SYMANTEC.™

HINWEIS: SYMANTEC GEWÄHRT IHNEN EINE LIZENZ FÜR DIE IN DIESEM PAKET ENTHALTENE SOFTWARE AUSSCHLIESSLICH UNTER DER VORAUSSETZUNG, DASS SIE DIE BEDINGUNGEN DIESER LIZENZVEREINBARUNG IN VOLLEM UMFANG ANERKENNEN. BITTE LESEN SIE DIE BESTIMMUNGEN SORGFÄLTIG, BEVOR SIE DIESE VERPACKUNG ÖFFNEN. MIT DEM ÖFFNEN DER VERPACKUNG ERKLÄREN SIE SICH MIT DEN BESTIMMUNGEN DES LIZENZVERTRAGES EINVERSTANDEN. SOLLTEN SIE NICHT EINVERSTANDEN SEIN, GEBEN SIE BITTE DIE UNGEÖFFNETE DISKETTENPACKUNG ZUSAMMEN MIT ALLEN ZUM LIEFERUMFANG GEHÖRENDEN GEGENSTÄNDEN UNVERZÜGLICH GEGEN ERSTATTUNG DES KAUFPREISES AN DIE STELLE ZURÜCK, VON DER SIE DIESE BEZOGEN HABEN.

LIZENZ UND GARANTIE

Die mit dieser Lizenz erworbene Software (im folgenden als "Software" bezeichnet) ist Eigentum der Firma Symantec oder deren Lizenzgeber und ist durch nationale Gesetze und internationale Verträge urheberrechtlich geschützt. Mit der Annahme der Lizenzbedingungen erhalten Sie das Recht zur Benutzung der Software. Sofern nicht durch eine mit dieser Lizenz ausgelieferte Zusatzvereinbarung andere Regelungen getroffen werden, unterliegt die Nutzung der Software folgenden Bestimmungen:

Sie sind berechtigt:

a) Verwenden Sie eine Kopie der Software nur für einen einzigen Computer; falls der Datenträger in diesem Paket mehr als eine Sprachversion der Software und/oder mehrere Software-Titel enthält, gilt Ihre Lizenz nur für eine Sprache pro Software-Titel auf dem Datenträger (Sie sind nicht berechtigt, Kopien der verschiedenen Sprachversionen anzulegen) und Sie sind nicht berechtigt, solche andere Versionen an andere Personen weiterzuleiten oder anderen Personen die Benutzung solcher Versionen zu gestatten;.

b) eine Kopie der Software zu Archivierungszwecken anzufertigen oder die Software auf die Festplatte Ihres Computers zu kopieren und die Originaldisketten zu archivieren.

c) die Software in einem Netzwerk einzusetzen, vorausgesetzt, daß Sie über eine lizenzierte Kopie der Software für jeden Computer verfügen, der über das Netzwerk auf die Software zugreifen kann.

d) nach schriftlicher Benachrichtigung an Symantec die Software dauerhaft einem Dritten zu überlassen, vorausgesetzt, daß Sie alle Kopien der Software und der Begleitdokumentation übergeben und der Empfänger der Software sich mit den Bestimmungen dieser Lizenzvereinbarung einverstanden erklärt.

e) als Einzelperson, die den Computer, auf dem die Software installiert ist, zu mindestens 80% der Betriebszeit benutzt, die Software ebenfalls auf einem tragbaren Computer oder einem einzelnen Heimcomputer zu benutzen (nach Einsendung der ausgefüllten Registrierkarte, die der Software beiliegt).

Sie sind nicht berechtigt:

a) die mit der Software gelieferte Dokumentation zu kopieren.

b) die Software ganz oder teilweise zu verleihen oder zu vermieten oder Unterlizenzen zu vergeben.

c) die Software zurückzuentwickeln (reverse engineering), zu dekompilieren, zu disassemblieren oder auf andere Weise zu versuchen, den Quellcode der Software zugänglich zu machen, die Software zu ändern, zu übersetzen oder davon abgeleitete Produkte zu erstellen.

d) nach Erhalt eines Austauschdiskettensatzes oder einer Upgrade-Version als Ersatz für eine frühere Version die vorher erhaltene Kopie oder die frühere Version der Software zu benutzen, es sei denn, daß Sie die frühere Version nach einem Upgrade einer gemeinnützigen Organisation Ihrer Wahl zur Verfügung stellen und diese Organisation schriftlich erklärt, das Produkt als alleiniger Endbenutzer einzusetzen und die Bestimmungen dieser Vereinbarung einzuhalten. In allen anderen Fällen müssen nach dem Erwerb einer aktualisierten Version der Software alle Kopien früherer Versionen vernichtet werden.

Beschränkte Garantie

Symantec gewährleistet für sechzig (60) Tage ab Empfangsdatum, daß das Medium, auf dem die Software ausgeliefert wird, keine Material- und/oder Herstellungsmängel aufweist. Im Falle, daß das gelieferte Produkt dieser Garantie nicht genügt, besteht Ihr alleiniger Anspruch nach Wahl von Symantec entweder im Ersatz der zusammen mit einem Kaufnachweis an Symantec innerhalb der Garantiezeit zurückgegebenen fehlerhaften Erzeugnisse oder in der Erstattung des bezahlten Kaufpreises.

DIESE BESCHRÄNKTE GARANTIE IST AUSSCHLIESSLICH UND ANSTELLE ALLER ANDEREN GARANTIEN, SOWOHL AUSDRÜCKLICHER ALS AUCH IMPLIZIERTER ART, EINSCHLIESSLICH DER IMPLIZIERTEN GARANTIE DER VERKÄUFLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTÜBERTRETUNG. DIESE GARANTIE GIBT IHNEN BESTIMMTE GESETZLICHE RECHTE. SIE HABEN MÖGLICHERWEISE ANDERE RECHTE, DIE VON STAAT ZU STAAT UNTERSCHIEDLICH SIND.

Haftungsausschluß

UNABHÄNGIG DAVON, OB EINES DER HIERIN DARGELEGTEN RECHTSMITTEL SEINEN WESENTLICHEN ZWECK NICHT ERFÜLLT, IST SYMANTEC IN KEINEM FALLE ERSATZPFLICHTIG FÜR IRGENDWELCHE INDIREKTEN, FOLGE- ODER ÄHNLICHEN SCHÄDEN (EINGESCHLOSSEN SIND SCHÄDEN AUS ENTGANGENEM GEWINN ODER VERLUST VON DATEN), DIE AUFGRUND DER BENUTZUNG DER SOFTWARE ODER DER UNFÄHIGKEIT, DIE SOFTWARE ZU VERWENDEN, ENTSTEHEN, SELBST WENN SYMANTEC VON DER MÖGLICHKEIT SOLCHER SCHÄDEN UNTERRICHTET WORDEN IST.

EINIGE STAATEN ERLAUBEN DIE BESCHRÄNKUNG ODER DEN AUSSCHLUSS DER HAFTUNG FÜR BEGLEIT- UND FOLGESCHÄDEN NICHT, SO DASS DIE OBEN ANGEFÜHRTE BESCHRÄNKUNG ODER DER AUSSCHLUSS FÜR SIE MÖGLICHERWEISE NICHT ZUTRIFFT.

IN JEDEM FALLE IST DIE HAFTUNG VON SYMANTEC AUF DEN FÜR DIE SOFTWARE BEZAHLTEN KAUFPREIS BESCHRÄNKT. Der oben dargelegte Ausschluß und die Beschränkung sind unabhängig von Ihrer Annahme der Software.

Beschränkte Rechte der U.S.-Regierung

Erklärung beschränkter Rechte. Benutzung, Vervielfältigung oder Offenlegung durch die Regierung unterliegen den Beschränkungen des Unterparagraphen (c) (1) (ii) der Klausel über die Rechte an technischen Daten und Computer-Software unter DFARS 252.227-7013 oder den Unterparagraphen (c) (1) und (2) der Klausel über die beschränkten Rechte in bezug auf kommerzielle Computer-Software unter CFR 52.227-19, wie anwendbar, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

Allgemein

Diese Vereinbarung kann nur durch eine mit dieser Lizenz ausgelieferte Zusatzlizenzvereinbarung oder durch ein anderes, sowohl von Ihnen als auch von Symantec unterzeichnetes schriftliches Dokument geändert werden. Sollten Sie Fragen zu dieser Vereinbarung haben oder sich aus anderen Gründen mit Symantec in Verbindung setzen wollen, wenden Sie sich bitte an: Symantec (Deutschland), Grafenberger Allee 136, 40237 Düsseldorf, Tel.: 0211/9917-0, Fax: 0211/9917-222.

91-70-00065-GE
Jul. 1994

Norton AntiVirus™ für Windows 95
Benutzerhandbuch

SYMANTEC.™

NORTON AntiVirus™ Version 4.0

07-30-90190-GE
MIP001

Norton AntiVirus™ für Windows 95

Die in diesem Buch beschriebene Software wird Ihnen gemäß den Bedingungen eines Lizenzabkommens zur Verfügung gestellt und darf nur unter den darin beschriebenen Bedingungen eingesetzt werden.

Copyright

Warenzeichen

Gedruckt in Irland.

10 9 8 7 6 5 4 3 2 1

INHALTSVERZEICHNIS

Über dieses Handbuch

Konventionen ix

Installation

Systemanforderungen xi
Installieren von Norton AntiVirus für Windows 95 xii
    Viren während Installation entfernen xii
    Fragen bei der Installation xiii
Testen der Rettungs- und Startdiskette xiv
Nachträgliches Erstellen des Rettungsdiskettensatzes xv
Deinstallieren von Norton AntiVirus xv

Schnelleinstieg

Starten von Norton AntiVirus xvii
Maßnahmen zum Schutz vor Viren xix

Kapitel 1 Über Norton AntiVirus für Windows 95

Ist mein Computer vor Viren geschützt? 1
Was ist ein Computervirus? 2
Lebenszyklus eines Virus 3
So schützt Norton AntiVirus Ihren Computer vor Viren 5
    Manuelle Virusprüfung 6
    Geplante Prüfungen 7
    Prüfung beim Systemstart 7
    Auto-Protect 7
    Impfung 8
    Virusdefinitionsdateien 8
So warnt Sie Norton AntiVirus 9

Kapitel 2 Verwendung von Norton AntiVirus

Tips zum Vermeiden von Viren 11
Starten und Beenden von Norton AntiVirus 12
Hilfe 13
Durchführen von Virusprüfungen 15
Aktivieren und Deaktivieren von Auto-Protect 18
Umgehen von Auto-Protect beim Systemstart 20
Impfen von Dateien 21
    Dateien und Boot-Sektoren neu impfen 23
    Impfung von Dateien oder Ordnern aufheben 24
Anzeigen der Protokolldatei 25
Erstellen eines Rettungsdiskettensatzes 27
Planen von Virusprüfungen 28

Kapitel 3 Entfernen von Viren

Entfernen von Viren, die bei Virusprüfungen entdeckt wurden 33
Schaltflächen 36
Entfernen von Viren, die von Auto-Protect entdeckt wurden 38
Reaktion auf Warnmeldungen von Auto-Protect über Viren im Arbeitsspeicher 40
Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren 42
Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten 44
Reaktion auf Impfalarme von Auto-Protect 45
Entfernen von Viren, die während der Prüfung beim Systemstart entdeckt wurden 47
Reaktion auf Warnmeldungen der Prüfung beim Systemstart über Viren im Arbeitsspeicher 48
Reaktion auf Warnmeldungen der Prüfung beim Systemstart über entdeckte Viren 49
Was tun, wenn die Reparatur nicht erfolgreich war? 50
Datei kann nicht repariert werden 50
Systemdatei kann nicht repariert werden 50
Reparatur eines Boot-Sektors fehlgeschlagen 50
Viren aus komprimierten Dateien entfernen 51

Kapitel 4 Schutz vor neuen Viren

Automatische Aktualisierung der Virusdefinitionen 53
Planen einer automatischen LiveUpdate-Sitzung 54
Manuelle Aktualisierung der Virusdefinitionen 56
Bezugsquellen für aktuelle Virusdefinitionen 56
Neue Virusdefinitionsdateien installieren 59
Anzeigen der Virusliste 60

Kapitel 5 Anpassen von Norton AntiVirus

Anpassen manueller Prüfoptionen 63
Hinweise zur Virusprüfung von Netzlaufwerken 68
Zu prüfende Dateien wählen 69
Programmdatei-Erweiterungen festlegen 70
Verwalten von Ausnahmen 72
Anpassen von Warnmeldungen 76
Netzwerkwarnmeldungen senden 77
Anpassen der Protokolldatei 78
Einstellen der allgemeinen Prüfoptionen 80

Anpassen der automatischen Schutzfunktion 81
Programmdateien automatisch schützen 81
Schutz vor unbekannten Viren mit Virus-Sensor 85
Überwachung auf virusähnliche Aktivitäten 87
Disketten automatisch schützen 88
Anpassen der Virusprüfung beim Systemstart 89
Anpassen der Impfung 90
Einrichten eines Kennwortschutzes 94

Anhang A Über Computerviren

Was sind Computerviren 98
Ziele von Viren 100
Programmviren 100
Boot-Viren 101
Makroviren 102
Technologien von Viren 104
Wie Sie Ihren Schutz aktuell halten 106

Anhang B NAV-Rettungsdisketten

Entfernen von Viren von einem ausgeschalteten Computer 107
Wiederherstellen der Festplatte 108

Anhang C Befehlszeilenschalter

NAVDX.EXE 111
NAVW32.EXE 114
RESCUE.EXE 116

Anhang D Systemmeldungen

Meldungen und ihre Bedeutungen 117

Anhang E Problemlösungen

Lösungen für bekannte Probleme 127

Glossar

Index

Kundendienst und technische Unterstützung

Über dieses Handbuch

Dieses Handbuch enthält alle nötigen Informationen zur Verwendung von Norton AntiVirus für Windows 95. Wenn Sie Norton AntiVirus installieren und die voreingestellten Optionen übernehmen, ist Ihr Computer vor Computerviren geschützt. Während des Installationsvorgangs wird Ihr Computer auf Viren geprüft. Nach der Installation bieten die automatischen Schutzfunktionen von Norton AntiVirus einen kontinuierlichen Schutz für Ihren Computer.

In diesem Handbuch erfahren Sie, wie Sie Viren entdecken und entfernen und wie Sie sicherstellen, daß Ihr Virenschutz immer auf dem neuesten Stand ist.

Konventionen

In diesem Handbuch werden die folgenden Konventionen verwendet.

Hinweis:	Enthält eine Erklärung oder eine Ausnahme.
Tip:	Enthält einen Tip oder eine Abkürzung.
Achtung:	Enthält eine Warnung über einen Umstand, der zu unerwarteten oder zerstörerischen Effekten bei Daten oder Software führen kann.
GROSSBUCHSTABEN	Pfad, Verzeichnis oder Datei.
Anführungszeichen	Menüs, Befehle, Dialogfenster, Optionen.
Taste+Taste	Tastenkombination. Halten Sie die erste Taste gedrückt, und drücken Sie die zweite Taste.
`Courier`	Text, den Sie mit der Tastatur eingeben oder auf dem Bildschirm sehen.
[Parameter]	Optionaler Befehlsparameter.. Geben Sie den Text ein, der in den eckigen Klammern steht, nicht aber die eckigen Klammern selbst.
Parameter|Parameter	Notwendige Parameteroptionen. Geben Sie nur einen Parameter ein.
wählen	Einen Befehl in einem Menü hervorheben und klicken, um ihn auszuführen.
auswählen	Eine Option mit der Maus oder einer Pfeiltaste hervorheben.

INSTALLATION

Wenn Sie Norton AntiVirus mit den Optionen installieren, die vom Installationsprogramm vorgegeben werden, ist der umfassende Virusschutz Ihres Computers gewährleistet, sobald Sie Ihren Computer neu starten. Zum Virusschutz zählen die folgenden Funktionen und Komponenten:

- Automatisches Laden von Norton AntiVirus bei jedem Systemstart
- Rettungsdisketten zum Starten Ihres Systems von Diskette, falls dies erforderlich sein sollte
- Mit Scheduler festgelegte, wöchentliche Prüfung Ihres Systems
- Schutz beim Herunterladen von Dateien aus dem Internet.

Systemanforderungen

Die Mindestsystemanforderungen sehen wie folgt aus:

- IBM PC oder kompatibler Rechner mit 486-Prozessor (oder höher)
- 8 MB großer RAM-Speicher
- Microsoft Windows 95
- 10 MB freier Festplattenbereich für die Dateien von Norton AntiVirus

Zusätzlich benötigen Sie:

- Drei 1,44-MB-Disketten und drei Diskettenetiketten (für den Rettungsdiskettensatz).

WOFÜR? Als letzter Schritt der Installation werden Sie aufgefordert, einen eigenen Rettungsdiskettensatz zu erstellen. Diese Rettungsdisketten sind eine elementare Komponente des Virusschutzes für Ihr System. Mit ihnen können Sie Ihr System neu starten, falls ein Virus im Speicher Ihres Computers entdeckt wird. Durch das Starten von Diskette können Sie den Virus aus dem Speicher entfernen und so seine weitere Ausbreitung verhindern.

Installieren von Norton AntiVirus für Windows 95

Den größtmöglichen Schutz Ihres Computers erzielen Sie, wenn Sie in allen vom Installationsprogramm angezeigten Bildschirmen auf „Weiter“ klicken, d.h. die von Norton AntiVirus vorgegebene Option oder Einstellung akzeptieren.

So starten Sie das Installationsprogramm für Windows 95:

1. Führen Sie einen der folgenden Schritte aus:
   - Installation von CD-ROM: Legen Sie die CD-ROM in das CD-ROM-Laufwerk Ihres Computers ein. Das Installationsprogramm für Norton AntiVirus wird automatisch gestartet.
   - Installation von Diskette: Legen Sie die Norton AntiVirus Diskette 1 in das Laufwerk A: Ihres Computers ein. Klicken Sie anschließend auf „Start“ in der Task-Leiste, wählen Sie „Ausführen“, geben Sie im nachfolgenden Dialogfeld den Befehl `A:SETUP` ein, und klicken Sie auf „OK“.
2. Befolgen Sie die Anleitungen, die auf dem Bildschirm angezeigt werden. *Hinweise zu Fragen, die Sie während der Installation beantworten müssen, finden Sie auf* *Seite xiii*.

   Kann Norton AntiVirus wegen eines Virus auf Ihrem System nicht installiert werden, befolgen Sie die Anweisungen im nachfolgenden Abschnitt „Viren während Installation entfernen“.
3. Testen Sie Ihre Norton AntiVirus Rettungs- und Startdiskette. Wie Sie dies tun, erfahren Sie auf Seite xiii.

Viren während Installation entfernen

Wenn Sie das Installationsprogramm von Norton AntiVirus starten, wird vor der eigentlichen Installation Ihr System auf Viren geprüft. Wird bei dieser Prüfung ein Virus entdeckt, müssen Sie mit Hilfe der Rettungsdiskette, die zum Lieferumfang von Norton AntiVirus gehört, den Virus entfernen. Erst danach können Sie die Installation von Norton AntiVirus fortsetzen und zu Ende führen.

So entfernen Sie einen Virus mit Hilfe der Rettungsdiskette:

1. Schalten Sie Ihren Computer mit dem Netzschalter aus.
2. Legen Sie die mit Norton AntiVirus gelieferte Rettungsdiskette in Laufwerk A: ein.
3. Schalten Sie Ihren Computer ein.

   Warten Sie, bis der Startbildschirm des Rettungsprogramms von Norton AntiVirus angezeigt wird.

4 Drücken Sie im Startbildschirm die Eingabetaste, um das Rettungsprogramm zu starten.

Nachdem das Rettungsprogramm geladen wurde, was einige Minuten dauern kann, wird Ihr Computer geprüft. Dabei werden die gefundenen Viren beseitigt.

Fragen bei der Installation

Norton AntiVirus unterstützt Sie bei der Installation durch ausführliche Anleitungen und durch das Hervorheben der empfohlenen Einstellungen und Optionen. Im Zuge der Installation müssen Sie die folgenden Etnscheidungen treffen:

Frage	Empfehlung	Begründung
In welchem Ordner soll Norton AntiVirus installiert werden?	Akzeptieren Sie den Standardordner: `C:\Programme\Norton AntiVirus`	Es gibt keinen Grund, der dagegen spricht. Wählen Sie einen anderen Ordner nur, wenn dies aus triftigen Gründen erforderlich ist.
Soll wöchentlich eine automatische Prüfung der Festplatten erfolgen?	Vergewissern Sie sich, daß das Kontollkästchen aktiviert ist.	Durch die wöchentliche Prüfung stellen Sie sicher, daß Ihr Computer frei von Viren bleibt.
Soll Auto-Protect automatisch gestartet werden?	Vergewissern Sie sich, daß das Kontollkästchen aktiviert ist.	Auto-Protect überwacht Ihren Computer, solange er eingeschaltet ist, und schützt Sie so wirksam vor einer Infizierung.
Soll der Computer beim Systemstart geprüft werden?	Vergewissern Sie sich, daß das Kontollkästchen aktiviert ist.	Auf diese Weise können Sie immer sicher sein, daß wichtige Systemdateien frei von Viren sind.
Norton AntiVirus hat einen Netscape-Browser entdeckt. Soll das Zusatzmodul für Netscape installiert werden?	Antworten Sie mit „Ja“.	Sie ermöglichen damit, daß Norton AntiVirus Dateien prüft, die mit dem Netscape-Browser heruntergeladen werden.
Sollen Rettungsdisketten erstellt werden?	Wir empfehlen Ihnen dringend, einen eigenen Rettungsdiskettensatz zu erstellen.	Die Rettungsdisketten können bei der Infizierung Ihres Computers mit bestimmten Viren buchstäblich die letzte Rettung sein.

Frage	Empfehlung	Begründung
Soll nach Abschluß der Installation LiveUpdate gestartet werden?	Vergewissern Sie sich, daß das Kontollkästchen aktiviert ist, wenn Sie ein Modem oder eine Internet-Verbindung haben.	LiveUpdate stellt die Verbindung zu einem Symantec-Server her, um von dort die neuesten Virusdefinitionen auf Ihren Computer zu laden.
Soll nach Abschluß der Installation das System geprüft werden?	Vergewissern Sie sich, daß das entsprechende Kontollkästchen aktiviert ist.	Durch die Prüfung stellen Sie sicher, daß Ihr Computer frei von Viren ist.
Soll der Computer nach Abschluß der Installation neu gestartet werden?	Wählen Sie „Ja“.	Durch den Neustart wird der umfassende Virusschutz für Ihren Computer aktiviert.

Testen der Rettungs- und Startdiskette

Norton AntiVirus erstellt die Rettungs- und Startdiskette nur für das Startlaufwerk, nicht für alle Laufwerke. Sie sollten die Rettungs- und Startdiskette, nachdem Sie sie erstellt haben, stets testen, um sicherzustellen, daß Sie Ihren Computer damit ordnungsgemäß starten können.

So testen Sie die Rettungs- und Startdiskette von Norton AntiVirus:

1. Klicken Sie in der Task-Leiste von Windows auf „Start“, wählen Sie „Beenden“ und danach „Windows herunterfahren“.
2. Schalten Sie den Computer mit dem Netzschalter aus.
3. Legen Sie die Rettungs- und Startdiskette (Diskette 1) in Laufwerk A: ein, und schalten Sie Ihren Computer ein.

   Während des Startvorgangs wird eine Meldung des Rettungsprogramms von Norton AntiVirus angezeigt. Diese Meldung können Sie ignorieren.
4. Geben Sie an der DOS-Eingabeaufforderung den Befehl `C:` ein, und drücken Sie die Eingabetaste.

   Wird auf dem Bildschirm die DOS-Meldung `C:\>` angezeigt, d.h., ist der Wechsel zu Ihrer Festplatte möglich, so bedeutet dies, das Ihre Norton AntiVirus Rettungs- und Startdiskette ordnungsgemäß funktioniert.

   Falls der Startvorgang mit der Rettungs- und Startdiskette nicht erfolgreich ist, befolgen Sie die Anleitungen im Abschnitt „Meine Norton AntiVirus Rettungs- und Startdiskette funktioniert nicht.“ auf Seite 127.
5. Schieben Sie den Schreibschutzschalter auf der Rückseite der Diskette nach oben, um den Schreibschutz für die Diskette zu aktivieren.

Nachträgliches Erstellen des Rettungsdiskettensatzes

Wenn Sie während der Installation keinen eigenen Rettungsdiskettensatz erstellt haben, sollten Sie dies unmittelbar nach Abschluß der Installation nachholen. Legen Sie hierzu drei 1,44-MB-Disketten sowie drei Etiketten bereit.

So erstellen Sie den Rettungsdiskettensatz:

1. Klicken Sie in der Task-Leiste auf „Start“, zeigen Sie auf „Programme“, wählen Sie Programmgruppe „Norton AntiVirus“ aus, und klicken Sie auf die Option zum Erstellen der Rettungsdisketten.
2. Befolgen Sie die Anleitungen, die auf dem Bildschirm angezeigt werden.
3. Testen Sie die Rettungs- und Startdiskette (Diskette 1). Die Anleitung dazu finden Sie auf Seite xiv.

Deinstallieren von Norton AntiVirus

So deinstallieren Sie Norton AntiVirus:

- Klicken Sie in der Task-Leiste auf „Start“, zeigen Sie auf „Programme“, wählen Sie Programmgruppe „Norton AntiVirus“ aus, und klicken Sie auf „Norton AntiVirus deinstallieren“.

S C H N E L L E I N S T I E G

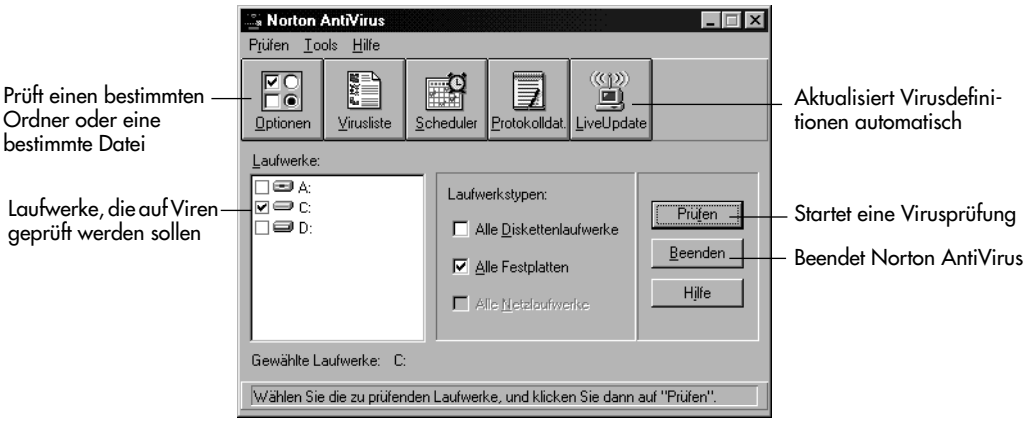
Starten von Norton AntiVirus

So starten Sie Norton AntiVirus:

- Klicken Sie auf „Start“ in der Windows-Task-Leiste. Zeigen Sie zunächst auf „Programme“ und anschließend auf „Norton AntiVirus“. Klicken Sie dann auf „Norton AntiVirus“.

  Das Hauptfenster von Norton AntiVirus für Windows 95 wird geöffnet.

Abbildung 0-1 Hauptfenster von Norton AntiVirus



So prüfen Sie ein oder mehrere Laufwerke auf Viren:

- Wählen Sie im Hauptfenster von Norton AntiVirus im Listenfeld „Laufwerke“ die zu prüfenden Laufwerke aus, und klicken Sie auf „Prüfen“.

So prüfen Sie eine bestimmte Datei oder einen bestimmten Ordner:

- Wählen Sie im Hauptfenster von Norton AntiVirus „Datei“ im Menü „Prüfen“.
- Wählen Sie im Hauptfenster von Norton AntiVirus „Ordner“ im Menü „Prüfen“.

So erhalten Sie Hilfe bei der Arbeit mit Norton AntiVirus:

1. Setzen Sie den Mauszeiger über die gewünschte Option, und klicken Sie mit der rechten Maustaste, um das Einblendmenü aufzurufen.
2. Wählen Sie eine der folgenden Menüoptionen aus:

- „Direkthilfe“ zeigt eine kurze Beschreibung der Option an.
- „Wie kann ich“ zeigt ein Untermenü für die entsprechende Option an.
- „Hilfethemen“ zeigt das Inhaltsverzeichnis des gesamten Hilfesystems an.

Wenn Sie eine vollständige Installation durchgeführt haben und die vorgeschlagenen Optionen übernommen haben, sind die Auto-Protect-Prüfung und die Prüfungen beim Systemstart bereits aktiviert. Außerdem ist eine automatische, wöchentliche Prüfung aller Ihrer Festplatten eingerichtet.

So aktivieren Sie Auto-Protect:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Auto-Protect“.
3. Aktivieren Sie „Auto-Protect beim Systemstart laden“.
4. Klicken Sie auf „OK“.

So aktivieren Sie die Prüfungen beim Systemstart:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Systemstart“.
3. Aktivieren Sie im Gruppenfeld „Prüfen“ die Optionen „Speicher“, „Master-Boot-Sektor“, „Boot-Sektoren“ und „Systemdateien“.
4. Klicken Sie auf „OK“.

Maßnahmen zum Schutz vor Viren

Um Ihren Computer virenfrei zu halten, beachten Sie die folgenden Regeln:

- Aktualisieren Sie Ihre Virusdefinitionsdateien jeden Monat. Nur so ist ein maximaler Schutz gegen neu entdeckte Viren gewährleistet. In Kapitel 4 „Schutz vor neuen Viren“ finden Sie eine Anleitung hierzu.
- Prüfen Sie mindestens einmal pro Woche alle Festplatten, um sicherzustellen, daß sie virenfrei sind.
- Prüfen Sie alle neuen Dateien und Disketten, bevor Sie sie verwenden.
- Erstellen Sie einen Norton AntiVirus-Rettungsdiskettensatz, mit dem Sie beschädigte Festplatten sowie Daten, die von bestimmten Boot-Viren befallen sind, wiederherstellen können. Weitere Informationen hierzu finden Sie unter „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27.
- Erstellen Sie regelmäßig Sicherungskopien Ihrer Festplatte.
- Erwerben Sie nur legale Kopien von Programmen, und erstellen Sie schreibgeschützte Sicherungskopien.

K A P I T E L 1

Über Norton AntiVirus für Windows 95

Norton AntiVirus für Windows 95 ist das wahrscheinlich am weitesten entwickelte und leistungsstärkste Programm zum Schutz Ihres Computers vor allen Arten von Virusinfektionen. Es bietet Schutz vor Viren, die sich über Festplatten oder Disketten ausbreiten, vor Viren, die sich über Netzwerke ausbreiten, und sogar vor Viren, die über das Internet übertragen werden.

Ist mein Computer vor Viren geschützt?

Wenn Sie Norton AntiVirus installieren und die voreingestellten Optionen übernehmen, ist Ihr Computer geschützt. Während des Installationsvorgangs wird Ihr Computer auf Viren geprüft. Nach der Installation bieten die automatischen Schutzfunktionen von Norton AntiVirus einen kontinuierlichen Schutz für Ihren Computer. Und falls ein Virus gefunden wird, können Sie ihn mit Hilfe von Norton AntiVirus problemlos entfernen.

Es ist nicht schlimm, wenn Sie wenig über Computer wissen. Da die voreingestellten Optionen von Norton AntiVirus eine Kombination aus Effektivität und maximalem Schutz bieten, müssen Sie keine Änderungen daran vornehmen. Sie installieren Norton AntiVirus einfach und sind sofort vor allen Computerviren geschützt.

Das führt Norton AntiVirus automatisch durch:

- Systemdateien und Boot-Sektoren beim Systemstart auf Viren prüfen.
- Programme beim Starten auf Viren prüfen.
- Computer einmal pro Woche auf Viren prüfen.
- Computer auf Aktivitäten hin überwachen, die von einem aktiven Virus verursacht sein könnten.
- Disketten bei der Verwendung auf Boot-Viren prüfen.

Das können Sie mit Norton AntiVirus tun:

- Bestimmte Dateien, Ordner oder ganze Laufwerke auf Viren prüfen.
- Virusprüfungen für bestimmte Zeiten planen.
- Virusdefinitionsdateien monatlich aktualisieren.
- Den Schutz durch Norton AntiVirus so anpassen, daß er dem Risikograd für eine Virusinfektion in Ihrer Arbeitsumgebung entspricht.

Was ist ein Computervirus?

Ein Computervirus ist, einfach ausgedrückt, ein Computerprogramm, das von einem Programmierer mit schlechten Absichten geschrieben wurde. Wenn ein Virusprogramm gestartet wird, hängt es eine Kopie seiner selbst an ein anderes Computerprogramm an. Immer, wenn das so infizierte Programm anschließend gestartet wird, tritt der Virus in Aktion und hängt sich an weitere Programme an. Beispielsweise kann ein Computervirus, den Sie über das Starten eines infizierten Programms von einer geliehenen Diskette erhalten haben, weitere Programme auf Ihrem Computer infizieren. Ein Computervirus existiert, um sich zu reproduzieren, und ähnelt in dieser Hinsicht einem biologischen Virus.

Manche Computerviren sind nicht nur auf Vermehrung programmiert. Sie zerstören Daten, indem sie Programme schädigen, Dateien löschen oder sogar Ihre gesamte Festplatte neu formatieren. Die meisten Viren sind allerdings nicht darauf programmiert, ernsthaften Schaden anzurichten; sie vermehren sich lediglich oder zeigen Meldungen an.

Viren können nur Dateien infizieren und Daten zerstören. Sie infizieren oder beschädigen keine Hardware wie Tastaturen oder Monitore. Wenn merkwürdige Effekte wie Bildschirmverzerrungen oder fehlende Zeichen auftreten, hat ein Virus lediglich die Programme, die den Bildschirm oder die Tastatur steuern, beschädigt. Auch befallene Laufwerke bzw. Disketten sind nicht selbst beschädigt; lediglich die darauf gespeicherten Daten sind betroffen.

Computerviren werden nach den Objekten klassifiziert, die sie infizieren:

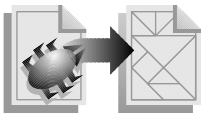
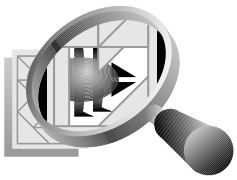
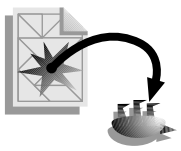
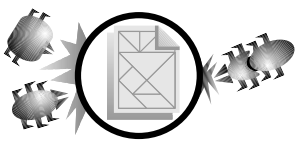
- **Programmviren:** Sie infizieren ausführbare Dateien, z.B. Textverarbeitungsprogramme, Tabellenkalkulationsprogramme, Computerspiele oder Betriebssystemprogramme.
- **Boot-Viren:** Einige Viren können Laufwerke oder Disketten infizieren, indem sie sich dort an bestimmte Programme in Bereichen anhängen, die *Boot-Sektor* und *Master-Boot-Sektor* genannt werden. Diese Bereiche enthalten die Programme, die Ihr Computer zum Starten benötigt.
- **Makroviren:** In vielen Textverarbeitungs- und Tabellenkalkulationsprogrammen können Sie eine Reihe von Aktionen als Makro aufzeichnen. Später können Sie dieses Makro dann ausführen und damit die aufgezeichneten Aktionen wiederholen. Makroviren infizieren *Datendateien mit Makrofähigkeit*. Beispielsweise können Dokument- und Vorlagendateien von Microsoft Word von Makroviren befallen werden.

Lebenszyklus eines Virus

Es gibt drei Phasen im Leben von Computerviren: *Infektion, Erkennung* und *Behandlung*. In der Infektionsphase wird eine Datei auf Ihrem Computer infiziert. In der zweiten Phase wird der Virus identifiziert und isoliert. In der Behandlungsphase wird der Virus entfernt. Wenn der Virus nicht entfernt wird, infiziert er weitere Dateien und zerstört möglicherweise Daten auf Ihrem Computer. Weitere Informationen dazu finden Sie in Tabelle 1-1, „Einzelheiten über den Lebenszyklus eines Virus“, auf Seite 4.

Norton AntiVirus verhindert, daß Viren Ihren Computer infizieren oder sich weiter ausbreiten. Es identifiziert und entfernt Viren, die es auf Ihrem Computer findet. Trotzdem sind *vorbeugende Maßnahmen* der beste Schutz gegen Computerviren. Mit den Funktionen zum automatischen Schutz können Sie verhindern, daß Ihr Computer überhaupt von Viren befallen wird.

Tabelle 1-1 Einzelheiten über den Lebenszyklus eines Virus

Infektion 	**Infektionsquelle**	Wiederverwendete Disketten unbekannter Herkunft Disketten von Zuhause oder aus der Schule Von Freunden geliehene Disketten Von einem BBS oder Online-Service heruntergeladene Programme Billige Software (von dubiosen Händlern) Wieder eingeschweißte oder geöffnete Software-Pakete Raubkopierte Software Vorformatierte Disketten
	Infektion	Start mit einer infizierten Diskette Neustart mit einer im Laufwerk verbliebenen, infizierten Diskette Starten eines infizierten Programms
	Verbreitung	Austausch von Disketten oder infizierten Programmen Anmeldung bei einem Netzwerk
Erkennung 	**Beobachtung**	Merkwürdiges Systemverhalten Dateien fehlen oder Programme laufen nicht
	Dienstprogramm	Ein Virus wird von einer Antivirus-Software erkannt
Behandlung 	**Entfernung**	Programme von Master-Disketten neu installieren Dateien mit einer Antivirus-Software reparieren Dateien von einer virusfreien Backup-Kopie wiederherstellen
	Nachbehandlung	Alle Dateien prüfen, um die Infektionsquelle zu finden Alle Disketten prüfen, um die Infektionsquelle zu finden Möglicherweise infizierte Backups löschen Virusschutz für eine Weile erhöhen
Vorsorge 		Verwenden Sie Norton AntiVirus, um Virusinfektionen zu vermeiden.

So schützt Norton AntiVirus Ihren Computer vor Viren

Computerviren lassen sich, unabhängig von ihrem Ziel, in zwei Klassen unterteilen:

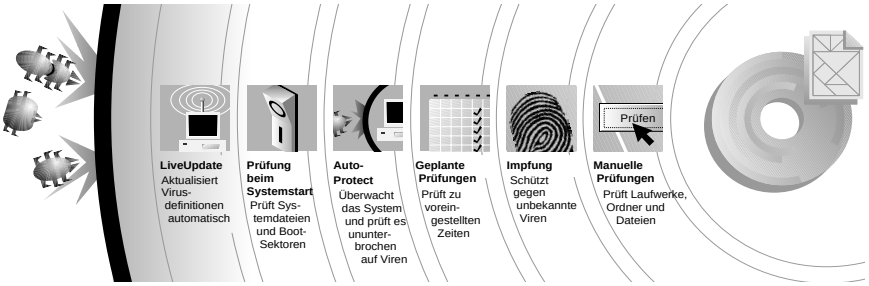
- **Bekannte Viren:** Ein *bekannter Virus* ist ein Virus, der bereits identifiziert wurde. Die Techniker von Symantec arbeiten Tag und Nacht, um anhand von Berichten über Virenbefall neue Computerviren zu identifizieren. Sobald ein Virus identifiziert ist, werden Informationen über ihn (die *Handschrift* oder *Signatur* des Virus) in einer Virusdefinitionsdatei gespeichert. Wenn Norton AntiVirus Ihre Laufwerke und Dateien prüft, sucht es in Ihren Dateien nach diesen charakteristischen Handschriften. Wenn eine Datei gefunden wird, die mit einem bekannten Virus infiziert ist, wird dieser von NAV automatisch eliminiert.

  Jedesmal, wenn ein neuer Virus gefunden wird, werden seine Charakteristika der Virusdefinitionsdatei hinzugefügt. Aus diesem Grund sollten Sie Ihre Virusdefinitionsdatei regelmäßig aktualisieren (bei Symantec ist jeden Monat eine neue Definitionsdatei erhältlich), so daß Norton AntiVirus über die nötigen Informationen zum Auffinden aller bekannten Viren verfügt. Wie Sie die neuesten Virusdefinitionsdateien erhalten, ist in Kapitel 4, „Schutz vor neuen Viren“, beschrieben.

- **Unbekannte Viren:** Ein *unbekannter Virus* ist ein Virus, der noch keine Virusdefinition hat. Norton AntiVirus findet unbekannte Viren, indem es Ihren Computer überwacht und Aktivitäten registriert, die für Viren typisch sind, wenn sie sich vermehren oder versuchen, Dateien zu beschädigen. Es sucht außerdem nach Programmen, die ohne Ihr Wissen geändert wurden. Wenn eine verdächtige Aktivität registriert wird, stoppt NAV diese Aktivität. Wenn ein geändertes Programm entdeckt wird, verhindert NAV, daß dieses Programm gestartet wird, und versucht, es zu reparieren.

Die Techniker von Symantec haben verschiedene, sich gegenseitig ergänzende Technologien entwickelt, um Ihren Computer auf Dauer frei von Viren zu halten. In Abbildung 1-1 ist dargestellt, wie diese Technologien zusammenarbeiten, um Viren – sowohl bekannte als auch unbekannte – zu erkennen, zu eliminieren und einem Virenbefall Ihres Computers vorzubeugen.

Abbildung 1-1 Norton AntiVirus Technologien



Der Scanner, der Programmdateien auf die Signaturen von bekannten Viren hin überprüft, ist das Kernstück des Schutzes von Norton AntiVirus. Er sucht nach Virussignaturen beim Start von manuellen Prüfungen, bei geplanten Prüfungen, die zu bestimmten Zeiten stattfinden, bei den automatischen Prüfungen beim Systemstart Ihres Computers, und er wird von der Auto-Protect-Funktion beim Bearbeiten einer Datei verwendet. Der Scanner überprüft auch, ob geimpfte Dateien durch einen unbekannten Virus verändert wurden.

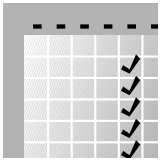
Auto-Protect überprüft Dateien nicht nur auf bekannte Viren, sondern stellt auch mit Hilfe seiner Viruserkennungstechnologie und der Untersuchung auf virusähnliche Aktivitäten sicher, daß unbekannte Viren Ihren Computer nicht infizieren und während der normalen Arbeit keine Daten beschädigen können.

Manuelle Virusprüfung

Sie können manuelle Virusprüfungen durchführen, indem Sie auf die Schaltfläche „Prüfen“ im Hauptfenster von Norton AntiVirus klicken oder indem Sie Virusprüfungen zu bestimmten Zeiten planen. Diese Prüfungen finden bekannte Viren. Sie erkennen außerdem Impfänderungen, die auf einen unbekannten Virus hinweisen können. Mit der manuellen Prüfung können Sie sicherstellen, daß Ihr Computer virenfrei ist.

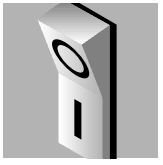
Informationen zum Prüfen von Dateien, Ordnern oder Laufwerken finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Geplante Prüfungen



Bei geplanten Prüfungen handelt es sich um manuelle Prüfungen, die automatisch zu bestimmten Zeiten gestartet werden. Sie ergänzen die anderen automatischen Schutzfunktionen und stellen so sicher, daß Ihr Computer virenfrei ist. Bei der Installation von Norton AntiVirus wird automatisch eine Prüfung Ihres Computers einmal pro Woche geplant. Informationen zum Planen von Prüfungen finden Sie unter „Planen von Virusprüfungen“ auf Seite 28.

Prüfung beim Systemstart



Den ersten Schutzwall gegen Virenangriffe bilden spezielle Prüfungen, die jedesmal durchgeführt werden, wenn Ihr Computer gestartet wird. Diese Prüfungen erkennen Viren, die die Dateien und Boot-Sektoren befallen, die Ihr Computer zum Starten benötigt. Die Prüfungen beim Systemstart sind ein wesentlicher Teil des Virenschutzes, da durch sie bei jedem Systemstart sichergestellt wird, daß Ihr Computer virenfrei ist.

Diese Funktion ist nach der Installation bereits aktiviert, es sei denn, Sie haben sie deaktiviert. Informationen zum Anpassen der Prüfungen beim Systemstart finden Sie unter „Anpassen der Virusprüfung beim Systemstart“ auf Seite 89.

Auto-Protect

Auto-Protect, die automatische Schutzfunktion von Norton AntiVirus, überprüft Programmdateien jedesmal, wenn sie gestartet werden.

Auto-Protect schützt Ihren Computer außerdem vor Viren, indem es ihn auf virusähnliche Aktivitäten untersucht (z.B. das versuchte Formatieren einer Festplatte) und Sie warnt, so daß Sie diese Aktivitäten stoppen können. Außerdem verfügt Auto-Protect über eine ausgereifte Methode zur Viruserkennung, die Sie warnt, wenn ein Virus versucht, sich an eine Programmdatei anzuhängen.

Diese Funktionen sind nach der Installation bereits aktiviert, es sei denn, Sie haben sie deaktiviert. Informationen zum Anpassen der Prüfungen beim Systemstart finden Sie unter „Anpassen der automatischen Schutzfunktion“ auf Seite 81.

Impfung

Wenn Sie Ihre Laufwerke geprüft haben, um sicherzustellen, daß die Dateien virenfrei sind, können Sie durch eine Impfung verhindern, daß die Dateien von Viren befallen werden. Wenn Sie eine Programmdatei oder einen Boot-Sektor impfen, zeichnet Norton AntiVirus diese Impfdaten (ähnlich einem Fingerabdruck) in einer speziellen Datei auf. Die ursprüngliche Datei wird in keiner Weise verändert.

Bei nachfolgenden Prüfungen – einschließlich manueller Prüfungen, Prüfungen beim Systemstart und Auto-Protect-Prüfungen von Programmdateien beim Ausführen – vergleicht Norton AntiVirus den aktuellen Fingerabdruck mit dem gespeicherten Fingerabdruck. Wenn irgendwelche Änderungen registriert werden, die auf das Vorhandensein eines Virus hinweisen, werden Sie informiert. Systemdateien und Boot-Sektoren werden während der Installation von Norton AntiVirus standardmäßig geimpft. Informationen zum Impfen von Programmdateien finden Sie unter „Impfen von Dateien“ auf Seite 21 und unter „Anpassen der Impfung“ auf Seite 90.

Virusdefinitionsdateien

Die Virusdefinitionsdateien enthalten Informationen, die Norton AntiVirus während der Prüfungen verwendet, um bekannte Viren zu finden. Dazu benötigt Norton AntiVirus die aktuellsten Informationen über Viren. Jedesmal, wenn ein neuer Virus entdeckt wird, muß seine Virussignatur zu einer Virusdefinitionsdatei hinzugefügt werden. Aktualisieren Sie Ihre Virusdefinitionsdateien regelmäßig, damit Norton AntiVirus über die nötigen Informationen verfügt, um alle bekannten Viren zu finden.

Neue Virusdefinitionsdateien sind jeden Monat kostenlos bei Symantec erhältlich. Wenn Sie ein Modem oder eine Internet-Verbindung haben, kann Norton AntiVirus Ihre Virusdefinitionsdateien automatisch aktualisieren. Wie das funktioniert, ist unter „Automatische Aktualisierung der Virusdefinitionen“ auf Seite 53 beschrieben.

So warnt Sie Norton AntiVirus

Norton AntiVirus kann Sie auf drei Arten auf eine mögliche Virusinfektion aufmerksam machen, je nachdem, wie der Virus entdeckt wurde:

- bei einer manuellen oder geplanten Prüfung (siehe Abbildung 1-2)
- von Auto-Protect (siehe Abbildung 1-3)
- bei einer Prüfung während des Systemstarts (siehe Abbildung 1-4)

Wenn während einer manuellen oder einer geplanten Prüfung ein Virus gefunden wird, erscheint der Norton AntiVirus-Reparaturassistent, mit dem Sie den Virus automatisch entfernen können. Abbildung 1-2 zeigt das erste Fenster des Reparaturassistenten.

Abbildung 1-2 Norton AntiVirus-Reparaturassistent

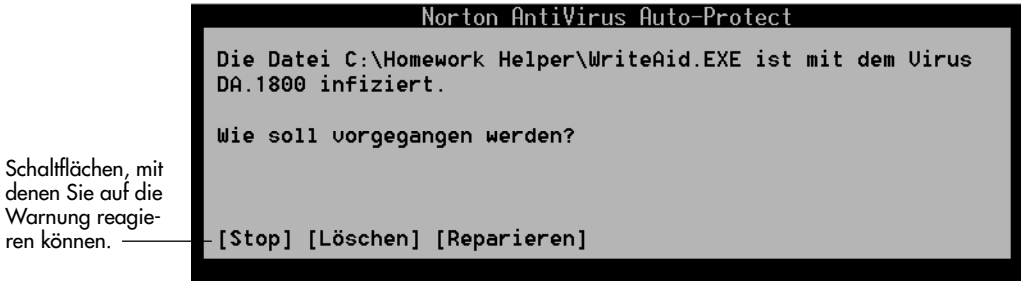
Norton AntiVirus entfernt alle Viren automatisch.

Klicken Sie auf „Weiter“, um die Virusentfernung zu starten.

Infizierte Objekte nacheinander reparieren.

Norton AntiVirus Auto-Protect überwacht Ihren Computer ständig auf Viren und zeigt sofort eine Warnmeldung an, wenn eine auf einen Virus hindeutende Aktivität auftritt. (Abbildung 1-3 zeigt ein Beispiel für eine Warnmeldung von Auto-Protect.) Jedes Viruswarnfeld enthält Schaltflächen, mit denen Sie den Virus entfernen können. Diese Warnmeldungen werden im Textmodus angezeigt, da alle Operationen, auch Bildschirmoperationen, unterbrochen werden, bis Sie auf die Warnmeldung reagiert und das mögliche Problem behoben haben. Informationen zur Verwendung des Reparaturassistenten finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Abbildung 1-3 Warnmeldung von Auto-Protect



Die Prüfungen beim Systemstart von Norton AntiVirus finden bei jedem Starten Ihres Computers statt. Sie finden Viren, die Systemdateien und Boot-Sektoren infizieren. (In Abbildung 1-4 sehen Sie ein Beispiel für eine Warnmeldung bei einer Prüfung beim Systemstart.) Genauso wie bei den Warnungen von Auto-Protect, enthält auch hier jedes Viruswarnfeld Schaltflächen, mit denen Sie den Virus entfernen können.

Abbildung 1-4 Warnmeldung bei einer Prüfung beim Systemstart

```
Norton AntiVirus Startprüfung...
Verwendete Virusdefinitionen: C:\PROGRA~1\GEMEIN~1\SYMANT~
1\VIRUSD~1\19970801.001
Verwendete Optionen: C:\PROGRA~1\NORTON~2

Speicher prüfen... OK
Master-Boot-Sektor prüfen... OK
Boot-Sektoren prüfen... OK

C:\WINDOWS\WIN.COM ist mit dem Virus Cascade (1) infiziert.
R)eparieren  L)öschen  W)eiter?
```

Unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33 finden Sie Anweisungen, was Sie tun können, wenn Sie eine Warnung während einer Prüfung beim Systemstart erhalten.

KAPITEL 2

Verwendung von Norton AntiVirus

Ein Virus kann nur aktiviert werden, wenn Sie Ihren Computer von einem Datenträger starten (bzw. versuchen zu starten), der mit einem Virus infiziert ist, wenn Sie ein infiziertes Programm ausführen oder wenn Sie ein infiziertes Dokument bzw. eine infizierte Vorlage öffnen.

Tips zum Vermeiden von Viren

Im folgenden finden Sie einige Vorsichtsmaßnahmen, die das Risiko eines Virusbefalls auf ein Minimum reduzieren:

- Stellen Sie sicher, daß der automatische Virenschutz immer aktiviert ist. Die automatische Schutzfunktion ist bereits eingerichtet, wenn Sie Norton AntiVirus mit den vordefinierten Optionen installiert haben. Weitere Informationen hierzu finden Sie unter „Anpassen der automatischen Schutzfunktion“ auf Seite 81 und unter „Anpassen der Virusprüfung beim Systemstart“ auf Seite 89.
- Prüfen Sie Ihre Laufwerke einmal pro Woche manuell auf Viren. (Oder legen Sie regelmäßige Virusprüfungen fest.) Diese Virusprüfungen ergänzen den automatischen Schutz und stellen sicher, daß Ihr Computer virenfrei ist. Wenn Sie Norton AntiVirus mit den voreingestellten Optionen installieren, ist bereits eine automatische Prüfung einmal pro Woche geplant. Anleitungen zum Prüfen finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15 und unter „Planen von Virusprüfungen“ auf Seite 28.
- Überprüfen Sie alle Disketten vor der Verwendung. Informationen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.
- Aktualisieren Sie monatlich die Virusdefinitionen. Informationen hierzu finden Sie unter „Automatische Aktualisierung der Virusdefinitionen“ auf Seite 53.

- Erstellen Sie einen NAV-Rettungsdiskettensatz, und heben Sie ihn gut auf. Damit ermöglichen Sie die Wiederherstellung der Betriebsfähigkeit bei einigen Boot-Sektor-Viren. Informationen hierzu finden Sie unter „Erstellen eines Rettungsdiskettensatzes“ in diesem Kapitel.
- Erstellen Sie regelmäßige Sicherungskopien vom Inhalt Ihrer Festplatte.
- Erwerben Sie Ihre Software grundsätzlich auf legalem Wege, und erstellen Sie schreibgeschützte Sicherungskopien davon.

Starten und Beenden von Norton AntiVirus

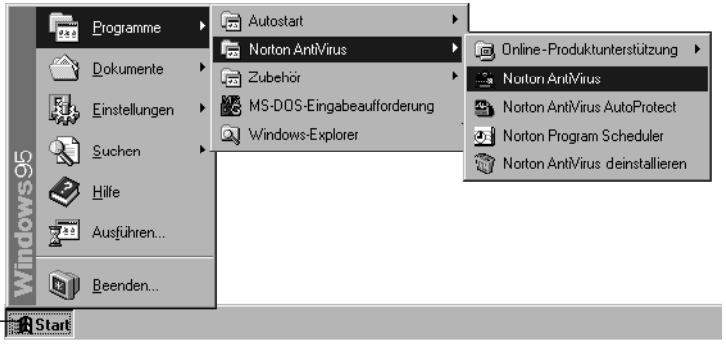
Im Hauptfenster von Norton AntiVirus können Sie Virusprüfungen starten, automatische Prüfungen planen, Konfigurationsoptionen anzeigen und ändern und die Virusdefinitionsdateien aktualisieren. Auto-Protect ist immer aktiviert (Informationen darüber finden Sie unter „Aktivieren und Deaktivieren von Auto-Protect“ auf Seite 18).

So starten Sie Norton AntiVirus:

- Klicken Sie auf „Start“ in der Task-Leiste, wählen Sie „Programme“ und anschließend die Gruppe „Norton AntiVirus“, und klicken Sie auf „Norton AntiVirus“ (Abbildung 2-1).

  Das Hauptfenster von Norton AntiVirus für Windows 95 wird geöffnet (siehe Abbildung 2-2).

Abbildung 2-1 Norton AntiVirus starten

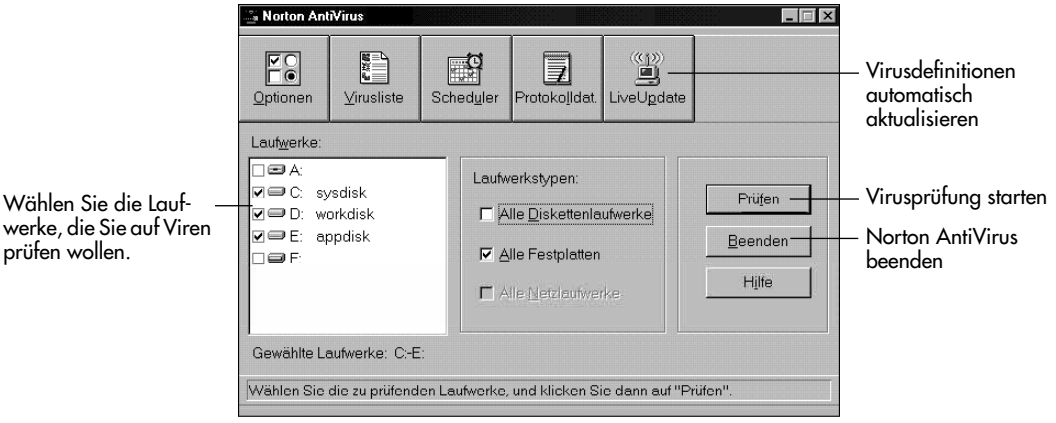


Klicken Sie auf „Start“, um Norton AntiVirus zu starten.

So beenden Sie Norton AntiVirus:

- Klicken Sie auf „Beenden“ im Hauptfenster von Norton AntiVirus.

Abbildung 2-2 Das Hauptfenster von Norton AntiVirus



Hilfe

Für alle Funktionen von Norton AntiVirus steht eine Online-Hilfe zur Verfügung. Sie haben mehrere Möglichkeiten, auf die Hilfe über Konzepte, Definitionen und Anleitungen zuzugreifen:

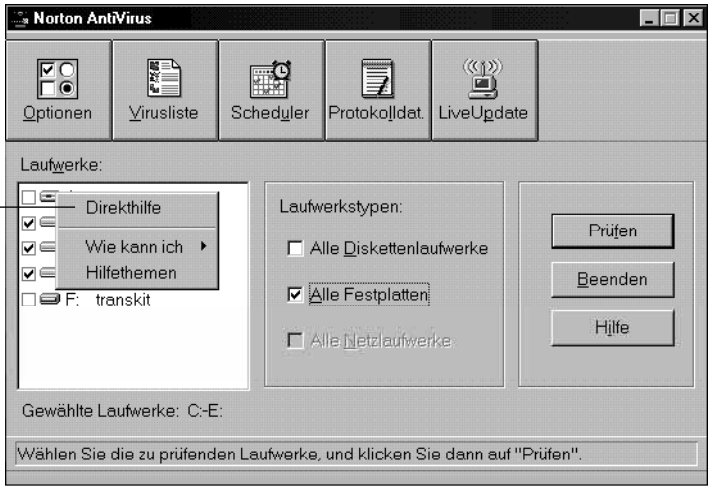
- Klicken Sie mit der rechten Maustaste auf Bereiche in einem Dialogfeld.
- Verwenden Sie die Befehle des Hilfe-Menüs.
- Klicken Sie in einem Dialogfeld auf die Schaltfläche „Hilfe“.

Zu dem Hilfe-System gehören ein Inhaltsverzeichnis, ein umfangreicher Themen-Index und ein Glossar. Im Hilfefenster können Sie nach Hilfethemen suchen, drucken, Anmerkungen hinzufügen oder Lesezeichen definieren. Zu den Neuerungen von Windows 95 gehört außerdem eine Funktion, mit der Sie in Norton AntiVirus unmittelbar auf kontextsensitive Hilfe für alle Optionen zugreifen können.

So greifen Sie auf die kontextsensitive Hilfe zu:

1 Zeigen Sie mit der Maus auf eine Option, und klicken Sie mit der rechten Maustaste. Das Hilfe-Einblendmenü wird geöffnet.

Abbildung 2-3 Menü der kontextsensitiven Hilfe

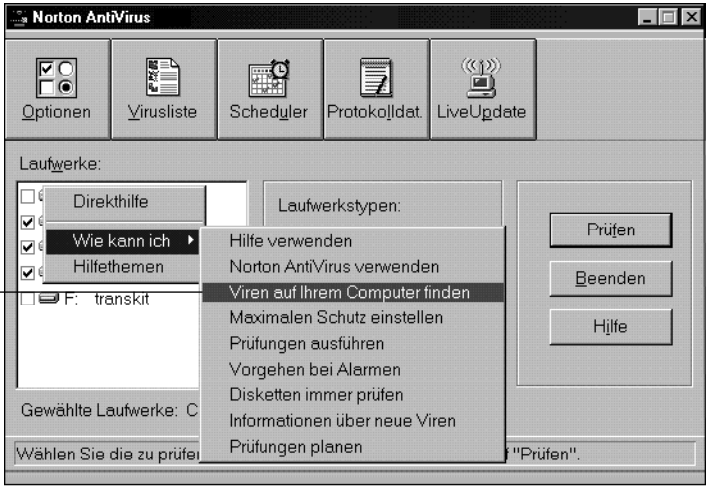


Hilfe-Einblendmenü (mit rechter Maustaste)

2 Wählen Sie eine der folgenden Optionen aus dem Einblendmenü:

- „Direkthilfe“ zeigt eine kurze Beschreibung der Option an.
- „Wie kann ich“ zeigt ein Untermenü für die entsprechende Option an (Abbildung 2-4).
- „Hilfethemen“ zeigt das Inhaltsverzeichnis des gesamten Hilfesystems an.

Abbildung 2-4 Menü „Wie kann ich“ der kontextsensitiven Hilfe



Schrittfolge anzeigen

Sie können auch mit Hilfe des Fragezeichens in der Titelleiste eines Dialogfeldes auf die kontextsensitive Hilfe zugreifen.

So bekommen Sie Hilfe zu Optionen:

1. Klicken Sie auf das Fragezeichen in der Titelleiste eines Dialogfeldes.

   Neben dem Mauszeiger wird ein Fragezeichen angezeigt.
2. Klicken Sie auf eine beliebige Option im Dialogfeld.

   Eine kurze Beschreibung der Option wird eingeblendet.

Durchführen von Virusprüfungen

Sie können eine Virusprüfung jederzeit durchführen. Sie sollten generell alle Disketten vor der ersten Verwendung und alle Dateien, die Sie von Bulletin Boards oder anderen Online-Diensten herunterladen, prüfen.

Nach jeder Prüfung berichtet Norton AntiVirus, ob etwas gefunden wurde. Falls Probleme aufgetreten sind, erscheint der Norton AntiVirus-Reparaturassistent, mit dem Sie Reparaturen ausführen können (siehe „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33). Nachdem die Probleme behoben sind und auch nach Prüfungen, bei denen keine Probleme aufgetreten sind, werden alle Vorkommnisse während der Prüfung in einer Zusammenfassung festgehalten.

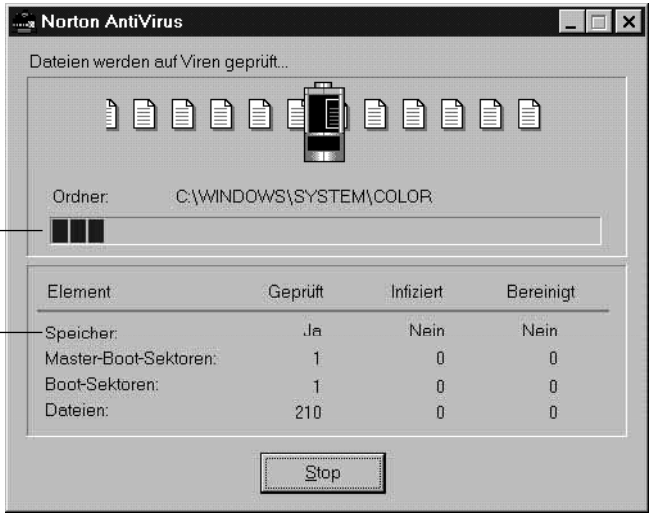
☞ **Tip:** Die voreingestellten Prüfoptionen von Norton AntiVirus kombinieren maximalen Schutz mit hoher Effizienz. In den meisten Fällen müssen Sie keine Änderungen vornehmen. Sie können aber einstellen, was geprüft werden soll und was passiert, wenn ein Virus gefunden wird. Siehe dazu „Anpassen manueller Prüfoptionen“ auf Seite 63.

So prüfen Sie ein oder mehrere Laufwerke:

1. Starten Sie Norton AntiVirus.
2. Wählen Sie im Hauptfenster von Norton AntiVirus die zu prüfenden Laufwerke in der Liste „Laufwerke“ aus. Wenn Sie mehrere Laufwerkstypen prüfen wollen, wählen Sie die entsprechenden Optionen im Gruppenfeld „Laufwerkstypen“ aus (siehe Abbildung 2-2).
3. Klicken Sie auf „Prüfen“.

   Der Status der Prüfung wird im Prüf-Dialogfeld angezeigt.

Abbildung 2-5 Eine Prüfung wird durchgeführt



So prüfen Sie eine einzelne Datei:

1. Wählen Sie im Hauptfenster von Norton AntiVirus „Datei“ im Menü „Prüfen“.
2. Wählen Sie die Datei aus, die Sie prüfen wollen, und klicken Sie auf „OK“.

So prüfen Sie einen einzelnen Ordner:

1. Wählen Sie im Hauptfenster von Norton AntiVirus „Ordner“ im Menü „Prüfen“.
2. Wählen Sie den Ordner aus, den Sie prüfen wollen.
3. Klicken Sie auf „Prüfen“.

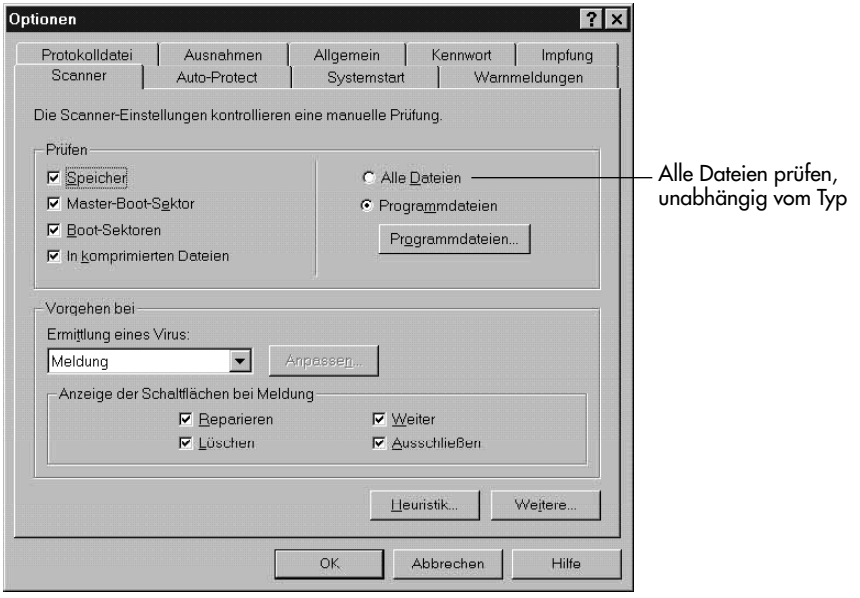
Norton AntiVirus ist so eingestellt, daß nur Programmdateien, Dokumente und Dokumentvorlagen geprüft werden, da sich Viren nur von diesen Dateiarten aus verbreiten können. In besonderen Fällen, z.B. nach einer Virusinfektion, möchten Sie vielleicht alle Dateien prüfen, um sicherzustellen, daß auch solche Dateien geprüft werden, die nicht als normale Programmdateien erscheinen.

So prüfen Sie alle Dateien, unabhängig von ihrem Typ:

1. Klicken Sie im Hauptfenster von Norton AntiVirus auf „Optionen“.
2. Klicken Sie auf das Register „Scanner“ (Abbildung 2-6).
3. Wählen Sie die Option „Alle Dateien“.
4. Klicken Sie auf „OK“, um zum Hauptfenster von Norton AntiVirus zurückzukehren.
5. Wählen Sie die zu prüfenden Laufwerke aus, und klicken Sie auf „Prüfen“.

Weitere Informationen über das Auswählen von Programmdateien oder allen Dateien für die Prüfung finden Sie unter „Zu prüfende Dateien wählen“ auf Seite 69.

Abbildung 2-6 Register der Scanneroptionen



Aktivieren und Deaktivieren von Auto-Protect

Norton AntiVirus ist so eingestellt, daß Auto-Protect – die automatische Virusschutzfunktion – bei jedem Start Ihres Computers geladen wird. Das Symbol von Norton AntiVirus Auto-Protect erscheint dann in der Windows Task-Leiste (Abbildung 2-7). Wenn das Symbol für Auto-Protect nicht in der Windows Task-Leiste angezeigt wird, ist Auto-Protect nicht geladen oder so eingerichtet, daß das Symbol nicht in der Task-Leiste angezeigt wird.

Es gibt nur wenige Situationen, in denen es sinnvoll ist, Auto-Protect zu deaktivieren. So kann es zum Beispiel erforderlich sein, den Virusschutz zu deaktivieren, wenn Sie ein bestimmtes Anwendungsprogramm auf Ihrem Computer installieren wollen. Normalerweise sollten Sie Auto-Protect aber nicht deaktivieren, da Auto-Protect der beste Schutz vor Virusbefall ist.

Abbildung 2-7 Die Windows Task-Leiste

So deaktivieren Sie Auto-Protect vorübergehend:

1 Doppelklicken Sie auf das Symbol für Auto-Protect in der Windows Task-Leiste (Abbildung 2-7).

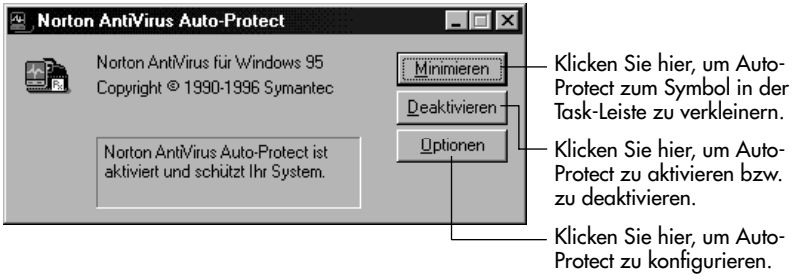
Das Dialogfeld „Norton AntiVirus Auto-Protect“ wird geöffnet (Abbildung 2-8).

2 Klicken Sie auf „Deaktivieren“.

Die Schaltfläche wechselt zu „Aktivieren“ und das Symbol zu  .

3 Klicken Sie auf „Minimieren“, um das Dialogfeld „Norton AntiVirus Auto-Protect“ zu schließen.

Abbildung 2-8 Dialogfeld „Norton AntiVirus Auto-Protect“



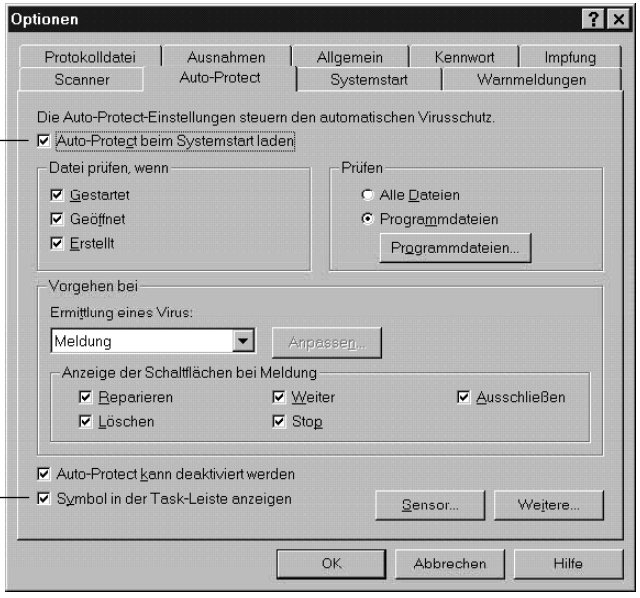
So laden Sie Auto-Protect bei jedem Systemstart:

1 Starten Sie Norton AntiVirus.

2 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus (siehe Abbildung 2-2).

3 Klicken Sie auf das Register „Auto-Protect“.

Abbildung 2-9 Optionen für Auto-Protect einstellen



Klicken Sie hier, um Auto-Protect beim Systemstart zu laden.

Klicken Sie hier, um das Symbol für Auto-Protect in der Task-Leiste anzuzeigen.

4 Aktivieren Sie „Auto-Protect beim Systemstart laden“, und klicken Sie auf „OK“.

Norton AntiVirus lädt Auto-Protect sofort und bei jedem Systemstart.

Umgehen von Auto-Protect beim Systemstart

Die Prüfungen beim Systemstart, durch die sichergestellt wird, daß die Dateien, die Ihr Computer für den Systemstart verwendet, nicht infiziert sind, sind ein wesentlicher Teil des Virenschutzes. Obwohl Sie generell davon absehen sollten, kann es Gründe dafür geben, daß Sie die Virusprüfung beim Systemstart verhindern möchten. Vielleicht wollen Sie versuchen, ein Problem beim Starten des Computers oder einen Konfigurationsdatei-Konflikt zu beheben.

So umgehen Sie die Virusprüfungen beim Systemstart:

- Halten Sie während des gesamten Startvorganges die angegebenen Umgehungstasten gedrückt. Standardmäßig müssen Sie beide Alt-Tasten drücken.

Mit diesem Verfahren umgehen Sie die Virusprüfung nur bei diesem einen Systemstart. In Abschnitt „Anpassen der Virusprüfung beim Systemstart“ auf Seite 89 erfahren Sie, was Umgehungstasten sind, wie Sie festlegen, was beim Systemstart geprüft wird, und wie Sie verhindern, daß eine Virusprüfung beim Systemstart umgangen wird.

Impfen von Dateien

Wenn Sie Norton AntiVirus mit den Standardoptionen installieren, sind Boot-Sektoren und Systemdateien durch Impfung geschützt. Weiter müssen Sie nichts tun. Wenn Ihr Computer allerdings in einer stark virusgefährdeten Umgebung betrieben wird, können Sie zur Verbesserung des Schutzes alle Programmdateien impfen.

Wenn Sie eine Programmdatei oder einen Boot-Sektor impfen, zeichnet Norton AntiVirus wichtige Informationen darüber (ähnlich einem Fingerabdruck) in einer speziellen Datendatei auf, die als *Impfdatei* bezeichnet wird. Für jedes Laufwerk, auf dem Sie Dateien impfen, wird eine eigene Impfdatei erstellt. Durch die Impfung wird die Datei oder der Boot-Sektor nicht verändert. Es können nur Programmdateien (einschließlich Systemdateien) und Boot-Sektoren von Systemstartdisketten bzw. -laufwerken geimpft werden, da sich Viren normalerweise von diesen Teilen Ihres Systems aus verbreiten.

Bei nachfolgenden Prüfungen – einer manuellen, geplanten oder von Auto-Protect durchgeführten Prüfung – vergleicht Norton AntiVirus die Dateien und Boot-Sektoren mit ihren Fingerabdrücken. Wenn irgendwelche Änderungen registriert werden, die auf das Vorhandensein eines unbekannten Virus hinweisen, werden Sie informiert.

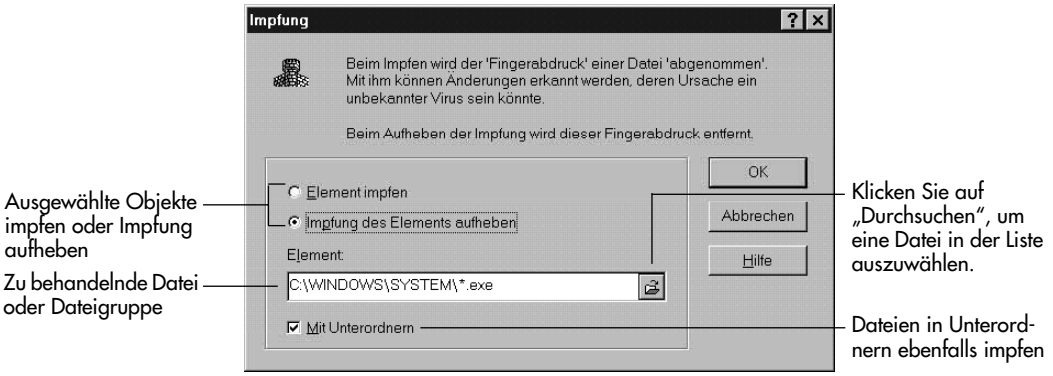
Wenn Sie in einer Umgebung mit hohem Risiko arbeiten und deshalb neben den Boot-Sektoren und Systemdateien auch Programmdateien impfen wollen, können Sie auf zwei Arten vorgehen:

- Sie können einzelne Dateien oder Ordner jederzeit mit dem Befehl „Impfung“ im Menü „Tools“ im Hauptfenster von Norton AntiVirus impfen.
- Sie können Programmdateien, Systemdateien und Boot-Sektoren während einer manuellen Virusprüfung impfen. Weitere Informationen hierzu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

So impfen Sie einzelne Dateien oder Ordner:

1 Wählen Sie „Impfung“ im Menü „Tools“ im Hauptfenster von Norton AntiVirus.

Abbildung 2-10 Dialogfeld „Impfung“



2 Aktivieren Sie „**Element impfen**“.

3 Geben Sie den Pfadnamen für die Datei, die Dateigruppe, den Ordner oder das Laufwerk in das Textfeld „Element“ ein.

Geben Sie nur den Ordnernamen ein, um alle Dateien im Ordner zu impfen. Um z.B. alle Dateien im DOS-Ordner zu impfen, geben Sie folgendes ein: `C:\WINDOWS\COMMAND`

Sie können auch Platzhalter verwenden, um eine Gruppe von Dateien anzugeben. Wenn Sie z.B. nur die .COM-Dateien im DOS-Ordner impfen wollen, geben Sie folgendes ein: `C:\WINDOWS\COMMAND\*.COM`

Sie können auch auf „Durchsuchen“ klicken, um eine einzelne Datei aus der Liste auszuwählen, und dann auf „Öffnen“.

☞ **Tip:** Wenn Sie Objekte impfen, speichert Norton AntiVirus Impfdaten über diese Objekte. Darüber hinaus müssen Sie sicherstellen, daß die Impfschutzfunktion aktiviert ist, damit die Objekte während der Prüfungen auf Impfänderungen untersucht werden. Sie können die Impfung mit den Optionen im Register „Impfung“ aktivieren und deaktivieren. Weitere Informationen dazu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

4 Wenn es sich bei dem Element um einen Ordner handelt, aktivieren Sie „Mit Unterordnern“, um auch die Dateien in allen Unterordnern zu impfen.

5 Klicken Sie auf „OK“.

So impfen Sie Dateien und Boot-Sektoren während einer Virusprüfung:

1 Vergewissern Sie sich, daß die Impfung aktiviert ist.

Aktivieren oder deaktivieren Sie die Impfung mit den Optionen im Register „Impfung“. Sie können Boot-Sektoren und Systemdateien auf Ihrem Startlaufwerk sowie Programmdateien impfen lassen. Weitere Informationen dazu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

2 Prüfen Sie die Dateien, Ordner oder Laufwerke, die Sie impfen wollen.

Alle Dateien werden vor dem Impfen geprüft, um sicherzustellen, daß sie nicht infiziert sind. Weitere Informationen zum Durchführen von Virusprüfungen finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Dateien und Boot-Sektoren neu impfen

Wenn Sie eine Programmdatei oder einen Boot-Sektor neu impfen, wird ein Fingerabdruck dieses Elements erstellt, der die bis dahin über das Element in der Impfdatei gespeicherten Daten ersetzt.

Sie sollten die Programmdateien impfen, wenn Sie folgendes tun:

- Die Programmdatei ändern, sie z.B. mit einer neuen Version aktualisieren
- Die Datei in ein anderes Verzeichnis bewegen

Sie sollten Boot-Sektoren und Systemdateien neu impfen, wenn Sie folgendes tun:

- Ein neues Betriebssystem auf Ihrer Festplatte installieren
- Ihre Festplatte neu partitionieren

☞ **Tip:** Wenn Sie eine Festplatte neu partitionieren oder ein neues Betriebssystem auf Ihrer Festplatte installieren, sollten Sie auch Ihren Norton AntiVirus Rettungsdiskettensatz neu erstellen. Weitere Informationen dazu finden Sie unter „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27.

So impfen Sie ein Element neu:

- Befolgen Sie die Anleitungen unter „So impfen Sie einzelne Dateien oder Ordner:“ oben in diesem Kapitel, um die Dateien neu zu impfen.

Wenn Norton AntiVirus während der Impfung eine Warnung ausgibt, z.B. wenn Sie ein Programm aktualisiert, die Programmdateien aber noch nicht neu geimpft haben, klicken Sie einfach auf „Impfen“ im Warnfeld. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Wenn Sie Elemente vom Warnfeld aus neu impfen wollen, müssen Sie Norton AntiVirus so konfigurieren, daß es Sie auf Impfänderungen hinweist. Weitere Informationen hierzu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

Impfung von Dateien oder Ordnern aufheben

Es gibt Situationen, in denen Sie die Impfung einer Datei oder eines Ordners aufheben wollen. So wollen Sie vielleicht die Impfung eines Ordners aufheben, bevor Sie die Programme in diesem Ordner aktualisieren, um bei einer nachfolgenden Prüfung Warnmeldungen über Impfänderungen zu vermeiden. Wenn Sie die Impfung einer Datei aufheben, werden deren Impfdaten aus der Impfdatei entfernt.

Impfungen von Systemdateien und Boot-Sektoren können nicht aufgehoben werden. Sie können Norton AntiVirus aber so konfigurieren, daß diese Bereiche nicht auf Impfänderungen überprüft werden. Weitere Informationen hierzu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

So heben Sie die Impfung von Dateien auf:

1. Wählen Sie „Impfung“ im Menü „Tools“ im Hauptfenster von Norton AntiVirus.
2. Aktivieren Sie „Impfung des Elements aufheben“.
3. Geben Sie den Pfadnamen für die Datei, die Dateigruppe, den Ordner oder das Laufwerk in das Textfeld „Element“ ein.

   Sie können auch Platzhalter verwenden, um eine Gruppe von Dateien anzugeben. Wenn Sie z.B. für alle .COM-Dateien in Ihrem DOS-Ordner die Impfung aufheben wollen, geben Sie folgendes ein:
   `C:\WINDOWS\COMMAND\*.COM`

   Sie können auch auf „Durchsuchen“ klicken, um eine einzelne Datei aus der Liste auszuwählen, und dann auf „Öffnen“.
4. Wenn es sich bei dem Element um einen Ordner handelt, aktivieren Sie „Mit Unterordnern“, um auch die Impfung der Dateien in allen Unterordnern aufzuheben.
5. Klicken Sie auf „OK“.

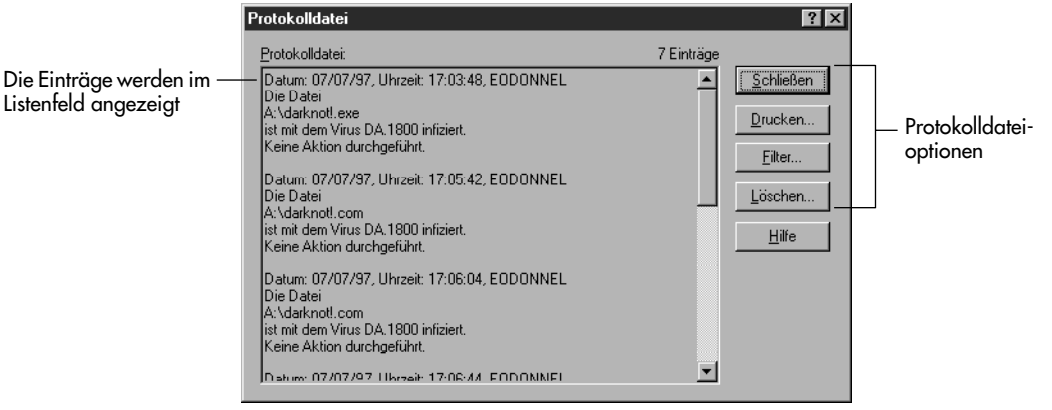
Anzeigen der Protokolldatei

Die Protokolldatei enthält verschiedene Informationen über die Aktivitäten von Norton AntiVirus, z.B. wann Probleme auftraten und wie sie gelöst wurden. Informationen zum Anpassen der Protokolldatei finden Sie unter „Anpassen der Protokolldatei“ auf Seite 78.

So zeigen Sie alle Einträge der Protokolldatei an:

1 Klicken Sie auf „Protokolldatei“ im Hauptfenster von Norton AntiVirus.

Abbildung 2-11 Protokolldatei



2 Klicken Sie auf „Schließen“, um die Protokolldatei zu schließen.

Im Dialogfeld „Protokolldatei“ können Sie folgendes tun:

Klicken Sie auf „Drucken“, um die Protokolldatei auf einem Drucker auszugeben oder in eine Datei zu drucken. Nur die im Listenfeld angezeigten Einträge werden ausgedruckt. Wenn Sie die Protokolldatei filtern, werden nur die gefilterten Einträge gedruckt.

Klicken Sie auf „Filter“, um die verschiedenen Ereignistypen anzuzeigen.

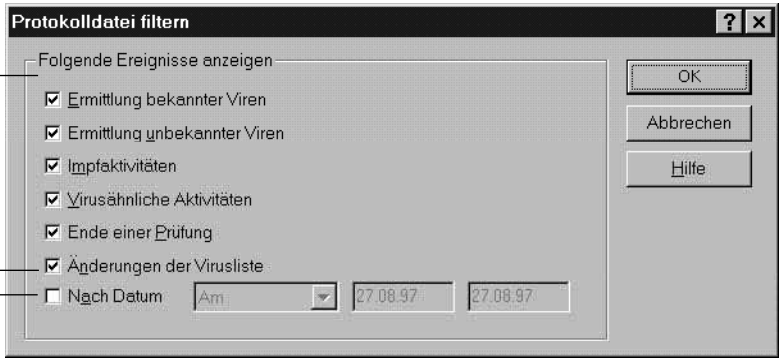
Klicken Sie auf „Löschen“, um alle Einträge aus der Protokolldatei zu löschen.

So filtern Sie die Einträge der Protokolldatei:

1 Klicken Sie auf „Filter…“ im Dialogfeld „Protokolldatei“ (siehe Abbildung 2-11).

Das Dialogfeld „Protokolldatei filtern“ wird geöffnet (Abbildung 2-12).

Abbildung 2-12 Protokolldatei filtern



2 Aktivieren Sie die Ereignisse, die Sie auflisten möchten. Wenn keine Einträge den eingegebenen Kriterien entsprechen, wird die Meldung „Die Protokolldatei enthält keine Einträge“ angezeigt.

- **Ermittlung bekannter Viren:** Zeigt Informationen über die Ermittlung bekannter Viren an.
- **Ermittlung unbekannter Viren:** Zeigt Informationen über die Ermittlung unbekannter Viren an.
- **Impfaktivitäten:** Zeigt Informationen über nicht geimpfte oder seit der letzten Impfung geänderte Dateien an.
- **Virusähnliche Aktivitäten:** Zeigt Informationen über die Ermittlung virusähnlicher Aktivitäten an.
- **Ende einer Prüfung:** Zeigt Informationen über die durchgeführten Prüfungen an. Dazu zählen nur manuelle und geplante Prüfungen.
- **Änderungen der Virusliste:** Zeigt Informationen über Änderungen an der Virusliste an.
- **Nach Datum:** Zeigt das Datum oder den Datumsbereich für die Anzeige der ausgewählten Ereignisse an. Wählen Sie eine Option in der Liste „Datum“ aus, und geben Sie dann ein Datum bzw. den Datumsbereich ein.

3 Klicken Sie auf „OK“.

Erstellen eines Rettungsdiskettensatzes

Der NAV-Rettungsdiskettensatz ist ein wichtiger Teil des Virenschutzes. Darin sind wichtige Systeminformationen und die für einen Systemstart notwendigen Programme gespeichert. Sie benötigen ihn außerdem, um die von verschiedenen Arten von Boot-Viren verursachten Schäden beheben zu können. Der Rettungsdiskettensatz besteht aus folgenden Disketten:

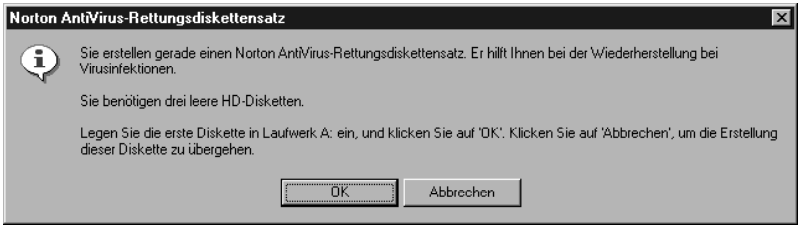
- **Norton AntiVirus Rettungs- und Startdiskette:** Zum Starten Ihres Computers
- **Norton AntiVirus Programmdiskette:** Zum Prüfen und zum Entfernen von Viren
- **Norton AntiVirus Virusdefinitionsdiskette**: Enthält die während der Prüfungen verwendeten Virusdefinitionsdateien

Schon bei der Installation von Norton AntiVirus können Sie Ihren Rettungsdiskettensatz erstellen. Wenn Sie dies nicht während der Installation getan haben, sollten Sie es jetzt nachholen. Sie benötigen dazu drei HD-Disketten.

So erstellen Sie einen Rettungsdiskettensatz:

1 Klicken Sie auf „Start“ in der Task-Leiste, wählen Sie „Programme“ und anschließend die Gruppe „Norton AntiVirus“, und klicken Sie auf die Option zum Erstellen der Rettungsdisketten.

Abbildung 2-13 Erstellen eines Rettungsdiskettensatzes



2 Legen Sie eine Diskette in Laufwerk A: ein, und klicken Sie auf „OK“.

Während des Vorgangs wird die Diskette formatiert. Verwenden Sie daher keine Diskette, auf der sich Dateien befinden, die Sie noch benötigen.

3 Befolgen Sie die Anleitungen. Sie werden benachrichtigt, wenn Sie die erste Diskette aus dem Laufwerk nehmen und die zweite Diskette einlegen müssen.

4 Nachdem Sie den Norton AntiVirus Rettungsdiskettensatz erstellt haben, beschriften Sie die Disketten gemäß den Anweisungen auf dem Bildschirm. Geben Sie dabei auch das Datum an und für welchen Computer der Satz erstellt wurde.

5 Verschieben Sie den Plastikschieber für den Schreibschutz der Disketten, so daß Sie durch die Öffnung hindurchsehen können, und bewahren Sie sie an einem sicheren Ort auf.

Planen von Virusprüfungen

Mit dem Scheduler können Sie Virusprüfungen planen, die dann automatisch zu festgelegten Zeiten oder in festgelegten Abständen durchgeführt werden. Wenn Sie mit dem Computer arbeiten, während eine Virusprüfung durchgeführt wird, läuft diese im Hintergrund, so daß Sie weiterarbeiten können.

Zum Schließen des Schedulers können Sie entweder auf „Beenden“ oder „Minimieren“ klicken. Wenn Sie wollen, daß der Scheduler aktiviert bleibt, klicken Sie auf „Minimieren“. Wenn geplante Virusprüfungen durchgeführt werden sollen, muß der Scheduler aktiviert sein.

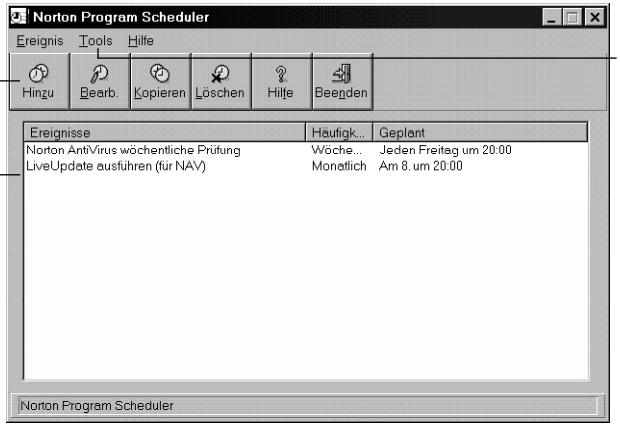
☞ **Tip:** Sie können Prüfungen auch mit dem Microsoft Plus! System Agent planen. Informationen zum Verwenden von NAVW32.EXE, dem Scanner von Norton AntiVirus, finden Sie in Anhang C, „Befehlszeilenschalter“ auf Seite 111.

So greifen Sie auf den Scheduler zu:

- Klicken Sie auf „Scheduler“ im Hauptfenster von Norton AntiVirus.
- Wählen Sie „Norton Program Scheduler“ im Menü „Start“ von Windows.

  Wenn noch keine Ereignisse geplant wurden, sind die Schaltflächen „Bearbeiten“, „Kopieren“ und „Löschen“ grau dargestellt.

Abbildung 2-14 Norton Program Scheduler

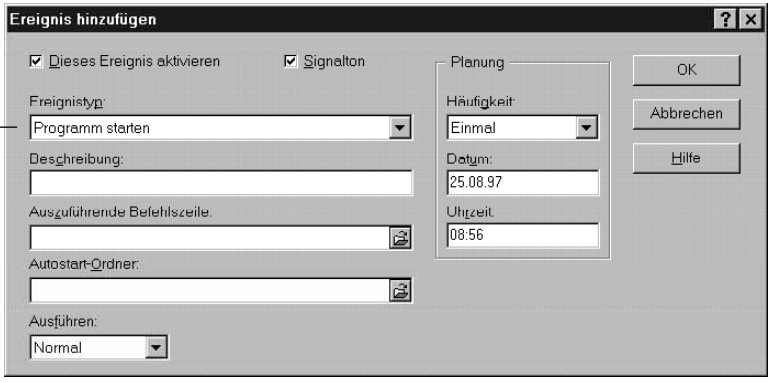


So planen Sie Virusprüfungen:

1 Klicken Sie auf „Hinzufügen“.

Das Dialogfeld „Ereignis hinzufügen“ wird geöffnet, in dem Sie beliebige Ereignisse planen können.

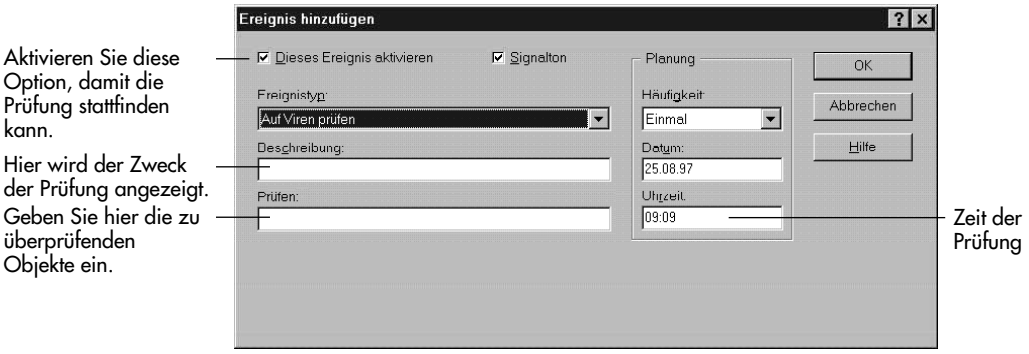
Abbildung 2-15 Dialogfeld „Ereignis hinzufügen“



2 Wählen Sie „Auf Viren prüfen“ in der Liste „Ereignistyp“.

Das Dialogfeld paßt sich an, so daß Sie die für eine Virusprüfung spezifischen Informationen eingeben können.

Abbildung 2-16 Dialogfeld „Ereignis hinzufügen“ mit Option für Virusprüfung



3 Aktivieren Sie „Dieses Ereignis aktivieren“.

Wenn Sie diese Option deaktivieren, kann die Virusprüfung nicht stattfinden.

4 Aktivieren Sie „Signalton“, um bei Beginn der Prüfung einen Signalton zu hören.

5 Geben Sie im Feld „Beschreibung“ eine kurze Beschreibung ein.

Dieser Text wird im Dialogfeld „Scheduler“ in der Liste der Ereignisse angezeigt.

6 Geben Sie im Feld „Was prüfen“ das Laufwerk, den Pfad, das Verzeichnis oder die Datei ein, die Sie überprüfen wollen.

☞ **Hinweis:** Sie müssen im Feld „Was prüfen“ eingeben, welche Elemente geprüft werden sollen.

Um Ihre Festplatte zu prüfen, geben Sie den entsprechenden Laufwerkbuchstaben und einen Doppelpunkt ein.

```
C:
```

Um mehr als ein Objekt zu scannen, trennen Sie die Objekte durch ein Leerzeichen.

```
C: D:\Programme
```

Wenn in der Pfadangabe Leerzeichen verwendet werden, schließen Sie die gesamte Zeile in Anführungszeichen ein.

```
"C:\Frank War Hier\Hallo.exe"
```

Sie können alle Schalter von NAVW32.EXE für den Scheduler verwenden. Im Abschnitt „NAVW32.EXE“ auf Seite 114 finden Sie eine Liste der Befehlszeilenschalter.

7 Wählen Sie in der Liste „Häufigkeit“ aus, wie oft das Ereignis stattfinden soll.

8 Geben Sie nötigenfalls noch die Uhrzeit, den Tag und das Datum ein, um die Virusprüfung zu planen.

9 Klicken Sie auf „OK“. Falls Sie dazu aufgefordert werden, klicken Sie im Dialogfeld zur Bestätigung erneut auf „OK“.

☞ **Tip:** Sie können mit dem Scheduler zur festgelegten Zeit jedes beliebige Programm ausführen oder Meldungen anzeigen. Wählen Sie einfach in der Liste den Ereignistyp aus, und geben Sie die erforderlichen Informationen ein. Das Dialogfeld wird entsprechend angepaßt.

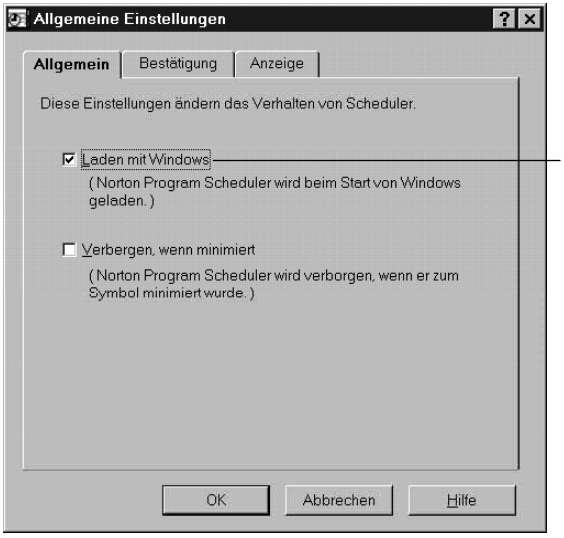
So stellen Sie sicher, daß der Scheduler beim Starten von Windows geladen wird:

1 Starten Sie Norton AntiVirus.

2 Klicken Sie auf „Scheduler“ im Hauptfenster von Norton AntiVirus.

3 Wählen Sie „Optionen“ im Menü „Tools“ des Schedulers.

Abbildung 2-17 Scheduler - Allgemeine Einstellungen



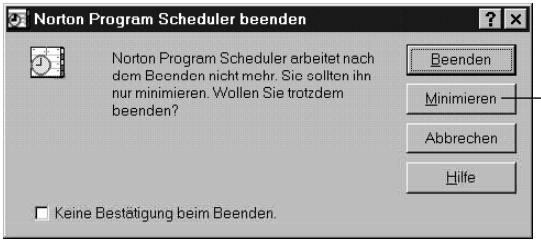
4 Vergewissern Sie sich, daß „Laden mit Windows“ im Register „Allgemein“ aktiviert ist.

Der Scheduler muß geladen sein, damit die geplanten Virusprüfungen durchgeführt werden.

So schließen Sie den Scheduler:

1 Klicken Sie auf „Beenden“ im Hauptfenster des Schedulers.

Abbildung 2-18 Scheduler beenden



2 Klicken Sie auf „Minimieren“.

Der Scheduler bleibt aktiviert, so daß die Virusprüfung zu der von Ihnen festgelegten Zeit stattfinden kann.

Die von Ihnen festgelegten Prüfungen werden automatisch durchgeführt. Wenn Ihr Computer zu dem für eine Prüfung festgelegten Zeitpunkt ausgeschaltet oder der Scheduler nicht geladen ist, werden Sie beim nächsten Laden des Schedulers darauf hingewiesen, daß die Prüfung nicht stattgefunden hat.

So verwalten Sie geplante Ereignisse:

Sie können im Dialogfeld „Scheduler“ (siehe Abbildung 2-14) außerdem folgendes tun:

Klicken Sie auf „Bearbeiten“, um Änderungen an einer geplanten Virusprüfung vorzunehmen.

Klicken Sie auf „Kopieren“, um eine Kopie einer geplanten Prüfung zu erstellen. Diese Option ist nützlich, wenn Sie eine Virusprüfung planen wollen, die einer bereits in der Liste vorhandenen Prüfung ähnelt.

Klicken Sie auf „Löschen“, um geplante Prüfungen zu löschen, die Sie nicht länger benötigen.

KAPITEL 3

Entfernen von Viren

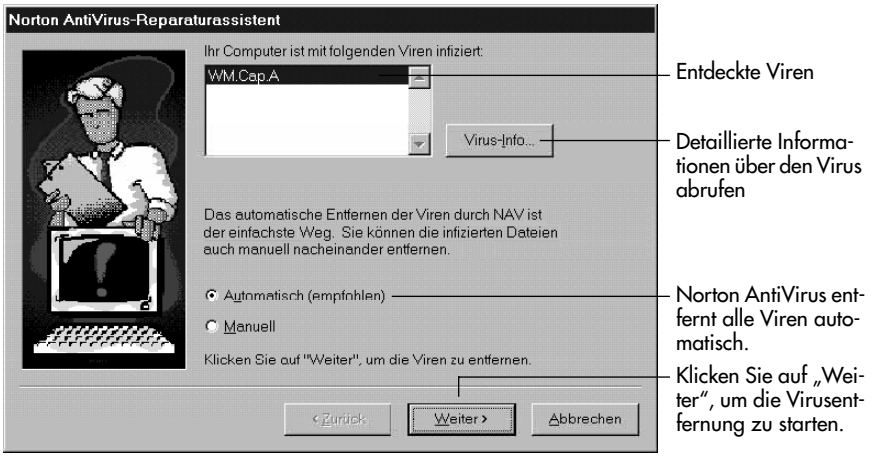
Norton AntiVirus warnt Sie auf drei Arten vor möglichen Virusinfektionen, je nachdem, wie der Virus entdeckt wurde:

- **Virus wurde während einer manuellen oder geplanten Prüfung entdeckt:** Der Norton AntiVirus-Reparaturassistent erscheint am Ende der Prüfung und entfernt alle gefundenen Viren automatisch. Siehe dazu „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.
- **Virus wurde von Auto-Protect entdeckt:** Auto-Protect überwacht Ihren Computer ständig auf Viren und zeigt sofort eine Warnmeldung an, sobald ein infiziertes Element gefunden wurde. Mit den Schaltflächen im Warnfeld können Sie auf die Warnung reagieren. Siehe dazu „Entfernen von Viren, die von Auto-Protect entdeckt wurden“ auf Seite 38.
- **Virus wurde während einer Prüfung beim Systemstart entdeckt:** Prüfungen beim Systemstart werden bei jedem Start Ihres Computers durchgeführt und finden Viren in den Dateien und Boot-Sektoren, die Ihr Computer für den Startvorgang benötigt. Wenn ein infiziertes Element gefunden wurde, wird eine Warnmeldung angezeigt. Mit den Schaltflächen im Warnfeld können Sie auf die Warnung reagieren. Siehe dazu „Entfernen von Viren, die während der Prüfung beim Systemstart entdeckt wurden“ auf Seite 47.

Entfernen von Viren, die bei Virusprüfungen entdeckt wurden

Wenn während einer Virusprüfung Viren entdeckt wurden, erscheint der Norton AntiVirus-Reparaturassistent nach der Prüfung (Abbildung 3-1). Sie können alle Viren automatisch von Norton AntiVirus entfernen lassen oder die Viren einen nach dem anderen manuell entfernen.

Abbildung 3-1 Der Norton AntiVirus-Reparaturassistent



So entfernen Sie alle Viren automatisch:

1 Prüfen Sie ein Laufwerk, einen Ordner oder eine Datei mit Norton AntiVirus.

Der Reparaturassistent erscheint nur, wenn ein Virus entdeckt wurde (Abbildung 3-1).

2 Wählen Sie „Automatisch“ im Norton AntiVirus-Reparaturassistenten aus, und klicken Sie auf „Weiter“.

Wenn Sie „Manuell“ auswählen, befolgen Sie die Anweisungen im Abschnitt „So entfernen Sie die Viren nacheinander manuell:“ auf Seite 35.

3 Lesen Sie die daraufhin angezeigten Fenster durch (Abbildung 3-2), damit Sie verstehen, was Norton AntiVirus tut, und klicken Sie dann auf „Weiter“, um fortzufahren.

Der Reparaturassistent bittet Sie jedesmal um eine Bestätigung, bevor er irgendetwas unternimmt.

Abbildung 3-2 Welche Elemente sind infiziert

☞ **Tip:** Wenn der Reparaturassistent seine Arbeit beendet hat, sehen Sie im letzten Fenster eine Zusammenfassung der von Norton AntiVirus durchgeführten Aktionen. Sie können in diesem Fenster auf „Weitere Infos" klicken, wenn Sie detaillierte Informationen über die Aktionen sehen oder einen Bericht über die infizierten und reparierten Elemente drucken wollen.

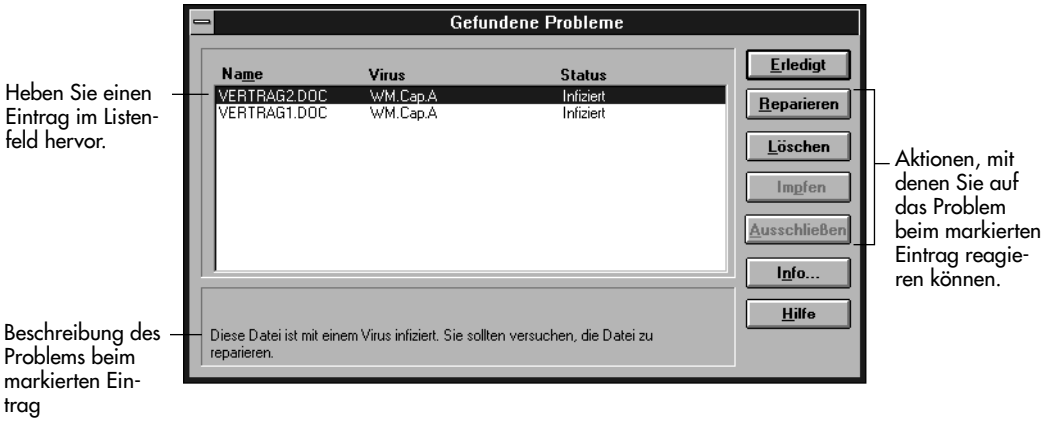
Wenn Sie „Manuell" im Norton AntiVirus-Reparaturassistenten auswählen, wird das Dialogfeld „Gefundene Probleme" (Abbildung 3-3) geöffnet. Darin sind alle infizierten Elemente aufgelistet.

So entfernen Sie die Viren nacheinander manuell:

1. Wählen Sie „Manuell" im Norton AntiVirus-Reparaturassistenten aus (siehe Abbildung 3-1), und klicken Sie auf „Weiter".

   Das Dialogfeld „Gefundene Probleme" wird geöffnet (Abbildung 3-3). Darin sind alle infizierten Elemente aufgelistet.
2. Heben Sie einen Eintrag im Listenfeld hervor.
3. Lesen Sie die Meldung unten im Dialogfeld, damit Sie wissen, um welche Art von Problem es sich jeweils handelt.
4. Klicken Sie dann auf eine der Schaltflächen. Informationen über die Schaltflächen im Dialogfeld „Gefundene Probleme" finden Sie unter „Schaltflächen" auf Seite 36.

Abbildung 3-3 Dialogfeld „Gefundene Probleme"



☞ **Hinweis:** Manche Benutzer möchten lieber sofort eine Warnmeldung angezeigt bekommen, wenn ein Virus während einer Prüfung entdeckt wird, und nicht erst am Ende der Prüfung. Wie Sie das einstellen, ist unter „So stellen Sie zusätzliche Prüfoptionen ein:" auf Seite 67 beschrieben.

Schaltflächen

Tabelle 3-1, „Schaltflächen", beschreibt alle Schaltflächen, die Norton AntiVirus als Reaktion auf einen Virusalarm anzeigen kann. Diese Schaltflächen werden im Dialogfeld „Gefundene Probleme", bei Virusalarmen von Auto-Protect und bei Virusalarmen der Prüfung beim Systemstart angezeigt. In späteren Abschnitten dieses Kapitels wird genau angegeben, wie Sie auf Virusalarme reagieren können. Beispiele für Virusalarme finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden" auf Seite 33 und „Entfernen von Viren, die während der Prüfung beim Systemstart entdeckt wurden" auf Seite 47.

Beachten Sie, daß einige Schaltflächen aus folgenden Gründen grau dargestellt sein können oder gar nicht angezeigt werden:

- Die Option kann in Ihrer speziellen Konfiguration von Norton AntiVirus nicht verwendet werden. Die Optionen werden in den Registern „Scanner“, „Auto-Protect“ und „Impfung“ eingestellt. Informationen dazu finden Sie in Kapitel 5, „Anpassen von Norton AntiVirus“.
- Norton AntiVirus hat festgestellt, daß eine bestimmte Aktion in der aktuellen Situation nicht durchgeführt werden kann.

Tabelle 3-1 Schaltflächen für die Reaktion auf Warnmeldungen

Schaltfläche	Ergebnis	Zusätzliche Informationen
Reparieren	Entfernt den Virus und stellt die infizierte Datei oder den Boot-Sektor in seinem ursprünglichen Zustand wieder her.	Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.
	Stellt bei Dateien oder Boot-Sektoren mit Impfänderungen den Zustand vor der letzten Änderung wieder her.	Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.
Löschen	Entfernt den Virus durch Löschen der infizierten Datei.	Gelöschte Dateien können nicht wiederhergestellt werden. Ersetzen Sie die Datei nach dem Löschen durch eine nichtinfizierte Kopie.
Stop	Stoppt die aktuelle Operation. Wenn gerade eine Prüfung durchgeführt wird, wird diese gestoppt. Wenn Sie auf eine Datei zugreifen (z.B. um ein Programm zu starten), wird der Zugriff verweigert.	Es reicht nicht aus, auf „Stop“ zu klicken, um das gemeldete Problem zu lösen. Wenn es sich allerdings um einen Virus handelt, wird dieser daran gehindert, den Speicher zu befallen.
Weiter	Setzt die aktuelle Operation fort. Wenn eine Prüfung durchgeführt wird, wird diese fortgesetzt. Wenn Sie auf eine Datei zugreifen (z.B. um ein Programm zu starten), wird der Zugriff gewährt.	Es reicht nicht aus, auf „Weiter“ zu klicken, um das gemeldete Problem zu lösen. NAV wird Sie in Zukunft über die gleiche Aktivität benachrichtigen.

Tabelle 3-1 Schaltflächen für die Reaktion auf Warnmeldungen

Schaltfläche	Ergebnis	Zusätzliche Informationen
Ausschließen	Setzt die Operation fort und schließt die Datei von zukünftigen Benachrichtigungen dieser Art aus.	Verwenden Sie diese Schaltfläche nur, wenn Sie sicher sind, daß es sich um einen zulässigen Vorgang handelt. Wenn Sie eine Datei ausschließen, zeigt Norton AntiVirus für diese Datei keine Meldungen mehr an.Weitere Informationen hierzu finden Sie unter „Verwalten von Ausnahmen“ auf Seite 72.
Impfen	Speichert Daten über die Datei oder den Boot-Sektor, die später zur Prüfung seiner Integrität verwendet werden.	Weitere Informationen hierzu finden Sie unter „Dateien zum ersten Mal impfen“ auf Seite 45.
	Aktualisiert die Impfdaten für Dateien oder Boot-Sektoren, die sich seit der letzten Impfung geändert haben.	Manchmal weisen Impfänderungen auf das Vorhandensein eines unbekannten Virus hin. Weitere Informationen hierzu finden Sie unter „Geänderte Dateien neu impfen“ auf Seite 46.
Info...	Zeigt detaillierte Informationen über den gefundenen Virus an.	Weitere Informationen hierzu finden Sie unter „Anzeigen der Virusliste“ auf Seite 60.

Entfernen von Viren, die von Auto-Protect entdeckt wurden

Norton AntiVirus Auto-Protect überwacht Ihren Computer ständig auf Viren und zeigt sofort eine Warnmeldung an, wenn eine mögliche Virusaktivität auftritt. Diese Warnmeldungen werden im Textmodus angezeigt, da alle Operationen, auch Bildschirmoperationen, unterbrochen werden, bis Sie auf die Warnmeldung reagiert und das mögliche Problem behoben haben.

Sie werden in folgenden Fällen gewarnt:

- Ein Virus wird in einem Programm gefunden, das Sie starten wollen, oder in einer Programmdatei, die Sie kopieren wollen.
- Ein Virus wird im Arbeitsspeicher gefunden.
- Eine virusähnliche Aktivität wird entdeckt (einen Vorgang, den Viren oft durchführen, wenn sie sich ausbreiten oder Dateien beschädigen).
- Ein Impfproblem wird entdeckt (entweder wurde eine Datei nicht geimpft, oder eine Datei hat sich seit der Impfung geändert).

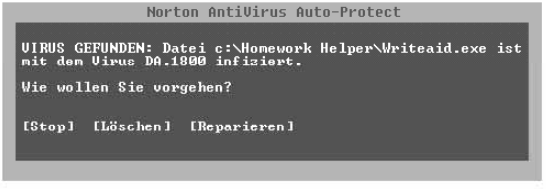
Abbildung 3-4 zeigt Beispiele für die verschiedenen Arten der Warnmeldungen von Auto-Protect.

☞ **Hinweis:** Eine kurze Beschreibung der Schaltflächen in Warnmeldungen finden Sie unter „Schaltflächen“ auf Seite 36.

Abbildung 3-4 Warnmeldungen von Auto-Protect

Warnmeldung bei einem Virus im Arbeitsspeicher

Warnmeldung bei einem entdeckten Virus



Warnmeldung bei einer virusähnlichen Aktivität

Warnmeldung bei einem Impfproblem

So gehen Sie vor, wenn eine Warnmeldung von Auto-Protect angezeigt wird:

1. Lesen Sie die Meldung im Warnfeld, damit Sie wissen, welche Art von Problem aufgetreten ist.
2. Lesen Sie im entsprechenden Abschnitt nach, wie Sie weiter vorgehen müssen:
   - „Reaktion auf Warnmeldungen von Auto-Protect über Viren im Arbeitsspeicher“ auf Seite 40
   - „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42
   - „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44
   - „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45
3. Wenn Sie eine andere Meldung sehen, die Sie nicht verstehen, schlagen Sie in Anhang D, „Systemmeldungen“ auf Seite 117 nach.

Reaktion auf Warnmeldungen von Auto-Protect über Viren im Arbeitsspeicher

Wenn ein Virus im Arbeitsspeicher ist, wurde er aktiviert, breitet sich auf andere Dateien aus und beschädigt im schlimmsten Fall Dateien auf Ihrer Festplatte. Wenn Norton AntiVirus Viren im Arbeitsspeicher entdeckt, werden alle Operationen des Computers sofort gestoppt.

Abbildung 3-5 Warnmeldung über einen Virus im Arbeitsspeicher

So reagieren Sie auf eine Warnmeldung über einen Virus im Arbeitsspeicher:

1. Wählen Sie „OK“, um Ihren Computer herunterzufahren.
2. Befolgen Sie die Windows-Anleitungen zum Beenden von Programmen und Speichern von Daten.
3. Wenn das Herunterfahren abgeschlossen ist, schalten Sie Ihren Computer mit dem Ein-/Ausschalter aus.

   Sobald Ihr Computer ausgeschaltet ist, wird der Virus aus dem Arbeitsspeicher entfernt und kann sich nicht weiter ausbreiten.
4. Verwenden Sie Ihre schreibgeschützte Rettungsdiskette, um Ihren Computer neu zu starten, und führen Sie eine erneute Prüfung durch, um den Virus zu finden und zu entfernen. Weitere Informationen finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

Wenn Sie nicht über einen Rettungsdiskettensatz verfügen, können Sie die schreibgeschützte Startdiskette von Windows 95 oder DOS (Version 5.0 oder höher) verwenden, um Ihren Computer neu zu starten. Dann verwenden Sie die Original-Installationsdiskette Norton AntiVirus Diskette 2 (Notfalldiskette), um NAVDX zu starten. Weitere Informationen finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

Sie können auch auf einem virenfreien Computer, auf dem DOS 5.0 oder höher installiert ist, eine Startdiskette erstellen. Im Handbuch zu Ihrem Betriebssystem finden Sie die dazu nötigen Anleitungen. Verwenden Sie dazu nicht den infizierten Computer; der Virus könnte die Startdiskette infizieren, die Sie gerade erstellen. Wenn Ihnen kein nichtinfizierter Computer zur Verfügung steht, sind die meisten Händler bereit, Ihnen eine Startdiskette zu erstellen.

☞ **Achtung:** Wenn Sie keine Rettungsdiskette bzw. keine nichtinfizierte Startdiskette zum Neustart Ihres Computers verwenden, laufen Sie Gefahr, den Virus wieder zu aktivieren.

Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren

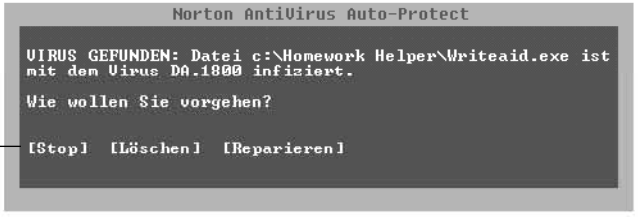
Es gibt zwei Möglichkeiten, einen Virus von Ihrem Computer zu entfernen:

- Reparieren Sie die infizierten Dateien, den Boot-Sektor oder Master-Boot-Sektor.
- Löschen Sie die infizierte Datei von der Festplatte.

  Sie können allerdings keine infizierten Systemdateien, Boot-Sektoren oder Master-Boot-Sektoren löschen, da diese Informationen enthalten, die Ihr Computer für den Systemstart benötigt. Im Abschnitt „Was tun, wenn die Reparatur nicht erfolgreich war?“ auf Seite 50 finden Sie Anleitungen für den Fall, daß Sie eine Datei nicht reparieren, aber auch nicht löschen können.

☞ **Achtung:** Dateien, die von Norton AntiVirus gelöscht werden, können selbst mit speziellen Programmen zur Dateiwiederherstellung, z.B. Norton Utilities, nicht wiederhergestellt werden.

Abbildung 3-6 Warnmeldung bei einem entdeckten Virus



Aktionen, mit denen Sie auf die Warnung reagieren können.

So reparieren Sie eine infizierte Datei oder einen Boot-Sektor:

1. Wählen Sie „Reparieren“ im Warnfeld.

   Wenn die Schaltfläche „Reparieren“ grau dargestellt ist, ist entweder Norton AntiVirus so konfiguriert, daß sie nicht aktiviert wird, oder das Element kann nicht repariert werden.

2. Überprüfen Sie nach der Reparatur von infizierten Dateien oder Boot-Sektoren die Laufwerke und Disketten erneut mit Norton AntiVirus. So stellen Sie sicher, daß keine anderen Dateien oder Boot-Sektoren mit Viren infiziert sind.

☞ **Hinweis:** Norton AntiVirus ist so eingestellt, daß es Sicherungskopien der Dateien erstellt, bevor sie repariert werden. Die Backup-Dateien haben die Erweiterung „VIR“ und werden im Ordner als „VIR Datei“ angezeigt. Diese Backup-Dateien werden in Zukunft nicht mehr überprüft. Wenn Sie wissen, daß eine Datei erfolgreich repariert wurde, löschen Sie die Backup-Datei. Weitere Informationen hierzu finden Sie unter „Einstellen der allgemeinen Prüfoptionen“ auf Seite 80.

So löschen Sie eine infizierte Datei:

1. Wählen Sie „Löschen“ im Warnfeld, und befolgen Sie anschließend die Anleitungen auf dem Bildschirm.

   Wenn die Schaltfläche „Löschen“ grau dargestellt ist, ist entweder Norton AntiVirus so konfiguriert, daß sie nicht aktiviert wird, oder das Element kann nicht gelöscht werden.

2. Nachdem Sie infizierte Dateien gelöscht haben, überprüfen Sie alle Laufwerke und Disketten mit Norton AntiVirus, um sicherzustellen, daß keine Dateien mehr infiziert sind.

3. Wenn Sie sicher sind, daß Ihr System virenfrei ist, können Sie die gelöschten Dateien durch nichtinfizierte Kopien ersetzen. Überprüfen Sie die Kopien, bevor Sie sie auf die Festplatte kopieren.

☞ **Tip:** Wenn Sie vergessen haben, welche Datei ersetzt werden muß, suchen Sie in der Protokolldatei nach dem Dateinamen. Informationen zum Anzeigen der Protokolldatei finden Sie unter „Anzeigen der Protokolldatei“ auf Seite 25.

Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten

Eine Warnmeldung über virusähnliche Aktivitäten wird angezeigt, wenn Norton AntiVirus Aktivitäten entdeckt, die für Viren typisch sind, wenn sie sich verbreiten oder Dateien beschädigen. Diese Warnmeldungen werden im Zeichenmodus und nicht im Grafikmodus angezeigt. Norton AntiVirus unterbricht alle Operationen, auch Bildschirmoperationen, bis das gefundene Problem behoben ist.

Abbildung 3-7 Warnmeldung bei einer virusähnlichen Aktivität

Aktionen, mit denen Sie auf die Warnung reagieren können.

☞ **Hinweis:** Eine Warnmeldung über eine virusähnliche Aktivität bedeutet nicht unbedingt, daß Ihr Computer mit Viren infiziert ist – es handelt sich lediglich um eine Warnung. Sie können entscheiden, ob die Aktivität in dem gegebenen Rahmen erlaubt ist oder nicht. Beschreibungen aller virusähnlichen Aktivitäten, die Norton AntiVirus entdeckt, finden Sie unter „Anpassen der automatischen Schutzfunktion“ auf Seite 81.

So reagieren Sie auf eine Warnmeldung über virusähnliche Aktivitäten:

Stop

Wenn die entdeckte Aktivität nicht zu dem Vorgang paßt, den Sie gerade durchführen, wählen Sie „Stop“, um die Aktivität zu unterbrechen.

Wenn Sie z.B. ein Computerspiel spielen und die Warnmeldung erhalten, daß versucht wird, in die Boot-Sektoren Ihrer Festplatte zu schreiben, wählen Sie „Stop“, um diesen Vorgang zu verhindern.

Weiter

Wenn die Meldung eine Aktivität beschreibt, die im Rahmen des von Ihnen ausgeführten Programms zulässig ist, wählen Sie „Weiter“, damit die Aktivität fortgesetzt werden kann.

Wenn Sie z.B. ein Programm aktualisieren und Norton AntiVirus Sie warnt, daß versucht wird, in eine Programmdatei zu schreiben, wählen Sie „Weiter“.

Ausschließen

Wenn die Aktivität im Rahmen des von Ihnen ausgeführten Programms zulässig ist und Sie zukünftig von Norton AntiVirus nicht mehr auf diese Aktivität (von diesem Programm) hingewiesen werden wollen, wählen Sie „Ausschließen“.

Falls Sie z.B. mit einem Programm zur Laufwerksformatierung eine Startdiskette erstellen und verhindern wollen, daß Norton AntiVirus Sie jedesmal warnt, wenn Sie dieses Programm verwenden, wählen Sie „Ausschließen“.

Reaktion auf Impfalarme von Auto-Protect

Norton AntiVirus zeigt in folgenden Fällen Impfalarme an:

- Dateien oder Boot-Sektoren wurden nicht geimpft.
- Dateien oder Boot-Sektoren wurden seit der letzten Impfung geändert. Änderungen an geimpften Dateien können auf einen Virus hinweisen.

Abbildung 3-8 Impfalarm

Aktionen, mit denen Sie auf die Warnung reagieren können.

Dateien zum ersten Mal impfen

Norton AntiVirus ist so konfiguriert, daß es Boot-Sektoren und Systemdateien impft. Wenn Sie festlegen, daß auch Programmdateien geimpft werden, wird Norton AntiVirus so konfiguriert, daß es nach ungeimpften Dateien sucht und diese automatisch impft.

Wenn Sie statt dessen „Meldung“ als Vorgehen bei „Ermittlung eines nicht geimpften Elements“ wählen, warnt Norton AntiVirus Sie, wenn eine ungeimpfte Datei entdeckt wird. Sie haben folgende Möglichkeiten, um auf einen Impfalarm zu reagieren. Unter „Anpassen der Impfung“ auf Seite 90 finden Sie weitere Anleitungen zum Anpassen der Impfoptionen.

So reagieren Sie auf eine Aufforderung zum erneuten Impfen:

Wählen Sie „Stop“, um den aktuellen Vorgang zu unterbrechen.

Wenn Sie z.B. auf eine Datei zugreifen (um beispielsweise ein Programm zu starten), wird der Zugriff verweigert.

Wenn Sie fortfahren wollen, ohne etwas zu unternehmen, wählen Sie „Weiter“.

Damit verhindern Sie nicht, daß Norton AntiVirus in der Zukunft Meldungen über diese Datei anzeigt.

Wählen Sie „Impfen“, um Impfdaten für die Datei oder den Boot-Sektor zu erstellen.

Wenn Sie eine Datei oder einen Boot-Sektor impfen, informiert Sie Norton AntiVirus, wenn die Datei geändert wird. Manchmal weisen Änderungen an einer Datei auf das Vorhandensein eines unbekannten Virus hin. Bei der Impfung werden keine Änderungen an der eigentlichen Datei oder dem Boot-Sektor vorgenommen, es wird lediglich die Datei mit den Impfdaten aktualisiert.

Wenn Sie die Datei nicht impfen und nicht mehr darüber informiert werden wollen, daß die Datei nicht geimpft ist, wählen Sie „Ausschließen“.

Wenn Sie die Datei ausschließen, wächst das Risiko einer Infektion dieser Datei durch einen unbekannten Virus.

Geänderte Dateien neu impfen

Es gibt folgende Ursachen für Impfänderungen an Dateien:

- Die Datei wurde seit der letzten Impfung geändert; die Änderungen sind zulässig. Sie haben vielleicht eine neue Version eines Programms installiert und vergessen, die Programmdateien zu impfen.
- Die Datei enthält einen Virus, der nicht in der Definitionsdatei enthalten ist. (Vielleicht verfügen Sie nicht über die aktuellsten Virusdefinitionen, oder es ist ein neuer Virus, dessen Definition Norton AntiVirus noch nicht kennt.)

☞ **Hinweis:** Impfänderungen in Boot-Sektoren und Systemdateien weisen mit ziemlicher Sicherheit auf einen unbekannten Virus hin. Boot-Sektoren und Systemdateien ändern sich nur in wenigen Fällen, z.B. bei der Installation eines neuen Betriebssystems oder einer Partitionierung der Festplatte.

So reagieren Sie auf eine Impfänderung:

Wenn die Änderungen an einer Datei oder einem Boot-Sektor zulässig sind, wählen Sie „Impfen“, um neue Impfdaten zu erstellen.

Wenn Sie eine Virusinfektion vermuten, wählen Sie „Reparieren“, um die Datei in ihrem Zustand vor der letzten Impfung wiederherzustellen.

Wenn Sie eine Virusinfektion einer Programmdatei vermuten und über eine nichtinfizierte Kopie dieser Datei verfügen, wählen Sie „Löschen“. Ersetzen Sie die Datei anschließend durch die nichtinfizierte Kopie. Mit Norton AntiVirus gelöschte Dateien können nicht wiederhergestellt werden.

Wenn Sie die Datei nicht neu impfen wollen und keine Meldungen über Impfänderungen an dieser Datei wünschen, wählen Sie „Ausschließen“.

Entfernen von Viren, die während der Prüfung beim Systemstart entdeckt wurden

Die Prüfungen beim Systemstart finden Viren, die solche Dateien und Boot-Sektoren infizieren, die Ihr Computer zum Systemstart benötigt. Diese Prüfungen stellen einen sehr wichtigen Teil des Virenschutzes dar, denn sie stellen bei jedem Systemstart sicher, daß Ihr Computer virenfrei ist. Wenn während einer Prüfung beim Systemstart Viren gefunden werden, sollten Sie das sehr ernst nehmen und sofort Gegenmaßnahmen ergreifen, da alle Ihre Dateien und Daten nun in Gefahr sind.

Sie werden in folgenden Fällen gewarnt:

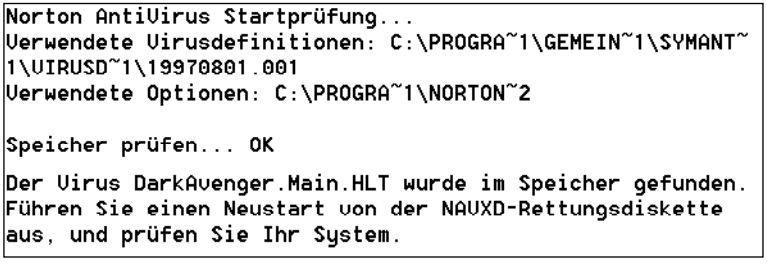
- Ein Virus wird im Arbeitsspeicher gefunden.
- Ein Virus wird in einem Systemprogramm oder Boot-Sektor gefunden.

Da die Prüfung beim Systemstart zu einem Zeitpunkt erfolgt, da Windows noch nicht geladen ist, werden die Warnmeldungen im Textmodus auf dem Bildschirm angezeigt. Sie können auf das Problem reagieren, indem Sie die Buchstabentaste drücken, die in der gewünschten Option hervorgehoben wird.

Reaktion auf Warnmeldungen der Prüfung beim Systemstart über Viren im Arbeitsspeicher

Ein Virus im Arbeitsspeicher bedeutet, daß der Virus aktiviert wurde, sich auf andere Dateien ausbreitet und, im schlimmsten Fall, Dateien auf Ihrer Platte beschädigt. Wenn Norton AntiVirus einen Virus im Arbeitsspeicher entdeckt, werden alle Verarbeitungsprozesse sofort gestoppt.

Abbildung 3-9 Meldung der Prüfung beim Systemstart über Viren im Speicher



So reagieren Sie auf eine Warnmeldung der Prüfung beim Systemstart über Viren im Arbeitsspeicher:

1. Schalten Sie Ihren Computer mit dem Netzschalter aus.

   Sobald Sie Ihren Computer ausschalten, wird der Virus aus dem Arbeitsspeicher entfernt und kann sich nicht weiter ausbreiten.

2. Verwenden Sie Ihre schreibgeschützte Norton AntiVirus Rettungs- und Startdiskette, um Ihren Computer neu zu starten, und führen Sie eine Prüfung mit dem Rettungsdiskettensatz durch, um den Virus zu finden und zu entfernen. Weitere Hinweise dazu finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

Wenn Sie nicht über einen eigenen Rettungsdiskettensatz verfügen, können Sie die schreibgeschützte Notfalldiskette verwenden, die mit Norton AntiVirus geliefert wird. Weitere Informationen dazu finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

Reaktion auf Warnmeldungen der Prüfung beim Systemstart über entdeckte Viren

Warnmeldungen über entdeckte Viren während einer Prüfung beim Systemstart zeigen ein ernstes Problem an. Wenn sich ein Virus in einer Systemdatei oder einem Boot-Sektor befindet, sind alle Daten Ihres Computers in unmittelbarer Gefahr. Reparieren Sie das infizierte Element mit Hilfe von Norton AntiVirus, um den Virus zu entfernen.

Abbildung 3-10 Meldung der Prüfung beim Systemstart über einen entdeckten Virus

```
Norton AntiVirus Startprüfung...
Verwendete Virusdefinitionen: C:\PROGRA~1\GEMEIN~1\SYMANT~
1\VIRUSD~1\19970801.001
Verwendete Optionen: C:\PROGRA~1\NORTON~2

Speicher prüfen... OK
Master-Boot-Sektor prüfen... OK
Boot-Sektoren prüfen... OK

C:\WINDOWS\WIN.COM ist mit dem Virus Cascade (1) infiziert.
R)eparieren  L)öschen  W)eiter?
```

So reparieren Sie eine infizierte Datei oder einen Boot-Sektor beim Systemstart:

1. Wählen Sie „Reparieren“.
2. Überprüfen Sie nach der Reparatur von infizierten Dateien oder Boot-Sektoren die Laufwerke und Disketten erneut mit Norton AntiVirus. So stellen Sie sicher, daß keine anderen Dateien oder Boot-Sektoren mit Viren infiziert sind.

Infizierte Boot-Sektoren, Master-Boot-Sektoren und einige Systemdateien können Sie nicht löschen, um einen Virus zu entfernen, da sie Informationen enthalten, die Ihr Computer zum Systemstart benötigt. Wie Sie vorgehen, wenn eine Reparatur nicht möglich ist und das Element nicht gelöscht werden kann, ist im Abschnitt „Was tun, wenn die Reparatur nicht erfolgreich war?“ auf Seite 50 beschrieben.

Was tun, wenn die Reparatur nicht erfolgreich war?

In dem seltenen Fall, daß Norton AntiVirus die Datei oder den Boot-Sektor nicht reparieren kann, werden Sie darauf hingewiesen, daß die Reparatur fehlgeschlagen ist.

Datei kann nicht repariert werden

Wenn Norton AntiVirus eine infizierte Datei nicht reparieren kann, müssen Sie die Datei löschen, um den Virus zu entfernen. Nachdem Sie die infizierte Datei gelöscht haben, können Sie sie durch eine nichtinfizierte Kopie ersetzen. Verwenden Sie eine nichtinfizierte Sicherungskopie oder die Original-Programmdiskette, die Sie mit dem Programm erhalten haben. Wenn Sie keine Sicherungskopie haben und auch die Originaldisketten nicht mehr finden können, wenden Sie sich an den Programmhersteller, um Ersatzdisketten zu erhalten.

Systemdatei kann nicht repariert werden

Wenn es sich bei der infizierten Datei um eine Systemdatei handelt, starten Sie Ihren Computer mit einer nichtinfizierten, schreibgeschützten Diskette, und installieren Sie Windows neu. Sie können dazu Ihre Norton AntiVirus Rettungsdiskette (siehe „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27) oder die Windows 95 Startdiskette verwenden, die Sie bei der Installation von Windows erstellt haben. Sie können auch die Startdiskette einer beliebigen Version von DOS ab Version 5.0 verwenden.

Reparatur eines Boot-Sektors fehlgeschlagen

Wenn Norton AntiVirus einen Master-Boot-Sektor oder einen Boot-Sektor auf Ihrer Festplatte nicht reparieren konnte, können Sie den Boot-Sektor mit Ihrer schreibgeschützten Rettungsdiskette wiederherstellen. Anleitungen hierzu finden Sie im Abschnitt „Wiederherstellen der Festplatte“ auf Seite 108.

Wenn Norton AntiVirus einen Boot-Sektor auf einer Diskette nicht reparieren konnte, können Sie trotzdem wichtige Dateien von dieser Diskette auf eine andere Diskette kopieren. Seien Sie allerdings vorsichtig – die Diskette ist immer noch infiziert. Überprüfen Sie erneut alle von der Diskette kopierten Dateien. Nachdem Sie die wichtigen Dateien von der infizierten Diskette kopiert haben, werfen Sie die Diskette weg, oder formatieren Sie sie neu. (Verwenden Sie dazu die Windows 95 Option „Vollständig“ als Formatiertyp.)

Viren aus komprimierten Dateien entfernen

Norton AntiVirus kann zwar eine infizierte Datei in einer komprimierten Datei entdecken, die Datei kann aber im komprimierten Zustand nicht repariert werden.

So entfernen Sie Viren aus infizierten komprimierten Dateien:

1. Erstellen Sie einen temporären Ordner.
2. Klicken Sie auf das Symbol von Auto-Protect in der Windows Task-Leiste, um Auto-Protect vorübergehend zu deaktivieren.
3. Entkomprimieren Sie die komprimierte Datei in den temporären Ordner.
4. Löschen Sie die infizierte komprimierte Datei.
5. Prüfen Sie den temporären Ordner, und reparieren oder löschen Sie alle infizierten Dateien.
6. Komprimieren Sie die Dateien im temporären Ordner erneut, wenn gewünscht.
7. Klicken Sie auf das Symbol von Auto-Protect in der Windows Task-Leiste, um Auto-Protect wieder zu aktivieren.

K A P I T E L 4

Schutz vor neuen Viren

Norton AntiVirus verwendet die Informationen in den Virusdefinitionsdateien, um die Viren während einer Prüfung zu erkennen. Wenn neue Viren entdeckt werden, werden ihre Virusdefinitionen zu den Virusdefinitionsdateien hinzugefügt. Um zu verhindern, daß neue Viren Ihren Computer befallen, sollten Sie die Virusdefinitionsdateien regelmäßig aktualisieren. Aktualisierte Virusdefinitionsdateien sind monatlich erhältlich.

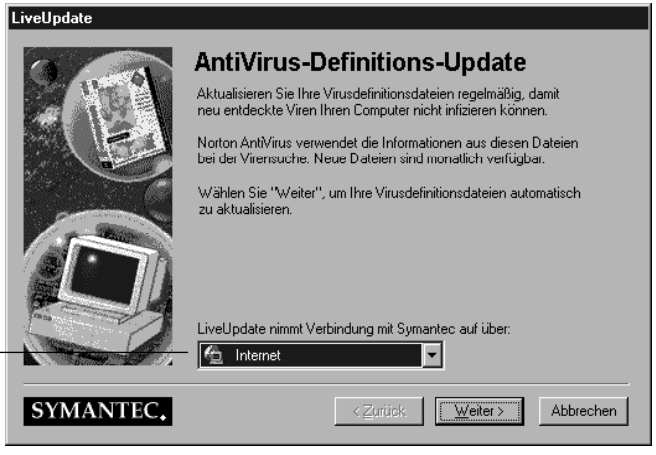
Automatische Aktualisierung der Virusdefinitionen

Um sicherzustellen, daß Ihr Virenschutz immer auf dem neuesten Stand ist, kann Norton AntiVirus die Virusdefinitionsdateien auf Ihrem Computer automatisch aktualisieren. Sie benötigen dazu lediglich folgende Komponenten:

- Einen Internet-Anschluß
- Ein korrekt angeschlossenes Modem

Am besten gewöhnen Sie sich an, Ihre Virusdefinitionen einmal monatlich zu aktualisieren.

Abbildung 4-1 Virusdefinitionen automatisch aktualisieren



Geben Sie die Verbindungsart an, oder lassen Sie sie auswählen.

So aktualisieren Sie die Virusdefinitionen automatisch:

1. Klicken Sie im Hauptfenster von Norton AntiVirus auf „LiveUpdate“ (siehe Abbildung 4-1).
2. Wählen Sie im Dropdown-Listenfeld eine der folgenden Optionen aus:
   - „Gerät automatisch finden“: Norton AntiVirus stellt fest, ob Sie einen Internet-Anschluß haben oder eine Verbindung über Ihr Modem herstellen müssen.
   - „Internet“: Norton AntiVirus stellt eine Verbindung zum FTP-Server (File Transfer Protocol) von Symantec im Internet her.
   - „Modem“: Norton AntiVirus wählt eine voreingestellte Nummer und stellt über Ihr Modem eine Verbindung zu einem Symantec-Server her.
3. Klicken Sie auf „Weiter“, um die automatische Aktualisierung zu starten.

Unabhängig davon, welche Option Sie wählen, stellt Norton AntiVirus die Verbindung her, lädt die richtigen Dateien herunter und installiert diese auf Ihrem Computer. Sie müssen nichts weiter mehr tun.

Nachdem die Aktualisierung beendet ist, lesen Sie die ebenfalls heruntergeladenen neuen Textdateien (*.TXT) in Ihrem Norton AntiVirus-Ordner. Sie enthalten die aktuellsten Informationen über neu entdeckte Viren und über besondere Vorsichtsmaßnahmen, die Sie treffen sollten. Normalerweise befinden sich die Dateien von Norton AntiVirus unter C:\Programme\Norton AntiVirus.

☞ **Hinweis:** Wenn die Verbindung über Ihr Modem hergestellt wird, erscheinen die Gebühren dafür auf Ihrer Telefonrechnung.

Planen einer automatischen LiveUpdate-Sitzung

Nachdem Sie erstmals eine LiveUpdate-Sitzung beendet und sich dabei von der korrekten Funktionsweise von LiveUpdate überzeugt haben, können Sie künftige LiveUpdate-Sitzungen mit Scheduler planen. LiveUpdate wird in diesem Fall zu einem bestimmten Zeitpunkt oder in regelmäßigen Intervallen gestartet und unbeaufsichtigt ausgeführt. Weitere Informationen über den Norton Program Scheduler finden Sie unter „Planen von Virusprüfungen“ auf Seite 28.

So planen Sie eine unbeaufsichtigte LiveUpdate-Sitzung:

1. Starten Sie den Norton Program Scheduler auf eine der folgenden Arten:
   - Klicken Sie auf „Scheduler“ im Hauptfenster von Norton AntiVirus.
   - Wählen Sie „Norton Program Scheduler“ im Windows-Menü „Start“.
2. Klicken Sie auf „Hinzufügen“.

   Daraufhin wird das Dialogfeld „Ereignis hinzufügen“ angezeigt.
3. Wählen Sie „LiveUpdate starten“ im Dropdown-Listenfeld „Ereignistyp“.

   Daraufhin ändert sich der Inhalt des Dialogfelds. Es enthält nun nur die Optionen, die für LiveUpdate relevant sind.

Abbildung 4-2 Dialogfeld „Ereignis hinzufügen“ mit ausgewählter Option „LiveUpdate starten“

4. Aktivieren Sie das Kontrollkästchen „Dieses Ereignis aktivieren“.

   Wenn Sie das Kontrollkästchen deaktivieren, kann LiveUpdate nicht gestartet werden.
5. Aktivieren Sie das Kontrollkästchen „Signalton“, wenn das Starten der LiveUpdate-Sitzung von einem Signalton begleitet werden soll.
6. Geben Sie in das Textfeld „Beschreibung“ eine kurze Beschreibung des Ereignisses ein.

   Dieser Text erscheint im Dialogfeld „Norton Program Scheduler“ in der Liste „Ereignisse“.
7. Geben Sie in das Textfeld „Auszuführende Befehlszeile“ den Befehlszeilenschalter `/PROMPT` ein, wenn Sie die LiveUpdate-Sitzung beim Starten zum geplanten Zeitpunkt bestätigen wollen.
8. Geben Sie im Dropdown-Listenfeld „Häufigkeit“ an, wie oft LiveUpdate gestartet und unbeaufsichtigt ausgeführt werden soll.

9 Schließen Sie die Ereignisplanung ab, indem Sie die gewünschte Uhrzeit und das gewünschte Datum für das Ereignis einstellen.

10 Klicken Sie auf „OK“. Sie werden aufgefordert, das neue Ereignis zu bestätigen. Klicken Sie in dem Dialogfeld mit der Bestätigungsmeldung ebenfalls auf „OK“.

Manuelle Aktualisierung der Virusdefinitionen

Sie können die von Symantec bereitgestellten Virusdefinitionsdateien auch manuell von verschiedenen Quellen herunterladen. Wählen Sie die für Sie geeignetste. Auch wenn Sie Ihre Virusdefinitionen automatisch aktualisieren, können Sie von diesen Quellen umfangreiche Informationen über Viren im allgemeinen beziehen sowie Informationen und Aktualisierungen zu allen von Symantec angebotenen Produkten.

Bezugsquellen für aktuelle Virusdefinitionen

Die Datei, die Sie herunterladen, ist ein spezielles Aktualisierungsprogramm, das Norton AntiVirus automatisch auf Ihrem Computer sucht und die neuen Virusdefinitionsdateien installiert. Ihr Name ändert sich von Monat zu Monat. Er hat folgendes Format: *mm*NAV*jj*.EXE, wobei *mm* für den Monat und *jj* für das Jahr steht. Informationen zur Verwendung des Aktualisierungsprogramms finden Sie unter „Neue Virusdefinitionsdateien installieren“ auf Seite 59.

Symantec BBS

Einstellungen für das Symantec BBS:

- 8 Datenbits, 1 Stopbit, keine Parität

Telefonnummer des Symantec BBS:

- Modems von 300 bis 14400 Baud: +31 71 5353169
- Modems von 300 bis 28800 Baud: +31 71 5322852

So greifen Sie im Hauptmenü des Symantec BBS auf Virusdefinitionen zu:

1 Drücken Sie F, um eine Datei zu laden.

2 Drücken Sie N, um die aktuellen NAV-Virusdefinitionen zu laden.

3 Befolgen Sie die Anleitungen auf dem Bildschirm, um die Dateien herunterzuladen.

Geben Sie bei einer beliebigen Eingabeaufforderung `/GO GETFILE` ein, um zu diesem Menü zurückzukehren.

America Online

So greifen Sie auf das Symantec Forum zu:

1. Wählen Sie „Keyword“ im Menü „GoTo“.
2. Geben Sie `SYMANTEC` ein.
3. Klicken Sie auf „Virus Control Center“.
4. Klicken Sie auf „Virus Definitions Library“.

CompuServe

Die aktuellen Virusdefinitionsdateien befinden sich im Symantec Forum.

So greifen Sie direkt auf das Symantec Forum zu:

1. Sie haben folgende Möglichkeiten:
   - Wählen Sie „Go“ im Menü „Services“, und geben Sie `SYMEUR` ein.
   - Geben Sie bei einer beliebigen Eingabeaufforderung (!) `GO SYMEUR` ein.
2. Die Dateien befinden sich in der `NAV-`Bibliothek.

Internet

Die aktuellen Virusdefinitionsdateien sind über Symantecs FTP-Dienst erhältlich.

So verwenden Sie den FTP-Dienst:

1. Greifen Sie auf `ftp.symantec.com` zu.
2. Die Dateien befinden sich im Verzeichnis `/public/AntiVirusDefs/nav/`.
3. Laden Sie die zuletzt dorthin gestellte Datei herunter.

So verwenden Sie den FTP-Dienst über das World Wide Web:

1. Greifen Sie auf `www.symantec.com` zu.
2. Klicken Sie auf „AntiVirus Research Center“.
3. Klicken Sie auf „Download Updates“.
4. Klicken Sie auf „Norton AntiVirus“.
5. Befolgen Sie die Anleitungen auf dem Bildschirm.

Microsoft Network

So greifen Sie auf den Symantec-Dienst zu:

1. Wählen Sie „Go To“ im Menü „View“.
2. Wählen Sie „Other Location“.
3. Geben Sie `SYMANTEC` ein.
4. Doppelklicken Sie auf „Support Solutions“.
5. Doppelklicken Sie auf „Symantec File Library“.
6. Die Virusdefinitionen befinden sich in der Bibliothek „Norton AntiVirus File Library“.

Monatliche Aktualisierung der Virusdefinitionsdiskette

Sie können bei Symantec monatliche Aktualisierungen der Virusdefinitionsdateien per Post anfordern.

Gehen Sie dazu folgendermaßen vor:

- Wenden Sie sich an Ihre regionale Symantec-Vertretung. Die Adressen finden Sie am Ende dieses Handbuchs.

Neue Virusdefinitionsdateien installieren

Die Aktualisierungsdatei, die Sie herunterladen, ist ein spezielles Programm, das die neuen Virusdefinitionsdateien automatisch auf Ihrem Computer installiert.

So installieren Sie die neuen Virusdefinitionen:

1. Laden Sie das Aktualisierungsprogramm in einen beliebigen Ordner auf Ihrem Computer herunter.

   Der Dateiname hat das Format *mm*NAV*jj*.EXE, wobei *mm* für den Monat und *jj* für das Jahr steht.

2. Doppelklicken Sie in einem Arbeitsplatz- oder Windows Explorer-Fenster auf das Aktualisierungsprogramm.

   Das Aktualisierungsprogramm sucht auf Ihrem Computer nach Norton AntiVirus.

3. Befolgen Sie alle Aufforderungen, die das Aktualisierungsprogramm anzeigt.

4. Das Aktualisierungsprogramm installiert die neuen Virusdefinitionsdateien automatisch im richtigen Ordner.

   Wenn Sie gefragt werden, ob Dateien überschrieben werden sollen, klicken Sie auf „Ja“. Die alten Virusdefinitionsdateien werden dann durch die neuen ersetzt.

5. Führen Sie eine Prüfung mit Norton AntiVirus durch, um die neuen Virusdefinitionen zu aktivieren.

6. Starten Sie Ihren Computer neu, damit auch Auto-Protect die neuen Virusdefinitionsdateien verwendet.

7. Lesen Sie die neuen Textdateien (*.TXT) in Ihrem Norton AntiVirus-Ordner. Sie enthalten die aktuellsten Informationen über neu entdeckte Viren und über besondere Vorsichtsmaßnahmen, die Sie treffen sollten.

Anzeigen der Virusliste

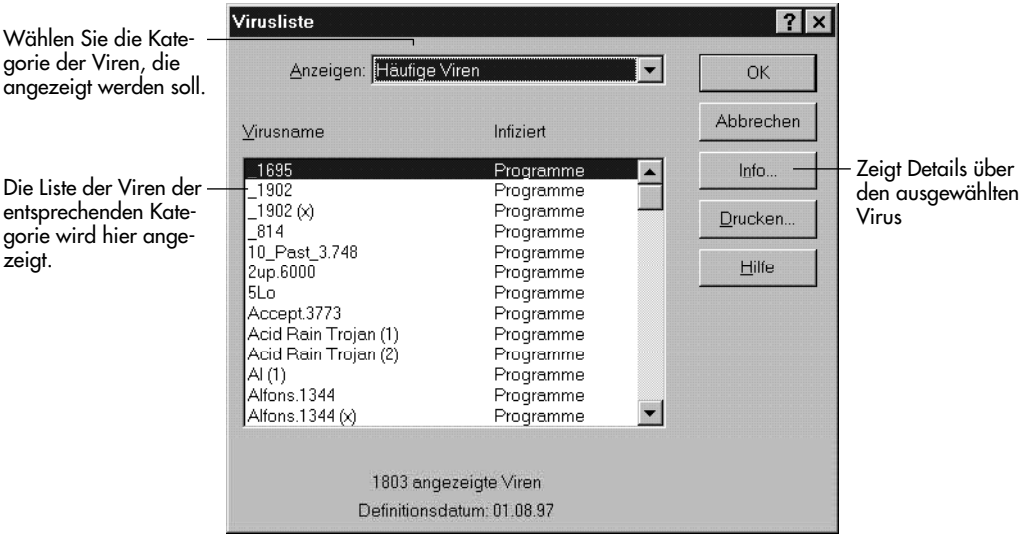
Sie können sehen, welche Viren Norton AntiVirus erkennt, indem Sie die Liste der Virusnamen anzeigen. Es handelt sich dabei um die Namen der Viren, die mit Hilfe der Informationen in den Virusdefinitionsdateien identifiziert werden können. Hier finden Sie auch Beschreibungen bestimmter Viren, einschließlich ihrer Symptome und Aliasnamen.

So zeigen Sie die Liste der Virusnamen an:

- Klicken Sie auf „Virusliste“ im Hauptfenster von Norton AntiVirus.

  Die Virusliste wird angezeigt (Abbildung 4-3).

Abbildung 4-3 Virusliste



Ein Listenfeld zeigt den Namen eines Virus an und welche Elemente er befällt. Sie können verschiedene Kategorien von Viren sehen, indem Sie eine Kategorie in der Liste wählen.

Alle Viren	Zeigt alle Viren an, die Norton AntiVirus entdecken kann.
Häufige Viren	Zeigt häufige Viren an. Diese Viren sind die Verursacher der meisten Infektionen.
Programmviren	Zeigt Viren an, die Programmdateien befallen können.

Boot-Viren	Zeigt Viren an, die sowohl Boot-Sektoren als auch Master-Boot-Sektoren von Datenträgern befallen können.
Stealth-Viren	Zeigt Viren an, die versuchen, sich zu tarnen, damit sie nicht entdeckt und entfernt werden.
Polymorphe Viren	Zeigt Viren an, die sich in jeder infizierten Datei anders verhalten, wodurch die Erkennung schwieriger wird.
Hybridviren	Zeigt Viren an, die sowohl Programmdateien als auch Boot-Sektoren befallen.
Makroviren	Zeigt Viren an, die Dokumente von Microsoft Word und Microsoft Excel infizieren.

Klicken Sie auf „Info“, um Details über einen bestimmten Virus abzufragen, z.B. Häufigkeit, Merkmale und Aliasnamen.

Klicken Sie auf „Drucken“ um die Virusliste über einen Drucker auszugeben oder in eine Datei zu drucken.

So suchen Sie nach einem Virusnamen:

1. Aktivieren Sie die Virusliste, indem Sie auf einen Bereich der Liste klicken (siehe Abbildung 4-3).
2. Geben Sie den Namen des gesuchten Virus ein.

   Ein Textfeld wird unterhalb des Listenfeldes angezeigt. Während Sie den Virusnamen eingeben, wird die Markierung zu dem entsprechenden Namen bewegt.

   Wenn sich der gesuchte Virusname nicht in der Liste befindet, zeigt die Liste möglicherweise nicht alle Viren an. Um alle Virusnamen anzuzeigen, wählen Sie „Alle Viren“ in der Liste „Anzeigen“.

K A P I T E L 5

Anpassen von Norton AntiVirus

Norton AntiVirus ist eine leistungsfähige und flexible Waffe im Kampf gegen Viren. Die Standardoptionen der Installation von Norton AntiVirus bieten für die meisten EDV-Umgebungen optimalen Schutz. Sie sollten die Konfiguration von Norton AntiVirus nur dann ändern, wenn bei Ihnen besondere Voraussetzungen vorliegen. Wenn Sie bei der Installation von Norton AntiVirus die vorgegebenen Optionen übernehmen, ist Ihr Computer geschützt, ohne daß Sie Änderungen an den Einstellungen vornehmen müssen.

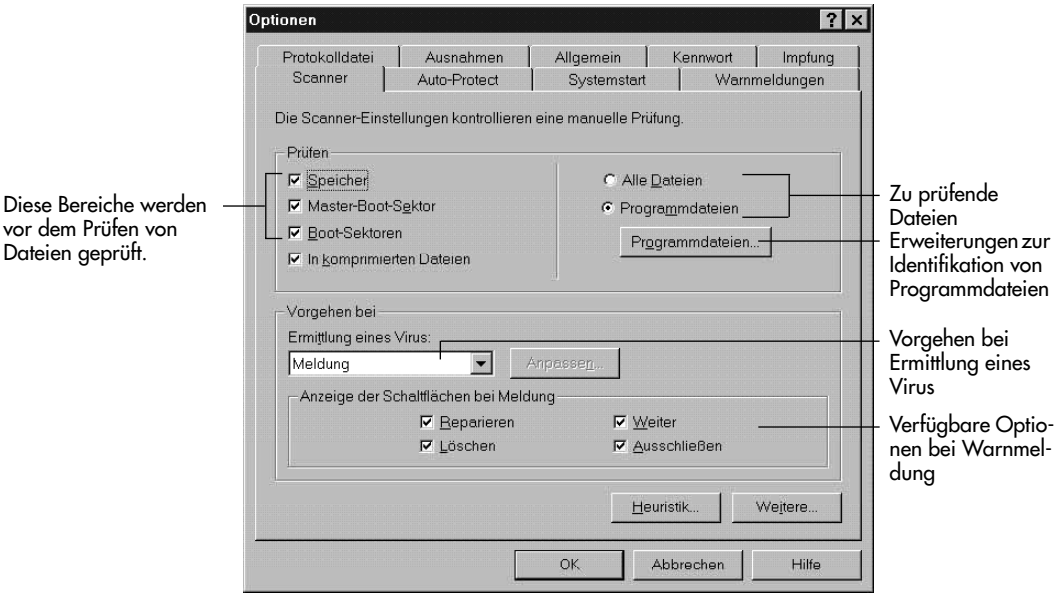
Anpassen manueller Prüfoptionen

Die manuellen Prüfoptionen beeinflussen die Prüfungen, die Sie durch Anklicken der Schaltfläche „Prüfen“ starten, und die Prüfungen, die Sie planen.

So passen Sie an, was überprüft wird:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Scanner“.

Abbildung 5-1 Scanner-Einstellungen



3 Wählen Sie im Gruppenfeld „Prüfen“ aus, welche Bereiche Ihres Computers Norton AntiVirus prüfen soll, bevor es Dateien prüft. Standardmäßig sind diese Optionen aktiviert, um einen generellen Schutz zu gewährleisten.

- **Speicher:** Überprüft den Arbeitsspeicher Ihres Computers auf Viren.

  Diese Option ist wichtig, da sich speicherresidente Viren auf andere Dateien ausbreiten. Wenn diese Option nicht aktiviert ist, kann ein speicherresidenter Virus jede geprüfte Datei befallen.

- **Master-Boot-Sektor:** Überprüft den Master-Boot-Sektor Ihrer Festplatte auf Viren.

- **Boot-Sektoren:** Prüft die Boot-Sektoren Ihrer Festplatte und überprüfter Disketten auf Viren.

- **In komprimierten Dateien:** Norton AntiVirus prüft Dateien, die mit einem der gängigen Komprimierungsprogramme (ZIP, LHA und LHZ) komprimiert wurden. Komprimierte Dateien innerhalb von komprimierten Dateien werden nicht geprüft.

  Die Prüfungen dauern möglicherweise etwas länger, wenn Sie viele komprimierte Dateien haben.

4 Legen Sie im Gruppenfeld „Prüfen“ außerdem fest, welche Dateitypen Sie scannen wollen:

- **Alle Dateien:** Es werden alle Dateien im angegebenen Ordner bzw. auf dem angegebenen Laufwerk überprüft. Auch solche Dateien werden überprüft, bei denen eine Virusinfektion weniger wahrscheinlich ist.
- **Nur Programmdateien:** Es werden nur die Dateien überprüft, bei denen eine Virusinfektion wahrscheinlich ist. Dies umfaßt alle Dateien, deren Erweiterung in der Liste der Programmdatei-Erweiterungen eingetragen ist.

  Weitere Informationen zu den Optionen und zur Liste der Programmdatei-Erweiterungen finden Sie unter „Zu prüfende Dateien wählen“ auf Seite 69.

☞ **Hinweis**: In der Liste der Programmdatei-Erweiterungen sind auch die Erweiterungen für Microsoft Word-Dokumente und Microsoft Excel-Tabellenkalkulationen enthalten. Diese Dokumente sind zwar keine Programmdateien, sie können aber von einer neuen Virusklasse mit der Bezeichnung „Makroviren“ infiziert werden.

5 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen oder mit der nächsten Prozedur weiterzumachen.

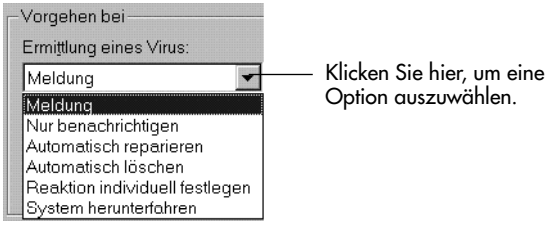
So stellen Sie ein, wie Sie auf die Entdeckung eines Virus reagieren können:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Scanner“ (siehe Abbildung 5-1).

3 Aktivieren Sie eine Option in der Liste „Vorgehen bei“.

Abbildung 5-2 Vorgehen bei Ermittlung eines Virus



- **Meldung:** Sie werden informiert, daß eine Datei oder ein Boot-Sektor geändert wurde, und können entscheiden, wie Sie reagieren wollen. Damit können Sie am besten steuern, was mit einer infizierten Datei passiert.

- **Nur benachrichtigen:** Sie werden lediglich benachrichtigt, wenn ein Virus gefunden wird. Sie können die infizierte Datei nicht reparieren oder löschen.
- **Automatisch reparieren:** Repariert infizierte Dateien oder Boot-Sektoren, ohne Sie zu fragen. Die Resultate der Reparatur werden am Ende der Prüfung angezeigt und außerdem in der Protokolldatei vermerkt.

  Norton AntiVirus ist so eingestellt, daß vor der Reparatur einer Datei eine Sicherungskopie dieser Datei erstellt wird. Weitere Informationen hierzu finden Sie unter „Einstellen der allgemeinen Prüfoptionen“ auf Seite 80.
- **Automatisch löschen:** Löscht eine infizierte Datei, ohne Sie zu fragen. Die gelöschten Dateien werden am Ende der Prüfung angezeigt und außerdem in der Protokolldatei vermerkt.
- **Reaktion individuell festlegen:** Ermöglicht Ihnen, für Datei-, Makro- und Boot-Viren unterschiedliche Reaktionen festzulegen. Wählen Sie „Reaktion individuell anpassen“, und klicken Sie danach auf „Anpassen“, um die gewünschten Reaktionen festzulegen.
- **Computer herunterfahren:** Fährt Ihren Computer herunter, wenn ein Virus gefunden wird. Sie müssen Ihren Computer dann neu starten.

  Um einen Virus nach dem Herunterfahren des Computers zu entfernen, müssen Sie Ihren Computer mit der Norton Rettungsstartdiskette (erste Diskette des Norton AntiVirus Rettungsdiskettensatzes) neu starten. Führen Sie eine erneute Prüfung durch, um den Virus zu finden und zu entfernen. Anleitungen hierzu finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

☞ **Achtung:** Wenn der Computer heruntergefahren wird, wird Norton AntiVirus angewiesen, alle Programme sofort zu beenden. Sie haben unter Umständen nicht die Möglichkeit, Ihre Arbeit zu speichern.

4 Wenn Sie in Schritt 3 „Meldung“ ausgewählt haben, legen Sie im Gruppenfeld „Anzeige der Schaltflächen bei Meldung“ fest, welche Optionen Sie zur Verfügung haben wollen, wenn eine Impfmeldung angezeigt wird.

- **Reparieren:** Ermöglicht die Reparatur der infizierten Datei bzw. des Boot-Sektors. Wenn ein Virus ein Element infiziert, das nicht repariert werden kann, z.B. eine gerade verwendete Datei, ist die Schaltfläche grau dargestellt.
- **Löschen:** Damit können Sie die Datei löschen. Wenn ein Virus ein Element infiziert, das nicht repariert werden kann, z.B. einen Boot-Sektor, ist die Schaltfläche grau dargestellt.

- **Weiter:** Hiermit können Sie die Prüfung fortsetzen, ohne das Problem zu lösen. Die Schaltfläche „Weiter“ ist nur verfügbar, wenn die Option „Sofortige Benachrichtigung“ aktiviert ist. (In der nächsten Anleitung finden Sie Details zu dieser Option.)
- **Ausschließen:** Eine Datei wird von zukünftigen Prüfungen auf bekannte Viren ausgeschlossen. Verwenden Sie diese Schaltfläche mit Vorsicht; sie kann den Schutz vor Viren verringern.

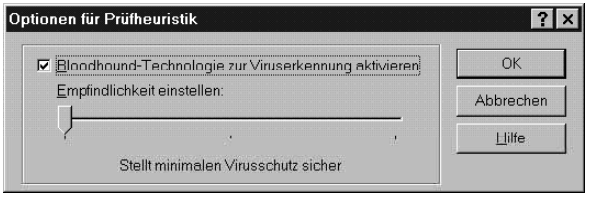
5 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen, oder machen Sie mit der nächsten Prozedur weiter.

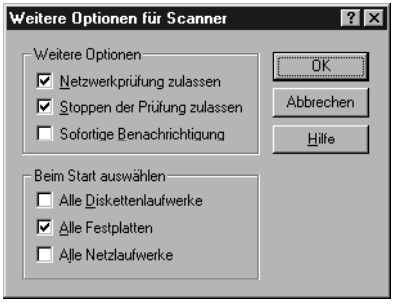
So stellen Sie zusätzliche Prüfoptionen ein:

1 Klicken Sie auf „Heuristik“ im Register „Scanner“ (siehe Abbildung 5-1).

Daraufhin wird das Dialogfeld „Optionen für Prüfheuristik“ angezeigt (siehe Abbildung 5-3).

Abbildung 5-3 Weitere Optionen für Scanner





2 Vergewissern Sie sich, daß das Kontrollkästchen „Bloodhound-Technologie zur Viruserkennung aktivieren“ aktiviert ist.

Mit der innovativen Bloodhound-Technologie kann Norton AntiVirus den Virusschutz vor schwer auszumachenden Viren entscheidend verbessern.

3 Sie können mit dem Regler die Empfindlichkeit der Bloodhound-Verarbeitung für Umgebungen mit sehr hohem Risiko erhöhen. Die Prüfung dauert dann jedoch etwas länger.

4 Klicken Sie auf „OK“, um das Dialogfeld „Optionen für Prüfheuristik“ zu schließen.

5 Klicken Sie auf „Weitere“ im Register „Scanner“ (siehe Abbildung 5-1).

Daraufhin wird das Dialogfeld „Weitere Optionen für Scanner“ angezeigt (siehe Abbildung 5-3).

6 Aktivieren Sie die gewünschten Optionen unter „Weitere Optionen“:

- **Netzwerkprüfung zulassen:** Ermöglicht die Prüfung von Netzlaufwerken. Im nächsten Abschnitt, „Hinweise zur Virusprüfung von Netzlaufwerken“, finden Sie Informationen zu Beschränkungen von Prüfungen im Netzwerk.
- **Stoppen der Prüfung zulassen:** Läßt zu, daß die Durchführung einer Prüfung abgebrochen wird. Wenn diese Option aktiviert ist, ist während der Prüfung die Schaltfläche „Stop“ verfügbar.
- **Sofortige Benachrichtigung:** Zeigt ein Warnfeld an, wenn während der Virusprüfung ein Problem entdeckt wird. So können Sie sofort antworten und müssen nicht warten, bis die Virusprüfung abgeschlossen ist.

☞ **Hinweis:** Wenn Sie „Sofortige Benachrichtigung“ auswählen, erscheint der Reparaturassistent nicht am Ende der Prüfung. Statt dessen werden die Probleme mit Hilfe der Warnfelder gelöst.

7 Legen Sie im Gruppenfeld „Beim Start auswählen“ fest, welche Laufwerke in der Liste „Laufwerke“ beim Start von Norton AntiVirus ausgewählt sein sollen.

8 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Hinweise zur Virusprüfung von Netzlaufwerken

Da Sie für Netzlaufwerke nicht immer die gleichen Zugriffsprivilegien besitzen wie für ein lokales Laufwerk, gibt es bei der Virusprüfung von Netzlaufwerken mit Norton AntiVirus Beschränkungen.

Privilegien für den Laufwerkszugriff	Operationen, die Sie durchführen können
Keine	Keine
Lesezugriff	Prüfung durchführen, aber infizierte Dateien nicht reparieren, löschen oder impfen
Schreib-/Lesezugriff	Prüfen, Reparieren, Löschen und Impfen

Das Prüfen von Netzlaufwerken ist zeitaufwendiger als das Prüfen von lokalen Laufwerken. Andere Benutzer erstellen, löschen oder bewegen möglicherweise gerade Dateien auf dem Laufwerk, das Sie mit Norton AntiVirus prüfen.

Zu prüfende Dateien wählen

In den meisten Fällen bietet das Prüfen von Programmdateien ausreichenden Virenschutz, da Viren sich nur von diesen Dateien ausbreiten können. Nachfolgend finden Sie eine Beschreibung der Optionen für die Dateiformate, so daß Sie entscheiden können, welche Einstellung in Ihrem Fall die beste ist.

Alle Dateien

Prüft alle Dateien – Datendateien (z.B. Datenbanken, Dokumente, Textdateien, Tabellenkalkulationsdateien) und Programmdateien (z.B. Systemdateien, Textverarbeitungsprogramme und Dienstprogramme). Das Prüfen aller Dateien dauert länger, schließt aber alle ausführbaren Dateien mit ein, deren Dateierweiterungen von den Standards abweichen. Normalerweise reicht es aus, nur Programmdateien zu überprüfen – es sei denn, auf Ihrem Computer ist ein Virus entdeckt worden. Prüfen Sie in einem solchen Fall alle Dateien, um sicherzustellen, daß alle Dateien auf Ihrem Computer virenfrei sind.

Programmdateien

Prüft Dateien, deren Erweiterung in der Liste der Programmdatei-Erweiterungen aufgeführt wird. Diese Liste enthält die gebräuchlichsten Erweiterungen für ausführbare Dateien, die von Viren befallen werden und diese verbreiten können. In den meisten Fällen reicht es aus, nur die Programmdateien zu überprüfen.

☞ **Hinweis:** In der Liste der Programmdatei-Erweiterungen sind auch die Erweiterungen für Microsoft Word-Dokumente und Microsoft Excel-Tabellenkalkulationen enthalten. Diese Dokumente sind zwar keine Programmdateien, sie können aber von einer neuen Virusklasse mit der Bezeichnung „Makroviren“ infiziert werden.

Wenn Sie ein besonderes Programm verwenden, dessen Erweiterung nicht in der Liste der Programmdatei-Erweiterungen zu finden ist, können Sie diese der Liste hinzufügen. Selbst wenn Sie dies nicht tun, wird Norton AntiVirus bei einer Infektion trotzdem Viren entdecken. Es ist wahrscheinlicher, daß ein Virus ein oder zwei der Dateien befällt, die in der Liste der Programmdatei-Erweiterungen aufgeführt sind, bevor er ein Programm mit einer ungewöhnlichen Dateierweiterung infiziert. Nachdem ein Virus gefunden wurde, prüfen Sie alle Dateien, um sicherzustellen, daß alle Dateien auf Ihrem Computer virenfrei sind. Informationen zum Einstellen dieser Optionen finden Sie unter „Anpassen manueller Prüfoptionen“ auf Seite 63 und „Anpassen der automatischen Schutzfunktion“ auf Seite 81.

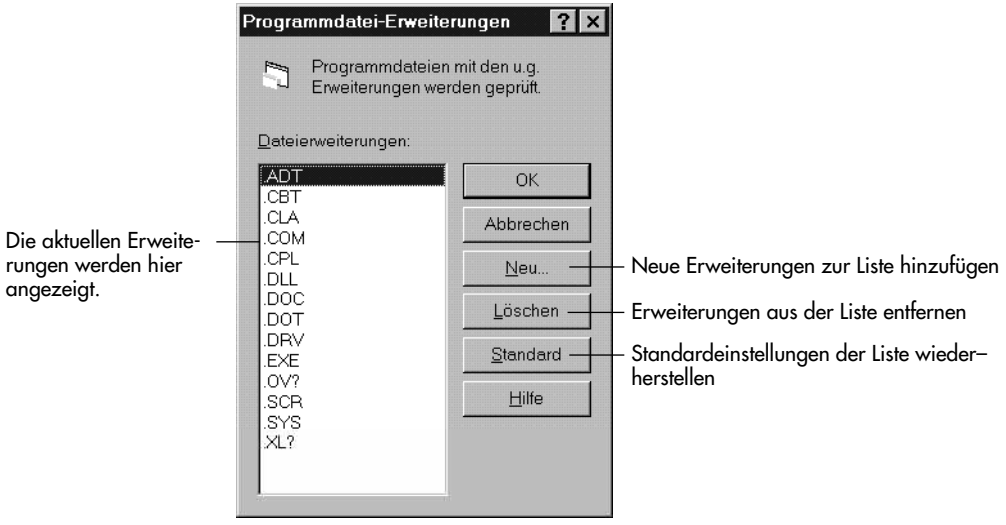
Programmdatei-Erweiterungen festlegen

Norton AntiVirus verwendet die Liste der Programmdatei-Erweiterungen zum Prüfen und Impfen von Programmdateien. Die Liste der Programmdatei-Erweiterungen enthält die gebräuchlichsten Erweiterungen für ausführbare Dateien, die von Viren befallen werden und diese verbreiten können. Dateierweiterungen bestehen immer aus drei Zeichen.

So zeigen Sie die aktuellen Programmdatei-Erweiterungen an:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Scanner“.
3. Wählen Sie im Gruppenfeld „Prüfen“ die Option „Programmdateien“ aus (siehe Abbildung 5-2).
4. Klicken Sie auf „Programmdateien“.

Abbildung 5-4 Dialogfeld „Programmdatei-Erweiterungen“



Die Liste der Dateierweiterungen enthält die gängigsten Dateierweiterungen für Programmdateien. Wenn Sie besondere Programme verwenden, die spezielle Dateierweiterungen haben, fügen Sie sie der Liste hinzu.

So fügen Sie eine Programmdatei-Erweiterung hinzu:

1 Klicken Sie auf „Neu“ im Dialogfeld „Programmdatei-Erweiterungen“ (siehe Abbildung 5-4).

Abbildung 5-5 Dialogfeld „Neue Programmdatei-Erweiterung“

2 Geben Sie die neue Dateierweiterung im Feld „Neue Erweiterung“ ein, und klicken Sie auf „OK“.

Sie können für die Erweiterung Platzhalter verwenden. Sie dürfen aber nicht alle drei Zeichen der Erweiterung ersetzen. OV? steht beispielsweise für Erweiterungen, die mit OV beginnen, so wie .OVL und .OV1.

So löschen Sie eine Programmdatei-Erweiterung:

1 Wählen Sie die Dateierweiterung in der Liste der Programmdatei-Erweiterungen aus (siehe Abbildung 5-4).

2 Klicken Sie auf „Löschen“ und anschließend auf „OK“.

So stellen Sie die Standardeinstellungen der Programmdatei-Erweiterungen wieder her:

1 Klicken Sie auf „Standard“ im Dialogfeld „Programmdatei-Erweiterungen“ (siehe Abbildung 5-4).

Es wird die Liste von Erweiterungen wiederhergestellt, die ursprünglich bei der Installation von Norton AntiVirus vorhanden war.

2 Klicken Sie auf „OK“.

Verwalten von Ausnahmen

Norton AntiVirus verwendet die Einträge in der Ausnahmeliste bei allen Prüfungen. Eine *Ausnahme* ist eine Bedingung oder eine virusähnliche Aktivität, die normalerweise gemeldet würde, die jedoch von Norton AntiVirus bei einer von Ihnen festgelegten Datei ignoriert wird. Dateien ausschließen bedeutet nicht: „Finde keine Viren“ (es sei denn, Sie wählen diese Option aus); es bedeutet lediglich, daß Aktivitäten ignoriert werden, von denen Sie wissen, daß sie nicht von einem Virus durchgeführt werden.

☞ **Achtung:** Verwenden Sie diese Option mit Vorsicht. Wenn Sie eine Ausnahme festlegen, könnte sich ein Virus einschleichen.

Da z.B. das Formatierungsprogramm des Betriebssystems in den Boot-Sektor einer Diskette schreiben darf, können Sie diese Aktivität für die Datei FORMAT.COM zulassen. Indem Sie diese Aktivität in die Ausnahmeliste aufnehmen, weisen Sie Norton AntiVirus an, alle von FORMAT ausgeführten Schreibversuche in Boot-Sektoren zu ignorieren. Die Datei wird trotzdem weiterhin auf Viren geprüft, wenn Sie eine Prüfung durchführen.

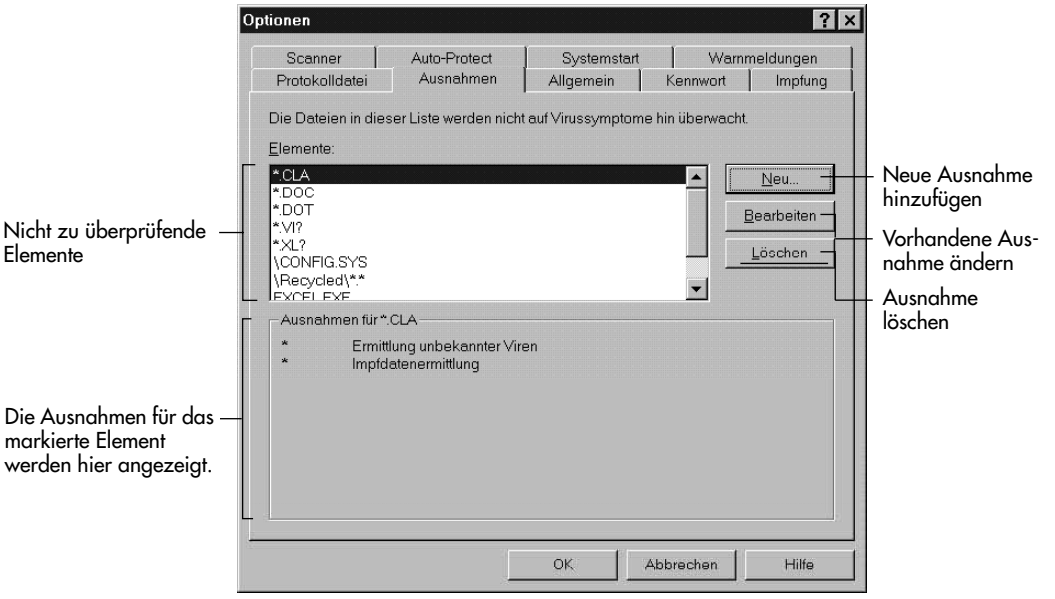
Sie weisen *Elementen*, d.h. Laufwerken, Ordnern, Gruppen von Dateien oder einzelnen Dateien, Ausnahmen zu. Jedes Element kann mehr als eine Ausnahme haben.

☞ **Hinweis:** Eine Ausnahme gilt für einen bestimmten Dateinamen. Wenn Sie eine Datei bewegen oder umbenennen, wird die Ausnahme für diese Datei automatisch ungültig.

So zeigen Sie die Ausnahmeliste an:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Ausnahmen“.

Abbildung 5-6 Einstellungen für die Ausnahmeliste



3 Wählen Sie eine Datei oder eine Gruppe von Dateien im Listenfeld „Elemente“ aus.

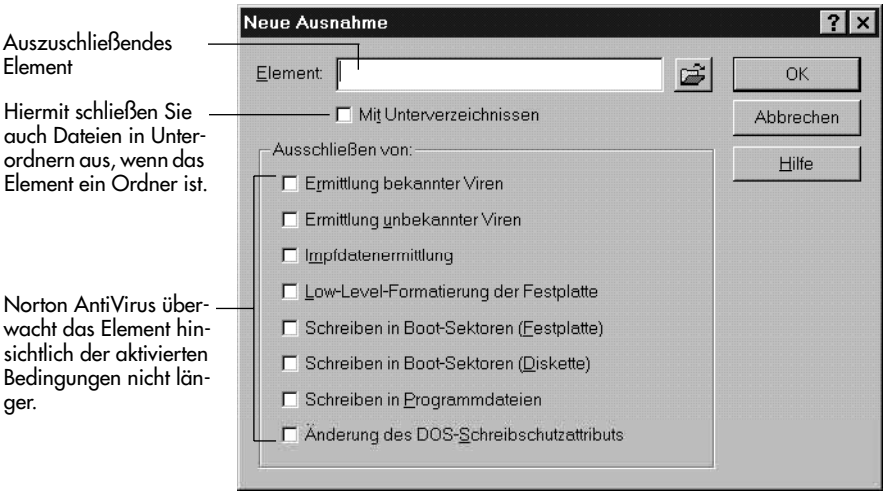
Die Aktivitäten, die bei dieser Datei oder den Dateien ignoriert werden, werden im Gruppenfeld „Ausnahmen für [Element] angezeigt“.

☞ **Hinweis:** In den meisten Fällen werden der Ausnahmeliste Elemente hinzugefügt, wenn Sie in einem Warnfeld auf „Ausschließen“ klicken, um auf eine Aktivität zu reagieren, die Norton AntiVirus gemeldet hat, die Sie aber für zulässig halten. Programmierer können beispielsweise die Impfdatenermittlung für Dateien deaktivieren, die während einer Entwicklungsphase ständig geändert werden. Obwohl Sie der Liste auch manuelle Ausnahmen hinzufügen können, ist davon abzuraten, wenn Sie die Folgen nicht genau abschätzen können.

So fügen Sie manuell Ausnahmen hinzu:

1 Klicken Sie auf „Neu“ im Register „Ausnahmen“ (siehe Abbildung 5-6).

Abbildung 5-7 Hinzufügen einer neuen Ausnahme



2 Geben Sie den Pfadnamen für die Datei oder die Dateigruppe im Textfeld „Element“ ein.

3 Aktivieren Sie „Mit Unterordnern“, wenn Sie wollen, daß auch die Dateien in den untergeordneten Ordnern von der Prüfung ausgeschlossen werden.

4 Markieren Sie die Aktivitäten, die Norton AntiVirus von der Prüfung ausschließen soll.

- **Ermittlung bekannter Viren:** Das Element wird von Prüfungen auf bekannte Viren ausgeschlossen.
- **Ermittlung unbekannter Viren:** Das Element wird von Prüfungen auf unbekannte Viren ausgeschlossen
- **Impfdatenermittlung:** Das Element wird nicht daraufhin geprüft, ob es geimpft oder seit der letzten Impfung geändert wurde.
- **Low-Level-Formatierung der Festplatte:** Das Element wird nicht daraufhin überprüft, ob es eine Low-Level-Formatierung Ihrer Festplatte vornimmt, durch die alle Informationen auf Ihrer Festplatte gelöscht werden.
- **Schreiben in Boot-Sektoren (Festplatte):** Das Element wird nicht daraufhin überprüft, ob es versucht, in die Boot-Sektoren Ihrer Festplatte zu schreiben. Diese Aktivität ist nur bei ganz wenigen Programmen zulässig.

- **Schreiben in Boot-Sektoren (Diskette):** Das Element wird nicht daraufhin überprüft, ob es versucht, in den Boot-Sektor einer Diskette zu schreiben. Diese Aktivität ist nur bei ganz wenigen Programmen zulässig.
- **Schreiben in Programmdateien:** Das Element wird nicht daraufhin überprüft, ob es versucht, in eine Programmdatei zu schreiben. Einige Programme speichern Konfigurationsinformationen nicht in separaten Dateien, sondern in der eigenen Programmdatei.
- **Ändern des Schreibschutzattributs:** Das Element wird nicht daraufhin überprüft, ob es versucht, den Schreibschutz einer Datei aufzuheben, so daß sie beschrieben werden kann. Diese Option gilt besonders für Operationen, die von DOS-Programmen durchgeführt werden.

☞ **Hinweis:** Obwohl es nützlich sein kann, bestimmte Dateien von der Prüfung auszuschließen, sollten Sie mit dieser Funktion vorsichtig umgehen, da Sie dadurch den Schutz vor Viren verringern können.

5 Klicken Sie auf „OK“.

So ändern Sie eine bestehende Ausnahme:

1 Wählen Sie eine Datei oder eine Gruppe von Dateien im Listenfeld „Elemente“ des Registers „Ausnahmen“ aus (siehe Abbildung 5-6).

2 Klicken Sie auf „Bearbeiten“, und nehmen Sie die gewünschten Änderungen vor.

3 Klicken Sie auf „OK“.

So löschen Sie eine Ausnahme:

1 Wählen Sie eine Datei oder eine Gruppe von Dateien im Listenfeld „Elemente“ des Registers „Ausnahmen“ aus (siehe Abbildung 5-6).

2 Klicken Sie auf „Löschen“ und anschließend auf „OK“.

Die Ausnahme wird aus der Liste entfernt und somit der vollständige Virenschutz wiederhergestellt.

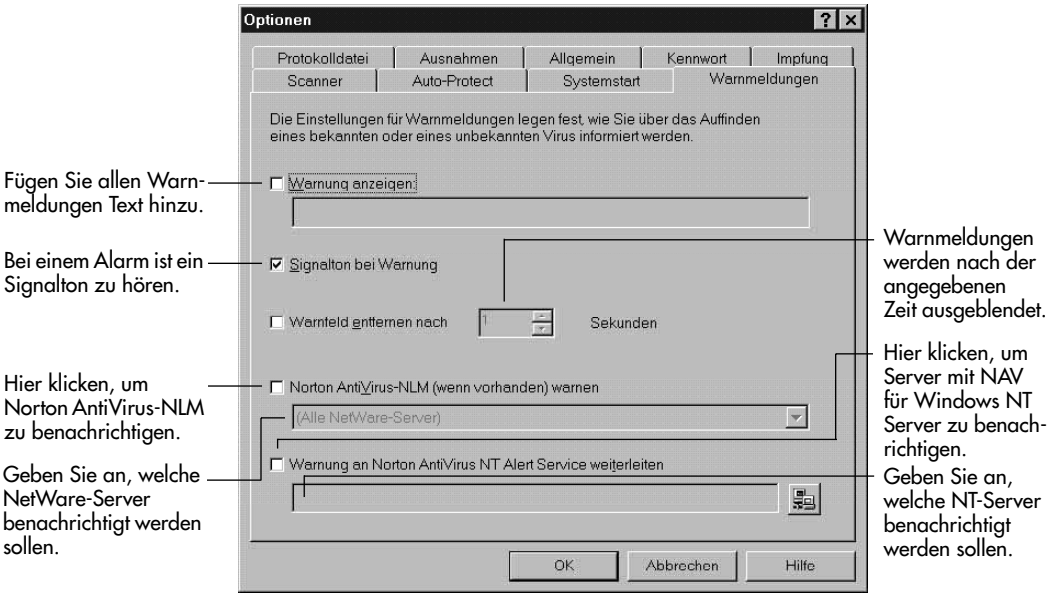
Anpassen von Warnmeldungen

Die Einstellungen für die Warnmeldungen legen fest, wie Norton AntiVirus Sie informiert, wenn es einen Virus oder einen möglichen Virus gefunden hat. Diese Optionen gelten für alle Prüfungen, die Norton AntiVirus durchführt (manuelle, geplante und automatische Prüfungen).

So passen Sie die Warnmeldungen an:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Warnmeldungen“.

Abbildung 5-8 Einstellungen für Warnmeldungen



3. Aktivieren Sie „Warnung anzeigen“, um allen Warnmeldungen, die von Norton AntiVirus angezeigt werden, einen Text hinzuzufügen (z.B. Anleitungen oder spezielle Warnungen). Geben Sie anschließend in das Textfeld den Text ein (bis zu 76 Zeichen).
4. Aktivieren Sie „Signalton“, wenn Sie wollen, daß gleichzeitig mit der Anzeige der Warnmeldung ein Signalton zu hören sein soll.
5. Aktivieren Sie „Warnfeld entfernen nach“, um festzulegen, wie lange die Meldung angezeigt werden soll. Geben Sie anschließend im Feld „Sekunden“ die Dauer in Sekunden ein (zwischen 1 und 99).
6. Klicken Sie auf „OK“.

Netzwerkwarnmeldungen senden

Wenn ein Virus oder ein anderes Norton AntiVirus-Ereignis auf einer Workstation entdeckt wird, kann Norton AntiVirus über Novell NetWare-Netzwerke Warnmeldungen an Norton AntiVirus für NetWare NLM senden. Sie können hierfür einen bestimmten Server angeben oder alle NetWare-Server benachrichtigen, auf denen das NLM ausgeführt wird. Bei Netzwerken mit Windows NT-Servern können Warnmeldungen an alle Server geleitet werden, auf denen Norton AntiVirus für Windows NT Server installiert ist.

So legen Sie die Optionen für die Netzwerkwarnmeldungen fest:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Warnmeldungen“ (siehe Abbildung 5-8).
3. Aktivieren Sie für Novell NetWare-Netzwerke „Norton AntiVirus-NLM (wenn vorhanden) warnen“.
4. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im Dropdown-Listenfeld den NetWare-Server aus, auf dem das Norton AntiVirus NLM ausgeführt wird.
   - Wählen Sie im Dropdown-Listenfeld „Alle NetWare-Server“ aus. Norton AntiVirus warnt alle NetWare-Server, auf denen das NLM läuft.
5. Aktivieren Sie für Windows NT-Server „Warnung an Norton AntiVirus NT Alert Service weiterleiten“.
6. Geben Sie den Namen des Empfängers in das Textfeld ein, oder klicken Sie auf das Schaltflächensymbol „Durchsuchen“, um den Empfänger auszuwählen.
7. Klicken Sie auf „OK“.

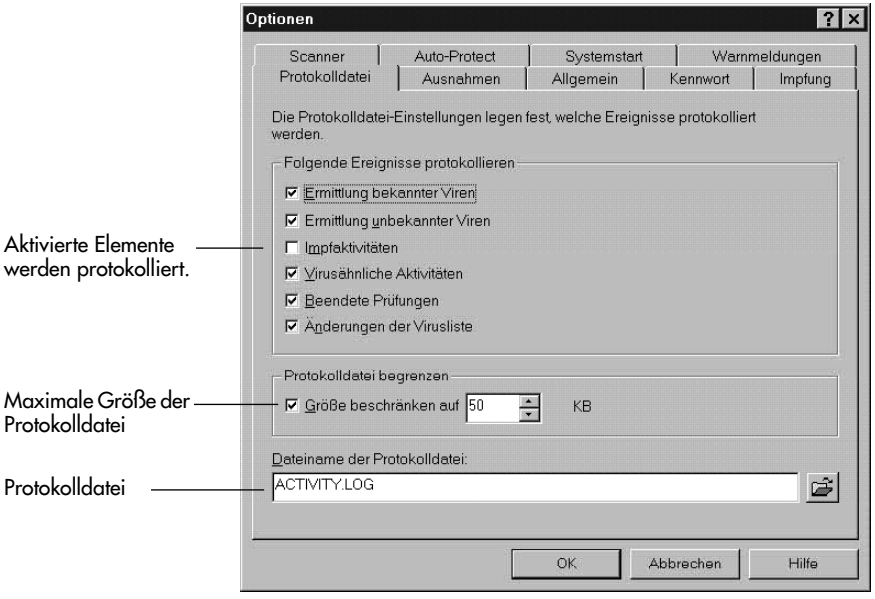
Anpassen der Protokolldatei

Die Protokolldatei enthält Informationen über die Aktivitäten von Norton AntiVirus. Norton AntiVirus ist standardmäßig so eingestellt, daß es die Erkennung von bekannten Viren und die durchgeführten Maßnahmen (infizierte Dateien repariert oder gelöscht, Dateien zur Ausnahmeliste hinzugefügt oder keine Behandlung durchgeführt) protokolliert. Sie können die Protokolldatei anpassen, um andere Ereignisse ebenfalls zu protokollieren (z.B. die Ermittlung unbekannter Viren und Änderungen der Virusliste).

So passen Sie die Protokolldatei an:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Protokolldatei“.

Abbildung 5-9 Einstellungen für die Protokolldatei



3 Markieren Sie im Gruppenfeld „Folgende Ereignisse protokollieren“ die Ereignisse, die Norton AntiVirus aufzeichnen soll:

- **Ermittlung bekannter Viren:** Protokolliert Informationen über die Ermittlung bekannter Viren (in der Virusliste erfaßte Viren).
- **Ermittlung unbekannter Viren:** Protokolliert Informationen über die Ermittlung unbekannter Viren (in der Virenliste noch nicht verzeichnete Viren).
- **Impfaktivitäten:** Protokolliert Ermittlungen ungeimpfter Dateien und Änderungen an den Impfdaten von Dateien.
- **Virusähnliche Aktivitäten:** Protokolliert die Ermittlung von virusähnlichen Aktivitäten (Aktivitäten, die Viren ausführen, wenn sie sich verbreiten oder Daten beschädigen, z.B. wenn sie versuchen, Ihre Festplatte zu formatieren).
- **Beendete Prüfungen:** Protokolliert das Datum und die Zeit des Abschlusses manueller und geplanter Virusprüfungen.
- **Änderungen der Virusliste:** Protokolliert Änderungen an der Virusliste.

4 Wenn Sie die Größe der Protokolldatei begrenzen wollen, aktivieren Sie „Größe der Protokolldatei begrenzen auf“ und geben die gewünschte Größe im Feld „Kilobyte“ ein.

Wenn die angegebene Dateigröße erreicht ist, werden alte Einträge in der Protokolldatei durch neue Einträge überschrieben.

5 Geben Sie den Pfadnamen für die Protokolldatei im Feld „Dateiname der Protokolldatei“ ein.

6 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Einstellen der allgemeinen Prüfoptionen

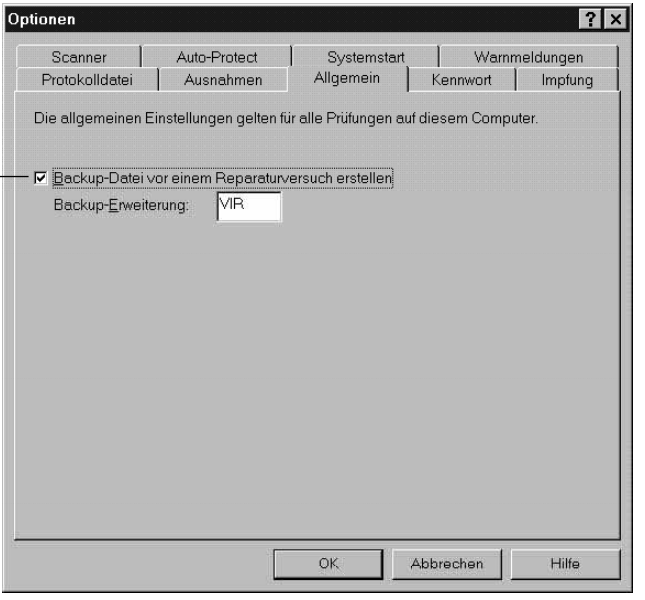
Diese Optionen gelten für alle Prüfungen, die Norton AntiVirus durchführt (manuelle, geplante und automatische Prüfungen).

So passen Sie die allgemeinen Prüfoptionen an:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Allgemein“.

Abbildung 5-10 Allgemeine Einstellungen



Erstellt eine Backup-Kopie der infizierten Datei

3 Aktivieren Sie „Backup-Datei vor einem Reparaturversuch erstellen“, damit Norton AntiVirus vor einem Reparaturversuch eine Kopie der infizierten Datei erstellt. Die Standarderweiterung für virusinfizierte Backup-Dateien ist „VIR“. Sie können allerdings im Feld „Backup-Erweiterung“ auch eine andere Erweiterung eingeben.

Alle Dateien mit der Backup-Erweiterung werden automatisch auf die Ausnahmeliste gesetzt, so daß Sie während einer Prüfung nicht untersucht werden. Im Windows-Explorer wird eine solche Datei mit dem Dateityp „VIR Datei“ angezeigt.

☞ **Hinweis:** Löschen Sie die Backup-Dateien, wenn die Reparatur erfolgreich durchgeführt werden konnte. Auch wenn die infizierten Backup-Dateien nicht ausgeführt werden können (wegen der Erweiterung .VIR) – sie enthalten Viren!

4 Klicken Sie auf „OK“.

Anpassen der automatischen Schutzfunktion

Die automatische Schutzfunktion schützt Sie folgendermaßen vor Viren:

- Sie überprüft Programme oder Disketten auf Viren, wenn Sie darauf zugreifen.
- Sie überwacht Ihren Computer auf Zeichen von unbekannten Viren oder virusähnliche Aktivitäten.
- Sie verhindert, daß Viren in Ihren Computer gelangen, wenn Sie Dateien kopieren oder installieren.

Informationen zu anderen Optionen, die die automatische Schutzfunktion betreffen, finden Sie unter „Anpassen manueller Prüfoptionen“ auf Seite 63.

Programmdateien automatisch schützen

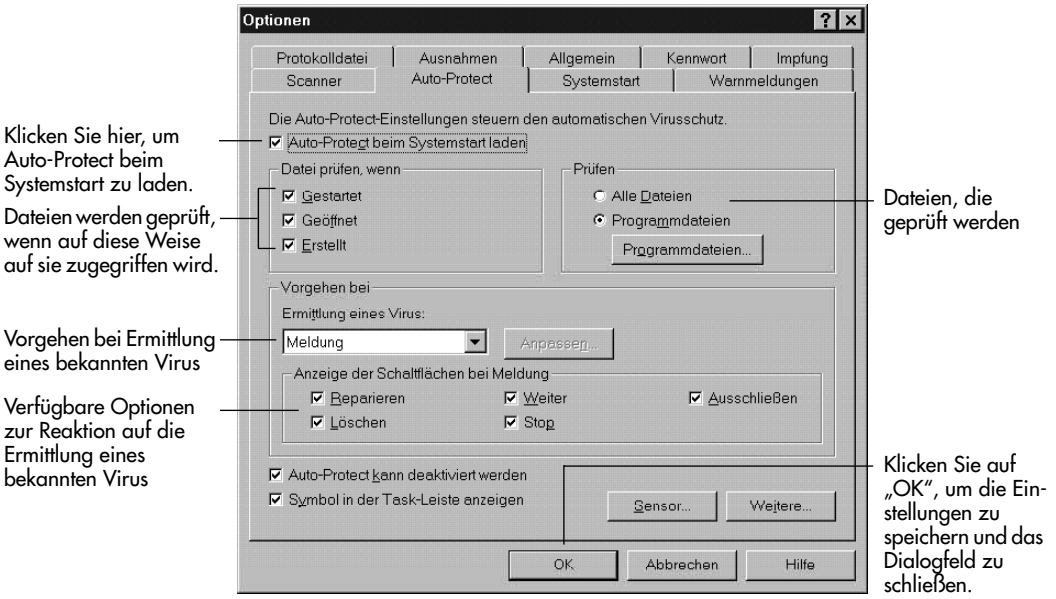
Norton AntiVirus kann Virusprüfungen immer dann durchführen, wenn Sie eine Datei öffnen oder ein Programm starten.

So schützen Sie Programmdateien automatisch:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Auto-Protect“.

Abbildung 5-11 Auto-Protect-Einstellungen



3 Aktivieren Sie „Auto-Protect beim Systemstart laden“, um sicherzustellen, daß die automatische Schutzfunktion bei jedem Systemstart geladen wird.

☞ **Hinweis:** Wenn Sie diese Option deaktivieren, ist der Schutz vor Viren erheblich geringer.

4 Legen Sie im Gruppenfeld „Datei prüfen, wenn“ fest, wann Norton AntiVirus die verwendeten Dateien prüfen soll:

- **Gestartet:** Die Programmdatei wird jedesmal geprüft, wenn sie gestartet wird.
- **Geöffnet:** Prüft Dateien, wenn sie geöffnet werden. Wenn Sie z. B. eine Datei kopieren, wird sie von Norton AntiVirus geprüft.
- **Erstellt:** Prüft Dateien, die durch ein Installationsprogramm auf Ihrem Laufwerk erstellt werden, sowie Dateien, die entkomprimiert oder von einem Bulletin Board System heruntergeladen werden.

5 Aktivieren Sie im Gruppenfeld „Prüfen“ die gewünschten Optionen:

- **Alle Dateien:** Prüft alle Dateien, auf die Sie zugreifen. Dazu zählen auch Dateien, die weniger häufig von Viren befallen werden.
- **Programmdateien:** Prüft Dateien, die häufiger von Viren befallen werden. Dies umfaßt alle Dateien, deren Erweiterung in der Liste der Programmdatei-Erweiterungen eingetragen ist.

Weitere Informationen zu den Optionen und zur Liste der Programmdatei-Erweiterungen finden Sie unter „Zu prüfende Dateien wählen“ auf Seite 69.

6 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen, oder machen Sie mit dem nächsten Abschnitt weiter.

So stellen Sie ein, wie Sie auf die Entdeckung eines Virus reagieren können:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Auto-Protect“ (siehe Abbildung 5-11).

3 Wählen Sie in der Liste „Ermittlung eines Virus“ die Optionen für Ihre Reaktion auf die Ermittlung eines Virus aus:

- **Meldung:** Sie werden informiert, daß ein bekannter Virus gefunden wurde, und können entscheiden, wie Sie reagieren wollen. Damit können Sie am besten steuern, was mit einer infizierten Datei passiert.
- **Zugriff verweigern:** Hindert Sie daran, eine Datei zu verwenden, wenn ein bekannter Virus entdeckt wurde. Diese Ereignisse werden in der Protokolldatei aufgezeichnet.
- **Automatisch reparieren:** Repariert eine infizierte Datei oder einen Boot-Sektor, ohne Sie zu benachrichtigen. Die Ergebnisse werden in der Protokolldatei vermerkt.

  Norton AntiVirus ist so eingestellt, daß vor der Reparatur einer Datei eine Sicherungskopie dieser Datei erstellt wird. Weitere Informationen hierzu finden Sie unter „Einstellen der allgemeinen Prüfoptionen“ auf Seite 80.
- **Automatisch löschen:** Löscht infizierte Dateien, ohne Sie zu fragen. Die Ergebnisse werden in der Protokolldatei vermerkt. Gehen Sie vorsichtig mit dieser Option um. Von Norton AntiVirus gelöschte Dateien können nicht wiederhergestellt werden.
- **Reaktion individuell festlegen:** Ermöglicht Ihnen, für Datei-, Makro- und Boot-Viren unterschiedliche Reaktionen festzulegen. Wählen Sie „Reaktion individuell anpassen“, und klicken Sie danach auf „Anpassen“, um die gewünschten Reaktionen festzulegen.

- **Computer herunterfahren:** Fährt Ihren Computer herunter, wenn ein Virus gefunden wird. Sie müssen Ihren Computer mit der Rettungsdiskette neu starten und eine erneute Prüfung durchführen, um den Virus aus der infizierten Datei oder dem Boot-Sektor zu entfernen.

☞ **Achtung:** Mit dem Befehl „Computer herunterfahren“ weisen Sie Norton AntiVirus an, alle Programme zu beenden und den Computer sofort herunterzufahren. Ungesicherte Arbeit geht unter Umständen verloren, allerdings wird so die Verbreitung eines Virus verhindert.

4 Wenn Sie in Schritt 3 „Meldung“ ausgewählt haben, legen Sie im Gruppenfeld „Anzeige der Schaltflächen bei Meldung“ fest, welche Optionen Sie zur Verfügung haben wollen, wenn eine Impfmeldung angezeigt wird.

- **Reparieren:** Ermöglicht die Reparatur der infizierten Datei bzw. des Boot-Sektors.
- **Löschen:** Damit können Sie die Datei löschen. Wenn ein Virus ein Element infiziert, das nicht repariert werden kann, z.B. einen Boot-Sektor, ist die Schaltfläche grau dargestellt.
- **Weiter:** Sie können weiter auf die Datei zugreifen. Wenn Sie auf „Weiter“ klicken, aktivieren Sie damit möglicherweise den Virus.
- **Stop:** Hiermit können Sie den Zugriff auf die Datei stoppen. Der Virus wird nicht aktiviert, aber die Datei ist weiterhin infiziert.
- **Ausschließen:** Eine Datei wird von zukünftigen Prüfungen auf bekannte Viren ausgeschlossen. Verwenden Sie diese Schaltfläche mit Vorsicht; sie kann den Schutz vor Viren verringern.

5 Aktivieren Sie „Auto-Protect kann deaktiviert werden“, wenn Sie in der Lage sein wollen, die automatische Schutzfunktion temporär zu deaktivieren, indem Sie auf das Symbol für Auto-Protect in der Windows Task-Leiste klicken.

6 Aktivieren Sie „Symbol in der Task-Leiste anzeigen“, damit Sie daran erinnert werden, daß die automatische Schutzfunktion aktiviert ist, und damit Sie diese temporär aktivieren und deaktivieren können.

7 Klicken Sie auf „OK“, um Ihre Einstellungen zu sichern und das Dialogfeld zu schließen, oder gehen Sie zur nächsten Anleitung.

Schutz vor unbekannten Viren mit Virus-Sensor

Ein unbekannter Virus ist ein Virus, der noch nicht identifiziert wurde. Da für den Virus keine Definition existiert, wird er bei einer Prüfung auf bekannte Viren nicht gefunden. Auto-Protect findet unbekannte Viren trotzdem, indem es den Computer mit einer speziellen Virus-Sensor-Technik auf Aktivitäten überwacht, die auf einen sich verbreitenden Virus hindeuten.

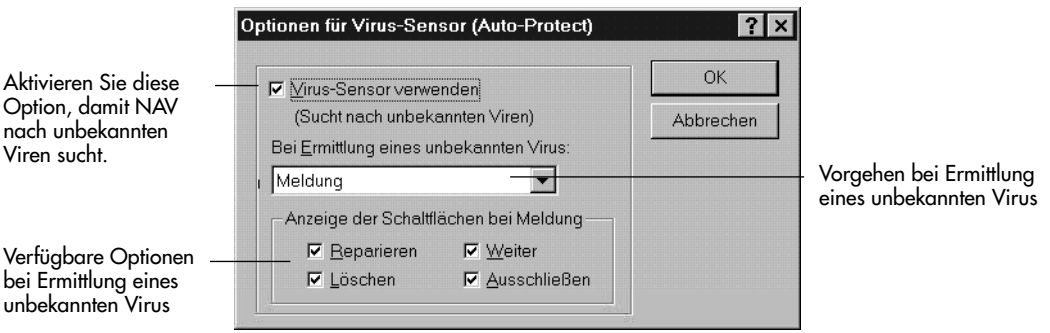
Der Virus-Sensor stellt eine zusätzliche Schutzfunktion dar, die bei der Installation von Norton AntiVirus nicht automatisch aktiviert wird. Wenn Sie diese Funktion einschalten, erhalten Sie während gewöhnlicher Operationen Warnmeldungen, die auf einen Virus hinweisen könnten. Sie müssen dann für jedes Ereignis entscheiden, ob die Aktivität im Rahmen der durchgeführten Operation zulässig ist oder ob es sich um eine Virusaktivität handelt.

Sie können sich außerdem durch das Impfen von Dateien vor unbekannten Viren schützen. Weitere Informationen hierzu finden Sie unter „Anpassen der Impfung“ auf Seite 90.

So überwachen Sie Ihren Computer auf unbekannte Viren:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Auto-Protect“.
3. Klicken Sie auf „Sensor“ im Register „Auto-Protect“ (Abbildung 5-11).

Abbildung 5-12 Virus-Sensor-Einstellungen



4. Aktivieren Sie „Virus-Sensor verwenden“, um Infektionen Ihrer Programme durch unbekannte Viren zu entdecken.

5 Wählen Sie eine der Optionen in der Liste „Bei Ermittlung eines unbekannten Virus“ aus:

- **Meldung:** Sie werden informiert, daß ein unbekannter Virus gefunden wurde, und können entscheiden, wie Sie reagieren wollen. Damit können Sie am besten steuern, was mit einer infizierten Datei passiert.
- **Automatisch reparieren:** Repariert eine infizierte Datei oder einen Boot-Sektor, ohne Sie zu benachrichtigen. Die Ergebnisse werden in der Protokolldatei vermerkt.

  Norton AntiVirus ist so eingestellt, daß vor der Reparatur einer Datei eine Sicherungskopie dieser Datei erstellt wird. Weitere Informationen hierzu finden Sie unter „Einstellen der allgemeinen Prüfoptionen“ auf Seite 80.
- **Automatisch löschen:** Löscht eine infizierte Datei, ohne Sie zu fragen. Das Ergebnis wird in der Protokolldatei aufgezeichnet. Vorsicht bei der Verwendung dieser Option. Mit Norton AntiVirus gelöschte Dateien können nicht wiederherstellt werden.
- **Computer herunterfahren:** Fährt Ihren Computer herunter, wenn ein Virus gefunden wird.

6 Wenn Sie in Schritt 5 „Meldung“ ausgewählt haben, legen Sie im Gruppenfeld „Anzeige der Schaltflächen bei Meldung“ fest, welche Optionen Sie zur Verfügung haben wollen, wenn ein unbekannter Virus gefunden wird.

- **Reparieren:** Ermöglicht die Reparatur der infizierten Datei.
- **Löschen:** Damit können Sie die Datei löschen.
- **Weiter:** Sie können fortfahren, ohne die Datei zu behandeln. Die Datei ist weiterhin mit dem unbekannten Virus infiziert.
- **Ausschließen:** Die Datei wird von zukünftigen Prüfungen auf unbekannte Viren ausgeschlossen. Die Verwendung dieser Schaltfläche kann den Schutz vor unbekannten Viren verringern.

7 Klicken Sie auf „OK“, um das Dialogfeld zu schließen.

8 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen, oder fahren Sie mit der nächsten Prozedur fort.

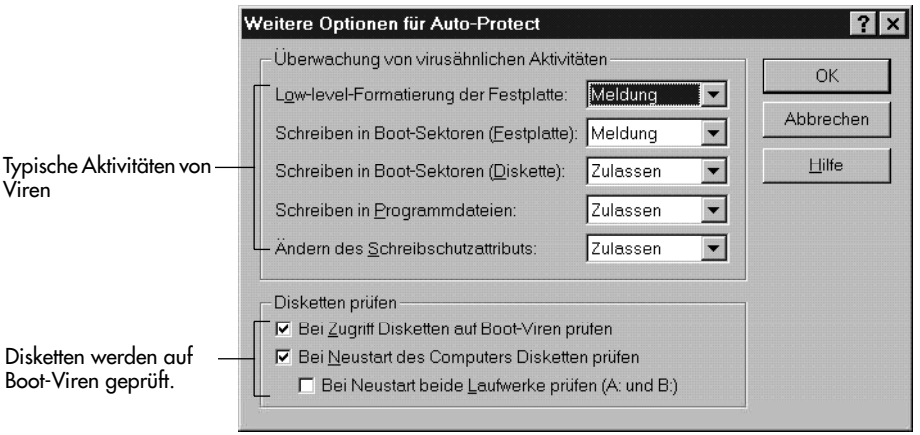
Überwachung auf virusähnliche Aktivitäten

Eine *virusähnliche Aktivität* ist eine Aktivität, die ein Virus typischerweise dann entfaltet, wenn er sich verbreitet. Bei einigen Programmen sind diese Aktivitäten zulässig; Norton AntiVirus kann diese Aktivitäten trotzdem überwachen, um so die Infektion Ihres Computers durch einen unbekannten Virus zu verhindern.

So führen Sie die Überwachung auf virusähnliche Aktivitäten durch:

1. Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.
2. Klicken Sie auf das Register „Auto-Protect“.
3. Klicken Sie auf „Weitere“ im Register „Auto-Protect“ (siehe Abbildung 5-11).

Abbildung 5-13 Weitere Optionen für Auto-Protect einstellen



4. Aktivieren Sie die gewünschten Optionen in den Listen, um festzulegen, wie Norton AntiVirus bei virusähnlichen Aktivitäten reagieren soll:
   - **Zulassen:** Die Aktivität wird zugelassen, und Sie werden nicht mehr darüber informiert. Wenn Sie diese Option aktivieren, sind Sie nicht mehr vor Viren geschützt, die diese Aktivität entfalten.
   - **Meldung:** Informiert Sie, wenn ein Programm versucht, diese Aktivität auszuführen, und ermöglicht Ihnen die Wahl zwischen den Optionen „Weiter“, „Stop“ und „Ausschließen“. Obwohl es sinnvoll sein kann, bestimmte Dateien von speziellen Prüfungen auszunehmen, sollten Sie damit vorsichtig sein. Wenn Sie Dateien ausschließen, kann dadurch der Schutz vor Viren verringert werden.
   - **Nicht zulassen:** Wenn die Aktivität ermittelt wird, wird sie jedesmal abgebrochen.

Es gibt folgende virusähnliche Aktivitäten:

- **Low-Level-Formatierung der Festplatte:** Alle Informationen auf der Festplatte werden gelöscht und können nicht mehr wiederhergestellt werden. Dieser Formatierungstyp wird normalerweise vom Hersteller durchgeführt. Wenn diese Aktivität entdeckt wird, weist das mit großer Wahrscheinlichkeit auf einen aktiven unbekannten Virus hin.
- **Schreiben in Boot-Sektoren (Festplatte):** Nur einige wenige Programme schreiben in Boot-Sektoren. Wenn Sie nicht gerade ein Programm wie FORMAT verwenden, das in die Boot-Sektoren der Festplatte schreibt, deutet diese Aktivität wahrscheinlich auf einen Virus hin.
- **Schreiben in Boot-Sektoren (Diskette):** Nur einige wenige Programme (z.B. die Formatierprogramme FORMAT oder SYS des Betriebssystems) schreiben in Boot-Sektoren einer Diskette.
- **Schreiben in Programmdateien:** Einige Programme schreiben Konfigurationsinformationen in die eigenen Programmdateien. Diese Aktivität ist zwar meist zulässig, sie kann aber auch auf einen unbekannten Virus hindeuten.
- **Ändern des DOS-Schreibschutzattributs:** Viele Programme ändern das Schreibschutzattribut von Dateien. Diese Aktivität ist zwar meist zulässig, sie kann aber auch auf einen unbekannten Virus hindeuten. Diese Option trifft vor allem auf Operationen zu, die von DOS-Programmen ausgeführt werden.

5 Klicken Sie auf „OK“, um das Dialogfeld zu schließen.

6 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen, oder fahren Sie mit der nächsten Prozedur fort.

Disketten automatisch schützen

Da Boot-Viren meistens durch Disketten übertragen werden, ist es wichtig, daß Sie jede verwendete Diskette prüfen. Norton AntiVirus kann Disketten überwachen, wenn Sie damit arbeiten oder eine Diskette versehentlich im Diskettenlaufwerk lassen, wenn Sie Ihren Computer ausschalten.

So schützen Sie Disketten automatisch:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Auto-Protect“.

3 Klicken Sie auf „Weitere“ im Register „Auto-Protect“.

4 Legen Sie im Gruppenfeld „Disketten prüfen“ (siehe Abbildung 5-13) fest, wie Norton AntiVirus Disketten auf Boot-Viren überprüfen soll:

- **Bei Zugriff Disketten auf Boot-Viren prüfen:** Überprüft jede Diskette, auf die Sie zugreifen, auf Boot-Viren (wenn Sie z.B. einen Ordner öffnen, eine Datei kopieren, in eine Datei schreiben oder eine Datei starten).
- **Bei Neustart des Computers Disketten prüfen:** Überprüft eine Diskette in Laufwerk A: auf Boot-Viren, wenn Sie Ihren Computer ausschalten.
- **Bei Neustart beide Laufwerke prüfen (A und B):** Überprüft auch Disketten in Laufwerk B: auf Boot-Viren, wenn Sie Ihren Computer ausschalten. Aktivieren Sie diese Option, wenn Sie einen Computer haben, der auch vom Laufwerk B: starten kann.

5 Klicken Sie auf „OK“, um das Dialogfeld zu schließen.

6 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Anpassen der Virusprüfung beim Systemstart

Die Prüfung beim Systemstart ist eine wichtige Maßnahme, um die Aktivierung und Verbreitung von Viren zu verhindern. (Wenn eine Systemdatei infiziert ist, wird der Virus beim Systemstart aktiviert und kann anschließend gestartete Programme infizieren.)

So passen Sie die Virusprüfung beim Systemstart an:

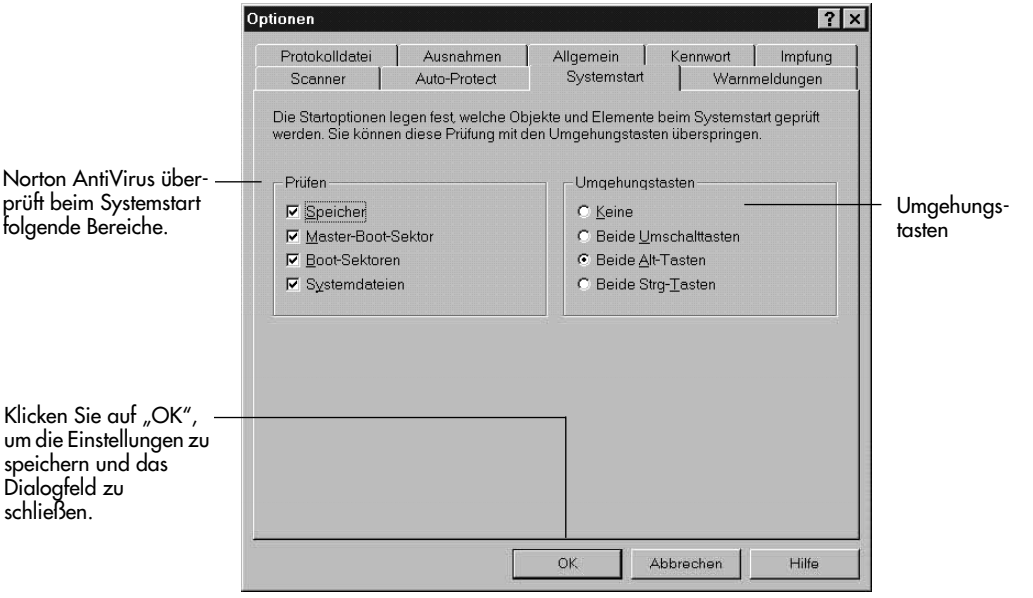
1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Systemstart“.

3 Legen Sie im Gruppenfeld „Beim Systemstart prüfen“ fest (siehe Abbildung 5-14), welche Bereiche Sie bei jedem Systemstart prüfen wollen:

- **Speicher:** Überprüft den Arbeitsspeicher Ihres Computers auf residente Viren. Speicherresidente Viren können Dateien befallen, auf die Sie zugreifen.
- **Master-Boot-Sektor:** Prüft den Master-Boot-Sektor auf Boot-Viren.
- **Boot-Sektoren:** Prüft die Boot-Sektoren Ihrer Festplatte auf Boot-Viren.
- **Systemdateien:** Prüft die Systemdateien, die Ihr Computer beim Systemstart und beim Starten von Windows verwendet.

Abbildung 5-14 Systemstart-Einstellungen



4 Legen Sie im Gruppenfeld „Umgehungstasten" die Tastenkombination fest, die Sie verwenden wollen, um die automatische Schutzfunktion beim Systemstart zu umgehen. Der Gebrauch der Umgehungstasten kann nützlich sein, wenn Sie ein Problem beim Starten des Computers oder einen Konfigurationskonflikt beheben wollen.

   Aktivieren Sie „Keine", wenn Sie keine Umgehungstasten verwenden wollen.

5 Klicken Sie auf „OK".

Anpassen der Impfung

Die Impfung von Dateien bietet zusätzlichen Schutz gegen unbekannte Viren. Wenn Sie eine Programmdatei, eine Systemdatei oder einen Boot-Sektor impfen, speichert Norton AntiVirus wichtige Informationen über diese Elemente (ähnlich einem Fingerabdruck). Danach überprüft Norton AntiVirus das geimpfte Element auf Änderungen, die auf einen unbekannten Virus hindeuten.

Beim Anpassen der Impfung legen Sie fest, was während einer Prüfung geimpft wird und wie reagiert werden soll, wenn Änderungen oder ungeimpfte Dateien gefunden werden.

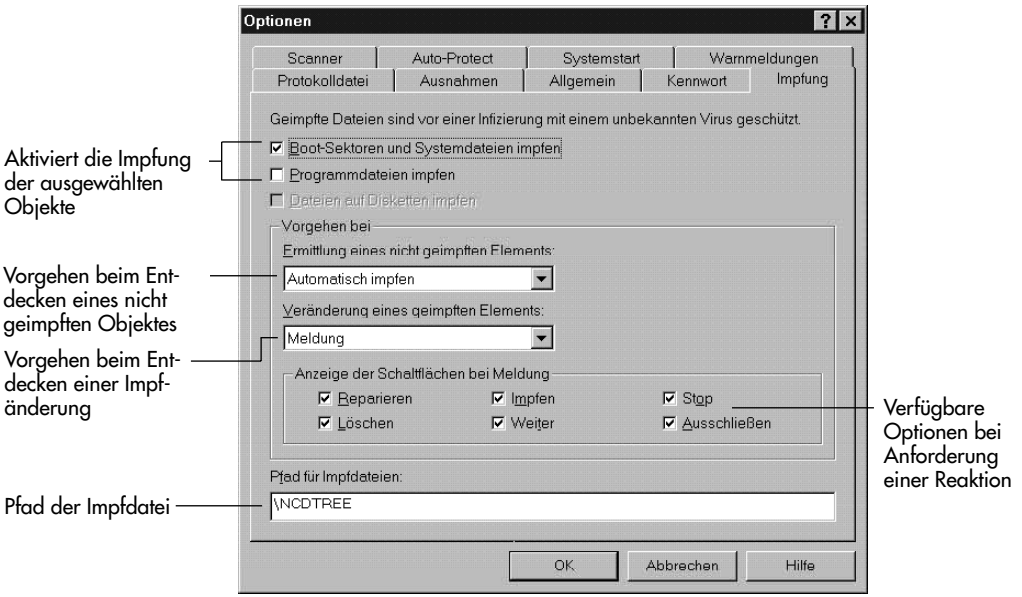
Die Impfung von Programmdateien stellt eine zusätzliche Schutzfunktion dar, die bei der Installation von Norton AntiVirus nicht automatisch aktiviert wird. Wenn Sie diese Funktion einschalten, erhalten Sie während gewöhnlicher Operationen Warnmeldungen, die auf einen Virus hinweisen könnten. Sie müssen dann für jedes Ereignis entscheiden, ob die Aktivität im Rahmen der durchgeführten Operation zulässig ist oder ob es sich um eine Virusaktivität handelt.

So passen Sie an, was geimpft wird:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Impfung“.

Abbildung 5-15 Impfeinstellungen



3 Aktivieren Sie „Boot-Sektoren und Systemdateien impfen“, so daß der Master-Boot-Sektor, die Boot-Sektoren und die Systemdateien Ihrer Festplatte geimpft und somit geschützt sind.

☞ **Tip:** Aktivieren Sie „Boot-Sektoren und Systemdateien impfen“, so daß Norton AntiVirus unbekannte Viren im Boot-Sektor findet.

4 Aktivieren Sie „Programmdateien impfen“, um Programmdateien auf den von Ihnen benutzten Festplatten und Netzlaufwerken zu impfen. Aktivieren Sie „Dateien auf Disketten impfen“, wenn Sie außerdem Dateien auf den Disketten impfen wollen, die Sie verwenden.

5 Klicken Sie auf „OK“, um die Änderungen zu speichern und das Dialogfeld zu schließen, oder fahren Sie mit dem in der nächsten Anleitung geschilderten Vorgang fort.

So stellen Sie ein, wie Sie auf Impfmeldungen reagieren können:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Impfung“ (siehe Abbildung 5-15).

3 Wählen Sie eine der Optionen in der Liste „Ermittlung eines nicht geimpften Elements“ aus (siehe Abbildung 5-15).

- **Meldung:** Sie werden informiert, daß eine Datei oder ein Boot-Sektor nicht geimpft wurde, und können entscheiden, wie Sie reagieren wollen.
- **Automatisch impfen:** Impft automatisch alle ungeimpften Dateien oder Boot-Sektoren. Das Element wird vor der Impfung auf bekannte Viren überprüft, um sicherzustellen, daß es virenfrei ist.
- **Nur benachrichtigen - Nicht impfen:** Informiert Sie lediglich darüber, daß eine Datei oder ein Boot-Sektor nicht geimpft wurde. Das Element wird nicht geimpft.
- **Zugriff verweigern:** Sie werden informiert, daß eine Programmdatei nicht geimpft wurde, und können das Programm nicht verwenden. (Diese Option gilt nicht für ungeimpfte Boot-Sektoren oder Systemdateien.)

4 Wählen Sie eine der Optionen in der Liste „Veränderung eines geimpften Elements“ aus:

- **Meldung:** Sie werden informiert, daß eine Datei oder ein Boot-Sektor geändert wurde, und können entscheiden, wie Sie reagieren wollen.
- **Nur benachrichtigen - Nicht impfen:** Informiert Sie lediglich darüber, daß eine Datei oder ein Boot-Sektor geändert wurde. Das Element wird nicht geimpft.
- **Zugriff verweigern:** Informiert Sie, wenn eine Impfänderung entdeckt wurde, und verhindert, daß Sie die Datei verwenden. (Diese Option gilt nicht für Boot-Sektoren.)

5 Wenn Sie in Schritt 3 oder 4 „Meldung“ ausgewählt haben, legen Sie im Gruppenfeld „Anzeige der Schaltflächen bei Meldung“ fest, welche Optionen Sie zur Verfügung haben wollen, wenn eine Impfmeldung angezeigt wird.

- **Reparieren:** Dateien oder Boot-Sektoren mit Impfänderungen reparieren, wobei ihr Zustand vor der letzten Impfung wiederhergestellt wird.

  Norton AntiVirus ist so eingestellt, daß vor der Reparatur einer Datei eine Sicherungskopie dieser Datei erstellt wird. Weitere Informationen hierzu finden Sie unter „Einstellen der allgemeinen Prüfoptionen“ auf Seite 80.

- **Löschen:** Programmdateien mit Impfänderungen löschen. Bei Systemdateien und Boot-Sektoren wird die Schaltfläche nicht angezeigt.
- **Impfen:** Dateien oder Boot-Sektoren impfen oder geänderte Dateien oder Boot-Sektoren neu impfen.
- **Weiter:** Aktuelle Operation (Prüfung oder Zugriff auf eine Datei) fortführen. Die Impfdaten werden nicht verändert.
- **Stop:** Aktuelle Operation (Prüfung oder Zugriff auf eine Datei) stoppen. Die Impfdaten werden nicht verändert.
- **Ausschließen:** Eine Datei von zukünftigen Prüfungen auf Impfung und Impfänderungen ausschließen.

6 Geben Sie einen Pfad für die Impfdateien im Feld „Pfad für Impfdateien“ ein. Der Standardpfad für die Impfdateien ist \NCDTREE.

Wenn Sie Dateien und Boot-Sektoren impfen, wird die Impfdatei auf jedem geimpften Laufwerk in das von Ihnen angegebene Verzeichnis gestellt.

☞ **Hinweis:** Wenn Sie Dateien in Netzwerkverzeichnissen impfen, müssen Sie für dieses Verzeichnis Schreibzugriff haben. Sie benötigen keinen Schreibzugriff für die Dateien, die Sie impfen.

7 Klicken Sie auf „OK“, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Einrichten eines Kennwortschutzes

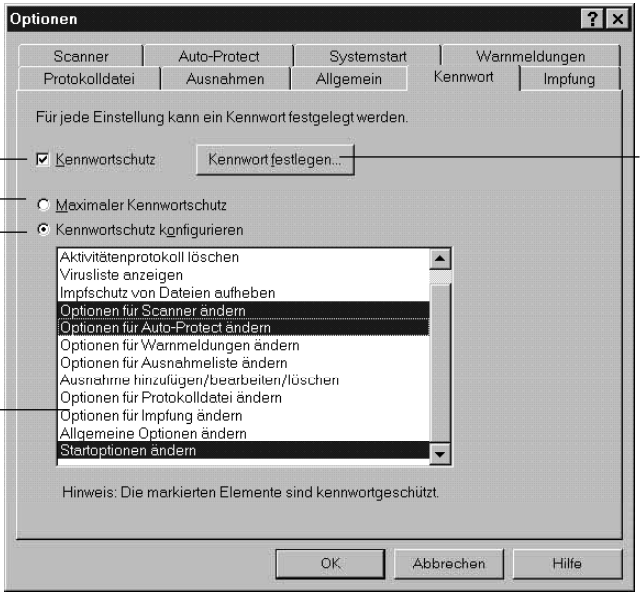
Sie können Ihre Konfiguration von Norton AntiVirus durch ein Kennwort schützen. Es können bestimmte Funktionen oder alle Einstellungen geschützt werden.

So schützen Sie bestimmte Funktionen durch ein Kennwort:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Kennwort“.

Abbildung 5-16 Kennworteinstellungen



3 Aktivieren Sie „Kennwortschutz“, um die Funktion für den Kennwortschutz einzuschalten.

4 Führen Sie einen der folgenden Schritte aus:

- Um alle Funktionen von Norton AntiVirus zu schützen, wählen Sie „Maximaler Kennwortschutz“.
- Um nur bestimmte Funktionen zu schützen, wählen Sie „Kennwortschutz konfigurieren“. Klicken Sie anschließend im Listenfeld auf die Funktion, die geschützt werden sollen.

5 Klicken Sie auf „Kennwort festlegen“, und geben Sie im Dialogfeld „Kennwort festlegen“ das gewünschte Kennwort ein. Das Kennwort gilt für alle geschützten Optionen.

   Kennwörter können zwischen 1 und 16 Zeichen enthalten. Die Groß- und Kleinschreibung ist ohne Belang. Bei der Eingabe des Kennwortes ersetzt Norton AntiVirus die Zeichen aus Sicherheitsgründen auf dem Bildschirm durch Sternchen (*).

6 Klicken Sie auf „OK“ im Dialogfeld „Kennwort festlegen“.

7 Klicken Sie auf „OK“.

Bevor Sie Änderungen an den Optionen mit Kennwortschutz vornehmen können, müssen Sie das Kennwort in Norton AntiVirus eingeben.

So ändern Sie Ihr Kennwort:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Kennwort“ (siehe Abbildung 5-16).

3 Geben Sie im Dialogfeld „Kennwort überprüfen“ Ihr Kennwort ein.

4 Klicken Sie auf „Kennwort festlegen“.

5 Geben Sie das bestehende Kennwort in das Textfeld „Altes Kennwort“ ein.

6 Geben Sie das neue Kennwort in das Textfeld „Neues Kennwort“ ein. Bestätigen Sie es im Feld „Neues Kennwort bestätigen“.

7 Klicken Sie auf „OK“.

So heben Sie den Kennwortschutz auf:

1 Klicken Sie auf „Optionen“ im Hauptfenster von Norton AntiVirus.

2 Klicken Sie auf das Register „Kennwort“ (siehe Abbildung 5-16).

3 Geben Sie im Dialogfeld „Kennwort überprüfen“ Ihr Kennwort ein.

4 Führen Sie einen der folgenden Schritte aus:

   - Um den Kennwortschutz vollständig aufzuheben, deaktivieren Sie die Option „Kennwortschutz“.
   - Um den Kennwortschutz für bestimmte Funktionen aufzuheben, wählen Sie „Kennwortschutz konfigurieren“, und klicken Sie im Listenfeld auf die gewünschten Funktionen.

5 Klicken Sie auf „OK“.

ANHANG A

Über Computerviren

Der Schutz von Computern durch eine richtig konfigurierte Antivirus-Software ist heute unabdingbar geworden, um ein sicheres und risikofreies Arbeiten zu gewährleisten. Zwar schwanken die Schätzungen über die Anzahl der bekannten Computerviren stark, es wird aber angenommen, daß es momentan ca. 8000 davon gibt. Diese Zahl berücksichtigt auch die Tatsache, daß es zu vielen der entdeckten Viren verschiedene Abarten gibt. Ein Virusprogrammierer muß einfach nur ein einziges Byte im Code eines vorhandenen Virus ändern, um eine neue Abart eines Virus zu erzeugen.

Virusprogrammierer kommunizieren oft über BBS-Systeme und das Internet, wo sie sich über ihre Aktivitäten unterhalten und Werkzeuge und Code austauschen. Die Mehrzahl aller Viren verbreitet sich aber nicht über die Grenzen dieser virusprogrammierenden Subkultur hinaus. Nur ein Bruchteil der tatsächlich existierenden Viren wird „freigelassen“, d.h. in Umgebungen gebracht, auf die von der Allgemeinheit der Computerbenutzer zugegriffen wird.

Im allgemeinen verfügen Virusprogrammierer über kein außergewöhnliches Talent, nicht einmal im Vergleich mit den Fähigkeiten professioneller Programmierer, die noch wenig Erfahrung haben. Viele Viren sind nicht dazu gedacht, den Betrieb eines Computers absichtlich zu stören. Da aber der Programmierer beim Schreiben des Viruscodes so viele Fehler gemacht hat, kann der Virus unter Umständen rücksichtslos Programme und Daten zerstören.

Die Anzahl der bekannten Viren aus verschiedenen Quellen und die Berichte über Infektionen nehmen kontinuierlich zu:

- Viele zerstörerische Viren haben bereits den Weg „ins Freie“ gefunden.
- Eine immer stärker wachsende Anzahl von Virustypen und -abarten gefährdet die Computerbenutzer.
- Die potentiellen Kosten, die durch Virusschäden verursacht werden können, sind astronomisch hoch.

Was sind Computerviren

Computerviren sind ausführbare Computerprogramme. Wie biologische Viren suchen sie einen Wirt und hängen sich an ihn an. Genauso wie ein Erkältungsvirus sich einen menschlichen Wirt sucht und diesen infiziert, hängt sich ein Computervirus an ein Element an, z.B. an den Boot-Sektor im Startbereich eines Computers oder an eine ausführbare Datei.

Nachdem ein Computervirus eine Datei oder einen anderen Teil Ihres Systems infiziert hat, verbreitet er sich auf benachbarte Elemente. Wenn er sich an ein Element anhängt, das von vielen Benutzern häufig verwendet oder im Rahmen der gemeinsamen Nutzung von Dateien weitergegeben wird, kann sich der Virus sehr weit verbreiten. Und je weiter sich der Virus verbreiten kann, desto größere Überlebenschancen hat er.

Es herrscht vielfach Ungewißheit darüber, was Computerviren wirklich tun und zu was sie nicht in der Lage sind. Diese Frage soll im folgenden geklärt werden.

Ein Virus kann folgende Elemente infizieren...

- Programmdateien, Bereiche, in denen keine Dateien abgelegt sind, da sie zum Starten des Computers verwendet werden (Boot-Sektoren) und Datendateien mit Makrofähigkeit
- Datenträger, die für den Austausch von Programmen verwendet werden
- Ihren Computer, wenn Sie Dateien von Online-Diensten herunterladen und verwenden
- Eine Datei, bevor sie an eine E-Mail-Nachricht angehängt wird

Ein Virus kann folgende Elemente nicht infizieren...

- Hardware, z. B. Tastaturen und Bildschirme, Grafikdateien, Datendateien ohne Makrofähigkeit, Software-Elemente, die keine Programmdateien sind
- Schreibgeschützte Disketten
- Ihren Computer, wenn Sie Texte eines Online-Dienstes lesen
- Textbasierte E-Mail-Nachrichten

Trojanische Pferde werden oft mit Computerviren verwechselt. Da sie sich aber nicht vermehren und verbreiten, handelt es sich bei ihnen nicht um Viren.

Ein Trojanisches Pferd ist ein Programm, das scheinbar nützlich oder interessant ist. Dadurch wird der Benutzer dazu verleitet, es zu starten. Doch wie das Trojanische Pferd aus der griechischen Sage hat es einen geheimen Zweck, z.B. Dateien zerstören oder einen Virus in Ihren Computer einschleusen.

Infektion

Computerviren werden aktiviert, wenn Sie ein infiziertes Programm ausführen oder einen Computer starten, dessen Boot-Sektoren infiziert sind. Nachdem sie aktiviert sind, verbreiten sich Computerviren auf zwei mögliche Arten, je nach ihrem Zweck:

- Direkte Infektion
- Speicherresidente Infektion

Ein Virus, der eine direkte Infektion verursacht, wird aktiviert, sobald die infizierte Datei ausgeführt wird. Er übernimmt die Kontrolle über das System, bevor andere Software geladen werden kann, und sucht nach „sauberen" Dateien, die er infizieren kann. Wenn das infizierte Programm geschlossen wird, kann auch der Virus keine weiteren Infektionen mehr vornehmen.

Ein Virus, der eine speicherresidente Infektion verursacht, verhält sich ähnlich wie ein speicherresidentes Programm (TSR-Programm). Er übernimmt die Kontrolle über das System, sobald er aktiviert wird. Dann bleibt er so lange im System und verbreitet sich, bis der Speicher durch Ausschalten oder einen Neustart gelöscht wird, auch dann, wenn Sie das infizierte Programm schließen.

Auslöser

Einige Programmierer versehen ihren Virus mit einer willkürlichen Inkubationszeit. Nachdem ein solcher Virus sich in Ihrem Computer eingenistet hat, wartet er auf einen *Auslöser*, der ihn aktiviert. Einige der vielen Arten von Ereignissen, die als Auslöser wirken können, sind ein bestimmtes Datum, der Ablauf von 60 Minuten nach dem Starten eines infizierten Programms oder die siebte Programmdatei, auf die der Virus trifft. Manche Viren verwenden auch einen Zufallsauslöser.

Ladung

Wie bei einem Gewehr, bei dem der Abzug betätigt wird, geben auch manche Viren eine *Ladung* frei, wenn der entsprechende Auslöser aktiviert wird. Einige Viren warten aber nicht auf einen Auslöser, sondern entledigen sich ihrer Ladung, sobald sie aktiviert werden.

Einige Ladungen wirken absichtlich zerstörerisch, z.B. solche, die Festplatten formatieren oder Dateien zerstören, wogegen andere relativ gutartig sind und z.B. lediglich eine Meldung am Bildschirm anzeigen. Wenn beispielsweise eine Datei mit dem Virus Windows 95 Boza infiziert ist, wird am 30. jeden Monats (der Auslöser) eine lange Meldung angezeigt, die mit „The taste of fame just got tastier!" beginnt (die Ladung).

Viren zeigen ihr Vorhandensein nicht unbedingt an, selbst dann nicht, wenn sie ihr Zerstörungswerk bereits begonnen haben. Der Virus Ripper z.B. nimmt willkürliche Änderungen an den Dateien auf einer Platte so langsam vor, daß dies vom normalen Computerbenutzer oft gar nicht bemerkt wird.

Ziele von Viren

Viren werden nach ihren Zielen kategorisiert:

- *Programmviren* infizieren Programmdateien, die meist eine der folgenden Dateierweiterungen haben: .COM, .EXE, .SYS, .DLL, .OVL oder .SCR. Am häufigsten werden Standard-DOS-Programme mit den Erweiterungen .COM und .EXE zum Ziel von Virusinfektionen. Programmdateien sind attraktive Ziele für Virusprogrammierer, da sie in weiten Kreisen verwendet werden und relativ einfache Formate haben, an die sich Viren leicht anhängen können.
- *Boot-Viren* infizieren die Systembereiche von Festplatten und Disketten, auf denen sich keine Dateien befinden. Diese Bereiche bieten den Viren eine effiziente Möglichkeit, sich von einem Computer auf einen anderen zu verbreiten. Boot-Viren sind im Hinblick auf die Weiterverbreitung und die Infektion ihrer Ziele erfolgreicher als Programmviren.
- *Makroviren* infizieren Datendateien mit Makrofähigkeit und stellen die neueste Gefahr für den Computerbenutzer dar. Beispielsweise können Dokument- und Vorlagendateien von Microsoft Word zum Opfer von Makroviren werden. Diese Viren verbreiten sich durch die gemeinsame Nutzung von infizierten Dokumenten oder das Herunterladen solcher Dokumente vom Internet sehr schnell.

Die einzelnen Virustypen und ihre verschiedenen Infektionsmechanismen werden in den folgenden Abschnitten behandelt.

Programmviren

Wie andere Programme auch, müssen Programmviren für ein bestimmtes Betriebssystem geschrieben sein. Die Mehrzahl dieser Viren wurde für DOS geschrieben, es gibt aber auch solche für Windows 3.x, Windows 95 und sogar für UNIX.

Alle Versionen von Windows sind kompatibel mit DOS und können deshalb mit unterschiedlich großem Erfolg DOS-Viren beherbergen. Die folgende Tabelle

beschreibt, wie sich DOS-Programmviren in den verschiedenen Windows-Versionen verhalten.

Windows-Version	Verhalten der Viren
Windows 3.x	Die meisten DOS-Viren können sich in dieser Umgebung gut verbreiten, da Windows 3.x für alle seine grundlegenden Dateifunktionen DOS verwendet.
Windows 95	Windows 95 ist mit fast jedem älteren Programm kompatibel und demnach auch mit Programmviren. Wenn ein speicherresidenter Virus, der Boot-Sektoren befällt, aktiv ist, kann es sein, daß Windows 95 während des Systemstarts Warnmeldungen anzeigt und sich die Leistung Ihres Systems verschlechtert.
Windows NT	Windows NT ist am wenigsten DOS-kompatibel, stellt aber immer noch eine gute Umgebung für Programmviren dar. Unter Windows NT können speicherresidente Viren nur in DOS-Sitzungen Infektionen verursachen und sich verbreiten. Wenn Sie die DOS-Sitzung beenden, wird der Virus so lange deaktiviert, bis Sie ein infiziertes Programm in einer anderen DOS-Sitzung starten. Da NT außerdem Dateisicherheit bietet, können Programmviren keine Dateien infizieren oder beschädigen, auf die Sie nicht zugreifen können.

Boot-Viren

Alle Festplatten und Disketten haben Boot-Sektoren, unabhängig davon, ob sie darüber hinaus auch Betriebssystemdateien enthalten. Bei einer Diskette muß es sich *nicht* um eine Startdiskette handeln, damit sie von einem Boot-Virus infiziert werden kann; auch Datendisketten können Boot-Viren enthalten. Eine typische Art und Weise, wie ein Computer mit einem Boot-Virus infiziert werden kann, ist ein Neustart, bei dem sich versehentlich eine infizierte Diskette im Diskettenlaufwerk befindet. Auch wenn es sich bei der Diskette nicht um eine Startdiskette handelt, kann der Virus aktiviert werden und sich verbreiten.

Anders als Programmviren können fast alle Boot-Viren DOS-, Windows 3.x-, Windows 95-, Windows NT- und sogar Novell Netware-Systeme infizieren. Der Grund dafür ist, daß sie nicht das Betriebssystem, sondern immanente Funktionen des Computers verwenden, um sich zu verbreiten und zu aktivieren.

Viele Boot-Viren gehen davon aus, daß die Festplatte ein normales DOS-Dateisystem verwendet. Eine solche Annahme ist aber nicht immer richtig, wenn Sie ein anderes Betriebssystem als DOS oder Windows 3.x verwenden. Bei Windows NT können Sie z.B. das NTFS-Dateisystem anstelle des DOS-kompa-

tiblen FAT-Dateisystems verwenden. Wenn ein Virus auf ein System trifft, das NTFS verwendet, kann er den Computer immer noch erfolgreich infizieren, dabei kann es aber passieren, daß er versehentlich einige Ihrer Dateien oder Boot-Sektoren (Systembereiche von Festplatten oder Disketten) beschädigt. Wenn das passiert, kann NT nicht mehr starten, und Sie müssen eventuell Windows neu installieren.

Ein weiterer interessanter Aspekt von Windows NT ist, daß es beim Starten (vorausgesetzt, daß es noch starten kann) alle Boot-Viren deaktiviert. Das bedeutet, daß Boot-Viren einen Computer, der Windows NT verwendet, zwar infizieren, sich aber nicht auf andere Systeme verbreiten können, während Windows NT läuft. Sie dürfen nun aber nicht annehmen, daß der Virus harmlos ist. Bei jedem Start Ihres Systems wird der Virus aktiviert und hat die Möglichkeit, seinen Auslöser zu aktivieren und sich seiner Ladung zu entledigen. Beispielsweise schreibt der Virus Stoned.Michelangelo am 6. März willkürlich Bytes auf jeden Zylinder der Festplatte, wodurch die ursprünglichen Daten dort überschrieben werden. Als erstes werden in Sekundenbruchteilen die Hauptsystembereiche, die der Computer zum Starten verwendet, überschrieben. Sobald der zerstörerische Vorgang durch den Auslöser aktiviert wurde, ist es schlicht unmöglich, den Virus vom Zerstören aller Daten auf der Festplatte abzuhalten.

Makroviren

Viele ältere Anwendungen enthielten einfache Makrosysteme, mit denen Sie eine Abfolge von Aktionen in der Anwendung aufzeichnen und ihnen eine bestimmte Tastaturkombination zuweisen konnten. Später konnten Sie dann dieselbe Abfolge von Aktionen wiederholen, indem Sie einfach die Tastaturkombination drückten.

Neuere Anwendungen bieten sehr viel komplexere Makrosysteme. Sie können komplette Makroprogramme schreiben, die innerhalb der Textverarbeitungs- oder Tabellenkalkulationsumgebung laufen und direkt mit Textverarbeitungs- oder Tabellenkalkulationsdateien verknüpft sind. Die Möglichkeit, ein oder mehrere Makros an eine Datendatei anzuhängen, ist eine sehr leistungsstarke Funktion. Doch leider wurde dadurch auch das Erzeugen von Makroviren ermöglicht.

Eine typische Abfolge einer Infektion mit einem Makrovirus beginnt mit dem Laden eines infizierten Dokuments oder Arbeitsblatts. Die Anwendung lädt dann gleichzeitig auch alle Makros, die mit der Datei verknüpft sind. Wenn ein oder mehrere dieser Makros bestimmte Bedingungen erfüllen, werden sie sofort ausgeführt. Makroviren bedienen sich dieser Möglichkeit der automatischen Ausführung, um die Kontrolle über das Makrosystem der Anwendung zu erhalten.

Nachdem der Makrovirus geladen und ausgeführt wurde, wartet er darauf, daß Sie ein neues Dokument bearbeiten, um wieder in Aktion zu treten. Er hängt seine Virus-Makroprogramme an das neue Dokument an und läßt dann die Anwendung das Dokument ganz normal speichern. Auf diese Weise verbreitet sich der Virus völlig unauffällig zu einer neuen Datei – Sie bemerken nichts von der Infektion. Wenn diese neue Datei später auf einem anderen Computer geöffnet wird, wird der Virus wieder geladen, von der Anwendung gestartet und kann sich unbemerkt auf weitere Dateien ausbreiten.

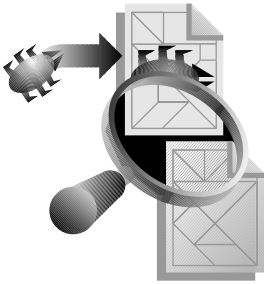
Und schließlich dient die Anwendung für den Makrovirus als „Betriebssystem“. Ein einziger Makrovirus kann sich auf alle anderen Plattformen ausbreiten, auf denen die Anwendung installiert ist und läuft. Beispielsweise kann ein Makrovirus, der Microsoft Word benutzt, sich heimlich auf Windows 3.x, Windows 95, Window NT und den Macintosh ausbreiten.

Technologien von Viren

Programm- und Boot-Viren werden auch nach den Technologien kategorisiert, die sie verwenden, um sich zu verbreiten und ihre Entdeckung zu verhindern. Dies wird in den folgenden Abschnitten beschrieben.

Stealth- oder Tarnkappen-Viren

Stealth- oder Tarnkappen-Viren versuchen gezielt, sich einer Analyse oder Entfernung zu entziehen. Zu diesen sogenannten Stealth-Techniken gehören das Umleiten von Festplattenlesevorgängen, um eine nichtinfizierte Kopie des Originalobjekts anstelle des infizierten Objekts zu präsentieren (Stealth (Volle Tarnung)), und die Veränderung von Ordnerdaten für die infizierten Programmdateien auf Diskette oder Festplatte (Stealth (Größentarnung)) oder beides.



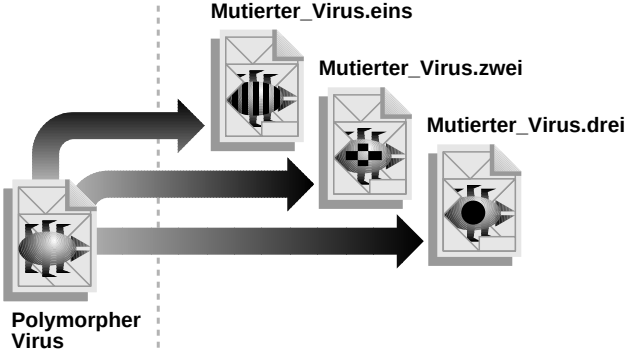
Der Whale-Virus ist z.B. ein Stealth-Virus mit Größentarnung. Er infiziert .EXE-Programmdateien und verändert die Ordnereinträge von infizierten Dateien, wenn andere Programme versuchen, sie zu lesen. Der Whale-Virus addiert 9216 Bytes zu einer infizierten Datei. Da Änderungen bei der Dateigröße auf das Vorhandensein eines Virus hindeuten können, subtrahiert er dann dieselbe Anzahl von Bytes (9216) von der angegebenen Dateigröße im Ordnereintrag, damit der Eindruck entsteht, daß sich die Dateigröße nicht geändert habe.

Polymorphe Viren

Die meisten einfachen Viren hängen identische Kopien ihrer selbst an die Dateien an, die sie infizieren. Ein Antivirus-Programm kann den Code des Virus (seine Handschrift) erkennen, da dieser immer gleich ist, und den Virus schnell aufspüren.

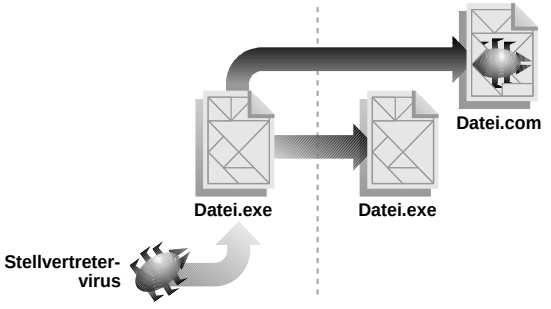
Polymorphe Viren gehen etwas anders vor, damit sie nicht so schnell entdeckt werden können. Im Gegensatz zu einem einfachen Virus verschlüsseln polymorphe Viren ihren Viruscode, wenn sie ein Programm infizieren. Diese Ver-

schlüsselung bewirkt, daß keine zwei Infektionen durch denselben Virus identisch sind, und erschwert so die Entdeckung.



Stellvertreterviren

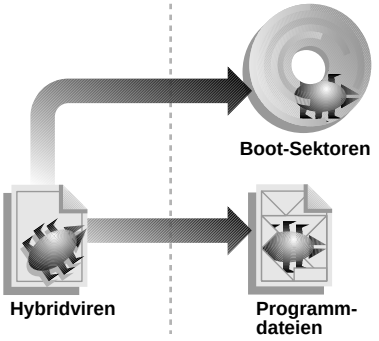
Ein *Stellvertretervirus* ist die Ausnahme zur Regel, daß ein Virus sich immer an eine Datei anhängt. Der Stellvertretervirus erstellt statt dessen eine neue Datei und vertraut auf eine Eigenschaft von DOS, diese Datei anstelle der Programmdatei auszuführen, die normalerweise ausgeführt werden würde.



Stellvertreterviren verwenden verschiedene Strategien. Einige erstellen eine .COM-Datei, die denselben Namen erhält wie eine vorhandene .EXE-Datei. Beispielsweise kann der Stellvertretervirus eine Datei namens CHKDSK.COM erstellen und sie im gleichen Verzeichnis ablegen wie die Datei CHKDSK.EXE. Immer wenn DOS beim Ausführen einer Datei zwischen zwei Dateien wählen muß, die denselben Namen haben, aber eine unterschiedliche Erweiterung (.EXE und .COM), führt es die .COM-Datei aus.

Hybridviren

Hybridviren sind sowohl Programm- als auch Boot-Viren. Wenn Sie z.B. ein Textverarbeitungsprogramm starten, das mit dem Tequila-Virus infiziert ist, wird der Virus aktiviert und infiziert den Master-Boot-Sektor auf Ihrer Festplatte. Beim nächsten Start des Computers wird dann der Tequila-Virus wieder aktiviert und infiziert jedes Programm, das Sie starten, unabhängig davon, ob es sich auf der Festplatte oder einer Diskette befindet.



Wie Sie Ihren Schutz aktuell halten

Norton AntiVirus entdeckt Viren anhand ihrer charakteristischen Handschriften oder Virussignaturen und verwendet dabei Techniken, die alle Bemühungen der Viren, unentdeckt zu bleiben, zunichte machen. Die Virussignaturen sind in den Virusdefinitionsdateien von Norton AntiVirus abgelegt. Ihr Schutz vor Viren ist deshalb nur so aktuell wie die Virusdefinitionsdateien, die Ihre Kopie von Norton AntiVirus verwendet.

Damit Ihr Computer immer optimal vor Viren geschützt ist, müssen Sie die Virusdefinitionsdateien regelmäßig aktualisieren. Symantec stellt Ihnen jeden Monat kostenfrei aktualisierte Virusdefinitionsdateien zur Verfügung. Sie können diese neuen Virusdefinitionsdateien auf verschiedenen Wegen erhalten, je nachdem, welches Produkt Sie verwenden. Detaillierte Informationen dazu finden Sie in Kapitel 4, „Schutz vor neuen Viren“.

Die Welt der Computerviren ändert sich ständig. Denken Sie deshalb daran, Ihre Virusdefinitionsdateien jeden Monat zu aktualisieren.

ANHANG B

NAV-Rettungsdisketten

Ein Norton AntiVirus-Rettungsdiskettensatz erleichtert die Reparatur von durch Viren verursachten Schäden. Es besteht aus folgenden Disketten:

- **Norton AntiVirus Rettungs- und Startdiskette:** Zum Starten Ihres Computers
- **Norton AntiVirus Programmdiskette:** Zum Prüfen auf und Entfernen von Viren
- **Norton AntiVirus Virusdefinitionsdiskette:** Enthält die während der Prüfungen verwendeten Virusdefinitionsdateien

Wenn Sie noch keinen Norton AntiVirus-Rettungsdiskettensatz erstellt haben, sollten Sie das jetzt tun. Siehe dazu „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27.

Entfernen von Viren von einem ausgeschalteten Computer

So entfernen Sie Viren mit dem NAV-Rettungsdiskettensatz:

1. Wenn Ihr Computer läuft, wählen Sie „Beenden“ im Menü „Start“ der Windows Task-Leiste, um ihn herunterzufahren.
2. Schalten Sie Ihren Computer mit dem Netzschalter aus. Dadurch werden alle Viren entfernt, die sich eventuell im Arbeitsspeicher befinden.

   Sie müssen die Stromzufuhr ausschalten. Bei bestimmten Viren reicht es nicht aus, „Neu starten“ zu wählen oder Strg+Alt+Entf zu drücken, um sie aus dem Arbeitsspeicher zu entfernen.
3. Legen Sie die schreibgeschützte Norton AntiVirus Rettungs- und Startdiskette in Laufwerk A: ein, und schalten Sie den Computer ein.

   Ihr Computer wird von der Rettungsdiskette gestartet.
4. Wenn Sie dazu aufgefordert werden, nehmen Sie die Rettungs- und Startdiskette aus dem Laufwerk, und legen Sie die Diskette mit dem Namen „Norton AntiVirus Programmdiskette“ ein.

5 Geben Sie bei der DOS-Eingabeaufforderung GO ein. Befolgen Sie danach die Anweisungen, die auf dem Bildschirm angezeigt werden.

6 Norton AntiVirus prüft das System und informiert Sie, sobald der Virus gefunden wurde. Wählen Sie danach „Reparieren“, um den Virus zu entfernen und das infizierte Element zu reparieren.

7 Nachdem alle Viren entfernt wurden, nehmen Sie alle Disketten aus dem Laufwerk heraus, und starten Sie den Computer neu. Schalten Sie ihn dazu aus und wieder ein. Sie kommen zurück zu Windows.

8 Versuchen Sie, die Quelle der Virusinfektion zu finden. Starten Sie Norton AntiVirus, und prüfen Sie erneut alle Festplatten. Prüfen Sie auch die Disketten, um herauszufinden, woher der Virus kam.

Wenn Sie keinen eigenen NAV-Rettungsdiskettensatz haben, können Sie die Notfalldiskette verwenden, die zum Lieferumfang von Norton AntiVirus gehört. Diese Diskette ist zwar nicht ganz so leistungsfähig wie ein eigener Rettungsdiskettensatz, häufig auftretende Viren werden aber auch mit dieser Diskette erkannt und zuverlässig entfernt.

So entfernen Sie Viren ohne eigenen NAV-Rettungsdiskettensatz:

1 Wenn Ihr Computer läuft, wählen Sie „Beenden“ im Menü „Start“ der Windows Task-Leiste, um ihn herunterzufahren.

2 Schalten Sie Ihren Computer mit dem Netzschalter aus. Dadurch werden alle Viren entfernt, die sich eventuell im Arbeitsspeicher befinden.

Sie müssen die Stromzufuhr ausschalten. Bei bestimmten Viren reicht es nicht aus, „Neu starten“ zu wählen oder Strg+Alt+Entf zu drücken, um sie aus dem Arbeitsspeicher zu entfernen.

3 Legen Sie die Notfalldiskette in Laufwerk A: ein, und schalten Sie Ihren Computer ein. Die Notfalldiskette muß sich in Laufwerk A: befinden, um den Computer damit zu starten.

4 Befolgen Sie die Anleitungen, die auf dem Bildschirm angezeigt werden.

Wiederherstellen der Festplatte

☞ **Achtung:** Der folgende Vorgang ist für den Notfall gedacht. Bevor Sie versuchen, Ihre Festplatte wiederherzustellen, lesen Sie die Datei VIRSPEC.TXT, die sich im Ordner „Norton AntiVirus“ befindet oder in der Aktualisierung der Virusdefinitionen enthalten ist. In dieser Datei wird erklärt, in welchen Fällen Sie eine Wiederherstellung versuchen sollten.

Manchmal werden wichtige Informationen über Ihre Festplatte durch einen Virus beschädigt und können nicht mehr repariert werden. In diesen Fällen können Sie den NAV-Rettungsdiskettensatz verwenden.

Die Fehlermeldung von Norton AntiVirus, z.B. „Boot-Sektor kann nicht repariert werden“ oder „Master-Boot-Sektor kann nicht repariert werden“, bestimmt, wie Sie Ihre Rettungsdisketten verwenden. Normalerweise stellen Sie die CMOS-Daten wieder her, wenn Ihre Festplatte „verschwindet“ oder die Anzahl der Laufwerke bzw. die Speichergröße falsch angegeben wird. Wenn Ihre Rettungsdisketten aktuell sind, können Sie gefahrlos alle drei Elemente wiederherstellen.

Partitionstabelle Master-Boot-Sektor
Der erste physische Sektor auf einer Festplatte. Er enthält das Programm für den Master-Boot-Sektor und die Partitionstabelle. Diese enthält Informationen über die Einrichtung der Festplatte, z.B. Größe und Lage der Partitionen, welches Betriebssystem die einzelnen Partitionen verwenden und von welcher Partition der Computer gestartet wird.

Boot-Sektor
Der erste logische Sektor einer Festplattenpartition. Er enthält Informationen über die Plattenarchitektur (Sektorgröße, Clustergröße usw.) sowie das Boot-Sektor-Programm.

CMOS
Abkürzung für Complimentary Metal Oxide Semiconductor. Ein batteriebetriebener Chip in 80286er (und neueren) Computern, der grundlegende Daten über die System-Hardware speichert.

☞ **Achtung:** Verwenden Sie niemals NAV-Rettungsdisketten, die für einen anderen Computer erstellt wurden. Rettungsdisketten sind nur für den Computer geeignet, auf dem sie erstellt wurden. Erstellen Sie deshalb immer neue Rettungsdisketten für Ihren Computer, wenn Sie ein neues Betriebssystem installieren, Hardware-Geräte, z.B. Festplatten, installieren oder den Arbeitsspeicher (RAM) erhöhen. Anweisungen dazu finden Sie unter „Erstellen eines Rettungsdisketten-satzes“ auf Seite 27.

Da die Notfallprogramme von Norton AntiVirus unter DOS (und nicht unter Windows) ausgeführt werden, müssen Sie die Tastatur für die Navigation in den Dialogfeldern verwenden. Die Maus wird nicht unterstützt. Für die Navigation stehen Ihnen die folgenden Tasten zur Verfügung:

- Drücken Sie die Tabulatortaste, um reihum die Optionen eines Dialogfelds anzusteuern.
- Mit der Auf- und der Abwärtspfeiltaste können Sie ein Element in einem Gruppenfeld (z.B. ein Laufwerk) hervorheben oder markieren.
- Mit der Leertaste können Sie ein Kontrollkästchen im Wechsel aktivieren und deaktivieren.
- Drücken Sie die Eingabetaste, um den Befehl der hervorgehobenen Schaltfläche auszuführen.
- Wenn Sie eine Option oder eine Schaltfläche direkt ansteuern und aktivieren wollen, drücken Sie die Taste Alt, halten Sie sie gedrückt, und drücken Sie danach die Buchstabentaste, die in der gewünschten Option oder Schaltfläche hervorgehoben ist. Geben Sie anschließend beide Tasten wieder frei.

So stellen Sie Ihre Festplatte wieder her:

1. Schalten Sie Ihren Computer mit dem Netzschalter aus.
2. Legen Sie die schreibgeschützte NAV-Rettungs- und Startdiskette in Laufwerk A: ein, und schalten Sie den Computer ein.

   Ihr Computer wird von der Rettungsdiskette gestartet.
3. Geben Sie RESCUE bei der Eingabeaufforderung A: ein, und drücken Sie die Eingabetaste. Das Dialogfeld „Rettungsinformation wiederherstellen“ wird geöffnet.
4. Vergewissern Sie sich, daß A:\ als Ablageort der Rettungsdaten angegeben ist.
5. Wählen Sie die wiederherzustellenden Elemente im Gruppenfeld „Wiederherzustellende Elemente?“ aus.

   Mit der Tabulatortaste können Sie sich im Dialogfeld bewegen. Mit der Leertaste können Sie Elemente auswählen oder die Auswahl zurücknehmen.
6. Wählen Sie „Wiederherstellen“, um die ausgewählten Elemente wiederherzustellen.
7. Nachdem der Vorgang beendet ist, entfernen Sie die NAV-Rettungsdiskette aus dem Laufwerk A:, und starten Sie Ihren Computer neu.
8. Starten Sie Norton AntiVirus, und prüfen Sie erneut alle Festplatten. Prüfen Sie auch Ihre Disketten, um herauszufinden, woher der Virus kam.

A N H A N G

C

Befehlszeilenschalter

Ein Schalter ist ein abgekürzter Befehl, den Sie zum Steuern von Norton AntiVirus oder zum vorübergehenden Ändern von Standardeinstellungen verwenden können. Die im folgenden aufgeführten Komponenten von Norton AntiVirus können mit Befehlszeilenschaltern ausgeführt werden. Wenn Sie diese Komponenten ohne Schalter ausführen, wird eine Benutzerschnittstelle angezeigt.

- NAVDX.EXE führt die Prüfungen beim Systemstart durch und prüft in Notfallsituationen auf Viren, z.B. wenn der Computer nach einer Virenwarnung abgeschaltet wurde.
- NAVW32.EXE ist die Schnittstelle und der Viren-Scanner für Windows.
- RESCUE.EXE stellt Boot-Sektoren von Festplatten, CMOS-Einstellungen und Partitionstabellen wieder her, die Sie vorher auf Ihrem Rettungsdiskettensatz gesichert haben. Wie Sie das machen, ist unter „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27 beschrieben.

Einige Schalter werden alleine verwendet, anderen folgt der Zusatz „+“ oder „-“. Sie können in einer Befehlszeile mehrere Schalter und mehrere Parameter verwenden. Der gerade Strich (|) bedeutet, daß Sie nur einen der beiden Parameter und nicht beide zusammen verwenden dürfen. Geben Sie die hier verwendeten eckigen Klammern um die Parameter in der Befehlszeile nicht mit ein.

NAVDX.EXE

DOS

NAVDX.EXE ist die Komponente von Norton AntiVirus, die Prüfungen beim Systemstart durchführt und das speicherresidente Programm für den DOS-Programmschutz lädt. Es wird von der DOS-Eingabeaufforderung aus gestartet und soll in Notfallsituationen eine Virusprüfung durchführen, z.B. wenn der Computer nach einer Virenwarnung abgeschaltet wurde. Weitere Informationen finden Sie im Abschnitt „Entfernen von Viren von einem ausgeschalteten Computer“ auf Seite 107.

Syntax

```
NAVDX [Pfadname] [Optionen]
```

`Pfadname`	Beliebige Laufwerke, Ordner, Dateien oder eine Kombination davon werden geprüft. Wenn Sie eine Kombination dieser Elemente überprüfen möchten, trennen Sie die einzelnen Elemente durch ein Leerzeichen. Bei der Angabe von Pfadnamen für eine Gruppe von Dateien können Sie auch Platzhalterzeichen verwenden (z.B. NAVDX A: C:\MEINVERZ*.EXE).
`/A`	Alle Laufwerke, mit Ausnahme der Laufwerke A: und B:, werden geprüft. Netzwerklaufwerke werden geprüft, wenn Sie die Option „Netzwerkprüfung zulassen“ im Dialogfeld „Weitere Optionen für Scanner“ ausgewählt haben.
`/L`	Alle lokalen Laufwerke, mit Ausnahme der Laufwerke A: und B:, werden geprüft.
`/S [+|-]`	Die Funktion zur Prüfung aller Unterordner der im Pfadnamen angegebenen Ordner wird aktiviert (+) bzw. deaktiviert (-).
`/M [+|-]`	Die Funktion zur Prüfung des Arbeitsspeichers wird aktiviert (+) bzw. deaktiviert (-) (z.B. NAVDX C: /M+ oder NAVDX D: /M-).
`/MEM`	Es wird nur der Arbeitsspeicher geprüft.
`/B [+|-]`	Die Funktion zur Prüfung von Boot-Sektoren wird aktiviert (+) bzw. deaktiviert (-) (z.B. NAVDX A: /B+ oder NAVDX B: /B-).
`/BOOT`	Es werden nur die Boot-Sektoren der angegebenen Laufwerke geprüft.
`/PROMPT`	Sie werden benachrichtigt, wenn ein Virus gefunden wird, und können entsprechende Gegenmaßnahmen wählen. Die zur Verfügung stehenden Maßnahmen werden durch die im Gruppenfeld „Anzeige der Schaltflächen bei Meldung“ im Dialogfeld „Optionen – Scanner“ ausgewählten Elemente bestimmt. Weitere Informationen hierzu finden Sie unter „Anpassen manueller Prüfoptionen“ auf Seite 63.
`/REPAIR`	Eine infizierte Datei wird repariert, ohne daß Sie benachrichtigt werden. Das Ergebnis wird in der Protokolldatei aufgezeichnet.

`/DELETE`	Eine infizierte Datei wird gelöscht, ohne daß Sie benachrichtigt werden. Das Ergebnis wird in der Protokolldatei aufgezeichnet.
`/HALT`	Ihr Computer wird angehalten, wenn ein Virus gefunden wird.
`/NOBEEP`	NAVDX läuft im Hintergrund.
`/ZIPS`	Dateien in komprimierten Dateien werden geprüft.
`/DOALLFILES`	Es werden nicht nur ausführbare, sondern alle Dateien geprüft.
`/LOG:datei`	Es wird eine neue Protokolldatei erstellt.
`APPENDLOG: datei`	Die Protokolleinträge werden einer vorhandenen Protokolldatei hinzugefügt.
`/CFG[:Ordner]`	Die im angegebenen Ordner enthaltenen Programmeinstellungen werden verwendet.
`/HELPERROR`	Die zurückgelieferten DOS-Fehlercodes werden angezeigt.
`/?`	Eine Beschreibung aller für NAVDX zur Verfügung stehenden Befehlszeilenschalter wird angezeigt.

NAVDX liefert auch folgende DOS-Fehlercodes zurück, die von einer Stapeldatei mit der Anweisung IF ERRORLEVEL verarbeitet werden können. Weitere Informationen hierzu finden Sie in Ihrer DOS-Dokumentation.

Code	**Fehler**
0	Es traten keine Fehler auf, und es wurden keine Viren entdeckt.
10	Im Speicher wurde ein Virus gefunden.
11	Ein interner Programmfehler trat auf.
13	Im Master-Boot-Sektor, oder in Boot-Sektoren und/oder in Dateien wurden ein oder mehrere Viren gefunden.
15	Der NAVDX-Selbsttest schlug fehl. NAVDX kann infiziert oder beschädigt sein.
102	Die Prüfung wurde mit Strg+C oder Strg+UntBr abgebrochen.

Anwendungsbeispiele

- Um alle .EXE-Dateien im Ordner SPIELE zu prüfen, geben Sie folgendes ein:

  ```
  NAVDX C:\SPIELE\*.EXE
  ```

- Um den Ordner SPIELE auf der Festplatte, das Laufwerk D: und die Datei C:\BEISPIEL\BEISPIEL.EXE zu prüfen, geben Sie folgendes an der DOS-Eingabeaufforderung ein:

  ```
  NAVDX C:\SPIELE D: C:\BEISPIEL\BEISPIEL.EXE
  ```

  Wenn C:\BEISPIEL der aktuelle Ordner ist, geben Sie folgendes ein:

  ```
  NAVDX C:\SPIELE D: BEISPIEL.EXE
  ```

- Um einen Ordner auf dem Netzwerklaufwerk P: namens PROGRAMM und alle seine Unterordner zu prüfen, geben Sie folgendes ein:

  ```
  NAVDX P:\PROGRAMM /S+
  ```

  Wenn Sie alle bei dieser Prüfung gefundenen infizierten Dateien sofort reparieren wollen, geben Sie folgendes ein:

  ```
  NAVDX P:\PROGRAMM /S+ /REPAIR
  ```

- Um nur den Speicher zu prüfen, geben Sie folgendes ein:

  ```
  NAVDX /MEM
  ```

- Um nur die Boot-Sektoren der Laufwerke C: und A: zu prüfen, geben Sie folgendes ein:

  ```
  NAVDX C: A: /BOOT
  ```

NAVW32.EXE

NAVW32.EXE ist die Schnittstelle und der Viren-Scanner für Windows. Sie kann mit Befehlszeilenschaltern ausgeführt werden, normalerweise mit dem Befehl „Ausführen“ im Menü „Start“, um Konfigurationseinstellungen vorübergehend zu ändern. Beim Prüfen von Laufwerken mit Hilfe von Befehlszeilenschaltern wird Norton AntiVirus zum Symbol verkleinert. Sobald es einen Virus findet, wird es wieder vergrößert.

Syntax

```
NAVW32 [[Pfadname] Optionen]
```

`Pfadname`	Beliebige Laufwerke, Ordner, Dateien oder eine Kombination davon werden geprüft. Wenn Sie eine Kombination dieser Elemente prüfen möchten, trennen Sie die einzelnen Elemente durch ein Leerzeichen. Bei der Angabe von Pfadnamen für eine Gruppe von Dateien können Sie Platzhalterzeichen verwenden (z.B. NAVW32 A: C:\MEINVERZ*.EXE).
`/A`	Alle Laufwerke, mit Ausnahme der Laufwerke A: und B:, werden geprüft. Netzwerklaufwerke werden geprüft, wenn Sie die Option „Netzwerkprüfung zulassen“ im Dialogfeld „Weitere Optionen für Scanner“ ausgewählt haben.
`/L`	Alle lokalen Laufwerke, außer A: und B:, werden geprüft.
`/S`	Alle Unterordner der im Pfadnamen angegebenen Ordner werden in den Prüfvorgang einbezogen.
`/M [+|-]`	Die Prüfung des Speichers wird aktiviert (+) bzw. deaktiviert (-) (z.B. NAVW32 C: /M+ oder NAVW32 D: /M-).
`/MEM`	Es wird nur der Arbeitsspeicher geprüft.
`/B [+|-]`	Die Prüfung von Boot-Sektoren wird aktiviert (+) bzw. deaktiviert (-) (z.B. NAVW A: /B+ oder NAVW B: /B-).
`/BOOT`	Es werden nur die Boot-Sektoren der angegebenen Laufwerke geprüft.

Anwendungsbeispiele

- Um alle .EXE-Dateien im Ordner SPIELE zu prüfen, geben Sie folgendes ein:

  ```
  NAVW32 C:\SPIELE\*.EXE
  ```

- Um den Ordner SPIELE auf der Festplatte, das Laufwerk D: und die Datei C:\BEISPIEL\BEISPIEL.EXE zu prüfen, verwenden Sie den Befehl „Ausführen…“ und geben folgendes ein:

  ```
  NAVW32 C:\SPIELE D: C:\BEISPIEL\BEISPIEL.EXE
  ```

  Wenn C:\BEISPIEL der aktuelle Ordner ist, geben Sie folgendes ein:

  ```
  NAVW32 C:\SPIELE D: BEISPIEL.EXE
  ```

- Um einen Ordner auf dem Netzwerklaufwerk P: namens PROGRAMM und alle seine Unterordner zu prüfen, geben Sie folgendes ein:

  ```
  NAVW32 P:\PROGRAMM /S
  ```

- Um nur den Speicher zu prüfen, geben Sie folgendes ein:

  ```
  NAVW32 /MEM
  ```

- Um nur die Boot-Sektoren der Laufwerke C: und A: zu prüfen, geben Sie folgendes ein:

  ```
  NAVW32 C: A: /BOOT
  ```

- Um Pfadnamen mit langen Dateinamen anzugeben, die Leerzeichen enthalten, verwenden Sie Anführungszeichen:

  ```
  NAVW32 C:\"Finanzen August"
  ```

RESCUE.EXE

RESCUE.EXE wird von der DOS-Eingabeaufforderung aus gestartet und stellt Boot-Sektoren von Festplatten, CMOS-Einstellungen und Partitionstabellen wieder her, die Sie vorher auf Ihrer Rettungsdiskette gesichert haben. Weitere Informationen hierzu finden Sie in Anhang B unter „Wiederherstellen der Festplatte“.

☞ **Tip:** Wenn Sie noch keine Rettungsdiskette erstellt haben, dann tun Sie das jetzt! Wie Sie das machen, ist unter „Erstellen eines Rettungsdiskettensatzes“ auf Seite 27 beschrieben.

Syntax

```
RESCUE [/RESTORE[:Pfadname]] [/G0] [/BW|/LCD]
```

`/RESTORE`	Es wird von der Rettungsdiskette wiederhergestellt.
`Pfadname`	Laufwerk und Verzeichnis der Rettungsdateien.
`/G0`	Die Grafikmaus und alle Grafikzeichen werden deaktiviert.
`/BW`	Die Anzeige bei Schwarzweiß-Bildschirmen wird verbessert.
`/LCD`	Die Anzeige bei LCD-Bildschirmen wird verbessert.
`/?`	Eine Beschreibung aller für RESCUE zur Verfügung stehenden Befehlszeilenschalter wird angezeigt.

Anwendungsbeispiel

- So stellen Sie Informationen für Laufwerk A: wieder her:

  ```
  RESCUE /RESTORE:A:\
  ```

A N H A N G D

Systemmeldungen

Dieser Anhang enthält eine Liste der Systemmeldungen, die bei der Arbeit mit Norton AntiVirus angezeigt werden können.

Angaben in spitzen Klammern wie <DATEINAME>, <LAUFWERK> oder <VIRUSNAME> werden in den Systemmeldungen auf dem Bildschirm durch den entsprechenden Dateinamen, die Laufwerksbezeichnung oder den Virusnamen ersetzt.

Meldungen und ihre Bedeutungen

<Dateiname> hat sich seit der Impfung geändert.

Die Datei hat sich seit der Impfung geändert. Dies bedeutet nicht zwangsläufig, daß die Datei mit einem Virus infiziert ist. Sie müssen bestimmen, ob die Änderung zulässig ist oder nicht. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Der Boot-Sektor hat sich seit der Impfung geändert.

Impfänderungen in einem Boot-Sektor weisen meist auf das Vorhandensein eines unbekannten Virus hin. Es gibt aber einige wenige Situationen, in denen eine solche Änderung zulässig ist. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Die Konfigurationsdatei NAVOPTS.DAT kann nicht gefunden werden.

Norton AntiVirus kann die Datei mit den Konfigurationseinstellungen nicht finden. Norton AntiVirus wird mit den Standardeinstellungen geladen.

Fehler auf Laufwerk <LAUFWERK>. Laufwerk oder Gerät nicht bereit.

Norton AntiVirus konnte auf das angegebene Laufwerk nicht zugreifen, da die Verriegelung des Laufwerks geöffnet ist oder es ein anderes Problem mit dem Laufwerk gibt.

Der Boot-Virus <VIRUSNAME> wurde auf Laufwerk <LAUFWERK> gefunden.

Ein Virus wurde im Boot-Sektor des angegebenen Laufwerks gefunden. Um den Virus zu entfernen, klicken Sie auf „Reparieren“. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Der Virus <VIRUSNAME> wurde im Speicher gefunden.

Ein Virus wurde im Arbeitsspeicher Ihres Computers gefunden. Das heißt, er ist aktiv und infiziert möglicherweise andere Dateien. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über Viren im Arbeitsspeicher“ auf Seite 40.

Der Boot-Sektor von Laufwerk <LAUFWERK> hat sich seit der Impfung geändert.

Impfänderungen in einem Boot-Sektor weisen meist auf das Vorhandensein eines unbekannten Virus hin. Es gibt aber einige wenige Situationen, in denen eine solche Änderung zulässig ist. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Der Boot-Sektor von Laufwerk <LAUFWERK> ist mit dem Virus <VIRUSNAME> infiziert.

Ein Virus wurde im Boot-Sektor auf dem angegebenen Laufwerk gefunden. Um den Virus zu entfernen, klicken Sie auf „Reparieren“. Weitere Informationen hierzu finden Sie unter„Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Der Boot-Sektor von Laufwerk <LAUFWERK> ist mit dem Virus <VIRUSNAME> infiziert. Kann Boot-Sektoren und Systemdateien nicht impfen.

Ein Virus wurde im Boot-Sektor auf dem angegebenen Laufwerk gefunden. Prüfen Sie das Laufwerk, um den Virus zu finden und zu entfernen, und impfen Sie dann die Boot-Sektoren und Systemdateien. Weitere Informationen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Die Boot-Sektoren und Systemdateien auf Laufwerk <LAUFWERK> wurden nicht geimpft.

Norton AntiVirus ist so konfiguriert, daß es die Boot-Sektoren und Systemdateien auf dem Startlaufwerk auf Impfdaten überprüft. Die genannten Dateien sind nicht geimpft. Weitere Informationen hierzu finden Sie unter „Dateien und Boot-Sektoren neu impfen“ auf Seite 23.

Die Boot-Sektoren und Systemdateien auf Laufwerk <LAUFWERK> wurden seit der Impfung geändert.

Impfänderungen in Boot-Sektoren und Systemdateien weisen mit ziemlicher Sicherheit auf einen unbekannten Virus hin. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Die Datei <DATEINAME> hat sich seit der Impfung geändert.

Die Datei hat sich seit der Impfung geändert. Dies bedeutet nicht zwangsläufig, daß die Datei mit einem Virus infiziert ist. Sie müssen bestimmen, ob die Änderung zulässig ist oder nicht. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Die Datei <DATEINAME> in der komprimierten Datei <DATEINAME> ist mit dem Virus <VIRUSNAME> infiziert.

In einer Datei, die sich in einer komprimierten Datei befindet, wurde ein Virus gefunden. Entkomprimieren Sie die Datei, und prüfen Sie anschließend die Dateien, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Die Datei <DATEINAME> versuchte, das Schreibschutzattribut der Datei <DATEINAME> zu ändern.

Norton AntiVirus ist so eingestellt, daß Sie über diesen Vorgang informiert werden, da er manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44.

Die Datei <DATEINAME> versuchte eine Low-Level-Formatierung der Festplatte.

Norton AntiVirus ist so eingestellt, daß Sie über diesen Vorgang informiert werden, da er manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44.

Die Datei <DATEINAME> versuchte, in Datei <DATEINAME> zu schreiben.

Norton AntiVirus ist so eingestellt, daß Sie über diesen Vorgang informiert werden, da er manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44.

Die Datei <DATEINAME> versuchte, in den Boot-Sektor von Laufwerk <LAUFWERK> zu schreiben.

Norton AntiVirus ist so eingestellt, daß Sie über diesen Vorgang informiert werden, da er manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44.

Die Datei <DATEINAME> versuchte, in den Master-Boot-Sektor der Festplatte zu schreiben.

Norton AntiVirus ist so eingestellt, daß Sie über diesen Vorgang informiert werden, da er manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über virusähnliche Aktivitäten“ auf Seite 44.

Die Datei <DATEINAME> ist mit dem Virus <VIRUSNAME> infiziert.

In der angegebenen Datei wurde ein Virus gefunden. Um den Virus zu entfernen, können Sie die infizierte Datei reparieren oder löschen. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Die Datei <DATEINAME> ist mit dem Virus <VIRUSNAME> infiziert. Die Datei wurde nicht geimpft.

In der Datei, die Norton AntiVirus zu impfen versuchte, wurde ein Virus gefunden. Prüfen Sie die Datei, entfernen Sie den Virus, und impfen Sie die Datei. Weitere Informationen hierzu finden Sie unter „Impfen von Dateien“ auf Seite 21.

Die Datei <DATEINAME> ist nicht geimpft.

Norton AntiVirus überprüft Dateien auf Impfung. Die Datei wurde noch nicht geimpft. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Die Datei <DATEINAME> enthält möglicherweise einen Virus.

Norton AntiVirus hat eine Änderung in der Datei gefunden, die möglicherweise auf einen unbekannten Virus hindeutet. Um den unbekannten Virus zu entfernen, können Sie die infizierte Datei reparieren oder löschen. Bedenken Sie beim Ersetzen der Datei, daß auch die Sicherungskopie mit dem unbekannten Virus infiziert sein kann. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Der Datei <DATEINAME> wurde nicht ermöglicht, das Schreibschutzattribut der Datei <DATEINAME> zu ändern.

Norton AntiVirus ist so konfiguriert, daß es keine Änderungen am Schreibschutz von Dateien zuläßt, da diese Funktion manchmal von Viren ausgeführt wird. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Wenn Sie eine Virusinfektion vermuten, prüfen Sie Ihre Datenträger, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Der Datei <DATEINAME> wurde nicht ermöglicht, die Festplatte zu formatieren.

Norton AntiVirus hat der angegebenen Datei nicht erlaubt, Ihre Festplatte zu formatieren, da diese Funktion manchmal von Viren durchgeführt wird. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Wenn Sie eine Virusinfektion vermuten, prüfen Sie Ihre Datenträger, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Der Datei <DATEINAME> wurde nicht ermöglicht, in den Boot-Sektor von Laufwerk <LAUFWERK> zu schreiben.

Norton AntiVirus hat der angegebenen Datei nicht erlaubt, in den Boot-Sektor des angegebenen Laufwerks zu schreiben, da dieser Vorgang manchmal von Viren verursacht wird. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Wenn Sie eine Virusinfektion vermuten, prüfen Sie Ihre Datenträger, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Der Datei <DATEINAME> wurde nicht ermöglicht, in die Datei <DATEINAME> zu schreiben.

Norton AntiVirus ist so konfiguriert, daß es keine Änderungen an Programmdateien zuläßt, da diese Funktion manchmal von Viren ausgeführt wird. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Wenn Sie eine Virusinfektion vermuten, prüfen Sie Ihre Datenträger, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Der Datei <DATEINAME> wurde nicht ermöglicht, in den Master-Boot-Sektor auf Laufwerk <LAUFWERK> zu schreiben.

Norton AntiVirus ist so konfiguriert, daß es keine Änderungen am Master-Boot-Sektor zuläßt, da diese Funktion manchmal von Viren ausgeführt wird. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Wenn Sie eine Virusinfektion vermuten, prüfen Sie Ihre Datenträger, um den Virus zu finden und zu entfernen. Weitere Informationen hierzu finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Der Master-Boot-Sektor von Laufwerk <LAUFWERK> hat sich seit der Impfung geändert.

Impfänderungen im Master-Boot-Sektor weisen meist auf das Vorhandensein eines unbekannten Virus hin. Es gibt aber einige wenige Situationen, in denen eine solche Änderung zulässig ist. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Der Master-Boot-Sektor von Laufwerk <LAUFWERK> ist mit dem Virus <VIRUSNAME> infiziert.

Ein Virus wurde im Master-Boot-Sektor auf dem angegebenen Laufwerk gefunden. Um den Virus zu entfernen, klicken Sie auf „Reparieren“. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Der Master-Boot-Sektor von Laufwerk <LAUFWERK> ist mit dem Virus <VIRUSNAME> infiziert. Kann Boot-Sektoren und Systemdateien nicht impfen.

Ein Virus wurde im Master-Boot-Sektor auf dem angegebenen Laufwerk gefunden. Prüfen Sie das Laufwerk, um den Virus zu finden und zu entfernen, und impfen Sie dann die Boot-Sektoren und Systemdateien. Weitere Informationen hierzu finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Nicht genügend Speicher für diesen Vorgang.

Ihr Computer hat nicht genügend konventionellen Speicher, um Norton AntiVirus zu laden, da Speicherplatz von speicherresidenten Programmen belegt wird.

Die Systemdatei <DATEINAME> ist mit dem Virus <VIRUSNAME> infiziert. Kann die Boot-Sektoren und Systemdateien nicht impfen.

In der angegebenen Systemdatei wurde ein Virus gefunden. Prüfen Sie das Laufwerk, um den Virus zu finden und zu entfernen, und impfen Sie dann die Boot-Sektoren und Systemdateien. Weitere Informationen hierzu finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Kein Zugriff auf Laufwerk <LAUFWERK>.

Norton AntiVirus konnte auf das angegebene Laufwerk nicht zugreifen, da die Verriegelung des Laufwerks geöffnet ist oder es ein anderes Problem mit dem Laufwerk gibt.

Kann Prüfung nicht abschließen.

Norton AntiVirus hat mehr Probleme gefunden (infizierte Dateien oder Impfänderungen), als es gleichzeitig melden kann. Lösen Sie die gemeldeten Probleme, und führen Sie eine erneute Prüfung durch. Norton AntiVirus meldet alle zusätzlichen gefundenen Probleme. Weitere Informationen zur Lösung der gefundenen Probleme finden Sie unter „Entfernen von Viren, die bei Virusprüfungen entdeckt wurden“ auf Seite 33.

Kann die schreibgeschützte Datei <DATEINAME> nicht löschen.

Die Datei, die Norton AntiVirus versucht zu löschen, ist schreibgeschützt bzw. befindet sich in einem schreibgeschützten Ordner, für den Sie keinen Schreibzugriff haben.

Kann nicht auf die Virusdefinitionsdateien zugreifen.

Die Dateien, die Norton AntiVirus zur Erkennung der bekannten Viren benötigt, können nicht gefunden werden. Sie sollten Norton AntiVirus neu installieren oder aktualisierte Virusdefinitionsdateien anfordern. Weitere Informationen zum Aktualisieren der Virusdefinitionsdateien finden Sie unter „Automatische Aktualisierung der Virusdefinitionen“ auf Seite 53.

Kann die Boot-Sektoren und Systemdateien auf Laufwerk <LAUFWERK> nicht impfen.

Norton AntiVirus kann die Systemdateien und Boot-Sektoren wegen eines Laufwerksfehlers nicht impfen. Auf dem Laufwerk befinden sich kreuzverbundene Dateien, oder es liegt ein Hardware-Problem vor.

Kann die Datei <DATEINAME> nicht impfen.

Die Datei kann aus folgenden Gründen nicht geimpft werden:

- Sie haben keinen Schreib-/Lesezugriff für die Impfdatei bzw. das Verzeichnis.
- Die Datei, die Norton AntiVirus zu impfen versucht, kann nicht gefunden werden. Wenn Sie eine Datei auf einem Netzlaufwerk impfen wollen, kann es vorkommen, daß die Datei in der Zeitspanne, nachdem Sie sie ausgewählt haben und bevor Norton AntiVirus sie impfen konnte, gelöscht wurde.
- Die Datei, die Sie impfen wollen, ist kleiner als 32 Byte.

Der angegebene Ordner kann nicht geimpft werden.

Der angegebene Ordner konnte nicht gefunden werden, oder Sie haben keinen Schreib-/Lesezugriff für die Impfdatei bzw. den Ordner.

Wenn Sie eine Datei auf einem Netzlaufwerk impfen wollen, kann es vorkommen, daß die Datei in der Zeitspanne, nachdem Sie sie ausgewählt haben und bevor Norton AntiVirus sie impfen konnte, gelöscht wurde.

Kann die Datei mit den Systemmeldungen nicht öffnen.

Die Datei mit den Systemmeldungen befindet sich nicht im Ordner von Norton AntiVirus. Installieren Sie Norton AntiVirus neu.

Die angeforderte Information kann nicht gedruckt werden.

Die Daten können nicht gedruckt werden, da der Drucker nicht angeschlossen bzw. eingeschaltet ist.

Kann den Boot-Sektor nicht lesen.

Norton AntiVirus konnte nicht auf den Boot-Sektor zugreifen, um ihn auf Impfung zu überprüfen. Dieses Problem kann auftauchen, wenn Sie ein Programm verwenden, das den Boot-Sektor „verriegelt“ und so verhindert, daß AntiVirus auf ihn zugreift.

Kann den Master-Boot-Sektor nicht lesen.

Norton AntiVirus konnte nicht auf den Master-Boot-Sektor zugreifen, um ihn auf Impfung zu überprüfen. Es handelt sich wahrscheinlich um ein Hardware-Problem. Dieses Problem kann außerdem auftauchen, wenn Sie ein Programm verwenden, das den Boot-Sektor „verriegelt“ und so verhindert, daß AntiVirus auf ihn zugreift.

Kann die Boot-Sektoren und Systemdateien auf Laufwerk <LAUFWERK> nicht neu impfen.

Die Boot-Sektoren und Systemdateien können nicht neu geimpft werden, weil Sie keinen Schreib-/Lesezugriff für die Impfdatei haben. Weitere Informationen zur Position der Impfdatei finden Sie unter „Anpassen der Impfung“ auf Seite 90.

Kann <DATEINAME> nicht reparieren. Die Datei ist weiterhin mit dem Virus <VIRUSNAME> infiziert.

Norton AntiVirus konnte den Virus nicht aus der angegebenen Datei entfernen. Sie können den Virus durch Löschen der infizierten Datei entfernen. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Kann den Boot-Sektor von Laufwerk <LAUFWERK> nicht reparieren.

Norton AntiVirus konnte den Boot-Sektor auf dem angegebenen Laufwerk nicht reparieren. Weitere Informationen hierzu finden Sie in Anhang B unter „Wiederherstellen der Festplatte“.

Kann den Master-Boot-Sektor auf <LAUFWERK> nicht reparieren.

Norton AntiVirus konnte den Master-Boot-Sektor auf dem angegebenen Laufwerk nicht reparieren. Weitere Informationen hierzu finden Sie in Anhang B unter „Wiederherstellen der Festplatte“.

Kann Systemdateien nicht reparieren.

Die Systemdateien auf Ihrem Startlaufwerk konnten nicht repariert werden. Zum Entfernen des Virus und Zurückversetzen der Systemdateien in den Zustand vor dem Virusbefall starten Sie Ihren Computer mit einer schreibgeschützten Startdiskette und geben den DOS-Befehl SYS ein. Der Befehl SYS befindet sich auf Ihrer NAV-Rettungsdiskette.

Kann den Boot-Sektor von Laufwerk <LAUFWERK> nicht mit Impfdaten reparieren.

Norton AntiVirus konnte den Boot-Sektor nicht in seinem ursprünglichen Zustand wiederherstellen. Weitere Informationen hierzu finden Sie in Anhang B unter „Wiederherstellen der Festplatte“.

Kann Datei <DATEINAME> mit Impfdaten nicht reparieren.

Norton AntiVirus konnte die Datei nicht in ihrem ursprünglichen Zustand wiederherstellen. Sie können einen möglichen Virus entfernen, indem Sie die Datei löschen und durch eine nichtinfizierte Sicherungskopie ersetzen. Weitere Informationen hierzu finden Sie unter „Reaktion auf Impfalarme von Auto-Protect“ auf Seite 45.

Kann Datei <DATEINAME> nicht reparieren.

Norton AntiVirus konnte die Datei nicht reparieren. Die Datei ist weiterhin mit einem unbekannten Virus infiziert. Sie können den unbekannten Virus durch Löschen der infizierten Datei entfernen. Weitere Informationen hierzu finden Sie unter „Reaktion auf Warnmeldungen von Auto-Protect über entdeckte Viren“ auf Seite 42.

Kann den Master-Boot-Sektor mit den Impfdaten nicht reparieren.

Norton AntiVirus konnte den Master-Boot-Sektor nicht in seinem ursprünglichen Zustand wiederherstellen. Weitere Informationen hierzu finden Sie in Anhang B unter „Wiederherstellen der Festplatte“.

Kann schreibgeschützten Boot-Sektor von Laufwerk <LAUFWERK> nicht reparieren.

Der Boot-Sektor, den Sie reparieren wollen, befindet sich auf einer schreibgeschützten Diskette. Entfernen Sie den Schreibschutz, und reparieren Sie anschließend den Boot-Sektor.

Kann die Impfung der Datei <DATEINAME> nicht aufheben.

Die Impfung der Datei kann nicht aufgehoben werden, da Sie für die Impfdatei keinen Schreib-/Lesezugriff besitzen. Weitere Informationen zur Position der Impfdatei finden Sie unter „Anpassen der Impfung“ auf Seite 90.

Kann die Protokolldatei nicht aktualisieren.

Die Protokolldatei konnte nicht aktualisiert werden, da Sie keinen Schreib-/Lesezugriff darauf haben.

Kann Exclude-Datei nicht aktualisieren.

Die Datei mit der Ausnahmeliste konnte nicht aktualisiert werden, weil Sie keinen Schreib-/Lesezugriff darauf haben.

Kann die Impfdatenbank nicht aktualisieren.

Die Impfdatei konnte nicht aktualisiert werden, weil Sie keinen Schreib-/Lesezugriff darauf haben.

Kann Impfdatei in schreibgeschütztem Ordner nicht aktualisieren.

Sie haben keinen Schreib-/Lesezugriff für das Verzeichnis, in dem sich die Impfdatei befindet.

A N H A N G

E

Problemlösungen

In diesem Anhang wird beschrieben, wie Sie einige bekannte Probleme, die unter Umständen bei der Arbeit mit Norton AntiVirus auftreten, lösen können. Versuchen Sie, diese Probleme anhand der hier angegebenen Lösungsvorschläge selbst zu beheben, bevor Sie die Technische Unterstützung von Symantec anrufen.

Lösungen für bekannte Probleme

Meine Norton AntiVirus Rettungs- und Startdiskette funktioniert nicht.

Norton AntiVirus kann nicht in jedem Fall automatisch eine startbare Norton AntiVirus Rettungs- und Startdiskette erstellen. Ursache dafür sind produktspezifische Technologien, die von Herstellern für die Konfiguration und die Initialisierung von Festplatten verwendet werden. Wenn Ihre Norton AntiVirus Rettungs- und Startdiskette nicht richtig funktioniert, führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine spezielle Boot- oder Startdiskette für Ihren Computer besitzen, fügen Sie diese dem Norton AntiVirus Rettungsdiskettensatz hinzu. Starten Sie in einem Virusnotfall Ihren Computer zunächst von dieser Diskette. (Achten Sie darauf, daß Sie vor dem Start den Plastikschieber auf der Rückseite der Diskette so einstellen, daß die Diskette schreibgeschützt ist.) Nehmen Sie, nachdem der Systemstart von Diskette beendet ist, die Boot-Diskette aus dem Laufwerk, und legen Sie die Diskette mit der Bezeichnung „Norton AntiVirus Programmdiskette“ ein. Geben Sie anschließend an der DOS-Eingabeaufforderung den Befehl A:GO ein, und drücken Sie die Eingabetaste. Befolgen Sie die Anleitungen, die auf dem Bildschirm angezeigt werden.
- Verwenden Sie den Disk Manager oder ein ähnliches Programm, das mit Ihrem Computer geliefert wurde, um die Norton AntiVirus Rettungs- und Startdiskette startbar zu machen. Vergessen Sie nicht, die modifizierte Rettungs- und Startdiskette zu testen.

Wenn die Norton AntiVirus Rettungs- und Startdiskette nicht richtig funktioniert, so kann dies auch daran liegen, daß auf Ihrem Computer mehrere Betriebs-

systeme installiert sind (z.B. Windows 95 und Windows NT). Gehen Sie in diesem Fall wie folgt vor, um die Rettungs- und Startdiskette zu modifizieren:

- Starten Sie Ihren Computer von der Festplatte. Legen Sie danach die Norton AntiVirus Rettungs- und Startdiskette in Laufwerk A: ein, geben Sie an einer DOS-Eingabeaufforderung den Befehl SYS A: ein, und drücken Sie die Eingabetaste. Dadurch werden die Betriebssystemdaten auf die Diskette kopiert. Vergessen Sie nicht, die modifizierte Rettungs- und Startdiskette zu testen.

Ich habe bei einer Prüfung einen Virus entdeckt und entfernt, aber er infiziert weiterhin meine Dateien.

Ursache: Die Infektionsquelle ist eine Diskette.

Lösung: Prüfen Sie alle Disketten. Anleitungen hierzu finden Sie unter „Durchführen von Virusprüfungen“ auf Seite 15.

Ursache: Der Virus kann sich in einer ausführbaren Datei mit nicht standardmäßiger Dateierweiterung befinden.

Lösung: Ändern Sie im Dialogfeld „Optionen – Scanner“ die Option „Programmdateien“ auf „Alle Dateien“, damit nicht nur Programmdateien überprüft werden. Überprüfen Sie alle Datenträger, die Sie benutzen, und reparieren Sie alle infizierten Dateien. Fügen Sie die Dateierweiterungen aller infizierten Dateien zur Liste der Erweiterungen für Programmdateien hinzu.
Weitere Informationen zum Ändern der Dateiauswahl für Virusprüfungen finden Sie unter „Zu prüfende Dateien wählen“ auf Seite 69 und „Programmdatei-Erweiterungen festlegen“ auf Seite 70.

Ich erhalte bei verschiedenen Anwendungen wiederholt Meldungen über einen gefundenen unbekannten Virus.

Ursache: Sie haben eine Datei mit einem unbekannten Virus auf einen von Ihnen verwendeten Datenträger kopiert. Der unbekannte Virus wird beim Infizieren eines neuen Programms entdeckt, doch die infizierte Originaldatei bleibt unentdeckt.

Lösung: Ändern Sie die Einstellungen für virusähnliche Aktivitäten so, daß Sie beim Auftreten jeglicher Virusaktivitäten gewarnt werden. Auf diese Weise erhalten Sie eine Meldung über eine virusähnliche Aktivität, wenn das Programm mit dem unbekannten Virus versucht, Informationen in eine Programmdatei zu schreiben.
Der Name der Datei mit dem unbekannten Virus wird in der Meldung angezeigt. Diese Datei müssen Sie löschen. Bedenken Sie beim Ersetzen der Datei, daß auch die Sicherungskopie mit dem unbekannten Virus infiziert sein kann.
Weitere Informationen darüber, wie Norton AntiVirus unbekannte Viren entdeckt, finden Sie unter „Schutz vor unbekannten Viren mit Virus-Sensor“ auf Seite 85.

Die automatische Schutzfunktion von Norton AntiVirus wird beim Starten meines Computers nicht geladen.

Ursache: Die Konfigurationseinstellungen für Norton AntiVirus sind falsch.

Lösung: Wie Sie die automatische Schutzfunktion aktivieren, ist unter „Aktivieren und Deaktivieren von Auto-Protect“ auf Seite 18 beschrieben. Informationen darüber, wie Sie den Arbeitsspeicher und die Boot-Sektoren beim Systemstart prüfen lassen, finden Sie unter „Anpassen der Virusprüfung beim Systemstart“ auf Seite 89.

Norton AntiVirus benachrichtigt mich nicht, wenn ich versuche, Vorgänge durchzuführen, die Norton AntiVirus meiner Meinung nach nicht zulassen sollte, wie z.B. das Schreiben in eine Programmdatei.

Ursache: Die Einstellungen für virusähnliche Aktivitäten lassen diesen Vorgang zu.

Lösung: Norton AntiVirus überprüft eine Aktivität nicht, wenn die entsprechende Option auf „Zulassen“ eingestellt ist. Wenn Sie bei dieser Aktivität gewarnt werden möchten, müssen Sie die Einstellung auf „Meldung“ ändern. Weitere Informationen hierzu finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Ursache: Für die entsprechende Aktivität wurde für diese Datei eine Ausnahme festgelegt.

Lösung: Möglicherweise meldet Ihnen Norton AntiVirus die Aktivität nicht, weil sie in der Ausnahmeliste enthalten ist. Das ist der Fall, wenn Sie in einem Warnfeld von Norton AntiVirus, in dem Sie auf eine virusähnliche Aktivität aufmerksam gemacht werden, auf die Schaltfläche „Ausschließen“ geklickt oder diese Aktivität manuell zur Ausnahmeliste hinzugefügt haben. In diesem Fall überprüft Norton AntiVirus diese Aktivität in der betreffenden Datei nicht mehr. Weitere Informationen hierzu finden Sie unter „Verwalten von Ausnahmen“ auf Seite 72.

Ursache: Die Aktivität gehört nicht zu den von Norton AntiVirus überprüften Aktivitäten. Eine Beschreibung der virusähnlichen Aktivitäten finden Sie unter „Überwachung auf virusähnliche Aktivitäten“ auf Seite 87.

Ich erhalte die Aufforderung, Dateien zu impfen, die ich bereits geimpft habe.

Ursache: Eventuell haben Sie den Ordner oder die Datei verschoben oder umbenannt. Die Impfdaten enthalten den Pfadnamen der Datei. Wenn Sie eine Datei verschieben oder umbenennen, werden die Impfdaten ungültig.

Lösung: Impfen Sie die Datei neu. Weitere Informationen hierzu finden Sie unter „Dateien und Boot-Sektoren neu impfen“ auf Seite 23.

Ich erhalte Meldungen über eine Impfänderung für eine oder mehrere Datendateien.

Ursache: Die Erweiterung der Datendateien ist zur Liste der Erweiterungen für Programmdateien hinzugefügt worden, so daß Norton AntiVirus sie beim Impfen berücksichtigt. Datendateien werden häufig geändert und sollten daher nicht geimpft werden.

Lösung: Heben Sie die Impfung aller Dateien mit der entsprechenden Erweiterung auf (Informationen hierzu finden Sie unter „Impfung von Dateien oder Ordnern aufheben“ auf Seite 24.) Löschen Sie anschließend die Erweiterung aus der Liste der Erweiterungen für Programmdateien (Informationen hierzu finden Sie unter „Verwalten von Ausnahmen“ auf Seite 72).

Sie können alle Dateien mit einer bestimmten Erweiterung von der Impfung ausschließen. Informationen dazu finden Sie unter „Verwalten von Ausnahmen“ auf Seite 72.

Nach dem Reparieren eines Programms mit Norton AntiVirus läuft es nicht mehr einwandfrei.

Ursache: Norton AntiVirus entfernt zwar den Virus, doch kann der Virus die Datei bereits so beschädigt haben, daß eine vollständige Reparatur nicht mehr möglich war.

Lösung: Ersetzen Sie das Programm durch ein nichtinfiziertes Originalprogramm.

Seit der Installation einer neuen Version eines Programms erhalte ich Meldungen über Impfänderungen an meinen Programmdateien.

Ursache: Beim Installieren einer neuen Version eines Programms werden viele Dateien durch neue, gleichnamige Dateien ersetzt. Diese Dateien wurden deshalb seit ihrer Impfung rechtmäßig geändert.

Lösung: Impfen Sie die Dateien neu. Weitere Informationen hierzu finden Sie unter „Dateien und Boot-Sektoren neu impfen“ auf Seite 23.

G L O S S A R

Anwendung *Siehe* Programm.

Arbeitsspeicher (RAM) Der Schreib-/Lesespeicher des Computers, von dessen Größe es abhängt, wie viele und wie umfangreiche Programme gleichzeitig ausgeführt werden können bzw. welche Datenmenge sofort verarbeitet werden kann.

Ausführbare Datei Eine Datei, die ein ausführbares Programm enthält. Ausführbare Dateien haben in der Regel die folgenden Erweiterungen: .COM, .EXE, .OVR, .OVL, .DRV, .BIN oder .SYS.

Ausnahme Eine Bedingung oder Aktivität, für die Sie festgelegt haben, daß Norton AntiVirus sie bei bestimmten Dateien ignoriert. Sie können z.B. festlegen, daß Norton AntiVirus das Formatieren einer Diskette durch das DOS-Programm FORMAT ignoriert.

AUTOEXEC.BAT Eine Textdatei mit Befehlen, die beim Starten des Computers automatisch ausgeführt wird. Mit den Befehlen werden der Pfad und die Eingabeaufforderung eingestellt und bestimmte Programme gestartet. *Siehe auch* CONFIG.SYS.

Autostart-Ordner Ein besonderer Ordner im Ordner „Windows\Startmenü\Programme“. Programme in diesem Ordner werden automatisch beim Starten von Windows geladen.

Befehlszeilenschalter Eine Option, die die Ausführung eines Programms steuert. Befehlszeilenschalter werden beim Starten eines Programms an der DOS-Eingabeaufforderung oder über den Befehl „Ausführen“ in Windows eingegeben.

Bekannter Virus Jeder Virus, den Norton AntiVirus erkennen und mit Namen identifizieren kann.

Betriebssystem Das Hauptsteuerprogramm, das in den Hauptspeicher geladen wird, wenn Sie Ihren Computer starten. Es steuert und verwaltet alle Operationen und Programme des Computers.

Booten Den Computer starten.

Boot-Sektor Der erste physikalische Sektor auf einer Diskette oder der erste logische Sektor einer Festplattenpartition. Er enthält Informationen über die Plattenarchitektur (Sektorgröße, Clustergröße usw.). Außerdem enthält er Boot-Sektor-Programme.

Boot-Sektor-Programm Das für das Laden des Betriebssystems zuständige Programm.

Boot-Virus Ein Virus, der das Boot-Sektor-Programm sowohl auf Festplatten als auch auf Disketten und/oder das Master-Boot-Sektor-Programm auf Festplatten infiziert. Ein Boot-Virus wird vor dem Betriebssystem in den Arbeitsspeicher geladen, übernimmt die Steuerung Ihres Computers und infiziert alle Disketten, auf die Sie zugreifen.

Bulletin Board System (BBS) Ein Online-Dienst, der den Austausch von Nachrichten, elektronischer Post und Dateien zwischen Computern mit Hilfe eines Modems ermöglicht.

CMOS Abkürzung für Complimentary Metal Oxide Semiconductor. Ein batteriebetriebener Chip in 80286er (und neueren) Computern, der grundlegende Daten über die System-Hardware speichert.

.COM-Datei *Siehe* Ausführbare Datei.

CONFIG.SYS Eine Textdatei mit Befehlen zum Konfigurieren von DOS und der System-Hardware sowie zum Laden von Gerätetreibern. Die Datei wird beim Starten Ihres Computers automatisch von DOS ausgeführt.

Datei-Server Eine oder mehrere zentrale Speichermedien, die an ein Netzwerk angeschlossen sind und den Netzwerkbenutzern den Zugriff auf gemeinsam genutzte Anwendungen und Datendateien ermöglichen.

Datendatei Eine Datei, die mit einer Anwendung erstellt wird oder mit ihr verknüpft ist und keinen ausführbaren Code enthält. Beispiele sind unter anderem Dateien, die mit Textverarbeitungs-, Datenbank- oder Tabellenkalkulationsprogrammen erstellt werden (.DOC, .DBF, .DAT, .WKS etc.).

Dropper Ein Programm, das einen Virus auf Ihrem Computer installiert. Dropper sind keine Viren, sondern Trojanische Pferde. *Siehe auch* Trojanisches Pferd.

.EXE-Datei *Siehe* Ausführbare Datei.

Gerätetreiber Eine speicherresidentes Programm, das von der Datei CONFIG.SYS bzw. SYSTEM.INI beim Systemstart in den Arbeitsspeicher geladen wird. *Siehe auch* TSR-Programm.

Herunterladen Das Übertragen einer Datei von einem Computersystem auf ein anderes über Modem. Meistens ist das Übertragen einer Datei (über Modem) von einem Datennetzdienst (BBS) gemeint.

Hybridvirus Ein Virus, der sowohl Programmdateien als auch Boot-Sektoren infiziert und sich von dort weiter ausbreitet.

Impfdatei Eine Datei mit Impfdaten zum Überprüfen der Integrität einer Datei. Für jedes Laufwerk, in dem Dateien geimpft werden, wird eine Impfdatei angelegt.

Impfen Das Erstellen von Informationen oder Daten zu einer Datei, mit denen zu einem späteren Zeitpunkt die Integrität der Datei überprüft werden kann.

Impfung aufheben Löschen der Impfdaten einer Datei, eines Ordners oder eines Laufwerks. *Siehe auch* Impfen.

Infizierte Datei Eine Datei, die einen Virus enthält.

Kaltstart Das Starten des Computers durch Einschalten der Netzspannung. Ein Kaltstart setzt den Arbeitsspeicher (RAM) Ihres Computers zurück und entfernt so alle Viren, die sich im Speicher befinden könnten. *Siehe auch* Warmstart.

Komprimierte Datei Eine einzelne Datei, die durch Komprimieren einer oder mehrerer Dateien mit PKZIP oder LHARC angelegt wurde.

Laden *Siehe* Starten.

.LHA-Dateien Mehrere Dateien, die mit LHARC in eine Datei komprimiert wurden (normalerweise mit der Erweiterung .LHA oder .LZN).

.LZN-Datei *Siehe* .LHA-Datei.

Makrovirus Ein Virus, der Dokumentdateien infiziert. Ein Makrovirus wird normalerweise ausgeführt, wenn ein infiziertes Dokument geöffnet, gespeichert oder geschlossen wird. Er breitet sich dann auf andere Dokumente aus. Makros sind kleine Programme, die mit Dokumentdateien verbunden sind und zur Automatisierung von Aufgaben verwendet werden.

Master-Boot-Sektor Der erste physische Sektor einer Festplatte. Er enthält Informationen über die Partitionierung der Festplatte und das Master-Boot-Sektor-Programm.

Master-Boot-Sektor-Programm Dieses Programm veranlaßt den Computer, das Boot-Sektor-Programm von der zum Starten verwendeten Festplatte zu laden.

Netzwerk Eine Reihe von Computern und Peripheriegeräten (Drucker usw.), die zur gemeinsamen Nutzung von Daten, Software und Hardware durch mehrere Benutzer in einer Arbeitsgruppe miteinander verbunden sind.

Neu impfen Das Ersetzen der Impfdaten einer zuvor geimpften Datei durch die Daten der Datei in ihrem aktuellen Zustand.

Neustart Einen Computer ausschalten und neu starten. *Siehe auch* Warmstart bzw. Kaltstart.

Ordner Ein Teil eines Datenträgers, der von Ihnen zum Speichern

bestimmter Dateien eingerichtet wird. Ordner erleichtern Ihnen die Organisation von Dateien auf der Festplatte. Wird auch als Verzeichnis bezeichnet.

Partitionstabelle Eine Tabelle im Master-Boot-Sektor einer Festplatte, welche die Strukturierung der Festplatte festlegt, d.h. die Größe und Position der Partitionen, welches Betriebssystem die verschiedenen Partitionen verwendet und von welcher Partition aus der Computer startet.

Pfadname Der „Weg“ zu einer Datei oder einem Ordner auf einem Datenträger. Wenn zum Beispiel eine Datei mit dem Namen QTR1.DOC im Ordner VERKAUF auf Laufwerk C: gespeichert ist, lautet der Pfadname für die Datei C:\VERKAUF\QTR1.DOC.

Polymorpher Virus Eine Virusart, die ihre typischen Code-Segmente ändert und so bei jeder infizierten Datei anders „aussieht“; auf diese Weise wird die Entdeckung schwieriger.

Programm Eine oder mehrere ausführbare Dateien, mit denen bestimmte Funktionen, z.B. das Anlegen und Bearbeiten von Textdokumenten oder Kalkulationstabellen, ausgeführt werden können.

Programmvirus Ein Virus, der ausführbare Programmdateien befällt, z.B. Dateien mit der Erweiterung .COM, .EXE, .OVL, .DRV (Treiber) und .SYS (Gerätetreiber).

Prüfen Die systematische Suche nach Viren, die von Norton AntiVirus durchgeführt wird.

RAM *Siehe* Arbeitsspeicher.

Registrierung Eine Datenbank, in der Windows 95 Informationen über Hardware- und Softwarekonfigurationen speichert.

Reparieren Das Entfernen eines Virus aus einer Datei und das Zurücksetzen der Datei in ihren ursprünglichen Zustand vor der Infektion (Wiederherstellen).

Schreibgeschützt Eine Diskette oder Datei, die nur gelesen, aber nicht beschrieben oder gelöscht werden kann.

Schreibgeschützte Diskette Eine Diskette, die nicht beschrieben werden kann. Schreibgeschützte Disketten können nicht durch Viren infiziert werden. Um eine 3,5-Zoll-Diskette mit Schreibschutz zu versehen, schieben Sie den Plastikschieber für den Schreibschutz der Diskette nach unten, so daß Sie durch die Öffnung hindurchsehen können.

Shell Ein Programm, das die Schnittstelle zwischen Benutzer und Betriebssystem darstellt. In Windows 95 besteht die Shell aus dem Desktop bzw. der grafischen Benutzeroberfläche.

Speicherresidentes Programm *Siehe* TSR-Programm.

Startdiskette Eine Diskette, die das Betriebssystem enthält, das zum Starten (Booten) des Computers erforderlich ist.

Starten Ein Programm aufrufen oder laden.

Stealth- oder Tarnkappen-Virus Ein Virus, der gezielt versucht, sich der Entdeckung zu entziehen oder sich vor Analyse- und Löschversuchen zu schützen.

Systemdateien Die Dateien, aus denen das Betriebssystem besteht.

Systemdiskette *Siehe* Startdiskette.

Task-Leiste Die Desktop-Komponente, in der Sie auf das Menü „Start“ und gerade geladene Programme zugreifen können. Wenn Auto-Protect und der Norton Scheduler geladen sind, werden die Symbole der beiden Programme in der Leiste angezeigt.

Trojanisches Pferd Ein Programm, das scheinbar nützlich oder interessant ist (z.B. ein Spiel), aber heimlich Dateien in Ihrem Computer zerstört oder löscht, während Sie mit diesem Programm arbeiten. Trojanische Pferde sind keine Viren, da Sie sich nicht vermehren und verbreiten.

TSR *Siehe* TSR-Programm.

TSR-Programm (TSR) Ein Programm, das sich selbst in den Arbeitsspeicher lädt und dort bleibt, so daß es sofort aktiviert werden kann. Ein TSR-Programm wird beim Ausschalten des Computers aus dem Speicher gelöscht.

Unbekannter Virus Ein Virus, für den in Norton AntiVirus keine Virusdefinition vorhanden ist. *Siehe auch* Virusdefinition.

Unterordner Ein Ordner in einem Ordner.

Unterverzeichnis *Siehe* Unterordner.

Verzeichnis *Siehe* Ordner.

Virus Ein sich selbst reproduzierendes Programm, das mit der Absicht geschrieben wurde, den normalen Betrieb Ihres Computers ohne Ihr Wissen oder Ihr Einverständnis zu stören.

Virusähnliche Aktivität

Durch fremde Software hervorgerufener Vorgang oder Ablauf, den Norton AntiVirus als Werk eines möglicherweise unbekannten Virus erkennt.

Virusdefinition

Die Information über einen Virus, anhand derer Norton AntiVirus das Vorhandensein eines bestimmten Virus erkennen und Sie entsprechend warnen kann.

VxD

Ein virtueller Gerätetreiber. Eine Erweiterung des Betriebssystems, die eine Computer-Ressource verwaltet. Auto-Protect ist ein Beispiel für ein VxD.

Warmstart

Das Neustarten des Computers durch Drücken der Tastenkombination Strg+Alt+Entf. Ein Warmstart kann von einigen Viren erkannt und emuliert werden, so daß der Virus nach Abschluß dieses Startvorgangs immer noch im Arbeitsspeicher vorhanden sein kann. *Siehe auch* Kaltstart.

Workstation

Ein Computer, der an ein Netzwerk angeschlossen ist und bei dem es sich nicht um den Netzwerk-Server handelt.

.ZIP-Datei

Mehrere Dateien, die mit dem Programm PKZIP zu einer Datei komprimiert wurden (normalerweise mit der Erweiterung .ZIP).

I N D E X

A

Abwehr von Virusattacken
    Siehe Virusattacken
Aktivieren
    Auto-Protect, xviii
    Prüfung beim Systemstart, xviii
Aktualisieren
    Rettungsdiskettensatz, 27
    Virusdefinitionen, 5, 8, 54–59
Allgemeine Einstellungen (Register), 80
Allgemeine Prüfoptionen, 80
    vor Reparatur Backup-Datei erstellen, 80
America Online
    aktuelle Virusdefinitionen, 57
Anpassen
    allgemeine Prüfoptionen, 80
    Ausnahmeliste, 72
    automatische Schutzfunktion, 81
    Impfung, 91, 92
    Liste der Programmdatei-Erweiterungen, 70
    manuelle Prüfungen, 63–72
    Protokolldatei, 78
    Virusprüfungen beim Systemstart, 89
    Warnmeldungen, 72, 76
Anzeigen
    Ausnahmen, 72
    Programmdatei-Erweiterungen, 70
    Protokolldatei, 25
    Virusliste, 60
Arbeitsspeicher
    Entfernen von Viren, 48
    Prüfen
        beim Systemstart, 89
        jederzeit, 64
    Reaktion auf Warnmeldungen über Viren, 48
Ausgeschalteter Computer
    Viren entfernen, 107
Auslöser eines Virus, 99
Ausnahmeliste, 72
    Einträge bearbeiten, 75
    Einträge hinzufügen
        Ausschließen (Schaltfläche), 38
    Einträge manuell hinzufügen, 73
Ausnahmeliste (Register), 72
Ausnahmen
    Entfernen und Ändern, 72–75
Ausschließen von Dateien
    Prüfung auf bekannte Viren, 67, 84
Automatische Schutzfunktion
    Anpassen, 81
        Diskettenoptionen, 88
        Optionen für virusähnliche Aktivitäten, 87
        Prüfoptionen für Dateien, 81
        Prüfung auf unbekannte Viren, 85
        Umgehungstasten beim Systemstart, 90
    beim Systemstart umgehen, 20
    Laden, 19
        funktioniert nicht, 129
Auto-Protect
    Aktivieren, xviii
    auf Warnmeldungen reagieren, 38–45
    Beschreibung, 7
    TSR
        Laden, 19
        Neu laden, 19
Auto-Protect (Register), 82
Auto-Protect-Viruserkennungstechnologie, 6

B

Backup-Dateien
    nach der Reparatur löschen, 43
    vor der Reparatur erstellen, 80
Bearbeiten
    Ausnahmeliste, 75

geplante Virusprüfungen, 32
Befehle
Anpassen…
allgemein, 80
Ausnahmeliste, 72
Auto-Protect, 82
Impfung, 91, 92
manuelle Prüfung, 63, 65
Protokolldatei, 78
Warnmeldungen, 76
Datei…, 17
Impfung…, 21
Ordner…, 17
Protokolldatei…, 25
Scheduler…, 28
Virusliste…, 60
Befehlszeilenschalter, 111
NAVDX.EXE, 111
DOS-Fehlerebenen, 113
NAVW32.EXE, 114
RESCUE.EXE, 116
Bekannte Viren, 5
Ermittlungsbericht anzeigen, 26
Liste anzeigen, 60
Prüfung anpassen, 63, 81
Schutz vor, 63–68
Siehe auch Unbekannte Viren; Viren
Berichte, 25
Boot-Sektoren
automatische Impfung, 8
Impfung, 23, 91
Impfung aufheben, 24
Infektion reparieren, 42
Neuimpfung, 23
Reparatur fehlgeschlagen, 50
Virusprüfung, 64
beim Systemstart, 89
Boot-Viren, 89
Beschreibung, 101
Disketten beim Systemstart prüfen, 89
Entfernen, 42
Impfung, 91
Liste anzeigen, 61
Prüfoptionen, 64
Verbreitungsart, 101
Bulletin Board System (BBS)
heruntergeladene Dateien
prüfen, 15, 82

C

CompuServe
aktuelle Virusdefinitionen, 57
Computer herunterfahren
Einstellungen bei Ermittlung eines Virus, 66
Konfiguration, 84
Computer vor Viren schützen, 1
Computervirus (Definition), 2

D

Datei… (Befehl), 17
Dateien
Änderungen, 45
auf Viren überwachen, 81
einzelne prüfen, xvii
für die Prüfung auswählen, 69
Impfung aufheben, 24
Neuimpfung, 23
Viren entfernen, 49–51
Virusprüfung, 17
alle Dateien, 65, 83
nur Programmdateien, 65
Programmdateien, 83
von der Befehlszeile aus prüfen, 111
von Prüfungen ausnehmen, 73
vor Reparatur Backup-Kopien erstellen, 80
Zugriff verweigern, 83
Dateien ausschließen
Ermittlung bekannter Viren, 74
Ermittlung unbekannter Viren, 74
Ermittlung virusähnlicher Aktivitäten, 74–75
Impfdatenermittlung, 74
Impfung, 46
Überwachung virusähnlicher Aktivitäten, 45

Dateien und Boot-Sektoren neu impfen, 23
Deinstallation, xv
Direkthilfe (Befehl im Menü „Hilfe“), 14
Disketten
    auf Viren prüfen, 15
    Überwachung auf Viren, 88
Dokumentkonventionen *Siehe* Konventionen
DOS-Fehlerebenen
    NAVDX.EXE, 113
Dropper, 134
Drucken
    Berichte, 25
    Protokolldatei, 25
    Virusliste, 61

E

Entdecken von Viren
    Auto-Protect, 33
    während einer Prüfung, 33
Entfernen von Viren
    aus Arbeitsspeicher, 41, 48
    aus Boot-Sektoren, 42–43, 49
    aus Dateien, 42–43, 49
    aus komprimierten Dateien, 51
    aus Master-Boot-Sektor, 42–43, 49
    aus Speicher, 40
    von ausgeschaltetem Computer, 107
Ereignis hinzufügen (Dialogfeld), 29, 30
Erstellen
    Rettungsdiskettensatz, 27

F

Festplatte
    auf Viren überwachen, 81
    beim Systemstart auf Viren überwachen, 89
    Wiederherstellen nach einer Virusinfektion, 108
Filter für Protokolldatei (Dialogfeld), 26

G

Gefundene Probleme (Dialogfeld), 36
Gelöschte Dateien wiederherstellen
    Warnung, 42
Geplante Prüfung
    Beschreibung, 7

H

Hauptfenster von Norton AntiVirus für Windows, xvii
Hilfe
    Direkthilfe (Befehl im Menü „Hilfe“), 14
    Hilfethemen (Befehl im Menü „Hilfe“), 14
    kontextsensitiv, 14–15
    während Installation, xiii
    Wie kann ich (Befehl im Menü „Hilfe“), 14
Hilfethemen (Befehl im Menü „Hilfe“), 14
Hybridviren
    Beschreibung, 106

I

Impfung
    Änderungen
        Bericht anzeigen, 26
        Reaktion, 47
    Anpassen, 91
    Aufheben, 24
    Beschreibung, 8, 21
    Boot-Sektoren und Systemdateien, 91
    Dateien
        auf Disketten, 92
        automatisch, 92
        im Netzwerk, 93
        Pfad, 93
    Reaktion auf Warnmeldungen, 45–47
Impfung (Dialogfeld), 22
Impfung (Register), 91, 92
Impfung… (Befehl), 21

Infizierte Boot-Sektoren
automatisch reparieren, 66
nach der Reparatur, 42
Reparatur fehlgeschlagen, 50
Reparieren, 42
Infizierte Dateien
automatisch löschen, 66, 86
automatisch reparieren, 66
Liste anzeigen, 25
Löschen, 43
nach dem Löschen, 43
nach der Reparatur, 42
Reaktion individuell festlegen, 66, 83
Reparatur fehlgeschlagen, 50
Reparieren, 42
vorher Backup-Datei erstellen, 80
Infizierte Dateien und Boot-Sektoren
Viren entfernen, 49–51
Infizierung
Siehe Virusbefall
Installation
Norton AntiVirus *Siehe* Installationskarte
Installieren von Norton AntiVirus, xi–xiv
Deinstallation, xv
Fragen, xiii
Systemanforderungen, xi
Virusentfernung während Installation, xii
Internet
aktuelle Virusdefinitionen, 57

K

Kennwort
Ändern, 95
Kennwort (Register), 94
Kennwort festlegen (Dialogfeld), 95
Kennwortschutz
Einrichten, 94–95
Entfernen, 95
individuell, 94
maximal, 94
Komprimierte Dateien
Prüfen, 64
Viren entfernen, 51
Konventionen für das Handbuch, ix

L

Laden
automatische Schutzfunktion, 19
Scheduler mit Windows, 31
Ladung eines Virus, 99
Laufwerke
beim Starten prüfen, 68
Netzlaufwerke prüfen, 68
Prüfen, 16
Laufwerke vor der Prüfung auswählen, 68
LiveUpdate, 54
Löschen
Ausnahmen, 75
Dateien
automatisch, 66
mit Impfänderungen, 47
geplante Virusprüfungen, 32
infizierte Dateien, 43
automatisch, 83, 86
Liste gelöschter Dateien anzeigen, 25
Programmdatei-Erweiterungen, 71
Protokolldateieinträge, 25
Schaltfläche nicht verfügbar, 43
Warnung, 42

M

Makroviren, 3
Beschreibung, 102
Liste anzeigen, 61
Manuelle Prüfungen
Anpassen, 63
Beschreibung, 6
Master-Boot-Sektor
Impfung, 23, 91
Impfung aufheben, 24
Neuimpfung, 23

Reparatur fehlgeschlagen, 50
Reparieren, 42
Virusprüfung, 64
beim Systemstart, 89
Meldungen, 117

N

Netzlaufwerke
Hinweise zur Virusprüfung, 68
Prüfung zulassen, 68
Netzwerkwarnmeldungen
Optionen für Warnmeldungen festlegen, 77
Senden an Norton AntiVirus für NetWare NLM, 77
Neue Ausnahme (Dialogfeld), 74
Norton AntiVirus
Beenden, 13
Deinstallieren, xv
Installation *Siehe* Installationskarte
Installieren, xi–xiv
Starten, xvii, 12
Starten und Beenden, 12
Norton Program Scheduler (Windows-Menü „Start"), Befehl, 55

O

Optionen (Menü), 72
Anpassen… (Befehl)
allgemein, 80
Ausnahmeliste, 72
Auto-Protect, 82, 83, 85, 87, 88
Impfung, 91, 92
manuelle Prüfung, 63, 65
Protokolldatei, 78
Optionen für Virus-Sensor (Auto-Protect) (Dialogfeld), 85
Ordner
Impfung aufheben, 24
Neu impfen, 23
Virusprüfung, 17
von Prüfungen ausschließen, 74
Ordner… (Befehl), 17

P

Polymorphe Viren
Beschreibung, 104
Liste anzeigen, 61
Probleme und Lösungen, 127
Programmdatei-Erweiterungen, 69
Angeben für Prüfungen, 70–71
Anzeigen, 70
Löschen, 71
Wiederherstellen der Liste, 71
Programmdatei-Erweiterungen (Dialogfeld), 70
Programmviren
Beschreibung, 100
Entfernen, 42
Liste anzeigen, 60
Verbreitungsart, 100
Protokolldatei
Anpassen, 78
Anzeigen, 25
Drucken, 25
Einträge löschen, 25
Optionen, 78
Pfad, 79
Protokolldatei (Dialogfeld), 25
Protokolldatei (Register), 78
Protokolldatei… (Befehl), 25
Prüfen (Menü)
Datei… (Befehl), 17
Ordner… (Befehl), 17
Prüfung beim Systemstart
Aktivieren, xviii
Anpassen, 89–90
Entfernen von Viren, 47–51
Info über, 7

R

Reaktion auf Warnmeldungen, 42–44
Reparaturassistent, 9, 34
Datei löschen, 35
Entfernen von Viren, die bei der Prüfung entdeckt wurden, 33–36

Viren automatisch entfernen, 33
Viren manuell entfernen, 33
Reparieren
Dateien mit Impfänderungen, 47
infizierte Dateien und Boot-Sektoren, 42
automatisch, 66, 83, 86
Reparatur fehlgeschlagen, 50, 131
Schaltfläche nicht verfügbar, 42
Viren
Boot-Sektoren, 42–43, 49
Dateien, 42–43, 49
Master-Boot-Sektor, 42–43, 49
vorher Backup-Dateien erstellen, 80
Reparieren von Dateien und Boot-Sektoren
als Reaktion auf Warnmeldungen, 49
Rettungs- und Startdiskette
testen, xiv
Rettungsdiskettensatz
Aktualisieren, 23
Erstellen, 27
Festplatte wiederherstellen, 108
Viren von ausgeschaltetem Computer entfernen, 107

S

Schaltflächen in Warnfeldern, 36–38
Scheduler, 28, 29
Deaktivieren, 28
Virusprüfungen
Bearbeiten, 32
Löschen, 32
Planen, 29
Scheduler (Dialogfeld), 29
Scheduler… (Befehl), 28
Schließen
Scheduler, 28
Schreibgeschützte Diskette
Definition, 136
zur Virusvermeidung, 12
Schreibschutz für Disketten, xiv
Sicherungskopien, 12
Signalton aktivieren, 76
Sofortige Benachrichtigung bei Virusinfektion, 36
Speicher
Viren entfernen, 40
Starten von Norton AntiVirus, xvii
Stealth-Viren
Beschreibung, 104
Liste anzeigen, 61
Stellvertreterviren
Beschreibung, 105
Symantec BBS
aktuelle Virusdefinitionen, 56
Systemanforderungen
Mindestanforderungen, xi
Systemdateien
Impfung, 23, 91
Impfung aufheben, 24
Neuimpfung, 23
Reparatur fehlgeschlagen, 50
Virusprüfung beim Systemstart, 89
Wiederherstellen, 50
Systemmeldungen, 117
Systemstart (Dialogfeld), 89

T

Tarnkappen-Viren
Beschreibung, 104
Tools (Menü)
Impfung… (Befehl), 22
Scheduler… (Befehl), 28
Virusliste… (Befehl), 60
Trojanisches Pferd, 137
TSR-Programm, 137

U

Überwachung auf Viren
auf Disketten, 88
beim Systemstart, 89
Virusprüfungen planen, 28
während der Laufzeit, 81

Umgehen von Prüfungen beim Systemstart, 20
Unbekannte Viren
Definition, 5
Entfernen, 42
Ermittlungsbericht anzeigen, 26
Überwachung, 85
Unterordner
Prüfen, 17
mit Befehlszeilenschalter, 112
von Prüfungen ausschließen, 74

V

Viren
aus Speicher entfernen, 40
Auslöser, 99
automatisch entfernen
Reparaturassistent, 33–36
Beschreibung, 61, 98
Dateien impfen, 21
Entdecken, 33
Entfernen, 40–42
Anpassen, 65
Schaltflächen, 36
von ausgeschaltetem Computer, 107
Entfernen aus Arbeitsspeicher, 48
Entfernen während der Prüfung, 33–36
fehlgeschlagene Reparatur
Boot-Sektor, 50
infizierte Datei, 50
im Arbeitsspeicher, 48–??
Ladung, 99
Lebenszyklus, 3–??, 3–4
Liste anzeigen, 60
Löschen infizierter Dateien, 42–43
Quellen, 4
Reaktion anpassen, 65
Reaktion auf Warnmeldungen, 36–38
Reparieren von infizierten Boot-Sektoren, 42
Reparieren von infizierten Dateien, 42
Schutz vor
bekannten Viren, 81–84
unbekannten Viren, 85–88, 90–93
Verbreitungsmechanismen, 4
Vermeiden, 11
Ziele, 100
Virusähnliche Aktivitäten
Bericht anzeigen, 26
Reaktion auf Warnmeldungen, 44–45
Überwachung, 87
Virusbefall
Behandlung, Übersicht, 4
Mechanismen, 4
Quellen von Viren, 4
Virusdefinitionen
Aktualisieren, 53–59
manuell, 56
Bezugsquellen, 56
CompuServe, 57
Internet, 57
monatliche Aktualisierungen, 58
Symantec BBS, 56
Virusdefinitionsdatei
Aktualisieren, 57
Gründe für die Aktualisierung, 8
Virusentfernung
während Installation, xii
Viruserkennung, Verfahren, 4
Virusliste
Aktualisieren, 53
Siehe auch Virusdefinitionsdatei, Aktualisieren
Anzeigen, 60
Bericht über Änderungen, 26
Drucken, 61
Virusname suchen, 61
Virusliste (Dialogfeld), 60
Virusliste… (Befehl), 60
Virusprüfung
Alle Dateien vs. Nur Programmdateien, 65, 69
Anpassen, 63–68, 89

Anzeigen
Berichte überprüfen, 25
beim Systemstart, 89
Dateien ausschließen, 72
Disketten, 88
im Arbeitsspeicher, 64
in Boot-Sektoren, 64
in komprimierten Dateien, 64
in Ordnern, 17
Planen, 28, 29
Prüfung stoppen, 68
von der Befehlszeile aus, 111
Virussignaturen, 5, 8

W

Warnfelder
Anzeige auf dem Bildschirm, 35
Schaltflächen, 36–38
Warnmeldung
Beschreibungen, 10
Warnmeldungen
Anpassen, 76
auslösende Situationen, 38, 47
Auto-Protect, 38, 47
Meldung hinzufügen, 76
Reaktion
Impfalarm, 46
Impfänderungen, 47
Methoden zum Entfernen von Viren, 49–51
Schnellanleitung, 36–38
virusähnliche Aktivitäten, 44
Virusalarm, 40–42
Schaltflächen, 44
Senden über Novell NetWare-Netzwerke, 77
Signalton aktivieren, 76
sofortige Benachrichtigung, 68
Viren im Arbeitsspeicher, 48–??
Warnmeldungen (Register), 76, 77
Warnungen
Prüfung beim Systemstart, 7
Weitere Optionen für Auto-Protect (Dialogfeld), 87
Weitere Optionen für Scanner (Dialogfeld), 67
Wiederherstellen
Festplatte, 108
Systemdateien, 50

Z

Zugriff auf Dateien verweigern, 83

Kundendienst und technische Unterstützung

Symantec bietet Ihnen weltweit exzellenten Kundendienst. Unsere professionellen Mitarbeiter helfen Ihnen gerne bei allen Fragen zur Symantec-Software.

Registrierung Ihrer Software

Um Ihr Symantec-Produkt zu registrieren, füllen Sie bitte die beigefügte Registrierkarte aus und senden sie an Symantec zurück.

Ihre neue Anschrift können Sie unserem Kundendienst telefonisch, per Post oder per Fax mitteilen. Anschriften und Rufnummern finden Sie weiter hinten in diesem Abschnitt.

Technische Unterstützung

Wenn Sie Fragen zu einem speziellen Programm der Produktlinie haben, wenden Sie sich an die Mitarbeiter der Technischen Unterstützung. Die entsprechenden Telefonnummern finden Sie weiter hinten in diesem Abschnitt. Außerhalb des deutschsprachigen Raums wenden Sie sich bitte an das zuständige Symantec-Büro oder an Ihren Symantec-Händler.

StandardCare-Unterstützung

Alle registrierten Benutzer von Symantec-Produkten sind berechtigt, folgende kostenlose Dienste in Anspruch zu nehmen:

- Unbegrenzte Anzahl von Anrufen innerhalb von 90 Tagen (ab dem ersten Anruf), um Fragen zur Installation, Konfiguration und allgemeinen Benutzung zu klären.
- Unbegrenzte technische Unterstützung über CompuServe und America Online. Diese Foren bieten elektronischen Zugang zu unseren Mitarbeitern von der technischen Unterstützung, Bibliotheken mit Beispieldateien und technische Dokumente. Hier können Sie auch mit anderen Benutzern von Symantec-Software Informationen austauschen.

- Unbegrenzten Zugriff auf das Bulletin Board System (BBS) von Symantec. Dieses BBS, das auch die Möglichkeit zum Herunterladen von Dateien bietet, wird ständig mit Beispieldaten und technischen Hinweisen zu den verschiedenen Produkten für den schnellen und einfachen elektronischen Zugriff aktualisiert.
- Unbegrenzten Zugriff auf Firmeninformationen über Internet. Mit einem Internet-Browser wie z. B. Cyberjack, Mosaic, Cello oder Netscape erhalten Sie die neuesten Informationen, wenn Sie die Internet-Adresse von Symantec eingeben:

  `http://www.symantec.com.`
- Unbegrenzte Benutzung des automatischen Fax-Abruf-Systems von Symantec, um per Fax einen schnellen Zugriff auf technische Hinweise, Bulletins, Produktliteratur und allgemeinen Informationen zu erhalten.
- StandardCare-Unterstützung können Sie von Montag bis Freitag von 9 bis 17 Uhr (MEZ) in Anspruch nehmen.

Elektronische Unterstützung

Technische Informationen sind rund um die Uhr auf elektronischen Bulletin Board Systemen verfügbar. Symantec bietet Ihnen Zugriff auf sein eigenes Symantec Bulletin Board System (BBS) und unterhält die Symantec-Foren auf CompuServe.

World Wide Web und FTP-Server

Der Internet-Anschluß von Symantec bietet Ihnen unbegrenzten Zugriff auf Produktinformationen. Besuchen Sie die Symantec Web-Seite unter folgender Adresse:

`http://www.symantec.com`

Oder verwenden Sie den FTP-Server, um technische Hinweise und Software-Patches direkt herunterzuladen:

`ftp.symantec.com`

CompuServe

Symantec unterhält das Symantec-Forum auf CompuServe. Hier können Sie Daten und Anregungen mit Angestellten von Symantec und anderen Benutzern von Symantec-Produkten austauschen. Wenden Sie sich an CompuServe, um Auskunft über die Einstellungen für den Datenaustausch zu erhalten.

Sie rufen das Symantec-Forum auf CompuServe auf, indem Sie „GO“ wählen und dann SYMEUR eingeben. Auskünfte zum Einrichten eines CompuServe-Kontos erhalten Sie bei CompuServe GmbH, Jahnstr. 2, 82002 Unterhaching, Deutschland, Tel.: 0130/4643. Wenn Sie nicht von Deutschland aus anrufen, wählen Sie bitte die Nummer 0049/89/665500.

Symantec BBS

Das Symantec Bulletin Board System (BBS) bietet ein Kundendienstforum, Shareware- und Public Domain-Software, "FAQ - Frequently Asked Questions" (oft gestellte Fragen) und Unterstützungsforen, in denen Sie Tips und Informationen mit anderen Endbenutzern austauschen können. Für das Symantec BBS gelten folgende Einstellungen: 8 Datenbits, 1 Stoppbit; keine Parität.

Modems von 300 bis 14400 Baud	+31 71 5353169
Modems von 300 bis 28800 Baud	+ 31 71 5322852
Virendefinitionsdateien können Sie unter der folgenden Nummer herunterladen:	+ 31 71 5353 292

Automatisches Fax-Abruf-System

Das automatische Fax-Abruf-System von Symantec kann rund um die Uhr benutzt werden, um Produktinformationen mit Hilfe Ihres Faxgerätes zu erhalten. Sie können von jedem Telefon aus anrufen, das die Möglichkeit bietet, auf Tonwahl umzuschalten, um ein Inhaltsverzeichnis der verfügbaren Dokumente zum Kundendienst und zur technischen Unterstützung zu erhalten, um sich dann eines dieser Dokumente zufaxen zu lassen.

Um technische Anwendungshinweise und Beispiele zu "Wie kann ich..." zu erhalten, rufen Sie unsere Fax-Abruf-Nummer der technischen Unterstützung an.

Um allgemeine Produktinformationen, Datenblätter und Bestellformulare für Produktaktualisierungen zu erhalten, wählen Sie die Fax-Abruf-Nummer unseres Kundendienstes.

Fax-Abruf-Nummer (Technische Unterstützung)	+31 (71) 5353 255
Fax-Abruf-Nummer (Kundendienst)	+49 (211) 676 115

Unterstützung für alte Versionen

Sobald eine neue Version der Software auf den Markt kommt, erhalten alle unsere registrierten Benutzer eine Information zum Upgrade. Telefonische Unterstützung ist für die Vorgängerversion noch sechs Monate nach dem Erscheinen der neuen Version erhältlich. Technische Informationen sind eventuell noch über die elektronische Unterstützung und das Fax-Abruf-System zu erhalten.

Unterstützung für nicht mehr hergestellte Produkte

Sobald Symantec bekanntgibt, daß ein Produkt nicht weiter hergestellt wird, wird die telefonische Unterstützung 60 Tage danach eingestellt. Nur über das Fax-Abruf-System oder Dokumentation der elektronische Unterstützung, wie das Symantec BBS, CompuServe oder das World Wide Web, können Sie noch weitere Unterstützung erhalten.

Symantec behält sich das Recht vor, die vorliegenden Informationen ohne vorherige Ankündigung zu ändern.

Bitte beachten Sie auch die beigefügte Karte, die Ihnen einen Überblick über sämtliche Symantec-Kontakte und die dazugehörigen Telefonnummern gibt.