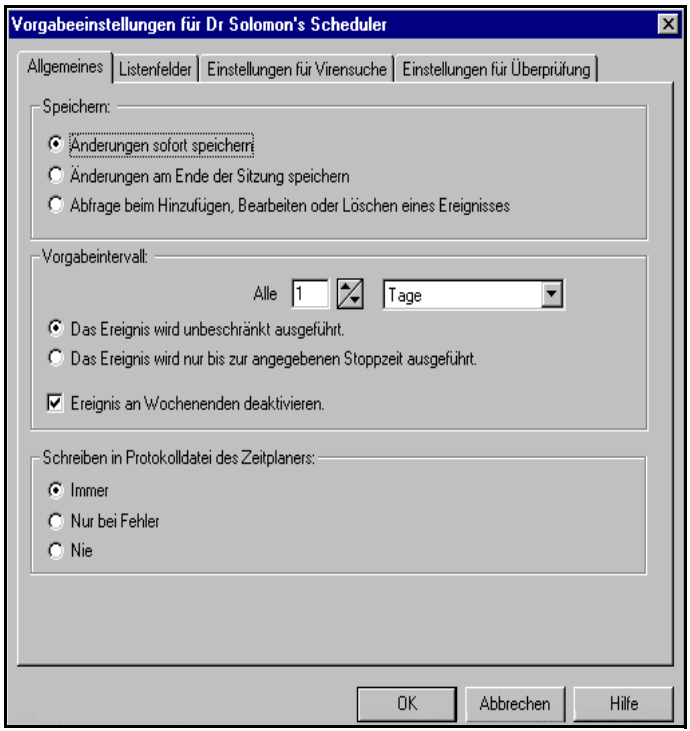
Die Anfangseinstellungen für die Registerkarten **Intervall**, **Einstellungen für Virensuche** und **Einstellungen für Überprüfung** des Dialogfelds **Neues Ereignis** werden durch die im Dialogfeld **Vorgabeeinstellungen für Dr Solomon's Scheduler** festgelegten Optionen bestimmt.

In diesem Dialogfeld legen Sie die Optionen für das Speichern von Ereignisdaten fest und erstellen Auswahloptionen für einige der Dropdown-Menüs im Dialogfeld **Neues Ereignis**.

So legen Sie die Einstellungen im Dialogfeld „Vorgabeeinstellungen für Dr Solomon's Scheduler“ fest:

1. Rufen Sie den Zeitplan-Editor auf.
2. Wählen Sie **Vorgabeeinstellungen** aus dem Menü **Einstellungen**.

   Das Dialogfeld **Vorgabeeinstellungen für Dr Solomon's Scheduler** wird angezeigt. Das Dialogfeld hat mehrere Registerkarten; anfangs wird die Registerkarte **Allgemein** angezeigt.



Tip

Wenn Sie keine weiteren Änderungen vornehmen möchten, können Sie jederzeit auf **OK** klicken, um das Dialogfeld zu schließen.

3. Markieren Sie eins der drei runden Optionsfelder im Abschnitt **Speichern**. Folgende Optionen stehen zur Verfügung:

- **Änderungen sofort speichern**: Alle vorgenommenen Änderungen werden direkt auf der Festplatte gespeichert und daher sofort wirksam. Wenn Sie ein Ereignis beispielsweise so konfigurieren, daß es in 5 Minuten ausgelöst werden soll, wird es unabhängig davon, ob der Zeitplan-Editor noch ausgeführt wird, an dem festgelegten Zeitpunkt ausgelöst.

- **Änderungen am Ende der Sitzung speichern**: Alle vorgenommenen Änderungen werden erst beim Beenden des Zeitplan-Editors auf der Festplatte gespeichert und auch erst dann wirksam.

- **Abfrage beim Hinzufügen, Bearbeiten oder Löschen eines Ereignisses**: Jedes Mal, wenn Sie eine Änderung vornehmen, werden Sie in einem Dialogfeld gefragt, ob Sie die Änderungen sofort übernehmen möchten (dies entspricht der Option **Änderungen sofort speichern**) oder erst später (dies entspricht der Option **Änderungen am Ende der Sitzung speichern**). Außerdem können Sie in diesem Dialogfeld das Kontrollkästchen **Getroffene Auswahl beibehalten - dieses Feld nicht wieder anzeigen** aktivieren.

4. Bearbeiten Sie das Vorgabeintervall so, daß die gewünschte Einstellung angezeigt wird, wenn Sie die Registerkarte **Intervall** des Dialogfelds **Neues Ereignis** aufrufen (siehe Schritt 6 auf Seite 126).

5. Aktivieren Sie das runde Optionsfeld **Das Ereignis wird unbeschränkt ausgeführt**, wenn beim ersten Aufrufen der Registerkarte **Intervall** des Dialogfelds **Neues Ereignis** die Felder in der Zeile **bis:** deaktiviert, d. h. grau unterlegt sein sollen.

6. Aktivieren Sie das runde Optionsfeld **Das Ereignis wird nur bis zur angegebenen Stoppzeit ausgeführt**, wenn beim ersten Aufrufen der Registerkarte **Intervall** des Dialogfelds **Neues Ereignis** die Felder in der Zeile **bis:** aktiviert sein sollen.

7. Legen Sie fest, ob beim Aufrufen des Dialogfelds **Neues Ereignis** die Option **Ereignis an Wochenenden deaktivieren** markiert sein soll.

8. Markieren Sie im Abschnitt **Schreiben in Protokolldatei des Zeitplaners** das runde Optionsfeld, das beim Aufrufen des Dialogfelds **Neues Ereignis** aktiviert sein soll.

9. Gehen Sie zur Registerkarte **Einstellungen für Virensuche**. Bearbeiten Sie die Einstellungen so, daß auf der gleichen Registerkarte beim ersten Aufrufen des Dialogfelds **Neues Ereignis** die gewünschten Einstellungen angezeigt werden (siehe Seite 128).

10. Gehen Sie zur Registerkarte **Einstellungen für Überprüfung**. Bearbeiten Sie die Einstellungen so, daß auf der gleichen Registerkarte beim ersten Aufrufen des Dialogfelds **Neues Ereignis** die gewünschten Einstellungen angezeigt werden (siehe Seite 134).

11. Gehen Sie zur Registerkarte **Listenfelder**.

12. Auf dieser Registerkarte können Sie Programme festlegen, die ausgeführt werden, wenn **Anwendung ausführen** ausgewählt ist. In Windows 3.x und Windows NT können Sie in das **Nachrichten-Listenfeld** auch Meldungen eingeben, die angezeigt werden, wenn **Nachricht senden** ausgewählt ist. Dieser Bereich wird auf der Registerkarte **Ereignis** in den Dialogfeldern **Neues Ereignis** (siehe Schritt 9 auf Seite 126) und **Ereignis bearbeiten** angezeigt, wenn **Anwendung ausführen** oder **Nachricht senden** ausgewählt ist.

    Klicken Sie im **Programm-Listenfeld** auf die Schaltfläche **Neu**, oder wählen Sie eine Beschreibung aus, und klicken Sie auf **Bearbeiten**. Das Dialogfeld **Programmangaben** wird angezeigt. In diesem Dialogfeld legen Sie die Angaben fest, die im Bereich **Programm** der Dialogfelder **Neues Ereignis** und **Ereignis bearbeiten** angezeigt werden, wenn Sie die Beschreibung eines Programms aus der Dropdown-Liste auswählen. Machen Sie in diesem Dialogfeld die gewünschten Angaben. Um ein Programm zu entfernen, markieren Sie es und klicken auf die Schaltfläche **Entfernen**.

Tip

Für Benutzer von Windows NT: Nur Administratoren haben Zugriff auf das **Programm-Listenfeld**.

Für Benutzer von Windows 3.x und Windows NT: Klicken Sie im **Nachrichten-Listenfeld** auf die Schaltfläche **Neu**, oder wählen Sie eine Meldung aus, und klicken Sie auf **Bearbeiten**. Das Dialogfeld **Nachricht** wird angezeigt. In diesem Dialogfeld können Sie Meldungen erstellen, die in der Dropdown-Liste angezeigt werden. Machen Sie in diesem Dialogfeld die gewünschten Angaben. Um eine Meldung zu entfernen, markieren Sie sie und klicken auf die Schaltfläche **Entfernen**.

5.6 Allgemeine Umgebungseinstellungen

Folgende Einstellungen sind verfügbar, um die Umgebung des Zeitplan-Editors zu ändern:

Elemente im Menü „Einstellungen“	Funktion
Schriftart	Öffnet ein Dialogfeld, in dem Sie die Anzeigeschriftart für den Zeitplan-Editor auswählen können.
Symbolleiste anzeigen	Aktiviert bzw. deaktiviert die Anzeige der Symbolleiste (siehe Seite 124).
Statusleiste anzeigen	Aktiviert bzw. deaktiviert die Anzeige der Statusleiste.
Hinweise aktivieren	Aktiviert bzw. deaktiviert die Anzeige der Hinweise (siehe Seite 124).

6. Entfernung von Viren

6.1 Entfernung von Viren aus Laufwerken

Am schnellsten entfernen Sie Viren mit Hilfe des Toolkit-Hauptbildschirms, unter Verwendung der Anfangseinstellungen oder der Einstellungen, die Sie zuletzt über das Menü **Entfernen** (und das Menü **Prüfen**) vorgenommen haben:

1. Wählen Sie die Laufwerke, von denen Viren entfernt werden sollen, im Feld **Laufwerke** aus.

2. Klicken Sie auf die Schaltfläche **Entfernen**. (**OS/2-Benutzer:** Klicken Sie auf die Schaltfläche **Reparieren**.)

3. Ein Dialogfeld wird aufgerufen, in dem zunächst der Fortschritt und anschließend die Ergebnisse der Entfernung angezeigt werden. Durch Klicken auf **Beenden** können Sie die Entfernung jederzeit abbrechen. Der Toolkit-Hauptbildschirm wird wieder angezeigt.

4. Sehen Sie sich nach Abschluß der Entfernung die Ergebnisse an, und klicken Sie dann auf **Beenden**, um zum Toolkit-Hauptbildschirm zurückzukehren.

Warnung

Für Benutzer von Windows NT: Wenn Ihr Benutzername (d. h. der Name, mit dem Sie sich angemeldet haben) nicht in der Administratorgruppe zu finden ist, kann FindVirus nicht auf den Partitionssektor und den Bootsektor des Laufwerks zugreifen. In diesem Fall werden die Meldungen „Partitionssektor kann nicht gelesen werden“ und „Bootsektor kann nicht gelesen werden“ angezeigt. Wenden Sie sich an den Systemadministrator, wenn Sie Viren aus diesen Sektoren entfernen müssen.

Sie können Viren mit Hilfe des Menüs **Entfernen** aus Dateien, Bootsektoren und Partitionssektoren entfernen. Das Menü bietet Optionen zur Änderung der Funktionsweise einer Überprüfung, bei der Viren entfernt werden.

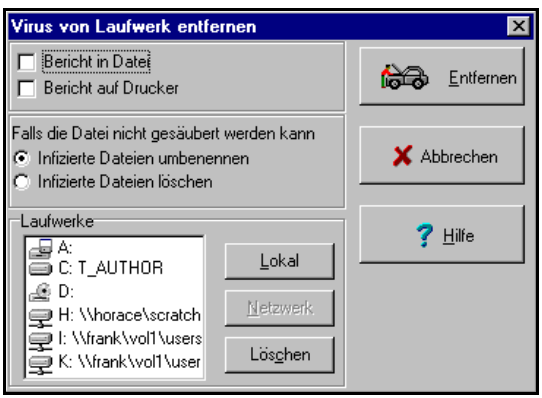
So ändern Sie die Einstellungen und entfernen Viren von Laufwerken:

1. Wählen Sie **Virus von Laufwerk entfernen** aus dem Menü **Entfernen**. Das Dialogfeld **Virus von Laufwerk entfernen** wird angezeigt.

Tip

Für OS/2Benutzer: Wählen Sie **Laufwerk reparieren** aus dem Menü **Reparieren**. Das Dialogfeld **Laufwerk reparieren** wird angezeigt.

.



2. Wählen Sie die Laufwerke, von denen Viren entfernt werden sollen, im Feld **Laufwerke** aus.

3. Sie können jetzt mit der Entfernung beginnen; Fahren Sie mit Schritt 8 fort. Wenn Sie noch weitere Optionen festlegen möchten, fahren Sie mit dem nächsten Schritt fort.

4. Wählen Sie **Bericht in Datei**, wenn die Ergebnisse der Entfernung zusätzlich zur Anzeige auf dem Bildschirm auch in eine ASCII-Datei kopiert werden sollen. Die Datei erhält den Namen FINDVIRU.REP und wird im Toolkit-Verzeichnis erstellt.

5. Wählen Sie **Bericht auf Drucker**, wenn die Ergebnisse der Entfernung zusätzlich zur Anzeige auf dem Bildschirm auch ausgedruckt werden sollen.

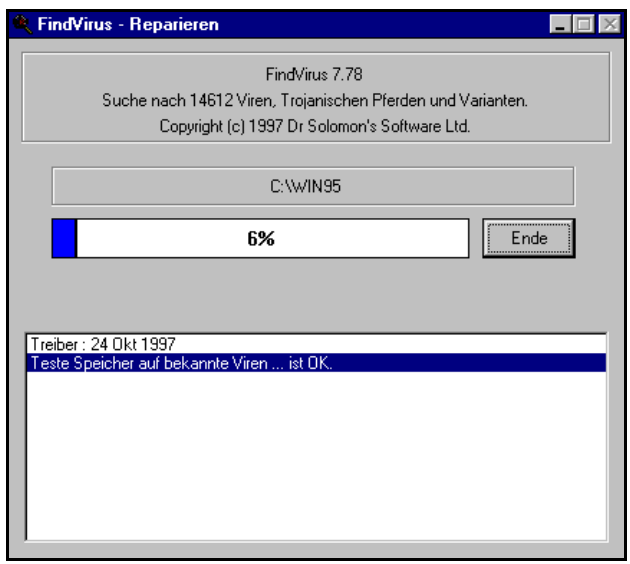
6. Wählen Sie **Infizierte Dateien umbenennen**, wenn Dateien, aus denen Viren nicht entfernt werden können, umbenannt anstatt gelöscht werden sollen. Wenn diese Option ausgewählt ist, wird der erste Buchstabe der Erweiterung einer infizierten Datei zu „V“. Beispiel: FORMAT.COM wird geändert zu FORMAT.VOM.

7. Wählen Sie **Infizierte Dateien löschen**, wenn infizierte Dateien, aus denen Viren nicht entfernt werden können, gelöscht anstatt umbenannt werden sollen.

8. Klicken Sie auf **Entfernen**.

Tip **Für OS/2-Benutzer:** Klicken Sie auf **Reparieren**.

Ein Dialogfeld wird angezeigt, in dem zunächst der Fortschritt und anschließend die Ergebnisse der Entfernung angezeigt werden.



Durch Klicken auf **Beenden** können Sie die Entfernung jederzeit abbrechen. Der Toolkit-Hauptbildschirm wird wieder angezeigt.

9. Sehen Sie sich nach Abschluß der Entfernung die Ergebnisse an, und klicken Sie dann auf **Beenden**, um zum Toolkit-Hauptbildschirm zurückzukehren.

Warnung

Für Benutzer von Windows NT: Wenn Ihr Benutzername (d. h. der Name, mit dem Sie sich angemeldet haben) nicht in der Administratorgruppe zu finden ist, kann FindVirus nicht auf den Partitionssektor und den Bootsektor des Laufwerks zugreifen. In diesem Fall werden die Meldungen „Partitionssektor kann nicht gelesen werden“ und „Bootsektor kann nicht gelesen werden“ angezeigt. Wenden Sie sich an den Systemadministrator, wenn Sie Viren aus diesen Sektoren entfernen müssen.

6.2 Ersetzen von Bootsektoren

Tip

Diese Option steht für das OS/2-Toolkit nicht zur Verfügung. Wenden Sie sich an die technische Unterstützung von Dr Solomon’s, wenn Sie mit OS/2 arbeiten und einen Boot- oder Partitionssektor finden. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

So ersetzen Sie den Bootsektor einer Diskette:

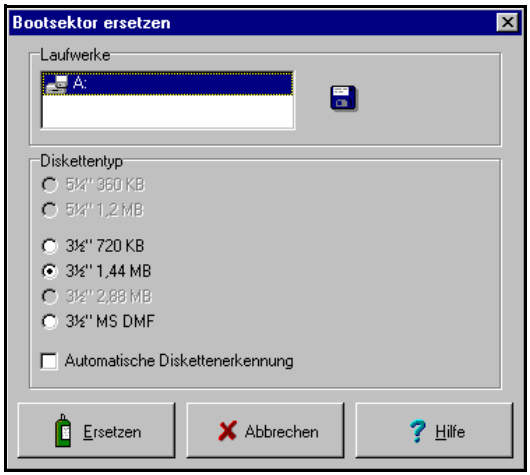
Tip

Viren müssen aus Bootsektoren von Festplatten (anders als bei Bootsektoren von Disketten) in Computern, auf denen Windows 3.x, Windows 95 oder DOS ausgeführt wird, mit Hilfe der SOS-Diskette entfernt werden. Informationen über die Verwendung der SOS-Diskette finden Sie im Abschnitt „SOS-Diskette“ auf Seite 1.

Wenn Sie mit Windows NT arbeiten und einen Boot- oder Partitionssektorvirus auf der Festplatte finden, wenden Sie sich an die technische Unterstützung von Dr Solomon’s. Adressen und Telefon- und Faxnummern von Dr Solomon’s Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

1. Wählen Sie **Bootsektor ersetzen** aus dem Menü **Entfernen**.

   Das Dialogfeld **Bootsektor ersetzen** wird angezeigt.



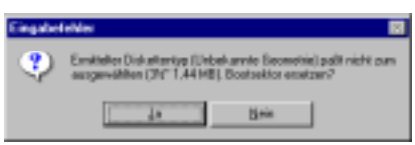
2. Wählen Sie den Laufwerksbuchstaben aus.

3. Aktivieren Sie das Kontrollkästchen **Automatische Diskettenerkennung**, wenn Sie eine Diskette säubern möchten, ohne den Diskettentyp auswählen zu müssen. Der Diskettentyp wird vor der Entfernung von Viren automatisch ausgewählt.

4. Klicken Sie auf **Ersetzen**.

5. Ein Dialogfeld mit der Meldung, daß der Virus erfolgreich entfernt wurde, wird angezeigt. Klicken Sie auf **OK**.

6. Wenn Sie **Automatische Diskettenerkennung** nicht aktiviert haben, müssen Sie einen Diskettentyp aus der Liste auswählen. Wenn Sie den falschen Diskettentyp gewählt haben, wird folgendes Dialogfeld angezeigt:



Wählen Sie nur dann **Ja**, wenn Sie sicher sind, daß Sie den Bootsektor durch den gewählten Diskettentyp ersetzen möchten. Klicken Sie auf **Nein**, wenn Sie nicht sicher sind. Wenn Sie auf **Nein** klicken, kehren Sie zurück zum Dialogfeld **Bootsektor ersetzen**. Aktivieren Sie in diesem Dialogfeld das Kontrollkästchen **Automatische Diskettenerkennung**, und klicken Sie dann auf **Ersetzen**.

7. Falls Sie im vorigen Schritt **Ja** gewählt haben und nach dem Ersetzen des Bootsektors nicht auf die Diskette zugreifen können:

Warnung

Schreiben Sie nicht auf die Diskette. Das Schreiben auf eine Diskette mit einem falschen Bootsektor kann Datenverluste zur Folge haben.

Wählen Sie **Bootsektor ersetzen** aus dem Menü **Entfernen**. Aktivieren Sie **Automatische Diskettenerkennung** im Dialogfeld **Bootsektor ersetzen**, und klicken Sie auf **Ersetzen**. Dadurch wird der richtige Bootsektor auf die Diskette geschrieben, und Sie können wie gewohnt auf die Diskette zugreifen.

Eine Meldung, daß der Bootsektor nicht geschrieben werden kann, bedeutet möglicherweise, daß die Diskette schreibgeschützt ist.

7. Online-Dokumentation

Tip

Die Informationen in diesem Kapitel gelten nur für Benutzer von Windows 3.x, Windows 95, Windows NT und OS/2 mit Dr Solomon's Anti-Virus Toolkit für Workstation auf CD-ROM.

Sie können auf das Handbuch „Dr Solomon's Anti-Virus Toolkit für Workstation" auf der Toolkit-CD zugreifen. Für die Anzeige des Handbuchs benötigen Sie einen PDF-Viewer. Wenn Sie noch keinen PDF-Viewer haben, können Sie Adobe Acrobat Reader von der Toolkit-CD installieren.

7.1 Windows 3.x

Tip

Sie können Adobe Acrobat Reader installieren und gleichzeitig das Handbuch kopieren. Anleitungen dazu finden Sie im Abschnitt „Gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs“ auf Seite 168.

Installation von Adobe Acrobat Reader

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.

2. Wählen Sie **Ausführen** aus dem Menü **Datei**.

3. Geben Sie in das angezeigte Eingabefeld den Laufwerksbuchstaben des CD-ROM-Laufwerks ein. Geben Sie dann

   ```
   \SETUP
   ```

   ein, und klicken Sie auf **OK**. Beispiel:

   ```
   D:\SETUP
   ```

4. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

5. Wählen Sie im nächsten Dialogfeld **Adobe Acrobat Reader installieren**.

   Wenn Sie Adobe Acrobat Reader in einer anderen Sprache installieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für Adobe Acrobat Reader aus, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Adobe Acrobat Reader installieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

6. Im folgenden Dialogfeld wird bestätigt, daß Sie Adobe Acrobat Reader installieren möchten. Klicken Sie auf **Installieren**.

7. Folgen Sie den angezeigten Anweisungen.

Kopieren des Handbuchs

1. Starten Sie den Computer, und rufen Sie Windows 3.x auf. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 3.x angezeigt wird.

2. Wählen Sie **Ausführen** aus dem Menü **Datei**.

3. Geben Sie in das angezeigte Eingabefeld den Laufwerksbuchstaben des CD-ROM-Laufwerks ein. Geben Sie dann

   ```
   \SETUP
   ```

   ein, und klicken Sie auf **OK**. Beispiel:

   ```
   D:\SETUP
   ```

4. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

5. Wählen Sie im nächsten Dialogfeld **Handbuch kopieren**. Wählen Sie ein Laufwerk und ein Verzeichnis für das Handbuch aus, indem Sie den Pfad im Eingabefeld am oberen Rand des Dialogfelds angeben. Sie können Laufwerk und Verzeichnis auch über die Schaltfläche **Durchsuchen** angeben, oder indem Sie den Pfad direkt in das Eingabefeld eingeben.

6. Wenn Sie ein Handbuch in einer anderen Sprache kopieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für das zu kopierende Handbuch, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Handbuch kopieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

7. Im folgenden Dialogfeld wird bestätigt, daß Sie das Handbuch kopieren möchten. Klicken Sie auf **Kopieren**.

8. Folgen Sie den angezeigten Anweisungen.

7.2 Windows 95

Tip

Sie können Adobe Acrobat Reader installieren und gleichzeitig das Handbuch kopieren. Anleitungen dazu finden Sie im Abschnitt „Gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs“ auf Seite 168.

Installation von Adobe Acrobat Reader

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.

2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

3. Wählen Sie im nächsten Dialogfeld **Adobe Acrobat Reader installieren**.

   Wenn Sie Adobe Acrobat Reader in einer anderen Sprache installieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für Adobe Acrobat Reader aus, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Adobe Acrobat Reader installieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

4. Im folgenden Dialogfeld wird bestätigt, daß Sie Adobe Acrobat Reader installieren möchten. Klicken Sie auf **Installieren**.

5. Folgen Sie den angezeigten Anweisungen.

Kopieren des Handbuchs

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop von Windows 95 angezeigt wird.

2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

3. Wählen Sie im nächsten Dialogfeld **Handbuch kopieren**. Wählen Sie ein Laufwerk und ein Verzeichnis für das Handbuch aus, indem Sie den Pfad im Eingabefeld am oberen Rand des Dialogfelds angeben. Sie können Laufwerk und Verzeichnis auch über die Schaltfläche **Durchsuchen** angeben, oder indem Sie den Pfad direkt in das Eingabefeld eingeben.

4. Wenn Sie ein Handbuch in einer anderen Sprache kopieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für das zu kopierende Handbuch, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Handbuch kopieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

5. Im folgenden Dialogfeld wird bestätigt, daß Sie das Handbuch kopieren möchten. Klicken Sie auf **Kopieren**.

6. Folgen Sie den angezeigten Anweisungen.

7.3 Windows NT

Tip

Sie können Adobe Acrobat Reader installieren und gleichzeitig das Handbuch kopieren. Anleitungen dazu finden Sie im Abschnitt „Gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs“ auf Seite 168.

Installation von Adobe Acrobat Reader

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein.

2. Wenn Sie Windows NT Version 4 ausführen, wird ein Toolkit-CD-Startbildschirm angezeigt.

Für Benutzer von Windows NT Version 3.51:
Wählen Sie nach dem Einlegen der Toolkit-CD in das CD-ROM-Laufwerk **Ausführen** aus dem Menü **Datei**.

Geben Sie in das angezeigte Eingabefeld den Laufwerksbuchstaben des CD-ROM-Laufwerks ein. Geben Sie dann

```
\SETUP
```

ein, und klicken Sie auf **OK**. Beispiel:

```
D:\SETUP
```

Der Toolkit-CD-Startbildschirm wird angezeigt.

3. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

4. Wählen Sie im nächsten Dialogfeld **Adobe Acrobat Reader installieren**.

   Wenn Sie Adobe Acrobat Reader in einer anderen Sprache installieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für Adobe Acrobat Reader aus, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Adobe Acrobat Reader installieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

5. Im folgenden Dialogfeld wird bestätigt, daß Sie Adobe Acrobat Reader installieren möchten. Klicken Sie auf **Installieren**.

6. Folgen Sie den angezeigten Anweisungen.

Kopieren des Handbuchs

1. Starten Sie den Computer, und melden Sie sich mit einem Benutzernamen, der zur Administratorgruppe gehört, am Desktop von Windows NT an. Legen Sie die Toolkit CD in das CD-ROM-Laufwerk ein.

2. Wenn Sie Windows NT Version 4 ausführen, wird ein Toolkit-CD-Startbildschirm angezeigt.

Für Benutzer von Windows NT Version 3.51:
Wählen Sie nach dem Einlegen der Toolkit-CD in das CD-ROM-Laufwerk **Ausführen** aus dem Menü **Datei**.

Geben Sie in das angezeigte Eingabefeld den Laufwerksbuchstaben des CD-ROM-Laufwerks ein. Geben Sie dann

```
\SETUP
```

ein, und klicken Sie auf **OK**. Beispiel:

```
D:\SETUP
```

Der Toolkit-CD-Startbildschirm wird angezeigt.

3. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

4. Wählen Sie im nächsten Dialogfeld **Handbuch kopieren**. Wählen Sie ein Laufwerk und ein Verzeichnis für das Handbuch aus, indem Sie den Pfad im Eingabefeld am oberen Rand des Dialogfelds angeben. Sie können Laufwerk und Verzeichnis auch über die Schaltfläche **Durchsuchen** angeben, oder indem Sie den Pfad direkt in das Eingabefeld eingeben.

5. Wenn Sie ein Handbuch in einer anderen Sprache kopieren möchten, klicken Sie auf **Sprache ändern**. Das daraufhin aufgerufene Dialogfeld enthält eine Liste mit den verfügbaren Sprachen. Wählen Sie die gewünschte Sprache für das zu kopierende Handbuch, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Handbuch kopieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

6. Im folgenden Dialogfeld wird bestätigt, daß Sie das Handbuch kopieren möchten. Klicken Sie auf **Kopieren**.

7. Folgen Sie den angezeigten Anweisungen.

7.4 OS/2

Installation von Adobe Acrobat Reader

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop des Präsentationsmanagers angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

   Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `D:` <Eingabetaste>

   Geben Sie dann folgendes ein:

   `CD <`*`SPRACHE`*`>\MANUALS\OS2` <Eingabetaste>

   Wenn Sie zum Beispiel die englische Version von Adobe Acrobat Reader installieren, geben Sie folgendes ein:

   `CD ENGLISH\MANUALS\OS2` <Eingabetaste>

   Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber die deutsche Version von Adobe Acrobat Reader installieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

   Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `DIR` <Eingabetaste>

   Durch diesen Befehl wird eine Liste aller Dateien des Verzeichnisses angezeigt. Eine dieser Dateien ist die ausführbare Datei von Adobe mit der Erweiterung .EXE. Geben Sie folgendes ein, um das Adobe-Installationsprogramm zu starten:

   `<`*`DATEINAME`*`>` <Eingabetaste>

<DATEINAME> ist der Name der ausführbaren Datei von Adobe mit der Erweiterung .EXE. Wenn Sie zum Beispiel die englische Version von Adobe Acrobat Reader installieren, heißt die Datei ARO2E30.

3. Folgen Sie den angezeigten Anweisungen.

Kopieren des Handbuchs

1. Starten Sie den Computer. Legen Sie die Toolkit-CD in das CD-ROM-Laufwerk ein, wenn der Desktop des Präsentationsmanagers angezeigt wird.

2. Öffnen Sie eine OS/2-Befehlssitzung.

   Geben Sie den Buchstaben des CD-ROM-Laufwerks ein, gefolgt von einem Doppelpunkt, und drücken Sie dann die Eingabetaste. Beispiel:

   `D:` <Eingabetaste>

   Geben Sie dann folgendes ein:

   `CD <`*`SPRACHE`*`>\MANUALS` <Eingabetaste>

   Wenn Sie zum Beispiel die englische Version des Handbuchs kopieren, geben Sie folgendes ein:

   `CD ENGLISH\MANUALS` <Eingabetaste>

   Der Name der Sprache muß in der entsprechenden Sprache sein. Wenn Sie beispielsweise auf einem englischen System arbeiten, aber ein deutsches Handbuch kopieren möchten, muß der Name des Verzeichnisses DEUTSCH sein, nicht GERMAN.

   Geben Sie an der neuen Eingabeaufforderung folgendes ein:

   `DIR` <Eingabetaste>

   Durch diesen Befehl wird der Name der Handbuchdatei angezeigt. In dem Verzeichnis befindet sich nur eine einzige Datei.

3. Geben Sie folgendes ein, um das Handbuch zu kopieren:

   `copy <HANDBUCHNAME>.PDF [<LAUFWERKSBUCHSTABE>:\<VERZEICHNISNAME>]` <Eingabetaste>

   `<HANDBUCHNAME>` ist der Dateiname des Handbuchs, und `[<LAUFWERKSBUCHSTABE>:\<VERZEICHNISNAME>]` sind Laufwerk und Verzeichnis, in das das Handbuch kopiert werden soll.

7.5 Gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs

Tip 

Diese Option ist nur für Benutzer von Windows 3.x, Windows 95 und Windows NT verfügbar.

1. Folgen Sie den Anleitungen für Ihr Betriebssystem, um das Toolkit-CD-Installationsprogramm zu starten.

2. Ein Toolkit-CD-Startbildschirm wird angezeigt. Wählen Sie **Handbuch** im nächsten angezeigten Dialogfeld, und klicken Sie auf **Weiter**.

3. Wählen Sie im nächsten Dialogfeld **Handbuch kopieren** und **Adobe Acrobat Reader installieren**.

4. Wählen Sie ein Laufwerk und ein Verzeichnis für das Handbuch aus, indem Sie den Pfad im Eingabefeld am oberen Rand des Dialogfelds angeben. Sie können Laufwerk und Verzeichnis auch über die Schaltfläche **Durchsuchen** angeben, oder indem Sie den Pfad direkt in das Eingabefeld eingeben.

5. Wenn das Handbuch und Adobe Acrobat Reader in einer anderen Sprache sein sollen, klicken Sie auf **Sprache ändern**. Das nächste Dialogfeld enthält eine Liste mit verfügbaren Sprachen. Wählen Sie eine Sprache für das Handbuch und Adobe Acrobat Reader aus, und klicken Sie auf **OK**. Das Dialogfeld, in dem Sie **Handbuch kopieren** und **Adobe Acrobat Reader installieren** ausgewählt haben, wird wieder angezeigt. Klicken Sie auf **Weiter**.

6. Im folgenden Dialogfeld wird bestätigt, daß Sie das Handbuch kopieren und Adobe Acrobat Reader installieren möchten. Klicken Sie auf **Installieren**.

7. Folgen Sie den angezeigten Anweisungen.

8. Überblick über Computerviren

In diesem Kapitel finden Sie Informationen über Computerviren sowie über Probleme, die zum Teil für Viren gehalten werden und Maßnahmen, die Sie zum Schutz gegen Virenbefall ergreifen können.

Viele Computerbenutzer geraten in Panik, wenn sie sich mit einem *Computervirus* konfrontiert sehen. Bedenken Sie dabei jedoch, daß Computerviren vorgebeugt werden kann, und wenn ein Virenbefall früh genug festgestellt wird, können die Schäden in Grenzen gehalten werden. Vorbeugende Maßnahmen sind von entscheidender Bedeutung, Sie sollten aber auch für den Fall einer Virusinfektion gerüstet sein.

Dr Solomon's Anti-Virus Toolkit bietet die Möglichkeit, Viren aufzufinden und Virusinfektionen zu beseitigen. Das Programm entdeckt und entfernt jeden in der aktuellen Treiberdatei erfaßten Virus. Darüber hinaus kann das Toolkit auch nach neuen, d. h. bisher unbekannten Viren suchen.

8.1 Was ist ein Virus?

Computerviren werden als Viren bezeichnet, weil sie sich selbst reproduzieren. Sie sind im allgemeinen darauf ausgelegt, dies ohne Ihr Wissen zu tun. Ein Virus könnte sich beispielsweise an das Programm FORMAT anhängen, so daß er jedes Mal ausgeführt wird, wenn Sie eine Diskette formatieren. Auf Ihrem Computer können aber auch andere Probleme auftreten, die nicht von Viren verursacht werden. Einige davon werden im Abschnitt „Weitere mögliche Probleme“ behandelt.

Fast alle Viren haben beabsichtige oder zufällige Auswirkungen. Manche dieser Auswirkungen sind harmlos: Der Virus zeigt vielleicht nur eine Meldung an, läßt die Buchstaben vom Bildschirm purzeln oder spielt eine Melodie. Andere Viren sind zerstörerischer Natur; sie überschreiben bestimmte Daten oder löschen Dateien von der Festplatte. Außerdem funktionieren viele Viren aufgrund von Fehlern in der Software nicht so, wie von ihren Programmierern beabsichtigt. Die Auswirkungen solcher Viren sind nicht vorhersehbar. Die meisten Viren setzen sich im Arbeitsspeicher des Computers fest, wo sie Probleme verursachen können, indem sie die Ausführung anderer Programme beeinflussen.

Computerviren sind niemals völlig harmlos. Dr Solomon's Anti-Virus Toolkit kann Ihnen dabei helfen, sicherzugehen, daß Ihr Computer von einem Virenbefall verschont bleibt.

Es gibt viele Arten von Viren, darunter:

- Dateiviren
- Makroviren
- Boot- und Partitionssektorviren
- Multivalente Viren

Hilfe

Weitere Informationen über Viren und ihre Eigenschaften finden Sie in der Hilfe zum Toolkit unter „Info über Viren".

8.2 Verbreitung von Viren

Viren werden meistens über infizierte Disketten oder an E-Mails angehängte Dateien verbreitet. Makroviren sind zur Zeit die am häufigsten auftretenden Viren, gefolgt von Bootsektorviren.

Makroviren können durch die Übertragung infizierter Dateien von Disketten oder als Anhänge an E-Mails verbreitet werden, oder auch durch das Laden von infizierten Dateien aus dem Internet.

Bootsektorviren können nur über Disketten verbreitet werden. Wenn Benutzer dieselben Disketten auf mehreren Computern verwenden, erhöht sich die Wahrscheinlichkeit, daß sie über eine infizierte Diskette einen Virus verbreiten.

Manche Computerbenutzer sind fälschlicherweise der Ansicht, daß Shareware, Demodisketten und Spiele die einzige „Brutstätte“ von Viren sind. Obwohl Viren manchmal über diese Arten von Software übertragen werden, da sie häufiger kopiert werden, wurden Viren auch in originalverpackter Software namhafter Hersteller sowie auf Hardware beiliegenden Disketten gefunden. Aus diesem Grund sollten Sie immer alle Disketten auf Viren prüfen, bevor Sie sie verwenden.

Dateiviren können auch durch das Laden infizierter Programme aus Bulletin Boards und dem Internet oder durch Übertragung infizierter Dateien als Anhänge an E-Mails verbreitet werden. Aus diesem Grund sollten Sie sich die Mühe machen, jede über ein Netzwerk oder eine Datenleitung übertragene Software auf Viren zu prüfen, bevor Sie sie verwenden.

Ein Arbeitsplatzrechner in einem Netzwerk kann auf die gleiche Weise infiziert werden wie ein Einzelcomputer, und ein Virus kann in einem Netzwerk sehr schnell verbreitet werden. Da die Auswirkungen besonders schwerwiegend sein können, wenn ein Dateiserver infiziert wird, müssen Netzwerke besonders sorgfältig geschützt werden.

8.3 Weitere mögliche Probleme

Wenn ein Computer nicht wie gewohnt funktioniert, wird häufig angenommen, daß ein Virus daran schuld ist. Leider gibt es jedoch auch viele andere Probleme, die ein Weiterarbeiten unmöglich machen und Daten zerstören können. Einige davon werden im folgenden beschrieben.

Softwarefehler

Bei einem Softwarefehler handelt es sich um eine nicht beabsichtigte Schwachstelle in einem Programm. Praktisch jede komplexe Software enthält Fehler. Kleinere Fehler sind meist nur unangenehm, grobe Fehler hingegen können schwerwiegende Datenverluste verursachen. Fehler lassen sich vorab nur schwer feststellen, so daß der einzige Schutz dagegen in regelmäßigen Sicherungen wichtiger Daten besteht.

Konflikte durch hardwarenahe Software

Hardwarenahe Softwareprogramme greifen direkt auf Datenträger zu. Sie werden deshalb als „hardwarenah“ bezeichnet, weil sie auf einer noch niedrigeren Ebene agieren als das Betriebssystem, das im allgemeinen den Zugriff auf Datenträger steuert und bestimmte Regeln erzwingt. Zu den hardwarenahen Programmen zählen:

- Disk-Editoren
- Plattencache-Programme
- Plattenkomprimierungsprogramme
- Defragmentierungsprogramme

Die Verwendung solcher Programme verursacht normalerweise keine Probleme, sofern jeweils nur ein Programm ausgeführt wird. Es können jedoch Probleme auftreten, wenn zwei oder mehr hardwarenahe Programme gleichzeitig ausgeführt werden. Wenn mehrere solcher Programme versuchen, auf einen Datenträger zuzugreifen, kann dies zu potentiell gefährlichen Konflikten führen. Da hardwarenahe Programme von immer mehr Benutzern eingesetzt werden, tritt diese Art von Problem immer häufiger auf.

So vermeiden Sie Probleme mit hardwarenahen Programmen:

- Sichern Sie immer Ihre Daten, bevor Sie ein Festplattendienstprogramm verwenden.
- Führen Sie jeweils nur ein Dienstprogramm aus.
- Vermeiden Sie es, hardwarenahe Programme auszuführen, wenn speicherresidente Software geladen ist.
- Lesen Sie immer die Handbücher und README-Dateien, die mit einem Produkt geliefert werden. Wenn der Hersteller bestimmte Warnungen in die Dokumentation aufnimmt, hat dies in der Regel auch einen guten Grund!

Trojanische Pferde

Trojanische Pferde sind Programme, die unerwartet eine Funktion ausführen, die meistens einen Schaden verursacht. Sie sind weniger weit verbreitet als Viren, da sie sich nicht vermehren. Allerdings stellen sie eine Gefahr dar, wenn sie kopiert werden. Viele Benutzer verwechseln Viren und trojanische Pferde: Die AIDS-Aufklärungsdiskette, die in den Medien oft als Beispiel für einen Virus genannt wurde, war in Wirklichkeit ein trojanisches Pferd. Außerdem enthalten Viren manchmal trojanische Pferde.

Sie bekommen ein trojanisches Pferd wahrscheinlich nie zu sehen, wenn Sie Ihre Software stets beim Fachhändler erwerben. Der beste Schutz gegen einen von solchen Programmen verursachten Schaden ist und bleibt jedoch eine vollständige Sicherung aller Daten Ihres Systems.

Das Toolkit findet und identifiziert einige bekannte trojanische Pferde und behandelt sie wie Viren.

Zeitbomben und logische Bomben

Bei Zeitbomben und logischen Bomben handelt es sich um besondere Arten von trojanischen Pferden. Eine Zeitbombe wird an einem festgelegten Datum aktiv, eine logische Bombe wird unter bestimmten Bedingungen ausgelöst, etwa durch die Anzahl der Dateien auf einem Datenträger oder die Eingabe einer bestimmten Zeichenfolge. Beide Arten verursachen in der Regel Schäden.

Scherzprogramme

Einige Programme geben vor, auf einem Computer Schäden anzurichten. In Wirklichkeit handelt es sich dabei jedoch um einen harmlosen Scherz. Es könnte zum Beispiel eine Meldung angezeigt werden, die angibt, daß Ihre Festplatte neu formatiert wird. Leider lösen solche Scherzprogramme oft eine Überreaktion aus, wodurch möglicherweise bei dem Versuch, den vermeintlichen Virus auszumerzen, tatsächlich ein Schaden entsteht.

Benutzerfehler

Wenn der Computer nicht wie erwartet funktioniert oder Daten verlorengehen, ist die Ursache meistens weder ein Virus noch ein Softwarefehler, sondern ein Benutzerfehler. Jeder Benutzer macht hin und wieder Fehler, drückt beispielsweise eine falsche Tastenfolge oder gibt DEL *.* im falschen Verzeichnis ein. Solche Fehler können drastische Folgen haben.

Tip

Bedenken Sie stets, daß der wertvollste Teil Ihres Computers die darauf gespeicherten Daten sind. Hardware und Programme lassen sich ersetzen, Daten jedoch nur dann, wenn sie gesichert wurden.

8.4 Vorkehrungen

Obwohl Computerviren ein Problem darstellen, sollte ihre Bedeutung nicht überbewertet werden. Die häufigste Ursache für Datenverluste sind Benutzerfehler. Die zweithäufigste Ursache sind Hardwarefehler, gefolgt von Softwarefehlern. Viren kommen erst an vierter Stelle.

Die Umsetzung einer konsequenten Anti-Virus-Strategie ist jedoch ein wirksamer Schutz vor allen Arten von Datenverlusten, auch solchen, die von Viren verursacht werden. Sie sollten vor allem die folgenden drei Aspekte des Virenschutzes berücksichtigen:

- Vorbeugung - um die Ausbreitung von Viren einzuschränken.
- Entdeckung - um sicherzustellen, daß ein Virus, der in das System eindringen konnte, so rasch wie möglich gefunden wird.
- Wiederherstellung - um sicherzugehen, daß Dateien, die verlorengegangen oder beschädigt sind, so rasch wie möglich wiederhergestellt werden können.

Datensicherungen

Warnung

Die wichtigste Vorsichtsmaßnahme, die Sie gegen alle möglichen Arten von Datenverlusten treffen können, sind regelmäßige Sicherungen aller Daten Ihres Systems.

Wenn Sie Ihre Daten nicht regelmäßig sichern, setzen Sie sie einem Risiko aus.

Denken Sie daran, Ihre Sicherungskopien regelmäßig zu überprüfen, und prüfen Sie auch, ob Ihre Daten mit Hilfe der Sicherungskopien wiederhergestellt werden können.

Überprüfen Sie, ob Sie saubere, d. h. virenfreie Kopien aller ausführbaren Dateien auf Diskette haben. Alle Sicherungsdisketten sowie Ihre Startdisketten sollten schreibgeschützt sein.

Softwarekauf

Sie sollten Ihre gesamte Software von Fachhändlern beziehen. Prüfen Sie, ob sich die Software in der Originalverpackung befindet.

Verwenden Sie niemals Raubkopien. Auch wenn Sie glauben, zwischenzeitlich eine weitere Kopie verwenden zu dürfen (etwa wenn Sie die lizenzierte Kopie an einem anderen Ort gelassen haben), bedenken Sie, daß Sie sich mit jeder Kopie dem Risiko eines Virenbefalls aussetzen.

Software kann über Datenleitungen und tragbare Datenträger auf Ihren Computer gelangen. Lassen Sie die nötige Vorsicht walten, wenn Sie Software auf bzw. von Laptops und innerhalb von Netzwerken übertragen oder durch Laden von Bulletin Boards oder aus dem Internet beziehen.

Disketten und andere Datenträger

Das Risiko eines Virenbefalls durch Dateiübertragungen von Disketten ist besonders hoch; Sie können jedoch mit Hilfe einiger einfacher Schritte die Sicherheit erhöhen.

- Versehen Sie Disketten nach Möglichkeit stets mit einem Schreibschutz, so daß keine Viren auf sie kopiert werden können.
- Lassen Sie keine Diskette im Laufwerk, wenn Sie den Computer ausschalten. Dadurch vermeiden Sie ein versehentliches Starten von einer Diskette, die mit einem Bootsektorvirus infiziert ist.
- Falls Sie das System versehentlich mit einer nicht startfähigen Diskette starten, sollten Sie den Computer aus- und wieder einschalten, anstatt den Startvorgang von Laufwerk C: fortzusetzen.
- Ändern Sie die entsprechende CMOS-Einstellung des Computers, so daß er zuerst von Laufwerk C: anstatt von Laufwerk A: startet. Dies ist allerdings bei SCSI-Laufwerken nicht immer möglich.
- Berücksichtigen Sie, daß auch Dateien auf Band infiziert sein können, da sie möglicherweise zum Zeitpunkt der Sicherung bereits infiziert waren.

Vermeiden von Verschlüsselung und Kennwortschutz

Durch Verschlüsselung und Kennwortschutz können Dateien vor unberechtigtem Zugriff geschützt werden

Leider können Virensuchprogramme nicht auf derart geschützte Dateien zugreifen, was dazu führen kann, daß Viren nicht entdeckt werden.

Wenn ein Dokument nicht durch ein Kennwort geschützt ist, kann es überprüft und ein möglicherweise vorhandener Virus gefunden werden.

Kooperation der Mitarbeiter

Arbeitgeber benötigen für jede Anti-Virus-Strategie die Kooperation ihrer Mitarbeiter. Wenn die Mitarbeiter annehmen müssen, daß die Entdeckung eines Virus für sie mit Nachteilen verbunden ist, werden sie Probleme wahrscheinlich niemals melden.

Manche Firmen haben versucht, Spielesoftware zu verbieten. Es ist jedoch wesentlich erfolgversprechender, sicherzustellen, daß Spiele von einem Fachhändler stammen und vor der Verwendung überprüft werden. Es kann sich als vorteilhaft erweisen, einer Person oder einer kleinen Gruppe die Verantwortung für die Überprüfung und Verteilung von Spielesoftware zu übertragen.

Das Anti-Virus Toolkit

Der Funktionsumfang von Dr Solomon's Anti-Virus Toolkit reicht von schneller und benutzerfreundlicher Virensuche auf Einzelcomputern bis zur Unterstützung von Anti-Virus-Strategien in großen Organisationen mit umfangreichen Netzwerken.

Das Anti-Virus Toolkit bietet Hilfsmittel für die Entdeckung und Entfernung von Viren. Es gibt zwei Hauptarten von Anti-Virus-Software:

- Ein *Virensuchprogramm* ist ein Programm, das nach Viren sucht. Da laufend neue Viren auftreten, müssen Suchprogramme regelmäßig aktualisiert werden.

- Ein *Prüfsummenprogramm* erkennt Änderungen an Dateien. Es berechnet für jede zu schützende Datei eine eindeutige numerische Prüfsumme. Das Prüfsummenprogramm kann dann die Prüfsumme einer Datei erneut berechnen, so daß Abweichungen erkannt werden. Ausführbare Dateien ändern sich im allgemeinen nicht; wenn also die neu berechnete Prüfsumme von der ursprünglichen Prüfsumme abweicht, ist möglicherweise ein Virus vorhanden.

Dr Solomon's Anti Virus Toolkit enthält folgende Elemente:

WinGuard

WinGuard wird beim Starten von Windows automatisch aufgerufen und läuft dann im Hintergrund. WinGuard überprüft Dateien, Boot- und Partitionssektoren automatisch, wenn auf sie zugegriffen wird. Wenn WinGuard einen Virus findet, wird der Zugriff blockiert und ein Warndialogfeld aufgerufen.

VirusGuard

VirusGuard ist ein Zugriffssuchprogramm, das fortlaufend im Hintergrund ausgeführt wird, wenn Sie im DOS-Modus arbeiten. VirusGuard überprüft Dateien, Boot- und Partitionssektoren automatisch, wenn auf sie zugegriffen wird.

FindVirus

FindVirus ist ein Virensuchprogramm, mit dessen Hilfe Sie die Festplatten und neu erhaltene Disketten regelmäßig auf Viren überprüfen können. Das Programm findet und meldet jeden in der aktuellen Version der Treiberdatei enthaltenen Virus. Es enthält darüber hinaus ein optionales heuristisches Suchprogramm, das in Dateien nach verdächtigem Code sucht, der auf einen bisher unbekannten Virus verweisen könnte.

FindVirus entdeckt Viren und entfernt sie aus Dateien, Bootsektoren und Partitionssektoren. Mit Hilfe von FindVirus können Sie neu erhaltene Disketten und Dateien auf einem sogenannten Quarantänecomputer überprüfen, d. h. einem Computer, der nur für diesen Zweck verwendet wird. Die Überprüfung durch FindVirus ist sehr schnell und daher für eine tägliche Untersuchung der Festplatten geeignet.

ViVerify

ViVerify ist ein Prüfsummenprogramm, das Änderungen an ausführbaren Dateien erkennt, die durch einen Virenbefall entstanden sein können. Sie können ViVerify einsetzen, um für jede Datei eine Prüfsumme zu berechnen. Danach können Sie ViVerify regelmäßig ausführen, um diese Prüfsumme neu zu berechnen und zu überprüfen, ob Änderungen aufgetreten sind. Obwohl eine Änderung an einer ausführbaren Datei nicht unbedingt bedeuten muß, daß sie infiziert ist, ändert sich ausführbarer Code im allgemeinen nicht. ViVerify meldet jede auf einen Virus hindeutende Änderung, auch wenn es sich um einen bisher nicht bekannten Virus handeln könnte.

SOS-Diskette

Bei der SOS-Diskette handelt es sich um eine Diskette, von der aus Sie den Computer starten und eine DOS-Version von FindVirus ausführen können.

Zeitplaner

Der Zeitplaner Dr Solomon’s Scheduler ist ein Hilfsprogramm, über das Sie Ereignisse zu vorher festgelegten Zeiten ausführen können, wie z. B. Überprüfungen auf Viren usw.

Virenlexikon

Die Online-Fassung des Virenlexikons enthält ausführliche Informationen über die am weitesten verbreiteten Viren, die vom Toolkit erkannt werden.

9. Fehlerbehebung und erweiterte Einstellungen

In diesem Kapitel werden potentielle Probleme und die technisch komplexeren Funktionen des Toolkit behandelt.

9.1 Fehlerbehebung

Dieser Abschnitt behandelt einige der möglichen Probleme bei der Installation und Benutzung des Toolkit und bietet Lösungsmöglichkeiten.

Meldung über fehlerhafte Datei MESSAGES.DRV

Beim Starten des Toolkit erhalten Sie möglicherweise eine Meldung über die fehlerhafte Datei MESSAGES.DRV.

Diese Meldung kommt daher, daß auf dem System mehrere Dateien mit dem Namen MESSAGES.DRV sind; der Grund dafür könnte sein, daß Sie vielleicht einzelne Toolkit-Komponenten auf einem System installiert haben, auf dem bereits ein vollständiges Toolkit installiert war.

Sie sollten alle Dateien mit dem Namen MESSAGES.DRV, die nicht im Toolkit-Verzeichnis sind, aus dem System löschen. Sie können die Dateien beispielsweise im Verzeichnis S&STEMP oder im Papierkorb finden.

Wenn das Problem damit nicht behoben ist, sollten Sie alle älteren Toolkits deinstallieren und dann die aktuelle Version erneut installieren.

Deinstallation ohne ein Deinstallationsprogramm

Die Toolkits für OS/2 und DOS müssen manuell deinstalliert werden; Informationen dazu finden Sie auf Seite 54 (OS/2) und Seite 63 (DOS).

Wenn Ihr Windows-Toolkit ein Dienstprogramm für die Deinstallation hat, sollten Sie dieses verwenden; Informationen dazu finden Sie auf Seite 19 (Windows 3.x) und Seite 38 (Windows 95).

So installieren Sie ein älteres Windows-Toolkit, das kein Dienstprogramm für die Deinstallation hat:

1. Deaktivieren Sie WinGuard.
2. Starten Sie den Computer neu.
3. Löschen Sie das Toolkit-Verzeichnis mit allen seinen Dateien.

Durch die Installation des Toolkit kann Windows 95 nicht mehr ausgeführt werden

Nach der Installation des Windows 95-Toolkit startet Windows 95 manchmal nur noch im abgesicherten Modus.

Der Grund dafür kann WinGuard sein. Deaktivieren Sie WinGuard, und starten Sie den Computer neu.

Wenn Windows 95 noch immer nur im abgesicherten Modus startet, müssen Sie das Toolkit wie auf Seite 38 beschrieben deinstallieren und sich an die technische Unterstützung von Dr Solomon's wenden. Adressen und Telefon- und Faxnummern von Dr Solomon's Software finden Sie im Abschnitt „Falls Sie Hilfe benötigen“ auf Seite xii.

Meldung „Legen Sie eine Diskette mit \COMMAND.COM ein.“

Wenn Sie an einer DOS-Eingabeaufforderung arbeiten, wird möglicherweise die Meldung „Legen Sie eine Diskette mit \COMMAND.COM in Laufwerk A: ein“ angezeigt.

Legen Sie eine Systemdiskette (d. h. Startdiskette) ein, und drücken Sie eine beliebige Taste.

9.2 Erweiterte Installationsoptionen

Auf dem Anfangsbildschirm des Installationsprogramms auf der CD können Sie **Erweiterte Installationsoptionen** auswählen; Informationen über diese Optionen finden Sie in der Hilfe zum Installationsprogramm auf der CD. Im wesentlichen haben Sie folgende Möglichkeiten:

- Ein vollständiges Toolkit installieren. Hierbei wird eine neue Installation vorgenommen, im Gegensatz zur Option **Schnellinstallation** auf dem Anfangsbildschirm, bei dem eine bereits vorhandene Toolkit-Version aktualisiert wird.
- Einzelne Toolkit-Komponenten installieren.
- Die Installationsdateien für das vollständige Toolkit oder ausgewählte Komponenten auf das System kopieren. Mit diesen Dateien können Sie das Toolkit später installieren. Diese Option ist zum Beispiel dann hilfreich, wenn Sie das Toolkit von einem zentralen Netzwerkverzeichnis auf einem Arbeitsplatzcomputer installieren möchten.
- Die Aktualisierungsdateien auf das System kopieren. Mit Hilfe dieser Dateien können Sie Toolkits von der Toolkit-Benutzeroberfläche aus aktualisieren.
- Installationsdiskettensätze erstellen. Sie können die Toolkit-Installation später von diesen Disketten vornehmen. Wenn Sie eine Unternehmenslizenz haben, können Sie Dr Solomon's-Software von diesen Disketten auf Einzelcomputern installieren.

9.3 Zusätzliche Dienstprogramme

Dieser Abschnitt enthält Informationen über die mit dem Toolkit gelieferten zusätzlichen DOS-Dienstprogramme.

CleanBoot

In Windows können Sie den Menübefehl **Bootsektor ersetzen** verwenden. Wenn Sie mit DOS arbeiten, müssen Sie das Dienstprogramm CleanBoot verwenden.

1. Legen Sie die verdächtige Diskette ein.
2. Geben Sie folgenden Befehl ein:

   `CLEANBOO [`*`Laufwerk`*`] [/`*`Typ`*`] [/`*`silent`*`]`

   Erläuterung:

   `Laufwerk` ist das Laufwerk, in dem sich die infizierte Diskette befindet.

   `Typ` wird aus der folgenden Tabelle gewählt:

Typ	Diskettengröße	Speicherkapazität
1	5¼ Zoll	360 KB
2	5¼ Zoll	1,2 MB
3	3½ Zoll	720 KB
4	3½ Zoll	1,44 MB
5	3½ Zoll	2,88 MB
A	Beliebig	Automatische Feststellung

   `silent` unterdrückt die Bildschirmanzeige.

   Es wird empfohlen, den Parameter `/oneonly` zusammen mit diesem Parameter zu verwenden, da Sie sonst unter Umständen vergessen, daß das Programm auf eine Angabe von Ihnen wartet, ob Sie eine weitere Diskette bearbeiten möchten, da Sie keine Aufforderung vom Programm erhalten.

Beispiel für einen Befehl:

```
CLEANBOO B: /4
```

Durch diesen Befehl wird ein sauberer Bootsektor auf einer 3½-Zoll-Diskette mit 1,44 MB Speicherkapazität in Laufwerk B: erstellt.

3. Geben Sie das Diskettenlaufwerk an, wenn Sie dazu aufgefordert werden (Sie erhalten keine Aufforderung, wenn Sie den Parameter `/silent` angegeben haben).

4. Geben Sie den Diskettentyp an, wenn Sie dazu aufgefordert werden (Sie erhalten keine Aufforderung, wenn Sie den Parameter `/silent` angegeben haben).

Tip

Wir empfehlen die automatische Feststellung, da die Wahrscheinlichkeit eines Fehlers bei der Erkennung des Diskettentyps äußerst gering ist.

---

5. Wenn Sie die automatische Feststellung angegeben haben, bestätigen Sie die automatische Diskettenauswahl.

6. Reagieren Sie auf das Meldungsfeld, in dem Sie informiert werden, daß keine Übereinstimmung vorliegt (diese Meldung wird nur angezeigt, wenn der angegebene Dateityp nicht dem festgestellten Dateityp entspricht).

7. Drücken Sie nach Abschluß des Vorgangs **J**, um eine weitere Diskette zu säubern, oder **N**, um zu beenden.

8. Geben Sie `dir` an der Eingabeaufforderung für das Diskettenlaufwerk ein, um zu sehen, welche Dateien auf der (den) Diskette(n) sind. Wenn Dateien fehlen oder Verzeichnisse beschädigt sind, ist möglicherweise der falsche Bootsektor auf die Diskette geschrieben worden. Versuchen Sie in diesem Fall, mit Hilfe von CleanBoot einen anderen Bootsektor auf die Diskette zu schreiben. Wenn Sie zunächst die automatische Diskettenerkennung deaktiviert hatten, sollten Sie diese Option jetzt aktivieren, da dann häufig ermittelt werden kann, welche Form der

Bootsektor haben sollte. Sie können auch versuchen, den Diskettentyp manuell anzugeben. Dateien gehen nur dann verloren, wenn Sie auf die Diskette schreiben, während sie den falschen Bootsektor hat.

Disketten mit geändertem Format

Eine Diskette kann so formatiert werden, daß sie eine andere Speicherkapazität als die hat, für die sie ursprünglich entwickelt wurde.

Wenn zum Beispiel eine 360-KB-Diskette so formatiert wird, als hätte sie 1,2 MB, werden Sie bei der Ausführung von CHKDSK unter Umständen informiert, daß die Diskette 800 bis 900 KB benutzbaren Speicherplatz und 300 bis 400 KB in fehlerhaften Sektoren hat. Falls diese Diskette zum Speichern von Daten verwendet wird, kann auf die Daten gegebenenfalls nicht mehr zugegriffen werden.

Dasselbe Problem kann auftreten, wenn eine 720-KB-Diskette so formatiert wird, daß sie 1,44 MB hat.

Diese Probleme werden durch Computer verursacht, die nicht zwischen den beiden Diskettentypen unterscheiden können, weil sie die zweite Öffnung nicht feststellen können, durch die HD-Disketten, d. h. Disketten mit hoher Dichte, identifiziert werden.

Falls Sie eine Diskette mit geändertem Format haben, sollten Sie die Daten auf einen anderen Datenträger übertragen und die Diskette so bald wie möglich mit dem richtigen Format neu formatieren.

CleanPart

Sowohl das Dienstprogramm CleanPart als auch FindVirus entfernen Viren aus Partitions- und Bootsektoren. CleanPart kann verwendet werden, wenn Sie erfolglos versucht haben, einen Virus mit Hilfe von FindVirus zu entfernen.

Warnung

Die nicht ordnungsgemäße Verwendung von CleanPart kann zu Datenträgerbeschädigungen führen. Sie sollten das Programm nur unter Anleitung durch Mitarbeiter der technischen Unterstützung von Dr Solomon’s verwenden; weitere Informationen finden Sie auf Seite xii.

TKUTIL

Tip

TKUTIL wird nicht mit dem Toolkit für Windows NT geliefert. Benutzer von Windows NT können diesen Abschnitt ignorieren.

Die TKUTIL-Dienstprogramme werden in der folgenden Tabelle aufgeführt und in den nachfolgenden Abschnitten detailliert erläutert.

Dienstprogramm	Zweck
ADD	Fügt Text an einer bestimmten Stelle in einer Textdatei hinzu.
ADUPDATE	Ersetzt eine ältere Datei durch eine neue mit demselben Namen.
ADD WINGUARD	Fügt Windows-.INI-Dateien Zeilen für den automatischen Start von WinGuard beim Starten von Windows hinzu.
ALARM	Erzeugt eine sichtbare Warnung.
CPU	Gibt den Typ des Hauptprozessors an.
DELETE	Löscht eine Zeile aus einer Textdatei.
DISKSPACE	Gibt an, wieviel freier Speicherplatz auf dem Laufwerk ist.
DRIVETYPE	Gibt den aktuellen Laufwerkstyp an.
FORMFEED	Sendet ein Formularvorschubzeichen an den Drucker.
FROM	Löscht Verweise auf andere Anti-Virus-Produkte aus den Systemdateien.
GUARDCHECK	Gibt an, ob VirusGuard installiert ist.
INIUPDATE	Synchronisiert .INI-Dateien.

Dienstprogramm	Zweck
LASTRUN	Gibt an, wann das Programm zuletzt ausgeführt wurde.
LOCK	Erzwingt einen Kaltstart des Computers.
MEMTYPE	Gibt den Typ des Arbeitsspeichers an.
MKDIR	Erstellt ein neues Verzeichnis.
MONTHDAY	Gibt den Tag des Monats an.
REGUARD	Initialisiert VirusGuard nach dem Netzwerkstart neu.
REMOVE WINGUARD	Löscht die Zeilen für den automatischen Start von WinGuard beim Starten von Windows aus den Windows-.INI-Dateien.
RETKEY	Gibt die ASCII-Zeichenfolge für den Tastenanschlag in Großbuchstaben an.
RETSR	Initialisiert alle speicherresidenten Programme des Toolkit nach dem Netzwerkstart neu.
RFCHECK	Gibt an, ob RingFence installiert ist.
SEARCH	Sucht in einer ASCII-Datei nach einer angegebenen Zeichenfolge.
TECHFILE	Erzeugt eine Datei mit Informationen über das System.
TSRMAP	Gibt eine Liste der Programme im Arbeitsspeicher zurück.
TUNE	Spielt eine Melodie ab.
UPDATE	Ersetzt eine ältere Datei durch eine neue mit demselben Namen.
WEEKDAY	Gibt den Tag der Woche an.

Angabe des Laufwerks

Durch den Befehl `DRIVETYPE` wird der Typ des aktuellen Laufwerks angegeben. Der Befehl hat die folgende Syntax:

```
TKUTIL DRIVETYPE
```

Die zurückgegebene Fehlerebene gibt den Laufwerkstyp an:

Fehlerebene	Laufwerk
1	Diskettenlaufwerk
2	Lokale Festplatte
3	Netzlaufwerk

Angabe des freien Speicherplatzes

Durch den Befehl `DISKSPACE` wird eine Fehlerebene des auf dem Laufwerk verbleibenden Speicherplatzes, abgerundet auf eine Ganzzahl von Megabyte, zurückgegeben.

Auf dem Bildschirm wird auch der auf dem Laufwerk verbleibende Speicherplatz in Byte angezeigt.

Angabe des Hauptprozessortyps

Der Befehl `CPU` gibt den Prozessortyp zurück. Der Befehl hat die folgende Syntax:

```
TKUTIL CPU
```

Die zurückgegebene Fehlerebene gibt den im Computer installierten Hauptprozessortyp an:

Fehlerebene	Prozessortyp
0	8086
2	80286
3	80386
4	80486
5	Pentium

Angabe des Arbeitsspeichertyps

Durch den Befehl MEMTYPE wird angegeben, welcher Typ von Arbeitsspeicher installiert ist. Der Befehl hat die folgende Syntax:

```
TKUTIL MEMTYPE
```

Die zurückgegebene Fehlerebene gibt den im Computer installierten Typ des Arbeitsspeichers an:

Fehlerebene	Arbeitsspeichertyp
0	Konventionell
1	EMS
2	XMS
3	EMS und XMS

Angabe der speicherresidenten Programme des Toolkit

Durch den Befehl TSRMAP werden alle im Arbeitsspeicher residenten Programme angegeben. Der Befehl hat die folgende Syntax:

```
TKUTIL TSRMAP
```

Wenn Sie mit DOS 5.0 oder höher arbeiten, können Sie auch den Befehl MEM /C verwenden, der dieselbe Funktion hat.

Angabe des letzten Tastenanschlags

Durch den Befehl RETKEY wird der ASCII-Code des aktuellen Tastenanschlags in Großbuchstaben angegeben. Sie können diesen Befehl verwenden, um zu überprüfen, ob der Benutzer als Antwort auf eine Eingabeaufforderung J oder N eingegeben hat. Der Befehl hat die folgende Syntax:

```
TKUTIL RETKEY
```

Der Tastenanschlag wird als die Fehlerebene zurückgegeben.

Angabe der Ausführung einer Stapeldatei

Durch den Befehl `TKUTIL LASTRUN` wird die Anzahl der Tage seit der letzten Ausführung zurückgegeben. Sie können diesen Befehl in einer Stapeldatei verwenden, um anzugeben, wann diese Datei zuletzt ausgeführt wurde. Geben Sie den Befehl beispielsweise in die Datei AUTOEXEC.BAT ein, um sicherzustellen, daß eine Überprüfung auf Viren nur beim ersten Systemstart eines Tages ausgeführt wird (wenn `TKUTIL LASTRUN=0` ist, findet keine Überprüfung statt).

Sie können den Befehl zusammen mit `TKUTIL WEEKDAY` verwenden, um eine Stapeldatei zu schreiben, durch die eine Überprüfung ausgelöst wird, wenn die Datei an einem bestimmten Wochentag ausgeführt wird und an diesem Tag noch keine Überprüfung stattgefunden hat.

Der Befehl hat die folgende Syntax:

`TKUTIL LASTRUN <`*`Datei`*`>`

Erläuterung:

<Datei>	wird verwendet, um die Datumsinformationen zu speichern. Wenn Sie keinen Dateinamen angeben, wird die Datei TKUTIL.DAT genannt.

Durch den Befehl wird die Anzahl Tage zurückgegeben, die seit der letzten Ausführung des Programms vergangen sind. In folgenden Fällen wird die Fehlerebene 254 zurückgegeben:

- Wenn die Anzahl der Tage seit der letzten Ausführung des Programms größer als 254 ist.
- Wenn das Stapelprogramm noch nie ausgeführt wurde.
- Wenn die angegebene Datendatei nicht gefunden werden kann.

Erstellung eines neuen Verzeichnisses

Mit Hilfe des Befehls `MKDIR` erstellen Sie ein neues Verzeichnis. Der Befehl hat die folgende Syntax:

`TKUTIL MKDIR <`*`Verzeichnis`*`>`

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
0	Verzeichnis erstellt.
1	Verzeichnis besteht bereits.
2	Verzeichnis konnte nicht erstellt werden.

Aktualisierung von Dateien

Mit Hilfe der Befehle UPDATE und ADUPDATE können Sie bestehende Dateien durch neuere Versionen ersetzen. Die beiden Befehle haben die folgende Syntax:

```
TKUTIL UPDATE <Quelle> <Ziel> [/A] [/N]
```

```
TKUTIL ADUPDATE <Ziel> <Quelle> [/A] [/N]
```

wobei <*Quelle*> und <*Ziel*> Verzeichnisnamen sind. Die Dateien im Zielverzeichnis werden durch neuere Dateien mit denselben Namen im Quellverzeichnis ersetzt. Es gibt zwei optionale Parameter:

/A	aktualisiert Dateien und fügt dem Zielverzeichnis neue Dateien aus dem Quellverzeichnis hinzu.
/N	kopiert neue Dateien aus dem Quellverzeichnis in das Zielverzeichnis.

Durch die Befehle UPDATE und ADUPDATE werden folgende Fehlerebenen zurückgegeben:

Fehlerebene	Bedeutung
0	Es wurde nichts unternommen.
1	Die Dateien wurden aktualisiert, aber nicht kopiert.
2	Die Dateien wurden kopiert, aber nicht aktualisiert.

Fehlerebene	Bedeutung
3	Die Dateien wurden kopiert und aktualisiert.
5	Ungültiges Quellverzeichnis.
6	Ungültiges Zielverzeichnis.
11	Zu wenig Arbeitsspeicher.
12	Quell- und Zielverzeichnis sind identisch.
14	Fehler beim Kopieren.
17	Leeres Quellverzeichnis (nur bei ADUPDATE).
18	Leeres Zielverzeichnis (nur bei UPDATE).
255	Fehler bei DOS-Version / Prüfsumme.

Synchronisierung von .INI-Dateien

Durch den Befehl INIUPDATE werden Windows-.INI-Dateien synchronisiert. Jeder Abschnitt wird aus der Quell-.INI-Datei in die Ziel-.INI-Datei kopiert, wodurch alle in der Zieldatei bereits vorhandenen Abschnitte überschrieben werden.

Der Befehl hat die folgende Syntax:

```
TKUTIL INIUPDATE <Dateiname1> <Dateiname2>
```

Erläuterung:

<Dateiname1> ist der Name der Quelldatei.

<Dateiname2> ist der Name der Zieldatei.

Hinzufügen von Text in einer Datei

Mit Hilfe des Befehls ADD können Sie einer Datei Text hinzufügen. Sie können diesen Befehl verwenden, um den Dateien AUTOEXEC.BAT und CONFIG.SYS Einträge hinzuzufügen. Der Befehl hat die folgende Syntax:

```
TKUTIL ADD <Datei> '<Text>' [/START][/END]
[/AFTER '<Eintrag>']
```

Erläuterung:

<Datei> ist die Datei, der der Text hinzugefügt wird.

<Text> ist der hinzuzufügende Text.

Einer der optionalen Parameter /START, /END oder /AFTER muß angegeben werden, um die Position des Textes in der Datei festzulegen.

Wenn Sie /AFTER angeben und *<Text>* bereits nach *<Eintrag>* in der Datei ist, wird *<Text>* nicht eingefügt. Wenn Sie /AFTER angeben und *<Text>* bereits in der Datei ist, aber vor *<Eintrag>*, wird *<Text>* nach *<Eintrag>* eingefügt (und kommt daher in der Datei doppelt vor).

Durch den Befehl ADD werden folgende Fehlerebenen zurückgegeben:

Fehlerebene	Bedeutung
1	Falsche Parameter.
2	Datei nicht gefunden.
3	Fehler beim Lesen der Datei.
4	Fehler beim Schreiben in die Datei.
5	Der Parameter /AFTER wurde angegeben, aber es wurde kein Text gefunden.

Beispiele für die Verwendung des Befehls ADD:

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /COPY=FLOPPY' /START
```

GUARD /COPY=FLOPPY wird am Anfang der Datei AUTOEXEC.BAT hinzugefügt.

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /REGUARD' /AFTER
'login'
```

GUARD /REGUARD wird der Datei AUTOEXEC.BAT nach der Zeile mit dem Text „login“ hinzugefügt.

Starten von WinGuard beim Systemstart

Durch den Befehl `ADD WINGUARD` werden den Dateien WIN.INI und SYSTEM.INI die für den automatischen Start von WinGuard beim Systemstart benötigen Zeilen hinzugefügt.

„....(Pfad)....\wgfe.exe“ wird der Zeile „run“ der Datei WIN.INI und „device=....(Pfad)....\windguard.386“ dem Anfang des Abschnitts „386Enh“ der Datei SYSTEM.INI hinzugefügt.

Der Befehl hat die folgende Syntax:

`TKUTIL ADD WINGUARD <Verzeichnis1> <Verzeichnis2>`

Erläuterung:

<Verzeichnis1>	ist das Verzeichnis, in dem das Toolkit installiert ist. Das Verzeichnis enthält die Datei WINGUARD.386.
<Verzeichnis2>	ist das Windows-Verzeichnis. Das Verzeichnis enthält die Dateien WIN.INI und SYSTEM.INI.

Löschen von Text aus einer Datei

Mit Hilfe des Befehls `DELETE` können Sie eine bestimmte Textzeile aus einer Datei löschen. Der Befehl hat die folgende Syntax:

`TKUTIL DELETE <Datei> '<Text>'`

Erläuterung:

<Datei>	ist die Datei, aus der Text gelöscht werden soll.
<Text>	ist die zu löschende Zeile.

Durch den Befehl werden folgende Fehlerebenen zurückgegeben:

Fehlerebene	Bedeutung
255	Datei- oder Befehlszeilenfehler.
1	Eintrag nicht gefunden.
0	Eintrag gefunden.

Deaktivierung des automatischen Starts von WinGuard beim Systemstart

Durch den Befehl `REMOVE WINGUARD` werden die Zeilen, durch die WinGuard beim Systemstart automatisch gestartet wird, aus den Dateien WIN.INI und SYSTEM.INI entfernt.

Der Befehl hat die folgende Syntax:

`TKUTIL REMOVE WINGUARD <Verzeichnis>`

Erläuterung:

<Verzeichnis>	ist das Windows-Verzeichnis. Das Verzeichnis enthält die Dateien WIN.INI und SYSTEM.INI.

Textsuche

Mit Hilfe des Befehls `SEARCH` können Sie in einer Datei nach einer bestimmten Textzeile suchen. Der Befehl hat die folgende Syntax:

`TKUTIL SEARCH <Datei> '<Text>'`

Erläuterung:

<Datei>	ist die zu durchsuchende Datei.
<Text>	ist der zu suchende Text.

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
255	Datei- oder Befehlszeilenfehler.
1	Text gefunden.
0	Text nicht gefunden.

Überprüfung, ob VirusGuard installiert ist

Mit Hilfe des Befehls GUARDCHECK können Sie überprüfen, ob VirusGuard installiert ist. Der Befehl hat die folgende Syntax:

```
TKUTIL GUARDCHECK
```

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
0	VirusGuard ist installiert.
1	VirusGuard ist nicht installiert.

Überprüfung, ob RingFence installiert ist

Mit Hilfe des Befehls RFCHECK können Sie überprüfen, ob RingFence installiert ist. Durch RingFence wird verhindert, daß Disketten benutzt werden, wenn sie nicht vorher auf dem Quarantänecomputer auf Viren überprüft worden sind. Dadurch kann die Benutzung jeder beliebigen Software verhindert werden, wobei gleichgültig ist, ob die Software sauber oder mit einem Virus infiziert ist. Weitere Informationen über RingFence erhalten Sie von Dr Solomon's.

Der Befehl hat die folgende Syntax:

```
TKUTIL RFCHECK
```

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
0	RingFence ist installiert.
1	RingFence ist nicht installiert.

Bestimmung des Wochentages

Mit Hilfe des Befehls `WEEKDAY` können Sie den Wochentag feststellen. Der Befehl hat die folgende Syntax:

```
TKUTIL WEEKDAY
```

Es wird eine Fehlerebene zwischen 1 und 7 zurückgegeben:

Fehlerebene	Bedeutung
1	Montag
2	Dienstag
3	Mittwoch
4	Donnerstag
5	Freitag
6	Samstag
7	Sonntag

Bestimmung des Monatstages

Mit Hilfe des Befehls `MONTHDAY` können Sie den Tag des Monats feststellen. Der Befehl hat die folgende Syntax:

```
TKUTIL MONTHDAY
```

Es wird eine Fehlerebene zwischen 1 und 31 zurückgegeben, durch die der Tag des Monats angegeben wird.

Sperren des Computers

Sie können den Befehl `LOCK` verwenden, um den Kaltstart des Computers zu erzwingen, falls ein Problem aufgetreten ist. Durch den Befehl wird die Tastenkombination Strg + Alt + Entf deaktiviert und der Benutzer zum Ausschalten des Computers gezwungen. Der Befehl hat die folgende Syntax:

```
TKUTIL LOCK
```

Ausgabe von Warnsignalen

Mit Hilfe des Befehls ALARM können Sie den Computer Warnsignale erzeugen lassen, wenn ein Problem auftritt. Der Befehl hat die folgende Syntax:

```
TKUTIL ALARM
```

Der Befehl bewirkt, daß bei einem Alarm eine blinkende Meldung angezeigt wird. Die Zeit, zu der der Alarm ausgelöst wurde, wird ebenfalls auf dem Bildschirm angezeigt.

Abspielen einer Melodie

Mit Hilfe des Befehls TUNE können Sie festlegen, daß bei einem Virusalarm eine von vier Melodien abgespielt wird. Der Befehl hat die folgende Syntax:

```
TKUTIL TUNE n
```

n ist eine Zahl zwischen 1 und 4.

Entfernung anderer Anti-Virus-Produkte

Wenn Sie bisher eine andere Anti-Virus-Software verwendet haben, können Sie mit Hilfe des Befehls FROM alle Verweise auf diese Software aus den Systemdateien löschen. Der Befehl hat die folgende Syntax (nach FROM steht kein Leerzeichen):

```
TKUTIL FROM[CPAV][NAV][MSAV] [<Laufwerk>\<Verzeichnis>]
```

Erläuterung:

CPAV	entfernt alle Verweise auf die Anti-Virus-Software Central Point.
NAV	entfernt alle Verweise auf die Norton Anti-Virus-Software.
MSAV	entfernt alle Verweise auf die Microsoft Anti-Virus-Software.
<Laufwerk>\ *<Verzeichnis>*	gibt an, wo die Software installiert ist. Wenn Sie diesen Parameter nicht angeben, werden Sie dazu aufgefordert.

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
255	Dateifehler.
0	Verweise entfernt.

Senden eines Formularvorschubzeichens an den Drucker

Durch den Befehl FORMFEED wird ein Formularvorschubzeichen an den Systemdrucker gesendet. Der Befehl hat folgende Syntax:

```
TKUTIL FORMFEED
```

Folgende Fehlerebenen werden zurückgegeben:

Fehlerebene	Bedeutung
1	Kein Drucker angeschlossen.
0	Formularvorschubzeichen gesendet.

Neustart von VirusGuard

Wenn Sie VirusGuard in einem Netzwerk ausführen, müssen Sie unter Umständen den Befehl REGUARD verwenden. Wenn Sie VirusGuard starten, bevor Sie sich im Netzwerk anmelden, funktioniert das Programm möglicherweise nicht einwandfrei, und Sie sollten es mit Hilfe des Befehls REGUARD erneut aktivieren. Der Befehl hat die folgende Syntax:

```
TKUTIL REGUARD
```

Der Befehl sollte am Ende des Anmeldeskripts stehen.

Neustart von speicherresidenten Programmen

Wenn Sie VirusGuard in einem Netzwerk ausführen, müssen Sie unter Umständen den Befehl RETSR ausführen. Durch diesen Befehl werden die speicherresidenten Programme nach der Anmeldung im Netzwerk erneut aktiviert und ihre einwandfreie Funktion sichergestellt. Der Befehl hat die folgende Syntax:

```
TKUTIL RETSR
```

Der Befehl sollte am Ende des Anmeldeskripts stehen. Wenn Sie RETSR verwenden, brauchen Sie REGUARD nicht zu verwenden.

Angabe technischer Informationen

Durch den Befehls TECHFILE wird eine Datei mit Systeminformationen erstellt, die den Inhalt der Dateien AUTOEXEC.BAT und CONFIG.SYS enthält. Falls Sie Probleme mit der Software haben und sich an die technische Unterstützung von Dr Solomon's wenden, werden Sie möglicherweise nach dieser Datei gefragt.

Der Befehl hat die folgende Syntax:

```
TKUTIL TECHFILE <Datei>
```

<Datei> gibt den Namen der zu erstellenden Datei an. Wenn Sie keinen Dateinamen angeben, wird die Datei TECHDATA.S&S genannt.

WTKUTIL

Tip

WTKUTIL wird nicht mit dem Toolkit für Windows NT geliefert. Benutzer von Windows NT können diesen Abschnitt ignorieren.

WTKUTIL ist ein Dienstprogramm zur Verwaltung der WinGuard-Installation. Es umfaßt verschiedene Befehle mit unterschiedlichen Funktionen.

Hinzufügen von WinGuard

Es gibt eine Funktion für die Änderung der Registrierung, so daß WinGuard beim Start von Windows 95 automatisch gestartet wird. Sie können diese Funktion verwenden, wenn Sie sich bei der Installation des Toolkit dafür entschieden haben, WinGuard nicht zu aktivieren.

Der Befehl hat die folgende Syntax:

```
WTKUTIL ADD WINGUARD <Toolkitpfad>
```

`Toolkitpfad` ist der vollständige Pfad des Toolkit-Verzeichnisses, das auch die ausführbare Datei von WinGuard enthält.

Entfernung von WinGuard

Wenn Sie WinGuard nicht über das Konfigurationsprogramm deaktivieren möchten, können Sie eine andere Funktion verwenden, bei der die Registrierung geändert wird, so daß WinGuard beim Start von Windows 95 nicht mehr automatisch gestartet wird.

Geben Sie folgenden Befehl ein:

```
WTKUTIL REMOVE WINGUARD
```

Überprüfung, ob WinGuard läuft

Es gibt eine Funktion, durch die eine Meldung angezeigt wird, ob WinGuard aktiviert ist. Wenn WinGuard geladen ist, wird die Fehlerebene 0 zurückgegeben; wenn es nicht geladen ist, die Fehlerebene 1.

Geben Sie folgenden Befehl ein:

```
WTKUTIL WINGUARDCHECK
```

Speichern der Einstellungen

Es gibt eine Funktion zum Speichern der aktuellen WinGuard-Einstellungen in einer Datei, im Textformat (.TXT). Wenn die Datei oder die Registrierung nicht geöffnet werden kann, wird die Fehlerebene 255 zurückgegeben; die Fehlerebene 0 wird zurückgegeben, wenn das Speichern erfolgreich war. Die Datei enthält Informationen über Optionen, deren Vorgabeeinstellungen geändert wurden.

Geben Sie folgenden Befehl ein:

```
WTKUTIL SAVESETTINGS WINGUARD <Dateiname>
```

Wiederherstellung von Einstellungen

Es gibt eine Funktion zum Ersetzen der aktuellen Einstellungen durch Einstellungen, die früher in einer Datei gespeichert wurden. Wenn die Datei nicht geöffnet werden kann, wird die Fehlerebene 255 zurückgegeben; Fehlerebene 0 wird zurückgegeben, wenn die Wiederherstellung erfolgreich war.

Geben Sie folgenden Befehl ein:

```
WTKUTIL LOADSETTINGS WINGUARD <Dateiname>
```

Vergleichen von Einstellungen

Es gibt eine Funktion zum Vergleich der aktuellen WinGuard-Einstellungen mit den Einstellungen, die in der angegebenen Datei gespeichert sind. Wenn die Einstellungen gleich sind, wird die Fehlerebene 1 zurückgegeben; die Fehlerebene 2 wird zurückgegeben, wenn die Einstellungen unterschiedlich sind, und Fehlerebene 255, wenn die Datei bzw. der Registrierungsabschnitt nicht geöffnet werden kann.

Geben Sie folgenden Befehl ein:

```
WTKUTIL CHECKSETTINGS WINGUARD <Dateiname>
```

Zusammenfassung aller Befehle

Sie erhalten eine Zusammenfassung der verfügbaren Befehle, wenn Sie folgenden Befehl eingeben:

```
WTKUTIL /?
```

oder

```
WTKUTIL /HELP
```

9.4 FindVirus-Fehlerebenen

FindVirus legt bei jeder Ausführung eine Fehlerebene fest. Sie können Fehlerebenen für bedingte Verzweigungen in Stapeldateien verwenden.

Um Fehlerebenen erfolgreich festzulegen, müssen Sie in der Stapeldatei folgenden Befehl eingeben:

```
start /w wfindv32 [Pfad[\Datei]] [/Parameter]
[/Parameter]...
```

Durch Angabe des Parameters `/exterror` (siehe nächster Abschnitt) können Sie einen erweiterten Satz von Fehlerebenen festlegen.

Die Standard-Fehlerebenen sind wie folgt:

255 Die Ausführung wurde durch den Benutzer abgebrochen.

2 Es wurde ein Virus gefunden.

1 Ein Problem ist aufgetreten, bei dem es sich nicht um einen Virus handelt. Der Grund kann zum Beispiel sein, daß eine Datei verschlüsselt ist oder von einer Anwendung benutzt wird. Diese Fehlerebene wird auch zurückgegeben, wenn FindVirus einen angegebenen Parameter nicht erkannt hat.

0 Es liegen keine Probleme vor.

Erweiterte Fehlerebenen von FindVirus

Durch Angabe des Parameters `/exterror` im Stapeldateibefehl zum Starten von FindVirus können Sie erweiterte Fehlerebenen festlegen (siehe voriger Abschnitt).

Die erweiterten Fehlerebenen sind wie folgt:

255 Die Ausführung wurde durch den Benutzer abgebrochen.

48 Dateivirus, Virus-Dropper oder Testvirus gefunden.

47 Partitionssektorvirus gefunden.

46	Bootsektorvirus gefunden.
45	Virus im Arbeitsspeicher gefunden.
44	Trojanisches Pferd gefunden.
22	Falsche Prüfsumme im Treiber.
21	Treiberdatei nicht gefunden.
20	Integritätsprüfung nicht bestanden.
11	Scherzprogramm gefunden.
10	Komprimierte Dateien gefunden.
1	Ein Problem ist aufgetreten, bei dem es sich nicht um einen Virus handelt. Der Grund kann zum Beispiel sein, daß eine Datei verschlüsselt ist oder von einer Anwendung benutzt wird. Diese Fehlerebene wird auch zurückgegeben, wenn FindVirus einen angegebenen Parameter nicht erkannt hat.
0	Es liegen keine Probleme vor.

Glossar

Aktualisierung	Eine neue Version des Toolkit, die aktualisiert wurde, um neu entdeckte Viren festzustellen. Aktualisierungen sind vierteljährlich oder monatlich erhältlich.
Alias	Anderer Name für einen *Virus*.
Ausführbare Datei	Eine Datei, die ein Programm enthält, das durch Eingabe des Dateinamens an der DOS-Eingabeaufforderung oder durch Klicken auf den Dateinamen in der vom Explorer angezeigten Programmliste aufgerufen werden kann.
AUTOEXEC.BAT	Diese Datei wird bei jedem Systemstart ausgeführt (gilt nicht für Windows NT). Für OS/2 wird die Datei AUTOEXEC.BAT bei jeder Ausführung einer Win-OS/2- oder DOS-Sitzung verwendet.
BBS	Bulletin Board System. Ein elektronisches Mail-System zum Senden von Nachrichten und Übertragen von Dateien.
BIOS	Basic Input/Output System. Programme, mit deren Hilfe beim Start des Computers das Betriebssystem geladen wird.
Bootsektor	Der Teil jeder Festplatte und Diskette, der vom Computer beim Systemstart gelesen wird.
Bootsektorvirus	Ein Virus, der in den *Bootsektor* einer Diskette übertragen wurde. Bootsektorviren infizieren den Bootsektor von Festplatten und häufig auch den *Partitionssektor*.
CARO	Computer Anti-Virus Researchers Organization. Mehrere Mitarbeiter von Dr Solomon's sind CARO-Mitglieder.

COM-Datei	Eine *ausführbare Datei* mit der Erweiterung .COM.
CONFIG.SYS	Diese Datei wird bei jedem Systemstart ausgeführt (gilt nicht für Windows NT).
Dateivirus	Ein Virus, der *ausführbare Dateien* infiziert. Wenn das entsprechende Programm ausgeführt wird, kopiert der Virus sich selbst. Die meisten Dateiviren sind *speicherresident*.
Defragmentierungs-programm	Ein Programm, das eine Festplatte neu organisiert, so daß verschiedene *Zuordnungseinheiten* jeder Datei möglichst zusammenhängend gespeichert werden. Dadurch wird der Festplattendurchsatz verbessert.
Dropper	Ein Programm, das weder selbst ein Virus noch mit einem Virus infiziert ist, bei der Ausführung jedoch einen Virus im Arbeitsspeicher, auf der Festplatte oder in einer Datei installiert. Dropper werden zum Teil als bequeme Träger von Viren und zum Teil als Sabotageakte geschrieben.
EICAR	European Institute for Computer Anti-Virus Research. Dr Solomon's ist Mitglied von EICAR.
EXE-Datei	Eine *ausführbare Datei* mit der Erweiterung .EXE.
Falscher Alarm	Die fälschliche Meldung eines Virus.
Festplatten-komprimierungs-programm	Ein Programm, das Dateien in komprimierter Form speichert, um eine maximale Ausnutzung des Speicherplatzes auf der Festplatte zu gewährleisten.
Formatierung	Die Methode, durch die ein Datenträger vorbereitet wird, bevor Daten auf ihn geschrieben werden. Der Formatierungsvorgang wird durch den Befehl FORMAT ausgelöst.

GDE	Generic Decryption Engine (allgemeine Entschlüsselungsroutinen). Ein Element von FindVirus, durch das die Anwendung in der Lage ist, auch die komplexesten polymorphen verschlüsselten Viren zu identifizieren.
Gerätetreiber	Ein Programm für die Steuerung der an den Computer angeschlossenen Hardware, wie zum Beispiel Laufwerke und Drucker.
Heuristisches Suchprogramm	Ein Element von FindVirus, das nach verdächtigem Code sucht, der möglicherweise auf einen neuen Virus hindeutet.
Hexadezimal	Darstellung mit der Basis 16.
Infizierte Datei	Eine Datei, die einen Virus enthält.
Logische Bombe	Eine Art von *trojanischem Pferd*, das durch bestimmte Konstellationen aktiviert wird.
Makrodatei	Eine Datei, die Anweisungen enthält, durch die von einem Programm auszuführende Funktionen angegeben werden.
Master Boot Record (MBR)	Der Partitionssektor einer Festplatte.
Multivalenter Virus	Ein Virus, der eine Kombination aus verschiedenen Verfahren nutzt, um sich auszubreiten, z. B. indem er sowohl Dateien als auch *Bootsektoren* infiziert.
Ordner	Eine logische Unterteilung eines Laufwerks, bei der Dateien in Gruppen angeordnet werden.
Partitionssektor	Der erste Teil einer Festplatte, der gelesen wird. Er enthält die Position und die Anzahl Sektoren jeder Partition.
Partitionssektorvirus	Ein Virus, der den normalen *Partitionssektor* einer Festplatte ersetzt.

Polymorpher Virus	Ein Virus, der versucht, der Entdeckung durch ein Virensuchprogramm zu entgehen, indem er sicherstellt, daß er kein festes Bytemuster hat. Das Toolkit kann polymorphe Viren mit Hilfe von allgemeinen Entschlüsselungsroutinen feststellen.
Prüfsumme	Eine eindeutige numerische Zeichenfolge, durch die eine Datei identifiziert wird. Prüfsummen werden von *Prüfsummenprogrammen* benutzt, um ausführbare Dateien auf Änderungen zu prüfen.
Prüfsummenprogramm	Ein Programm, das Viren feststellt, indem es *ausführbare Dateien* auf Änderungen überprüft. ViVerify ist ein Beispiel für ein Prüfsummenprogramm.
Public Domain-Software	Software, die legal kopiert und verteilt werden darf.
Quarantänecomputer	Ein Computer, auf dem eingehende Dateien und Disketten auf Viren überprüft werden.
Sauber	Virenfrei.
Scherzprogramm	Programme, mit denen jemand an der Nase herumgeführt werden soll. Es handelt sich dabei nicht um Viren, manchmal ist jedoch in einem Scherzprogramm ein Virus enthalten.
Schnellinfizierender Virus	Dateivirus, der ein Programm sowohl beim Öffnen oder Kopieren als auch bei der Ausführung infiziert.
Schreibschutz	Datenträger und Dateien können mit einem Schreibschutz versehen werden, damit nicht in sie geschrieben werden kann. Eine 5¼-Zoll-Diskette wird mit einem Schreibschutz versehen, indem ein Etikett über die Kerbe geklebt wird. Eine 3½-Zoll-Diskette wird schreibgeschützt, indem ein kleiner Plastikriegel nach oben geschoben wird, um die Öffnung zu schließen.

Shareware	Software, die legal kopiert werden darf, für die jedoch eine Registrierungsgebühr fällig wird, wenn sie dauerhaft verwendet wird.
Sicherung	Eine Kopie Ihrer Daten, die an einem anderen Ort gespeichert ist, als Vorsichtsmaßnahme für den Fall, daß die Kopie, mit der Sie arbeiten, verlorengeht oder beschädigt wird.
Softwarefehler	Ein unbeabsichtigter Fehler in einem Programm.
Speicherresidentes Programm	Ein Programm, das nach Ausführung im Arbeitsspeicher des Computers verbleibt. Diese Programme werden auch *TSR* oder *VxD* genannt.
Stammverzeichnis	Der oberste Ordner auf einem Laufwerk, in dem alle anderen Ordner und Dateien gespeichert sind.
Stapelverarbeitungs-programm	Eine Datei, die eine Reihe von Befehlen enthält, die durch Eingabe eines einzigen Befehls ausgeführt werden können. Stapelverarbeitungsdateien haben die Dateierweiterung .BAT.
Startdiskette	Eine Diskette, die Betriebssystemdateien enthält, mit denen der Computer gestartet werden kann.
Starten	Starten des Computers.
Stealth-Virus	Virus, der versucht, seine Entdeckung z verhindern, indem er sich tarnt. Stealth-Viren greifen in DOS- und *BIOS-Interruptleitungen* ein, um ihr Vorhandensein zu verbergen.
SYS-Datei	Eine Datei, meistens ein *Gerätetreiber*, mit der Erweiterung .SYS.
Treiberdatei	Eine Datei, die vom Toolkit dafür verwendet wird, die Identifizierung von und Berichterstellung über Viren zu aktivieren.

Trojanisches Pferd	Ein Programm, das einen unerwarteten Vorgang ausführt. Trojanische Pferde sind keine Viren, da sie sich nicht vermehren, sie verursachen jedoch häufig Schäden und werden vom Toolkit erkannt.
TSR	Terminate and Stay Resident. Ein DOS-Programm, das nach der Ausführung im Arbeitsspeicher verbleibt. Siehe *Speicherresident*.
Überschreibender Virus	Ein Virus, der die Dateien überschreibt, die er infiziert hat.
Variante	Eine Variante eines Virus, die meistens durch Ergänzung des Codes eines existierenden Virus verursacht wird.
Verzeichnis	Siehe „Ordner“.
Virensuchprogramm	Ein Programm, das Viren feststellt, indem es nach ihnen sucht. FindVirus ist ein Beispiel für ein Virensuchprogramm.
Virus	Ein Programm, das sich selbst reproduziert.
VxD	Virtueller Gerätetreiber. Ein Windows-Programm, das nach der Ausführung im Arbeitsspeicher verbleibt. Siehe *Speicherresident*.
Zeitbombe	Eine Art von *trojanischem Pferd*, das zu einem bestimmten Zeitpunkt aktiviert wird.

Index

A
Abspielen einer Melodie mit TKUTIL 197
ADD, Befehl 191
Adobe Acrobat Reader installieren
  OS/2 165
  Windows 3.x 158
  Windows 95 160
  Windows NT 162
Adressen xii
  CompuServe xiv
  Dr Solomon's xii
  Dr Solomon's Australien xiii
  Dr Solomon's Deutschland xii
  Dr Solomon's Großbritannien xiii
  Dr Solomon's USA xiii
  Technische Unterstützung xii
  World Wide Web xiv
ADUPDATE, Befehl 190
Aktivierung
  WinGuard 97
Aktualisierung
  DOS Toolkit 72
  OS/2-Toolkit 70
  Windows 3.x-Toolkit 65
  Windows 95-Toolkit 67
  Windows NT-Toolkit 68
Aktualisierung von CD-ROM
  DOS-Toolkit 72
  OS/2-Toolkit 70
  Windows 3.x-Toolkit 65
  Windows 95-Toolkit 67
  Windows NT-Toolkit 68
Aktualisierung von Dateien mit TKUTIL 190
Aktualisierung von Diskette
  DOS-Toolkit 73
  OS/2-Toolkit 71
  Windows 3.x-Toolkit 66
  Windows 95-Toolkit 67
  Windows NT-Toolkit 69
Aktualisierungen xi, 65
ALARM, Befehl 197
Angabe der Ausführung einer Stapeldatei mit TKUTIL 189
Angabe der speicherresidenten Toolkit-Programme mit TKUTIL 188
Angabe des Arbeitsspeichertyps mit TKUTIL 188
Angabe des freien Speicherplatzes mit TKUTIL 187
Angabe des Hauptprozessortyps mit TKUTIL 187
Angabe des Laufwerkstyps mit TKUTIL 187
Angabe des letzten Tastenanschlags mit TKUTIL 188
Angabe technischer Informationen mit TKUTIL 199
Ansicht
  Protokolldatei des Zeitplaners 144
Anti-Virus-Strategie 174
Arbeitsspeichertyp
  Angabe mit TKUTIL 188
ASCII-Code 188
Auflistung von speicherresidenten Programmen 188
Ausführung von Stapeldateien angeben 189
Ausgabe von Warnsignalen mit TKUTIL 197
Automatische Diskettenerkennung 155
Automatische Entfernung
  WinGuard für Windows 3.x und Windows 95 99
Automatische Überprüfung 77

B
Befehle
  ADD 191
  ADUPDATE 190
  ALARM 197
  CPU 187
  DELETE 193
  DRIVETYPE 187
  FORMFEED 198
  FROM 197
  GUARDCHECK 195
  LASTRUN 189
  LOCK 196
  MEMTYPE 188
  MKDIR 189
  MONTHDAY 196
  REGUARD 198
  RETKEY 188
  RETSR 198

RFCHECK 195
SEARCH 194
TECHFILE 199
TSRMAP 188
TUNE 197
UPDATE 190
WEEKDAY 196
Benutzerdefinierte Virensuche
FindVirus 83
Benutzerfehler 174
Bericht auf Drucker
Ergebnisse der Entfernung 152
Bericht in Datei 84
Ergebnisse der Entfernung 152
Besondere Hardware 1, 2
Bestimmung des Monatstages mit TKUTIL 196
Bestimmung des Wochentages mit TKUTIL 196
BIOS 205
Bootsektor 205
Bootsektor ersetzen 154, 155
Bulletin Boards 171, 175

C
CD-ROM-Installation
erweiterte Installationsoptionen 181
CleanBoot, Dienstprogramm 182
Disketten mit geändertem Format 184
CleanPart, Dienstprogramm 184
CMOS 176
CompuServe xiv
Computer sperren mit TKUTIL 196
CPU, Befehl 187

D
Dateien aktualisieren mit TKUTIL 190
Deaktivierung
WinGuard-Start beim Systemstart mit TKUTIL 194
Deinstallation
DOS-Toolkit 63
OS/2-Toolkit 54
Windows 3.x-Toolkit 19
Windows 95-Toolkit 38
Windows NT-Toolkit (Version 3.51) 50
Windows NT-Toolkit (Version 4)t 50
Deinstallation ohne Deinstallationsprogramm 179
DELETE, Befehl 193
Disketten mit geändertem Format 184
DOS
Bootsektor ersetzen 154
FindVirus 75
FindVirus, erweiterte Virensuche 83
Viren von Laufwerken entfernen 151
VirusGuard 79
VirusGuard, erweiterte Virensuche 92
ViVerify 77
ViVerify, erweiterte Virensuche 86
DOS-Toolkit
Aktualisierung von CD-ROM 72
Aktualisierung von Diskette 73
Deinstallation 63
Installation von CD-ROM 55
Installation von Diskette 60
Dr Solomon's
Adressen xii
Australien xiii
Deutschland xii
Großbritannien xiii
USA xiii
DRIVETYPE, Befehl 187

E
Entfernen
DOS-Toolkit 63
OS/2-Toolkit 54
Windows 3.x-Toolkit 19
Windows 95-Toolkit 38
Windows NT-Toolkit (Version 3.51) 50
Windows NT-Toolkit (Version 4) 50
Entfernen anderer Anti-Virus-Produkte mit TKUTIL 197
Erstellen eines neuen Verzeichnisses mit TKUTIL 189
Erstmalige Überprüfung 1
Erweiterte Fehlerebenen, FindVirus 202
Erweiterte Installationsoptionen 181
Extratreiber
Anmerkungen hinzufügen 100
WinGuard 100

F
Fehlerbehebung 179
Deinstallation ohne Deinstallationsprogramm 179
Diskette mit COMMAND.COM einlegen 180
erweiterte Einstellungen 179

fehlerhafte Datei MESSAGES.DRV 179
Toolkit-Installation stoppt Windows 95 180
Fehlerebenen, FindVirus 202
Fehlerhafte Meldungsdatei 179
Festplatte
Dienstprogramme zur Komprimierung 2
Festplattenspeicher 26, 32, 41, 44, 47
FindVirus 75
erweiterte Fehlerebenen 202
erweiterte Virensuche 83
Fehlerebenen 202
Überprüfung auf Viren 75
Verwendung 75
FORMFEED, Befehl 198
Freier Speicherplatz
Angabe mit TKUTIL 187
FROM, Befehl 197

G
GUARDCHECK, Befehl 195

H
Handbuch kopieren
OS/2 166
Windows 3.x 159
Windows 95 161
Windows NT 163
Hardware 2
Hardware, besondere 2
Hardwarenahe Software 172
Hardwarevoraussetzungen
Windows NT-Toolkit 39
Hauptprozessortyp 187
Angabe mit TKUTIL 187
Hilfe xii, 179
Hinzufügen von Text in einer Datei mit TKUTIL 191

I
Infizierte Dateien
löschen 153
umbenennen 153
INI-Dateien
Synchronisierung mit TKUTIL 191
Installation
Adobe Acrobat Reader für OS/2 165
Adobe Acrobat Reader für Windows 3.x 158
Adobe Acrobat Reader für Windows 95 160
Adobe Acrobat Reader für Windows NT 162
Aktualisierung für DOS 72
Aktualisierung für OS/2 70
Aktualisierung für Windows 3.x 65
Aktualisierung für Windows 95 67
Aktualisierung für Windows NT 68
Aktualisierungen 65
DOS-Toolkit 55
OS/2-Toolkit 51
Windows 3.x-Toolkit 7
Windows 95-Toolkit 21
Windows NT-Toolkit 40
Zeitplaner (für Windows 3.x) 9, 13, 17
Zeitplaner (für Windows 95) 23, 27, 33
Zeitplaner (für Windows NT) 41, 44, 48
Installation von Adobe Acrobat Reader
OS/2 165
Windows 95 160
Windows NT 162
Installation von Adobe Acrobat Reader und Kopieren des Handbuchs
Windows 3.x 168
Windows 95 168
Windows NT 168
Internet 171

K
Komprimierte Festplatte 206
Komprimiertes Laufwerk 1, 2
Konfiguration
WinGuard für Windows NT, Registerkarte „Ausgabe“ 117
WinGuard für Windows NT, Registerkarte „Ausnahmen“ 122
WinGuard für Windows NT, Registerkarte „Entfernung“ 116
WinGuard für Windows NT, Registerkarte „Erweitert“ 120
WinGuard für Windows NT, Registerkarte „FindVirus“ 119
WinGuard für Windows NT, Registerkarte „Info“ 121
WinGuard für Windows NT, Registerkarte „Meldung“ 118
WinGuard für Windows NT, Registerkarte „Operation“ 114
WinGuard für Windows NT, Registerkarte „Scanner“ 113
Kontaktadressen xii
Konventionen viii

Kopieren des Handbuchs
OS/2 166
Windows 3.x 159
Windows 95 161
Windows NT 163

L
Laden von Software 175
LASTRUN, Befehl 189
Laufwerk, komprimiert 2
Laufwerkstyp 187
Angabe mit TKUTIL 187
Letzter Tastenanschlag
Angabe mit TKUTIL 188
LOCK, Befehl 196
Logische Bomben 173
Löschen
infizierte Dateien 153
Text aus einer Datei mit TKUTIL 193

M
Makroviren 98
McAfee, Scanshield 7, 21, 40
Melodie
Abspielen mit TKUTIL 197
MEMTYPE, Befehl 188
Menü „Entfernen“
Bootsektor ersetzen 155
MKDIR, Befehl 189
Monatstag
Bestimmung mit TKUTIL 196
MONTHDAY, Befehl 196

N
Netzwerk
Virenbefall 171
Neues Verzeichnis
Erstellung mit TKUTIL 189
Neustart von speicherresidenten Toolkit-Programmen mit TKUTIL 198
Neustart von VirusGuard mit TKUTIL 198

O
OLE, überprüfen 94
Online-Dokumentation
OS/2 165
Windows 3.x 158
Windows 95 160
Windows NT 162
OS/2
Adobe Acrobat Reader installieren 165
Bootsektor ersetzen 154
FindVirus 75
FindVirus, erweiterte Virensuche 83
Handbuch kopieren 166
Online-Dokumentation 165
Viren von Laufwerken entfernen 151
ViVerify 77
ViVerify, erweiterte Virensuche 86
OS/2-Toolkit
Aktualisierung von CD-ROM 70
Aktualisierung von Diskette 71
Deinstallation 54
Installation von CD-ROM 51
Installation von Diskette 52

P
Partitionssektor 207
Probleme xii, 179
Deinstallation ohne Deinstallationsprogramm 179
Diskette mit COMMAND.COM einlegen 180
fehlerhafte Datei MESSAGES.DRV 179
Toolkit-Installation stoppt Windows 95 180

R
Ratschläge xii
Raubkopien 175
README-Dateien xii, 5, 172
Regelmäßige Aktualisierungen xi
Registerkarten
„Ausgabe“, WinGuard für Windows NT-Konfiguration 117
„Ausnahmen“, WinGuard für Windows-NT-Konfiguration 122
„Erweitert“, WinGuard für Windows NT-Konfiguration 120
„FindVirus“, WinGuard für Windows NT-Konfiguration 119
„Info“, WinGuard für Windows NT-Konfiguration 121
„Meldung“, WinGuard für Windows NT-Konfiguration 118
„Operation“, WinGuard für Windows NT-Konfiguration 114
Registrierung xi
REGUARD, Befehl 198

Reparaturdatenbank 87
RETKEY, Befehl 188
RETSR, Befehl 198
RFCHECK, Befehl 195
RingFence 195
  Installationsüberprüfung mit TKUTIL 195

S
Scanshield 7, 21, 40
Schaltflächen
  Entfernen 151
  Ersetzen 155
  Reparieren 151
  Suchen 76
Scherzprogramme 173
Schlüsselwort (ViVerify) 88, 90
SEARCH, Befehl 194
Senden eines Formularvorschubzeichens an den Drucker mit TKUTIL 198
SETUP 53, 71
Shareware 171
Sicherungen 174, 175
Software
  Konflikte vermeiden 7, 21, 40
Softwarefehler 171
Softwarekauf 175
Softwarevoraussetzungen
  Windows NT-Toolkit 39
SOS-Diskette
  besonderes Überprüfungsverfahren 2
  Standardüberprüfung 1
Speicher
  DOS 55
  OS/2 51
  Windows 3.x 6
  Windows 95 21
  Windows NT 39
Speicherresidente Toolkit-Programme
  Angabe mit TKUTIL 188
  Neustart mit TKUTIL 198
Sperren des Computers mit TKUTIL 196
Spiele 171
Stapeldatei-Ausführung
  Angabe mit TKUTIL 189
Startdiskette 209
Starten von WinGuard beim Systemstart mit TKUTIL 193
Suchen nach Text mit TKUTIL 194
Synchronisierung von .INI-Dateien mit TKUTIL 191
Systemdiskette 2
Systemvoraussetzungen
  DOS 55
  OS/2 51
  Windows 3.x 6
  Windows 95 21
  Windows NT 39

T
Tag des Monats bestimmen 196
TECHDATA.S&S 199
TECHFILE, Befehl 199
Technische Informationen
  Angabe mit TKUTIL 199
Technische Unterstützung xii
  Adressen xii
  Hinweis auf 10, 14, 18, 25, 31, 37, 42, 46, 50, 52, 53, 59, 62
Telefonnummern xii
Testen
  VirusGuard 92
Text
  Löschen aus einer Datei mit TKUTIL 193
  Suche mit TKUTIL 194
TKUTIL 185
  .INI-Dateien synchronisieren 191
  ADD 185, 191
  ADD WINGUARD 185
  ADUPDATE 185, 190
  ALARM 185, 197
  andere Anti-Virus-Produkte entfernen 197
  Arbeitsspeichertyp angeben 188
  Ausführung einer Stapeldatei angeben 189
  Computer sperren 196
  CPU 185, 187
  Dateien aktualisieren 190
  DELETE 185, 193
  DISKSPACE 185
  DRIVETYPE 185, 187
  Erläuterung 185
  FORMFEED 185, 198
  Formularvorschubzeichen an Drucker senden 198
  freien Speicherplatz angeben 187
  FROM 185, 197
  GUARDCHECK 185, 195
  Hauptprozessortyp angeben 187

INIUPDATE 185
LASTRUN 186, 189
Laufwerkstyp angeben 187
letzten Tastenanschlag angeben 188
LOCK 186, 196
Melodie abspielen 197
MEMTYPE 186, 188
MKDIR 186, 189
Monatstag bestimmen 196
MONTHDAY 186, 196
neues Verzeichnis erstellen 189
REGUARD 186, 198
REMOVE WINGUARD 186
RETKEY 186, 188
RETSR 186, 198
RFCHECK 186, 195
RingFence-Installation überprüfen 195
SEARCH 186, 194
speicherresidente Toolkit-Programme angeben 188
speicherresidente Toolkit-Programme neu starten 198
TECHFILE 186, 199
technische Informationen angeben 199
Text aus einer Datei löschen 193
Text in einer Datei hinzufügen 191
Textsuche 194
TSRMAP 186, 188
TUNE 186, 197
UPDATE 186, 190
VirusGuard neu starten 198
VirusGuard-Installation überprüfen 195
Warnsignale ausgeben 197
WEEKDAY 186, 196
WinGuard beim Systemstart starten 193
WinGuard-Start beim Systemstart deaktivieren 194
Wochentag bestimmen 196
Toolkit
Aktualisierungen xi
andere Versionen x
Installation stoppt Windows 95 180
Registrierung xi
Treiberdatei 209
Virensuchprogramm 210
Windows-Version 60, 73
zusätzliche Dienstprogramme 181
Toolkit-Installation
erweiterte Installationsoptionen 181
Treiber, besondere 2
Trojanische Pferde 173
TSRMAP, Befehl 188
TUNE, Befehl 197

U
Überprüfen der VirusGuard-Installation mit TKUTIL 195
Überprüfung
automatisch 77
bei Bedarf 75
erstmalig 1
Magic Bullet 1
Systemdiskette 2
Überprüfung auf Viren vor Installation 1, 2
Überprüfung der RingFence-Installation mit TKUTIL 195
Umbenennen
infizierte Dateien 153
Unterstützung xii
UPDATE, Befehl 190

V
Vermeiden, Softwarekonflikte 7, 21, 40
Verwandte Produkte x
Viren
Alias 205
Bootsetor 205
Dateiviren 206
Definition 169
Dropper 206
falscher Alarm 206
heuristisches Suchprogramm 207
infizierte Datei 207
logische Bombe 207
Makro 207
multivalente Viren 207
Partitionssektor 207
polymorphe Viren 208
Scherzprogramme 173, 208
schnellinfizierende Viren 208
Stealth-Viren 209
Trojanische Pferde 173, 210
über E-Mail 171
überschreibende Viren 210
Variante 210
Vorbeugung 174
Zeitbomben 173, 210

Viren entfernen
von Laufwerken 151
Viren suchen
Dialogfeld 83
Zusätzliche Einstellungen 84
Virenlexikon x
VirusGuard 79
bei Virenbefall 81
erweiterte Virensuche 92
Installationsüberprüfung mit TKUTIL 195
Neustart mit TKUTIL 198
Testen 92
Warnungt 81
ViVerify 77, 86
ausgeschlossene Dateien 87
Dateien überprüfen 90
erweiterte Virensuche 86
geänderte Dateien suchen 88
Papierkorb 87
Prüfsumme 208
Prüfsummen berechnen 88, 90
Prüfsummenprogramm 208
Reparaturdatenbank 87
Schlüsselwort 88, 90

W
Warndialogfeld
Benutzerdefinierte Meldung 111
Bisher-Liste 110
Warnsignale
Ausgabe mit TKUTIL 197
WEEKDAY, Befehl 196
Windows 3.x
Adobe Acrobat Reader installieren 158
Bootsektor ersetzen 154
FindVirus 75
FindVirus, erweiterte Virensuche 83
gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs 168
Handbuch kopieren 159
Online-Dokumentation 158
Viren von Laufwerken entfernen 151
VirusGuard 79
VirusGuard, erweiterte Virensuche 92
ViVerify 77
ViVerify, erweiterte Virensuche 86
WinGuard 77
WinGuard, allgemeine Hinweise 94
WinGuard, bei Virenbefall 105
WinGuard, Berichterstellung 103
WinGuard, Berichterstellung aktivieren 103
WinGuard, Einstellungen ändern 95
WinGuard, erweiterte Virensuche 93
WinGuard, Konfiguration ändern 94
WinGuard, Protokolldatei ansehen 104
WinGuard, Übersicht über Einstellungen 97
Zeitplan-Editor, allgemeine Umgebungseinstellungen 149
Zeitplan-Editor, aufrufen 123
Zeitplan-Editor, neues Ereignis erstellen 124
Zeitplan-Editor, Registerkarte „Einstellungen für Überprüfung“ 134
Zeitplan-Editor, Registerkarte „Einstellungen für Virensuche“ 128
Zeitplan-Editor, Registerkarte „Ereignis“ 124
Zeitplan-Editor, Registerkarte „Intervall“ 127
Zeitplan-Editor, Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“ 145
Zeitplaner, ausführen 138
Zeitplaner, Ereignisse aktivieren 141
Zeitplaner, Ereignisse ausschneiden und einfügen 142
Zeitplaner, Ereignisse bearbeiten 140
Zeitplaner, Ereignisse deaktivieren 141
Zeitplaner, Ereignisse kopieren und einfügen 143
Zeitplaner, Ereignisse löschen 141
Zeitplaner, Ereignisverwaltung 140
Zeitplaner, Gültigkeitsprüfung von Ereignissen 143
Zeitplaner, Protokolldatei 144
Zeitplaner, Protokolldatei anzeigen 144
Zeitplaner, Protokolldatei umbenennen 145
Windows 3.x-Toolkit
Aktualisierung von CD-ROM 65
Aktualisierung von Diskette 66
Deinstallation 19
erweiterte Installationsoption auf CD-ROM 10
Installation von CD-ROM 7
Installation von Diskette 15
Schnellinstallation von CD-ROM 7
Windows 95 97
Adobe Acrobat Reader installieren 160

Bootsektor ersetzen 154
FindVirus 75
FindVirus, erweiterte Virensuche 83
gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs 168
Handbuch kopieren 161
Online-Dokumentation 160
Probleme, Toolkit-Installation stoppt Windows 180
Viren von Laufwerken entfernen 151
VirusGuard 79
VirusGuard, erweiterte Virensuche 92
ViVerify 77
ViVerify, erweiterte Virensuche 86
WinGuard 77
WinGuard, allgemeine Hinweise 94
WinGuard, bei Virenbefall 105
WinGuard, Berichterstellung 103
WinGuard, Berichterstellung aktivieren 103
WinGuard, Einstellungen ändern 95
WinGuard, erweiterte Virensuche 93
WinGuard, Konfiguration ändern 94
WinGuard, Protokolldatei ansehen 104
Zeitplan-Editor, allgemeine Umgebungseinstellungen 149
Zeitplan-Editor, aufrufen 123
Zeitplan-Editor, neues Ereignis erstellen 124
Zeitplan-Editor, Registerkarte „Einstellungen für Überprüfung“ 134
Zeitplan-Editor, Registerkarte „Einstellungen für Virensuche“ 128
Zeitplan-Editor, Registerkarte „Ereignis“ 124
Zeitplan-Editor, Registerkarte „Intervall“ 127
Zeitplan-Editor, Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“ 145
Zeitplaner, ausführen 138
Zeitplaner, Ereignisse aktivieren 141
Zeitplaner, Ereignisse ausschneiden und einfügen 142
Zeitplaner, Ereignisse bearbeiten 140
Zeitplaner, Ereignisse deaktivieren 141
Zeitplaner, Ereignisse kopieren und einfügen 143
Zeitplaner, Ereignisse löschen 141
Zeitplaner, Ereignisverwaltung 140
Zeitplaner, Protokolldatei 144
Zeitplaner, Protokolldatei anzeigen 144
Zeitplaner, Protokolldatei umbenennen 145
Windows 95-Toolkit
Aktualisierung von CD-ROM 67
Aktualisierung von Diskette 67
Deinstallation 38
erweiterte Installationsoption auf CD-ROM 25
Installation von CD-ROM 21
Installation von Diskette 31
Schnellinstallation von CD-ROM 22
Windows NT 77, 124
Adobe Acrobat Reader installieren 162
Bootsektor ersetzen 154
FindVirus 75
FindVirus, erweiterte Virensuche 83
gleichzeitiges Installieren von Adobe Acrobat Reader und Kopieren des Handbuchs 168
Handbuch kopieren 163
Online-Dokumentation 162
Viren von Laufwerken entfernen 151
ViVerify 77
ViVerify, erweiterte Virensuche 86
WinGuard, bei Virenbefall 107
WinGuard, Einstellungen ändern 112
WinGuard, erweiterte Virensuche 107
WinGuard, Konfigurationsdienstprogramm starten 112
WinGuard, Warndialogfeld - Benutzerdefinierte Meldung 111
WinGuard, Warndialogfeld - Bisher-Liste 110
WinGuard-Konfiguration, Registerkarte „Ausgabe“ 117
WinGuard-Konfiguration, Registerkarte „Ausnahmen“ 122
WinGuard-Konfiguration, Registerkarte „Entfernung“ 116
WinGuard-Konfiguration, Registerkarte „Erweitert“ 120
WinGuard-Konfiguration, Registerkarte „FindVirus“ 119
WinGuard-Konfiguration, Registerkarte „Info“ 121
WinGuard-Konfiguration, Registerkarte „Meldung“ 118

WinGuard-Konfiguration, Registerkarte „Operation“ 114
WinGuard-Konfiguration, Registerkarte „Scanner“ 113
Zeitplan-Editor, allgemeine Umgebungseinstellungen 149
Zeitplan-Editor, aufrufen 123
Zeitplan-Editor, neues Ereignis erstellen 124
Zeitplan-Editor, Registerkarte „Einstellungen für Überprüfung“ 134
Zeitplan-Editor, Registerkarte „Einstellungen für Virensuche“ 128
Zeitplan-Editor, Registerkarte „Intervall“ 127
Zeitplan-Editor, Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“ 145
Zeitplaner, ausführen 138
Zeitplaner, Ereignisse aktivieren 141
Zeitplaner, Ereignisse ausschneiden und einfügen 142
Zeitplaner, Ereignisse bearbeiten 140
Zeitplaner, Ereignisse deaktivieren 141
Zeitplaner, Ereignisse kopieren und einfügen 143
Zeitplaner, Ereignisse löschen 141
Zeitplaner, Ereignisverwaltung 140
Zeitplaner, Protokolldatei 144
Zeitplaner, Protokolldatei anzeigen 144
Zeitplaner, Protokolldatei umbenennen 145
Zeitplaner-Dienst, Konfiguration 139
Windows NT-Toolkit
Aktualisierung von CD-ROM 68
Aktualisierung von Diskette 69
erweiterte Installationsoption auf CD-ROM 43
Installation von CD-ROM 40
Installation von Diskette 47
Schnellinstallation von CD-ROM 40
Windows NT-Toolkit (Version 3.51)
Deinstallation 50
Windows NT-Toolkit (Version 4)
Deinstallation 50
WinGuard 77
aktiviert 97
Alle Dateien überprüfen 97
Alle OLE-Dateien überprüfen 94, 98
Automatische Entfernung 99
bei Virenbefall 106
Berichterstellung 103
Bestätigung vor Virusentfernung 99
Dateiüberprüfung auf Laufwerken 100
DOS-Box bei Virusbefall schließen 99
erweiterte Virensuche 93
Extratreiber 100
Heuristische Suche, Programmdateien 99
Heuristische Suche, Word-Makros 99
Protokolldatei 105
Starten beim Systemstart mit TKUTIL 193
Treiberdatei 99
Überprüfen beim Schreiben 94
Warndialogfeld 107, 117
Warnmeldungen ändern 101
WinGuard für Windows 3.x und Windows 95
allgemeine Hinweise 94
bei Virenbefall 105
Berichterstellung 103
Berichterstellung aktivieren 103
Einstellungen ändern 95
Einstellungen, Übersicht 97
Konfiguration ändern 94
Protokolldatei ansehen 104
Testen 93
WinGuard für Windows NT
bei Virenbefall 107
Einstellungen ändern 112
erweiterte Virensuche 107
Konfiguationsdienstprogramm starten 112
Warndialogfeld - Benutzerdefinierte Meldung 111
Warndialogfeld - Bisher-Liste 110
WinGuard für Windows NT-Konfiguration
Registerkarte „Ausgabe“ 117
Registerkarte „Ausnahmen“ 122
Registerkarte „Entfernung“ 116
Registerkarte „Erweitert“ 120
Registerkarte „FindVirus“ 119
Registerkarte „Info“ 121
Registerkarte „Meldung“ 118
Registerkarte „Operation“ 114
Registerkarte „Scanner“ 113
WinGuard, Übersicht über Einstellungen 97
WinGuard-Start beim Systemstart deaktivieren mit TKUTIL 194
Wochentag
Bestimmung mit TKUTIL 196
World Wide Web xiv

WTKUTIL
Einstellungen speichern 200
Einstellungen vergleichen 201
Einstellungen wiederherstellen 201
Überprüfung, ob WinGuard läuft 200
WinGuard entfernen 200
WinGuard hinzufügen 199
Zusammenfassung aller Befehle 201
WTKUTIL, Dienstprogramm 199
WWW xiv

Z
Zeitbomben 173
Zeitplan-Editor
allgemeine Umgebungseinstellungen 149
aufrufen 123
neues Ereignis erstellen 124
neues Ereignis erstellen, Registerkarte „Einstellungen für Überprüfung“ 134
neues Ereignis erstellen, Registerkarte „Einstellungen für Virensuche“ 128
neues Ereignis erstellen, Registerkarte „Ereignis“ 124
neues Ereignis erstellen, Registerkarte „Intervall“ 127
Registerkarte „Einstellungen für Überprüfung“ 134
Registerkarte „Einstellungen für Virensuche“ 128
Registerkarte „Ereignis“ 124
Registerkarte „Intervall“ 127
Symbolleiste 124
Vorgabeeinstellungen im Dialogfeld „Neues Ereignis“ 145
Zeitplaner
ausführen 138
Ereignis hinzufügen 124
Ereignisse aktivieren 141
Ereignisse ausschneiden und einfügen 142
Ereignisse bearbeiten 140
Ereignisse deaktivieren 141
Ereignisse kopieren und einfügen 143
Ereignisse löschen 141
Ereignisverwaltung 140
FindVirus-Einstellungen 129
Gültigkeitsprüfung von Ereignissen 143
Intervalleinstellungen 127
Protokolldatei 144
Protokolldatei anzeigen 144
Protokolldatei umbenennen 145
ViVerify-Einstellungen 135
Zugriffs-Scanner 77
Zusätzliche Dienstprogramme 181
CleanBoot 182
CleanPart 184
TKUTIL 185
WTKUTIL 199