Norton Personal Firewall™ für Macintosh Benutzerhandbuch

Norton
Personal Firewall™
für Macintosh

20% Minimum

07-30-00437-GE

Norton Personal Firewall™ für Macintosh Benutzerhandbuch

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

Copyright

Dokumentation Version 1.0

PN: 07-30-00437

Marken

Gedruckt in Irland.

10 9 8 7 6 5 4 3 2 1

I N H A L T S V E R Z E I C H N I S

Verwendung einer Firewall

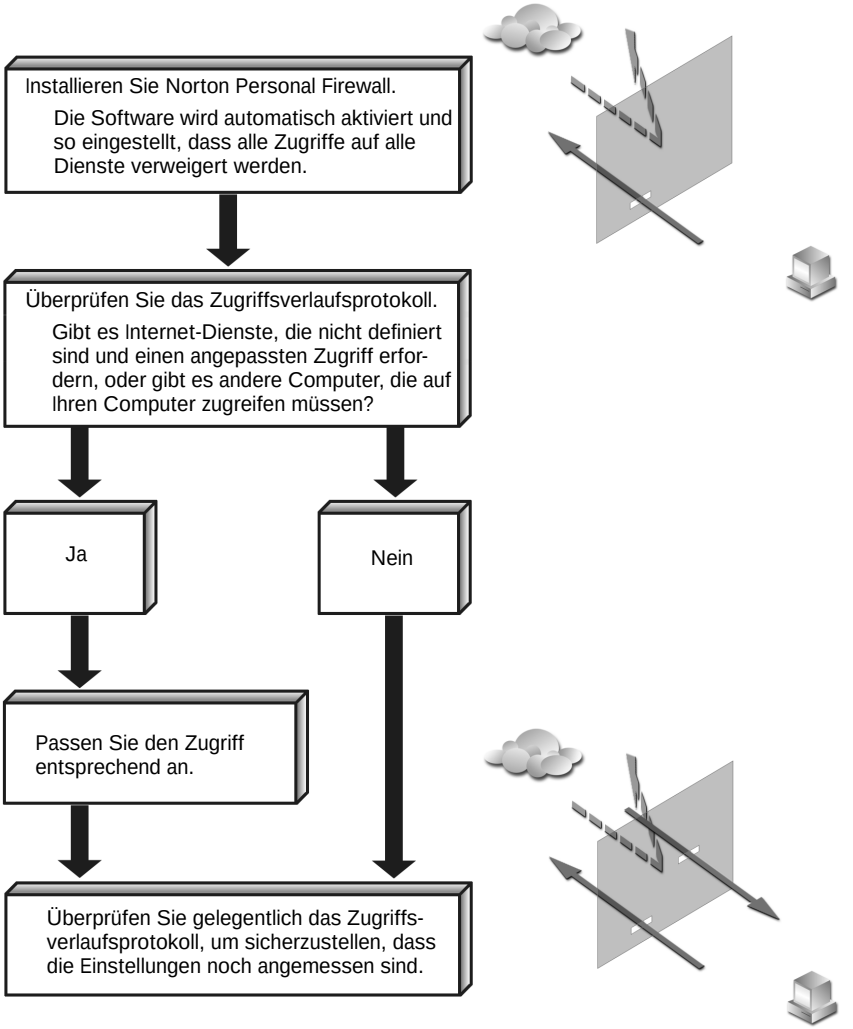
Anhang A Programmdateien aktualisieren

Glossar

Index

Symantec-Lösungen für Service und Unterstützung

Verwendung einer Firewall



K A P I T E L 1

Norton Personal Firewall

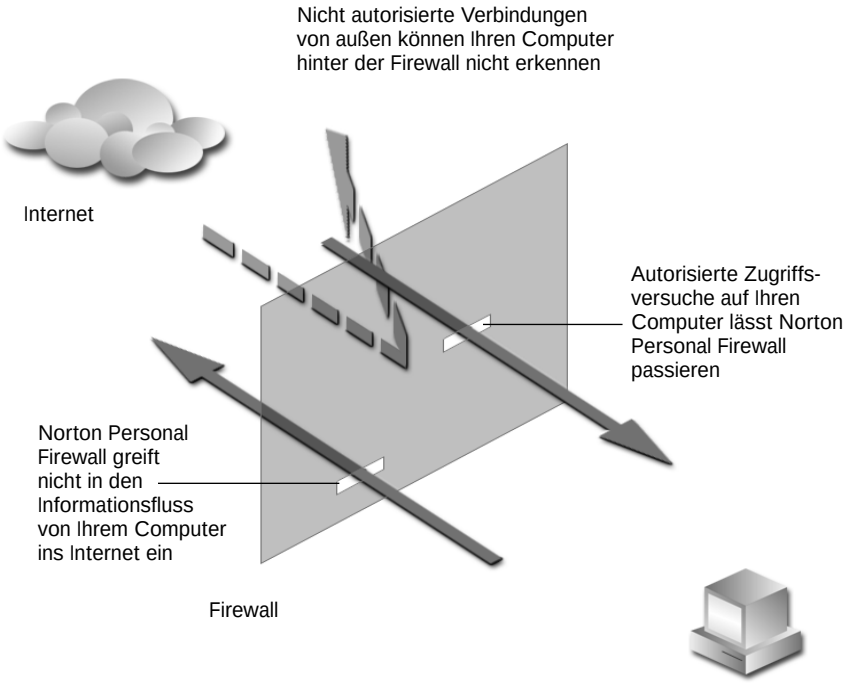
Millionen von Computern sind mit dem Internet verbunden, und ihre Zahl wächst täglich. Indem Sie eine Verbindung zum Internet herstellen, stellen Sie Verbindungen zu Millionen anderer Computern her. Diese Computer können umgekehrt aber auch Verbindungen zu Ihrem Computer herstellen. Ungeschützte Verbindungen zum Internet machen Ihren Computer anfällig für Angriffe durch *Hacker*, *Viren*, *Trojanische Pferde* und viele andere Gefahren aus dem Internet. (Hacker sind Personen, die ohne Ihr Wissen und Ihre Zustimmung in Ihren Computer eindringen. Viren und Trojanische Pferde sind Programme, die die Daten auf Ihrem Computer korrumpieren können.)

Mit Norton Personal Firewall können Sie die Verbindungen zu Ihrem Computer überwachen und steuern. Die Software hilft Ihnen, die Sicherheit und die Integrität Ihrer privaten Daten zu wahren.

Funktionsweise von Norton Personal Firewall

Norton Personal Firewall stellt eine als *Firewall* bezeichnete Barriere zwischen Ihrem Computer und dem Internet dar. Firewall-Programme sind Filter, die bestimmte Verbindungen über das Internet blockieren oder zulassen. Durch das Filtern von Verbindungen schützt die Firewall Ihren Computer vor bösartigen Aktivitäten aus dem Internet.

Norton Personal Firewall verwendet Zugriffseinstellungen für die Entscheidung darüber, ob eine bestimmte Verbindung abgeblockt werden muss oder zugelassen werden kann. Da Sie diese Einstellungen ändern können, können Sie entscheiden, welchen anderen Computern der Zugriff auf Ihren Computern erlaubt werden soll und welchen nicht.



Sie können angeben, welche Dienste (beispielsweise Web Sharing oder File Sharing) geschützt werden sollen und beim Zugriff von welchen Computern der Schutz greifen soll. Sie können den Zugriff auf einen bestimmten Dienst ebenso zulassen oder verweigern, wie Sie den Zugriff auf einen Dienst von bestimmten Computern zulassen oder verweigern können. Sie können zum Beispiel jeglichen Zugriff auf den Dienst ‚File Sharing' verweigern, während Sie gleichzeitig Computern von Personen, die Sie kennen, den Zugriff auf den Dienst ‚Web Sharing' erlauben.

Identifizieren zugriffsberechtigter Computer

In den meisten Fällen muss niemand auf Ihren Computer zugreifen können. Für bestimmte Computerkonfigurationen und Umgebungen, in denen über die Dienste ‚Web Sharing' und ‚File Sharing' Daten ausgetauscht werden sollen, ist es aber erforderlich, den Zugriff zuzulassen. Beispiele:

- Von zwei oder mehr Computern in einem Netzwerk hat mindestens ein Computer einen Zugang zum Internet. In diesem Fall muss auf jedem Computer mit Internet-Zugang eine Kopie von Norton Personal Firewall installiert und so konfiguriert werden, dass nur die übrigen Computer im Netzwerk auf den Internet-Computer zugreifen können.
- Sie haben eine persönliche Website auf Ihrem Computer (zum Beispiel mit Familienfotos), und Sie wollen den Zugriff darauf beschränken. Mit Norton Personal Firewall können Sie über den Dienst ‚Web Sharing' die Personen bestimmen (z. B. die Mitglieder Ihrer Familie), die die Möglichkeit haben sollen, Ihre Website zu besuchen.
- Wenn Sie einen freien ISP (Internet Service Provider) verwenden, wird für den Zugriff und die Aufrechterhaltung der Verbindung möglicherweise ein bestimmter Port auf Ihrem Computer benötigt. Wenn Sie dem ISP diesen Zugriff verwehren, geht die Verbindung verloren.

Bei der Installation wird Norton Personal Firewall so eingestellt, das alle Zugriffsversuche verweigert werden. Im Fenster mit dem Zugriffsverlaufsprotokoll können Sie jederzeit überprüfen, ob jemandem der Zugriff verweigert wurde, der eigentlich die Möglichkeit haben sollte, auf Ihren Computer zuzugreifen.

Weitere Informationen über das Fenster „Zugriffsverlauf" finden Sie im Abschnitt „Auf Zugriffsversuche reagieren" auf Seite 32.

Gefahren bei der Arbeit ohne Firewall

Solange Sie mit dem Internet oder einem Netzwerk verbunden sind, können andere Computer, die ebenfalls mit diesem Netzwerk verbunden sind, auf Ihren Computer zugreifen. Diese Situation ist besonders gefahrenträchtig, wenn Sie den Dienst ‚File Sharing' oder ‚Programmverbindungen' aktiviert haben. Die Gefahr geht dabei von Personen aus, die Hacker genannt werden.

Für Programmierer ist ein Hacker zunächst nur eine Person, die Spaß daran hat, Computer und ihre Möglichkeiten bis ins kleinste Detail zu erforschen; der Begriff ‚Hacker' ist also keineswegs negativ gemeint. Hacker mit bösartigen Absichten werden von Programmierern als *Cracker* bezeichnet. Bei Personen, die mit der Sicherheit von Computern befasst sind, wird der Begriff ‚Cracker' wiederum auf Leute angewendet, die Codes knacken, und das nicht notwendigerweise aus böser Absicht. Da im allgemeinen Sprachgebrauch aber der Begriff ‚Hacker' als Bezeichnung für jemanden verwendet wird, der in Computer mit dem Ziel eindringt, Schaden anzurichten, wird auch in diesem Handbuch der Begriff in dieser Bedeutung verwendet.

Hacker dringen aus den verschiedensten Gründen in Computer anderer Leute ein:

- Sie wollen in den Besitz von Informationen kommen, die sie zu Ihrem Nutzen oder Vorteil verwerten können.
- Sie wollen Daten zerstören oder die Funktionsweise eines Computers auf andere Weise stören.
- Sie wollen einfach beweisen, dass sie dazu in der Lage sind.

Es gibt ebenso viele Motive für das Hacken, wie es Hacker gibt. Die Vermutung, dass Sie und Ihr Computer sicher sind, nur weil Sie unbekannt und anonym sind, ist falsch. Hackern geht es nicht notwendigerweise darum, in wessen Computer sie eindringen. Sie suchen nur nach einem Computer, der nicht geschützt ist.

K A P I T E L 2

Installieren von Norton Personal Firewall

Norton Personal Firewall bietet einen umfassenden Schutz Ihres Macintosh Computers vor Zugriffsversuchen von außen. Die Software überwacht alle Internet-Verbindungen von und zu Ihrem Computer, protokolliert alle Zugriffsversuche und benachrichtigt Sie bei einem Zugriffsversuch.

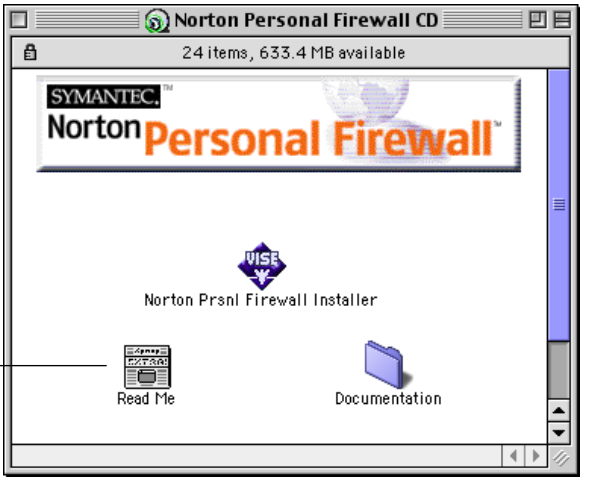
Systemanforderungen

Für die Arbeit mit Norton Personal Firewall muss Ihr Computer die folgenden Mindestanforderungen erfüllen:

- Macintosh Power PC-Prozessor
- CD-ROM-Laufwerk
- 24 MB RAM
- 2 MB freier Festplattenspeicher
- Internet-Verbindung
- Macintosh OS 8.1 oder höher (8.5 oder höher für Kontrollleistenfunktionalität)
- Open Transport 1.3 oder höher

Info über Ihre CD-ROM Norton Personal Firewall für Macintosh

Installieren Sie Ihre Software von der CD-ROM Norton Personal Firewall für Macintosh.



Außer dem Installationsprogramm für Norton Personal Firewall für Macintosh enthält die CD-ROM die folgenden Objekte:

- Liesmich-Datei: Diese Datei enthält die neuesten Informationen, Tipps zur Fehlersuche, Installationsanleitungen und den standardmäßigen Ablageort aller für Norton Personal Firewall installierten Dateien.
- Anwendung SimpleText: Mit dieser Anwendung können Sie die Liesmich-Datei lesen.
- Ordner „Dokumentation“: Dieser Ordner enthält das *Norton Personal Firewall Benutzerhandbuch* im PDF-Format sowie die Installationsdateien für Adobe Acrobat Reader.

Norton Personal Firewall für Macintosh installieren

Die Liesmich-Datei auf der CD-ROM enthält neueste Informationen und Tipps zur Behebung von Fehlern, die bei der Installation auftreten können.

So können Sie die Datei lesen:

- Legen Sie die CD-ROM in das CD-ROM-Laufwerk ein und doppelklicken Sie auf die **Liesmich-Datei**.

Installieren Sie, nachdem Sie die Liesmich-Datei gelesen haben, die Software Norton Personal Firewall.

Wenn Sie Norton Personal Firewall im gleichen Ablageort wie Ihre Kopie der DoorStop Firewall von Open Door installieren, werden zwar die DoorStop Dateien gelöscht; die Einstellungen für DoorStop werden in Norton Personal Firewall aber beibehalten.

So installieren Sie Norton Personal Firewall für Macintosh:

1. Legen Sie die CD-ROM Norton Personal Firewall für Macintosh in das CD-ROM-Laufwerk ein.

   Wenn das Fenster für die CD-ROM nicht automatisch geöffnet wird, doppelklicken Sie auf das **CD-ROM**-Symbol, um die CD-ROM zu öffnen.
2. Doppelklicken Sie im Fenster der CD-ROM auf das Symbol „Norton Prsnl Firewall Aktualisierer“.
3. Folgen Sie den Anweisungen in den nun angezeigten Informationsbildschirmen.

   Wenn Sie im Fenster mit der Lizenz- und Garantievereinbarung auf „Ablehnen“ klicken, wird der Installationsvorgang abgebrochen.
4. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie „Einfache Installation“, um die komplette Software zu installieren.
   - Wenn Sie nur bestimmte Komponenten installieren wollen, klicken Sie auf „Manuelle Installation“ und wählen Sie die gewünschten Komponenten aus.
5. Übernehmen Sie das angezeigte Zielvolume oder geben Sie den Ordner an, in dem die Software installiert werden soll.
6. Klicken Sie auf „Installieren“.

7 Befolgen Sie die Anleitungen auf dem Bildschirm, bis die Installation beendet ist, und klicken Sie danach auf „Neustart“.

Wenn Sie nach der Installation von Norton Personal Firewall Ihren Computer erstmals starten, wird das Programm Norton Personal Firewall gestartet und der Statusbereich des Fensters „Setup“ angezeigt, um zu bestätigen, dass die Firewall aktiviert wurde. Beenden Sie das Programm, um das Fenster vom Bildschirm zu löschen. Die Firewall bleibt trotzdem aktiviert.

Wenn Sie nach dem Neustart Probleme beim Auswerfen der CD-ROM haben, versuchen Sie eine der folgenden Möglichkeiten:

- Drücken Sie auf die Auswerftaste des CD-ROM-Laufwerks, wenn Sie den Startton Ihres Macintosh hören.
- Drücken Sie bei neueren Macintosh Computern mit CD-ROM-Laufwerken ohne Schublade während des Systemstarts die Maustaste, um die CD-ROM auszuwerfen.

Nachdem Sie Norton Personal Firewall installiert haben, ist Ihr Computer bis zum Neustart vor jeglichen Zugriffsversuchen geschützt. Die Systemerweiterung für Norton Personal Firewall wird bei jedem Start Ihres Computers geladen und schützt Ihr System aktiv und zuverlässig, solange Sie sie nicht deaktivieren.

Zusätzliche Informationsquellen

Die Anwendung Norton Personal Firewall hat eine kontextsensitive Hilfefunktion.

So starten Sie die Hilfefunktion:

- Klicken Sie in einem beliebigen Fenster von Norton Personal Firewall auf „Hilfe“.

Der Hilfetext wird daraufhin in Ihrem Web-Browser angezeigt.

Das *Norton Personal Firewall Benutzerhandbuch* ist als PDF-Datei auf der CD-ROM verfügbar und kann mit Adobe Acrobat gedruckt werden. Sofern noch nicht geschehen, kann auch Adobe Acrobat Reader auf Ihrem Computer installiert werden.

Hinweis: Die Liesmich-Datei auf der CD-ROM Norton Personal Firewall for Macintosh enthält Informationen, die zum Zeitpunkt der Veröffentlichung dieses Benutzerhandbuchs noch nicht verfügbar waren. Lesen Sie diese Informationen, bevor Sie fortfahren.

Norton Personal Firewall für Macintosh registrieren

Über Ihre Internet-Verbindung können Sie Norton Personal Firewall für Macintosh über das *Internet* (das weltweite Computernetzwerk) registrieren.

Wenn Sie Macintosh OS 8.5 oder höher verwenden, können Sie über ein Symbol im Ordner „Norton Personal Firewall für Macintosh“ Ihren Browser starten und die Verbindung zur Website von Symantec herstellen, auf der Sie Ihr Produkt registrieren können. Wenn Sie eine frühere Mac OS Version verwenden, gehen Sie mit Ihrem Browser zur Symantec Website.

So registrieren Sie Ihre Software über das Internet:

1 Stellen Sie die Verbindung zum Internet her.

Wenn Sie America Online (AOL) für die Verbindung zum Internet verwenden, finden Sie weitere Informationen im Abschnitt „So registrieren Sie Ihre Software mit AOL:“ auf Seite 19.

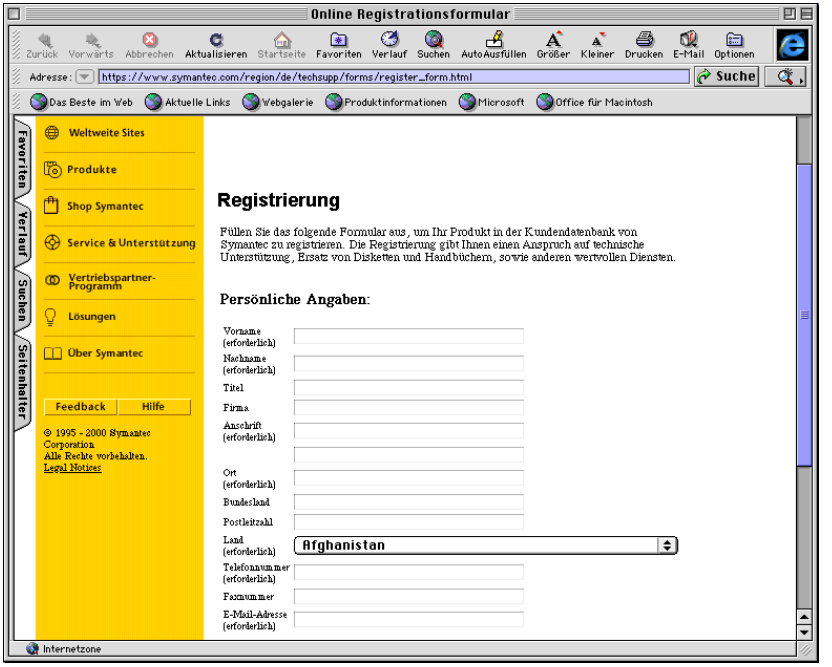
2 Doppelklicken Sie im Ordner „Norton Personal Firewall für Macintosh“ auf „Registrieren Sie Ihre Software“.

In Ihrem Internet-Standardbrowser wird daraufhin die für die Registrierung verwendete Symantec Website „Online Registrationsformular“ angezeigt.

3 Wenn Sie Macintosh OS 8.1 verwenden, starten Sie Ihren Browser und gehen Sie zu folgender Website von Symantec:

www.symantec.com/region/de/techsupp/forms/register_form.html

4 Geben Sie auf dem angezeigten Registrationsformular alle erforderlichen Angaben ein.



5 Klicken Sie auf „Registrierung abschicken“.

Neueste Informationen lesen

Norton Personal Firewall für Macintosh installiert eine Verbindung zur Symantec WebSite mit neuesten Informationen. Verwenden Sie diese Verbindung, um aktuelle Informationen über die von Ihnen installierte Software abzurufen.

So lesen Sie die neuesten Informationen:

1 Stellen Sie die Verbindung zum Internet her.

Wenn Sie America Online (AOL) für die Verbindung zum Internet verwenden, finden Sie weitere Informationen im Abschnitt „So lesen Sie die neuesten Informationen mit AOL:“ auf Seite 19.

2 Doppelklicken Sie im Ordner „Norton Personal Firewall für Macintosh“ auf „Neueste Informationen“.

In Ihrem Internet-Browser wird daraufhin die Website von Symantec mit den neuesten Informationen für Ihr Produkt angezeigt.

3 Wenn Sie Macintosh OS 8.1 verwenden, starten Sie Ihren Browser und gehen Sie zu folgender Website von Symantec:

http://www.symantec.com/product/home-mac.html

Mit America Online eine Verbindung zur Website von Symantec herstellen

Wenn Sie America Online (AOL) als Internet Service Provider (ISP) verwenden, müssen Sie zunächst die Verbindung zu AOL herstellen, damit Sie Ihre Software bei Symantec registrieren oder die neuesten Informationen für Ihr Produkt anzeigen können.

So registrieren Sie Ihre Software mit AOL:

1 Melden Sie sich bei AOL an.

2 Klicken Sie auf der Begrüßungsseite von AOL auf den AOL Internet-Browser.

3 Verschieben Sie das Fenster des AOL-Browsers und andere offene AOL-Fenster zur Seite.

4 Doppelklicken Sie im Fenster „Norton Personal Firewall“ auf „Registrieren Sie Ihre Software“.

5 Geben Sie auf dem angezeigten Registrationsformular alle erforderlichen Angaben ein.

6 Klicken Sie auf „Registrierung abschicken“.

7 Trennen Sie die Verbindung zu AOL.

So lesen Sie die neuesten Informationen mit AOL:

1 Melden Sie sich bei AOL an.

2 Klicken Sie auf der Begrüßungsseite von AOL auf den AOL Internet-Browser.

3 Verschieben Sie das Fenster des AOL-Browsers und andere offene AOL-Fenster zur Seite.

4 Doppelklicken Sie im Ordner „Norton Personal Firewall für Macintosh“ auf „Neueste Informationen“.

In Ihrem Internet-Browser wird daraufhin die Website von Symantec mit den neuesten Informationen für Ihr Produkt angezeigt.

5 Trennen Sie die Verbindung zu AOL, nachdem Sie die neuesten Informationen gelesen haben.

Norton Personal Firewall deinstallieren

Sie benötigen die CD-ROM Norton Personal Firewall für Macintosh, um Norton Personal Firewall von Ihrem System zu deinstallieren.

So deinstallieren Sie Norton Personal Firewall:

1 Legen Sie die CD-ROM Norton Personal Firewall für Macintosh in das CD-ROM-Laufwerk ein.

Wenn das Fenster für die CD-ROM nicht automatisch geöffnet wird, doppelklicken Sie auf das **CD-ROM**-Symbol, um die CD-ROM zu öffnen.

2 Doppelklicken Sie im Fenster der CD-ROM auf das Symbol „Norton Prsnl Firewall Aktualisierer“.

3 Blättern Sie durch Klicken in den verschiedenen Informationsbildschirm bis zum Bildschirm mit den Installationsoptionen.

4 Wählen Sie „Deinstallieren“ in der Liste der Installationsoptionen.

5 Wählen Sie den Ordner, aus dem Norton Personal Firewall deinstalliert werden soll.

6 Klicken Sie auf „Deinstallieren“.

KAPITEL 3

Zugriffsschutz für Volumes, Dateien und Daten

Norton Personal Firewall schützt Ihren Computer vor Verbindungen auf der Basis der Zugriffseinstellungen, die Sie festlegen. Sie können den Zugriff für bestimmte Computer freigeben, die Sie über ihre IP-Adressen auswählen, und Sie können zusätzliche Dienste wählen, die auf Ihrem Computer geschützt werden sollen. Norton Personal Firewall verfolgt alle Zugriffsversuche und steuert in Verbindung mit AppleTalk den Zugriff. Sie können Norton Personal Firewall bei Bedarf jederzeit deaktivieren und wieder aktivieren.

Schutzfunktion von Norton Personal Firewall

Norton Personal Firewall schützt Ihren Computer vor externen Zugriffen über *TCP/IP* (Transmission Control Protocol/Internet Protocol) und (optional) über *UDP* (User Datagram Protocol). Das bedeutet für Sie, dass ohne Ihre Zustimmung kein Computer auf Dateien, Programme oder andere Informationen auf Ihrem Computer zugreifen kann, solange Sie mit dem Internet oder einem anderen Netzwerk verbunden sind. Die entsprechende Berechtigung erteilen Sie für einen Computer, nicht für eine bestimmte Person; das heißt, dass jeder Benutzer des zugriffsberechtigten Computers auf Ihren Computer zugreifen kann.

Sie können Norton Personal Firewall nicht dazu verwenden, Informationen, die nach außen gehen, zu steuern und zu kontrollieren. Sie können die Software zum Beispiel weder dazu verwenden, den Zugriff auf dubiose Websites zu verhindern, noch dazu, pesönliche Informationen wie eine Kreditkartennummer zu verschlüsseln, die Sie an eine andere Website übermitteln. Die Software blockiert auch keine direkten *AppleTalk* Verbindungen; (AppleTalk ist ein Macintosh spezifisches Kommunikationsprotokoll).

Weitere Informationen über das Zusammenwirken von Norton Personal Firewall und AppleTalk finden Sie im Abschnitt „Norton Personal Firewall und AppleTalk“ auf Seite 23.

Zugriffssteuerung per IP-Adressen

Wenn Sie den Zugriff für bestimmte Computer zulassen oder verweigern wollen, müssen Sie die Computer nach ihren Internet Protocol-Adressen (kurz IP-Adressen) auflisten; (*Protokolle* sind Regelwerke für die Datenübertragung). *IP-Adressen* setzen sich aus vier Zahlen zwischen 0 und 255 zusammen, die durch Punkte getrennt werden (z. B.: 216.35.137.202). Jeder Computer im Internet hat eine IP-Adresse, die ihn eindeutig identifiziert.

Sie kennen einen Computer aber möglicherweise nicht unter seiner IP-Adresse, sondern unter seinem *Hostnamen*. Ein Hostname ist eine Name, der einen Computer in einem Netzwerk identifiziert. Der Hostname der Website von Symantec lautet beispielsweise ‚www.symantec.com‘. Hostnamen werden durch das *Domain Name System (DNS)* in die entsprechenden IP-Adressen umgesetzt. In Norton Personal Firewall können Sie den Hostnamen eines Computers eingeben, um seine IP-Adresse zu ermitteln.

Sie können einzelne IP-Adressen, einen Bereich von IP-Adressen ab einem bestimmten Wert oder einen Bereich wählen, der einem bestimmten *Teilnetz* (oder Subnet) entspricht. Ein Teilnetz ist ein lokales Netzwerk, das Bestandteil eines größeren Intranet oder des Internet ist.

Schutzes für Ports einrichten

Sie können die Liste der IP-Adressen verwenden, um für jeden Dienst auf Ihrem Computer festzulegen, ob der Zugriff jeweils erlaubt sein soll oder nicht. Die gebräuchlichsten Dienste sind bereits im Fenster „Setup“ vordefiniert. Für Dienste, die nicht aufgelistet sind, können Sie einen Listeneintrag erstellen, indem Sie den Namen des Diensts und die Nummer des verwendeten Ports eingeben.

Internet-Dienste kommunizieren über solche Ports, wobei jeder Dienst einen spezifischen Port verwendet. So wird zum Beispiel für Web Sharing normalerweise der Port mit der Nummer 80 und für File Sharing über TCP/IP der Port mit der Nummer 548 verwendet. Für bestimmte Dienste stehen mehrere Ports als Alternativen zur Verfügung. Werden zum Beispiel zwei *Webserver* (Systeme, die Web-Inhalte an Ihren Browser übermitteln) auf demselben Computer ausgeführt, können Sie nicht denselben Port verwenden; für einen der beiden Server würde in diesem Fall ein alternativer Port verwendet. Die Portnummer ist ein geeignetes Mittel, um die Schutzfunktion für Dienste zu aktivieren, für die der Schutz durch Norton Personal Firewall nicht vordefiniert wird, und für Dienste, die einen alternativen Port verwenden.

Sie können die Schutzfunktion auch für Dienste definieren, die UDP-Ports verwenden. Allerdings sollten nur Personen von dieser Möglichkeit Gebrauch machen, die Erfahrung mit Internet-Protokollen haben, da die Funktionsweise eines Computers im Internet beeinträchtigt werden kann, wenn der Zugriff auf die falschen UDP-Ports verweigert wird.

Zugriffsversuche verfolgen

Norton Personal Firewall protokolliert alle Informationen über versuchte Zugriffe auf Ihren Computer. Sie können bestimmen, ob alle verweigerten Zugriffe und/oder alle zugelassenen Zugriffe protokolliert werden sollen und ob Sie bei einem verweigerten und/oder zugelassenen Zugriffsversuch unmittelbar benachrichtigt werden wollen.

Norton Personal Firewall und AppleTalk

Auf einem Macintosh Computer werden im Wesentlichen zwei Netzwerkprotokolle verwendet: AppleTalk und TCP/IP. Dabei wird AppleTalk in der Regel für lokale, d. h. nicht über das Internet verfügbare Dienste verwendet, zum Beispiel zum Drucken, zum Austausch von Dateien zwischen Computern im gleichen Netzwerk und für firmenspezifische Anwendungsprogramme. TCP/IP unterstützt dagegen die globalen, weltweiten Dienste wie Internet-Dienste, E-Mail und Zugriffe auf Websites. Bei Macintosh OS 9 stellt TCP/IP darüber hinaus Dienste bereit, die traditionell über AppleTalk verfügbar waren, z. B. File Sharing und Programmverbindungen über das Internet oder ein Intranet.

Benutzer und Benutzergruppen

Die Datei „Benutzer & Gruppen“ ist die wichtigste, für die Sicherheit im Netzwerk relevante Komponente, die in das Macintosh Betriebssystem integriert ist. Mit der Datei „Benutzer & Gruppen“ (auf die Sie über das Kontrollfeld „Benutzer & Gruppen“ und bei Macintosh OS 9 über das Kontrollfeld „File Sharing“ zugreifen) können Sie als Eigentümer eines Computers Benutzerkonten und Kennwörter für den Zugriff auf die integrierten Netzwerkdienste des Computers einrichten und festlegen, welche Konten Zugriff auf welche Dienste haben sollen. Benutzerkonten werden eingesetzt, um den Zugriff auf diese Dienste über TCP/IP bzw. AppleTalk zu beschränken. Der Zugriff als Gast (d. h. als Benutzer ohne Kennwort) kann ebenfalls eingerichtet werden. Zu den Diensten, die mit der Datei „Benutzer & Gruppen“ geschützt werden können, gehören ‚Programmverbindungen‘, ‚File Sharing‘, ‚Web Sharing‘ und ‚Remote Access‘; (mit letzterem können Benutzer einen bestimmten Computer anwählen). Die Zugriffe auf diese Dienste werden meist über das entsprechende Kontrollfeld konfiguriert.

TCP/IP-Schutz von Norton Personal Firewall

Norton Personal Firewall aktiviert einen bestimmten Schutzgrad für jede Anwendung, die das Protokoll TCP verwendet, indem der Zugriff nur für bestimmte, per IP-Adressen ausgewählte Computer im Internet ermöglicht wird. Dieser Schutz ist somit unabhängig von Kennwörtern, wie sie für die Schutzfunktion mit der Datei „Benutzer & Gruppen“ nötig sind. Wenn Sie zum Beispiel File Sharing über TCP/IP aktivieren, genügt ein in der Datei „Benutzer & Gruppen“ definiertes Kennwort allein nicht, damit der betreffende Benutzer auf Ihren Computer zugreifen kann. Zusätzlich müssen Sie in Norton Personal Firewall festlegen, dass der Computer der betreffenden Person auf den Dienst ‚File Sharing‘ zugreifen darf. Sie können in Norton Personal Firewall jeglichen Zugriff zulassen und sich ganz auf die Schutzfunktion der Datei „Benutzer & Gruppen“ verlassen, oder Sie können den Zugriff nur für bestimmte IP-Adressen zulassen, so dass für den File-Sharing-Zugriff zwei sicherheitsrelevante Merkmale überprüft werden.

AppleTalk und das Internet

Beim Starten von Norton Personal Firewall wird eine Warnmeldung angezeigt, wenn AppleTalk auf Ihrem Computer denselben Port wie die Internet-Verbindung verwendet. Wenn beide Verbindungstypen denselben Port verwenden, kann dies dazu führen, dass der Zugriff auf Ihren Computer aus dem Internet möglich ist. Wenn diese Warnung angezeigt wird, sollten Sie einen der folgenden Schritte ausführen:

- Deaktivieren Sie in der Datei „Benutzer & Gruppen“ die Möglichkeit, als Gast auf Ihren Computer zuzugreifen.
- Deaktivieren Sie AppleTalk, solange Sie mit dem Internet verbunden sind, da Norton Personal Firewall keinen Schutz für AppleTalk Verbindungen bietet.
- Wenn Sie Timbuktu oder ein anderes Produkt verwenden, das den Computer-zu-Computer-Zugriff über AppleTalk oder über TCP/IP unterstützt, ist es möglicherweise ratsam, die AppleTalk Funktionalität zu deaktivieren, da sie von Norton Personal Firewall nicht geschützt wird.

Firewall-Schutz aktivieren und deaktivieren

Bei der Installation wird Norton Personal Firewall so konfiguriert, dass alle Zugriffe auf TCP/IP-Dienste verweigert werden. Für die meisten Benutzer bieten diese Einstellungen den Schutz, den sie benötigen, ohne dass ihre Arbeit mit dem Computer in irgendeiner Form beeinflusst wird. Außer in dem Fall, dass Sie bestimmte Zugriffsregeln festlegen wollen, müssen Sie daher nach der Installation von Norton Personal Firewall keine Änderungen an den Einstellungen vornehmen.

Sie können den Schutz jederzeit stoppen, indem Sie Norton Personal Firewall deaktivieren. Sie können Norton Personal Firewall beispielsweise für die Arbeit mit *FTP* (File Transfer Protocol) vorübergehend deaktivieren. Sie können den Schutz für eine bestimmte Zeit aussetzen oder stoppen, bis Sie ihn wieder manuell starten.

Sie können Norton Personal Firewall an zwei Stellen deaktivieren (bzw. wieder aktivieren): im Fenster „Setup“ oder mit der Kontrollleiste (bei Macintosh OS 8.5 oder höher).

So aktivieren bzw. deaktivieren Sie Norton Personal Firewall im Fenster „Setup“:

1 Starten Sie Norton Personal Firewall durch Doppelklicken auf das Programmsymbol „Norton Personal Firewall“.

2 Wählen Sie „Schutz deaktivieren“.

Ist Norton Personal Firewall bereits deaktiviert, erscheint die Option „Schutz aktivieren“, mit der Sie den Schutz durch Norton Personal Firewall wieder aktivieren können.

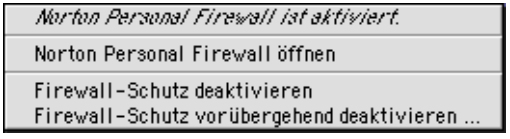
3 Sie müssen bestätigen, dass Sie Norton Personal Firewall deaktivieren wollen.

4 Schließen Sie die Anwendung Norton Personal Firewall.

So aktivieren bzw. deaktivieren Sie Norton Personal Firewall mit der Kontrollleiste:

1 Klicken Sie in der Kontrollleiste auf das Modul von Norton Personal Firewall, um das zugehörige Menü zu öffnen.

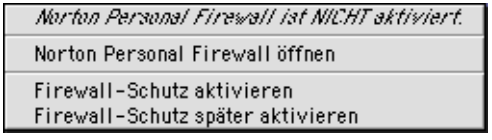
In der obersten Zeile des Menüs wird daraufhin der aktuelle Status von Norton Personal Firewall angezeigt.



2 Klicken Sie auf „Firewall-Schutz deaktivieren“, um den Schutz auszuschalten.

Ist Norton Personal Firewall bereits deaktiviert, erscheint die Option „Firewall-Schutz aktivieren“.

3 Sie müssen bestätigen, dass Sie Norton Personal Firewall deaktivieren wollen.



Sie können das Kontrollleistenmenü auch verwenden, um Norton Personal Firewall zu starten und den Schutz für eine bestimmte Zeitdauer auszusetzen oder zu stoppen, bis Sie ihn wieder manuell aktivieren.

So erreichen Sie, dass Norton Personal Firewall deaktiviert und nach einer bestimmten Zeitdauer automatisch wieder aktiviert wird:

1 Klicken Sie in der Kontrollleiste auf das Modul von Norton Personal Firewall, um das zugehörige Menü zu öffnen.

2 Wählen Sie „Firewall-Schutz vorübergehend deaktivieren“ bzw. „Firewall-Schutz später aktivieren“.

3 Geben Sie die Anzahl der Minuten ein, nach denen Norton Personal Firewall gestartet werden soll.

4 Klicken Sie auf „OK“.

Basismodus und erweiterter Modus

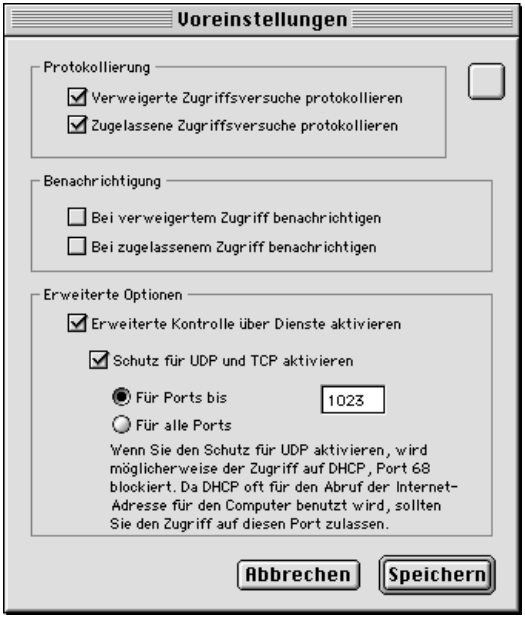
Norton Personal Firewall hat zwei Betriebsmodi: den Basismodus und den erweiterten Modus. Im Basismodus werden die Zugriffseinstellungen für die gebräuchlichsten Dienste definiert. Norton Personal Firewall ist so konfiguriert, dass standardmäßig der Basismodus verwendet wird.

Den erweiterten Modus benötigen Sie, wenn Sie:

- die Zugriffseinstellungen für einen Dienst definieren wollen, der noch nicht in der Liste der Dienste von Norton Personal Firewall enthalten ist,
- für die Liste der IP-Adressen ein von Ihrem eigenen Teilnetz abweichendes Teilnetz angeben wollen,
- die Schutzfunktion auf UDP-Ports ausweiten wollen,
- weitere Informationen über Zugriffsversuche anzeigen wollen.

So wechseln Sie in den erweiterten Modus:

1 Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.



2 Aktivieren Sie die Option „Erweiterte Kontrolle über Dienste aktivieren“.

3 Klicken Sie auf „Speichern“.

K A P I T E L 4

Reaktionen auf Zugriffsversuche

Es lässt sich nicht immer auf Anhieb erkennen, ob Norton Personal Firewall aktiv ist: Sie können Ihren Computer wie gewohnt verwenden, ohne dass Sie eine Veränderung bemerken. Und genau so soll es auch sein. Die Firewall ist aktiviert und blockt alle ungewollten Zugriffe ab.

Norton Personal Firewall protokolliert alle Zugriffsversuche unabhängig davon, ob sie abgewiesen oder zugelassen wurden. Anhand dieses Protokolls können Sie prüfen, ob Norton Personal Firewall korrekt funktioniert.

Firewall-Aktivitäten überwachen

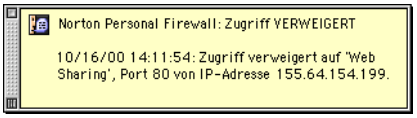
Bei der Installation wird Norton Personal Firewall so konfiguriert, dass verweigerte und zugelassene Zugriffsversuche protokolliert werden. Diese Versuche werden im Fenster „Zugriffsverlauf“ angezeigt, das Sie jederzeit ansehen können.

In bestimmten Situation ist es ratsam, wenn Sie sich bei einem Zugriffsversuch unmittelbar benachrichtigen lassen. Sie sollten zum Beispiel nach dem Installieren von Norton Personal Firewall sofort alle Zugriffsversuche auswerten, um sicherzustellen, dass Norton Personal Firewall funktioniert. Die sofortige Benachrichtigung ist auch ratsam, wenn Sie Einstellungen geändert haben und sicherstellen wollen, dass sie zum gewünschten Ergebnis führen.

Zur Überprüfung der Schutzeinstellungen und eventueller Änderungen an diesen Einstellungen bietet Norton Personal Firewall eine Selbsttestfunktion. Beim Selbsttest werden eine TCP-Verbindung simuliert, ein Zugriffsversuch protokolliert und eine Benachrichtigung an Sie gesendet, sofern Sie diese Option aktiviert haben.

Benachrichtigung bei Zugriffsversuchen

Sie können entscheiden, ob Sie nur bei abgewiesenen oder nur bei zugelassenen Versuchen oder bei Zugriffsversuchen beider Kategorien benachrichtigt werden wollen. Wenn Sie die Option für die Benachrichtigung aktivieren, wird eine Warnung angezeigt, sobald ein Zugriff der jeweiligen Kategorie protokolliert wird.



Beschreibungen möglicher Reaktionen auf eine solche Warnung finden Sie im Abschnitt „Info über Warnmeldungen“ auf Seite 33.

Das Protokollieren der Zugriffsversuche erfolgt unabhängig davon, ob Sie sich für oder gegen die Benachrichtigung entscheiden. Umgekehrt hat das Deaktivieren der Protokollfunktion keine Auswirkung auf die Benachrichtigung; allerdings ist die Benachrichtigung in diesem Fall Ihre einzige Informationsquelle für einen Zugriffsversuch.

So aktivieren bzw. deaktivieren Sie die Benachrichtigung bei einem Zugriffsversuch:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.
3. Aktivieren Sie die Option „Benachrichtigung“.
4. Klicken Sie auf „Speichern“.

Testen der Firewall-Einstellungen

Beim Selbsttest wird der Firewall-Schutz mit Hilfe eines simulierten Zugriffs auf einen Dienst überprüft. Sie können den Selbsttest im Basismodus und im erweiterten Modus veranlassen. Vergewissern Sie sich vor dem Starten des Selbsttests, dass Zugriffsversuche protokolliert werden.

Im Basismodus können Sie die Einträge im Fenster „Setup“ testen, die von Norton Personal Firewall vordefiniert wurden oder die Sie selbst erstellt haben. Für den Test wird die IP-Adresse Ihres Computers verwendet. Wenn Ihr Computer eine *PPP*-Verbindung (Point-to-Point-Protokoll) verwendet und momentan keine Verbindung besteht oder wenn Ihrem Computer keine IP-Adresse zugeordnet wurde, wird für den Selbsttest die IP-Adresse 127.0.0.1 verwendet.

Im erweiterten Modus können Sie die erweiterte Liste der Dienste testen und eine andere IP-Adresse angeben, die für den Test anstelle der IP-Adresse Ihres Computers verwendet werden soll. Sie können zum Beispiel eine IP-Adresse eingeben, für die Sie den Zugriff verweigert haben.

Das Ergebnis des Selbsttests wird im Fenster „Zugriffsverlauf“ angezeigt. Wenn Sie einen Dienst einer Kategorie testen, für die Sie die Benachrichtigung aktiviert haben, wird auch beim Selbsttest die entsprechende Warnung angezeigt. Wenn Sie Norton Personal Firewall nicht aktivieren, ist der Zugriff auf alle Dienste möglich; auch dies wird vom Selbsttest reflektiert.

So starten Sie den Selbsttest im Basismodus:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Selbsttest“ aus dem Menü „Fenster“.

3. Wählen Sie einen Dienst/Port.

   Der für den Dienst definierte Schutz wird unter dem Namen des Diensts angezeigt.
4. Klicken Sie auf „Testen“.

So starten Sie den Selbsttest im erweiterten Modus:

1 Wählen Sie „Selbsttest“ aus dem Menü „Fenster“.

2 Wählen Sie einen Port für den Dienst.

Der für den Dienst definierte Schutz wird unter dem Namen des Diensts angezeigt.

3 Geben Sie an, ob Sie für den Test die IP-Adresse Ihres Computers oder eine spezielle IP-Adresse verwenden wollen.

Wenn Ihr Computer keine eigene IP-Adresse hat, wird die Option „Test auf Basis der IP-Adresse dieses Computers“ abgeblendet.

4 Geben Sie ggf. eine IP-Adresse ein.

5 Klicken Sie auf „Testen“.

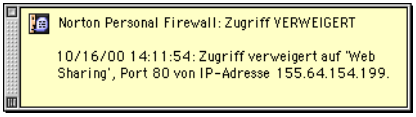
Sowohl im Basismodus als auch im erweiterten Modus werden nur TCP-Dienste getestet. Der Schutz für einen spezifischen UDP-Port kann abhängig von der Konfiguration von Norton Personal Firewall mit dem Schutz für den entsprechenden TCP-Dienst übereinstimmen oder davon abweichen.

Auf Zugriffsversuche reagieren

Öffnen Sie gelegentlich das Fenster „Zugriffsverlauf“, um zu überprüfen, ob ungewöhnliche Aktivitäten verzeichnet wurden oder der Zugriff für jemanden verweigert wurde, der eigentlich zugriffsberechtigt sein müsste.

Info über Warnmeldungen

Wenn Sie sich für die Benachrichtigung bei Zugriffsversuchen entschieden haben, wird eine Warnmeldung angezeigt, sobald ein Zugriffsversuch verzeichnet wird.



Die Warnmeldung enthält nähere Angaben zum jeweiligen Zugriffsversuch. Lesen Sie die Informationen im Fenster „Zugriffsverauf“, wenn Ihnen der Zugriffsversuch verdächtig erscheint. Wenn Sie im Fenster „Zugriffsverlauf“ auf den Eintrag doppelklicken, der für den Zugriffsversuch generiert wurde, erhalten Sie weitere Informationen über den jeweiligen Versuch.

Solange die Warnmeldung für einen Zugriffsversuch geöffnet ist, erfolgt keine Benachrichtigung bei weiteren Zugriffsversuchen. Bei Versionen des Macintosh Betriebssystems vor OS 9 ist es auch möglich, dass die Verarbeitung in anderen Anwendungsprogrammen unterbrochen wird, bis die Warnmeldung geschlossen wurde. Machen Sie daher bei früheren Versionen des Macintosh Betriebssystems keinen Gebrauch von der Benachrichtigung, wenn andere Anwendungen aktiv sind und Sie sich nicht bei Ihrem Computer aufhalten.

Zugriffsverlauf anzeigen

Alle protokollierten Zugriffe werden im Fenster „Zugriffsverlauf“ angezeigt. Verwenden Sie dieses Protokoll von Zugriffsversuchen, um potentielle Sicherheitsrisiken zu erkennen. Achten Sie beim Lesen des Protokolls auf diese und ähnliche Regelmäßigkeiten:

- Sehr viele abgewiesene Zugriffsversuche, speziell von einer immer gleichen Client-IP-Adresse;
- Aufeinanderfolgende Portnummern von derselben Client-IP-Adresse, ein mögliches Indiz für eine Port-Suche; (jemand prüft nacheinander alle Ports auf Ihrem Computer ab, um einen Port zu finden, über den der Zugriff möglich ist).

Ein gelegentlicher abgewiesener Zugriffsversuch von einer beliebigen IP-Adresse ist eine normale Erscheinung; (kritisch ist es nur, wenn alle Versuche von derselben IP-Adresse erfolgen oder wenn aufeinanderfolgende Ports abgefragt werden). In einigen Fällen gehen Zugriffsversuche auch auf Aktivitäten auf Ihrem eigenen Computer zurück, zum Beispiel wenn Sie die Verbindung zu einem FTP-Server herstellen oder eine E-Mail senden.

So zeigen Sie das Fenster „Zugriffsverlauf“ an:

1 Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.

2 Wählen Sie „Zugriffsverlauf“ aus dem Menü „Fenster“.

Format im erweiterten Modus

Sie können das Fenster „Zugriffsverlauf“ im Basismodus oder im erweiterten Modus anzeigen. Im Basismodus werden die Spalten „Port“, „Modus“ und „IP-Adresse“ nicht angezeigt.

Die Anleitung zum Wechseln in den erweiterten Modus finden Sie im Abschnitt „So wechseln Sie in den erweiterten Modus:“ auf Seite 28.

Die Kategorien (Typen) der protokollierten Zugriffsversuche werden oben im Bildschirm angezeigt. Im Fenster werden die folgenden Spalten angezeigt.

Datum & Uhrzeit	Zeitpunkt, an dem der Zugriffsversuch verzeichnet wurde;
Aktion	Angabe, ob der Zugriff zugelassen oder verweigert wurde;
Dienst	Name (sofern verfügbar) des Internet-Diensts, dem der Versuch galt;
Port	Nummer des Ports, über den der Versuch erfolgte;
Modus	Angabe des verwendeten Protokolls (TCP oder UDP);

IP-Adresse	IP-Adresse des Computers, von dem aus der Versuch erfolgte;
Hostname	Hostname des Computers, von dem aus der Zugriff erfolgte;

Zeilen in Fettdruck sind weniger als 15 Minuten alt.

Spalten sortieren

Standardmäßig sind die Zeilen nach dem Datum sortiert; der zuletzt erfolgte Versuch erscheint dabei zuoberst in der Liste.

So sortieren Sie die Liste nach einer anderen Spalte:

- Klicken Sie auf die Kopfzeile der gewünschten Spalte.

  Die Kopfzeile der Spalte, nach der die Liste sortiert ist, ist dunkelgrau unterlegt.

Sie können die Sortierfolge (aufsteigend oder absteigend) umkehren, indem Sie auf das kleine Dreieck am rechten Ende der Spaltenkopfzeile klicken.

Zugriffsverlaufsdaten exportieren

Sie können den Inhalt des Fenster „Zugriffsverlauf“ in eine Textdatei exportieren, in der die Informationseinheiten durch Tabulatoren getrennt werden. Damit Sie den Inhalt des Fensters „Zugriffsverlauf“ exportieren können, muss es geöffnet sein.

So exportieren Sie die Zugriffsverlaufsdaten:

1. Öffnen Sie das Fenster „Zugriffsverlauf“ und wählen Sie „Exportieren“ aus dem Menü „Ablage“.
2. Geben Sie im Fenster „Exportieren“ den Speicherort und den Namen für die Exportdatei ein.

   Klicken Sie auf „Neuer Ordner“, wenn Sie einen neuen Ordner erstellen wollen.
3. Klicken Sie auf „Speichern“.

Inhalt des Fensters „Zugriffsverlauf“ löschen

Wenn die Liste im Fenster „Zugriffsverlauf“ zu umfangreich wird, können Sie den Fensterinhalt löschen.

So leeren Sie das Fenster „Zugriffsverlauf“:

- Öffnen Sie das Fenster „Zugriffsverlauf“ und wählen Sie „Zugriffsverlauf löschen“ aus dem Menü „Bearbeiten“.

  Diese Menüoption hat keine Auswirkung auf die Protokolldatei; sie enthält auch nach dem Löschen noch alle Zugriffsversuche bis zum aktuellen Zeitpunkt.

Weitere Informationen über spezifische Zugriffsversuche

Sie können für jeden Eintrag im Fenster „Zugriffsverlauf“ weitergehende Informationen anzeigen.

So öffnen Sie das Dialogfenster „Zugriffsinformationen“:

- Doppelklicken Sie im Fenster „Zugriffsverlauf“ auf einen Listeneintrag, oder markieren Sie einen Eintrag und wählen Sie „Infos abrufen“ aus dem Menü „Bearbeiten“.

So kopieren Sie die Informationen in die Zwischenablage zur weiteren Verwendung in einer anderen Anwendung:

- Klicken Sie im Fenster „Zugriffsinformationen“ auf „Kopieren“.

Ändern der Voreinstellungen für die Protokollierung

Standardmäßig werden alle Zugriffsversuche protokolliert. Sie sollten diese Einstellung beibehalten, bis Sie sicher sind, dass Ihre Konfiguration von Norton Personal Firewall wie erwartet funktioniert. Da aber das Protokollieren aller Zugriffe schnell zu einer sehr großen Protokolldatei führen kann, ist es unter Umständen ratsam, das Protokollieren einzuschränken.

So ändern Sie die Voreinstellungen für das Protokollieren:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.
3. Legen Sie die Voreinstellungen für das Protokollieren fest.
4. Klicken Sie auf „Speichern“.

Protokollierung deaktivieren

Die Protokollfunktion und der Schutz für die Dienste sind voneinander unabhängig. Wenn Sie zum Beispiel festlegen, dass zugelassene Zugriffsversuche protokolliert werden, und Norton Personal Firewall deaktivieren, setzt Norton Personal Firewall das Protokollieren fort und erfasst alle Zugriffe, da alle Zugriffe zugelassen sind. In bestimmten Situationen (zum Beispiel wenn Sie eine neue Protokolldatei anlegen wollen) müssen Sie die Protokollfunktion ganz ausschalten. Das Deaktivieren der Protokollfunktion hat keine Auswirkung auf den Schutz durch Norton Personal Firewall.

So deaktivieren Sie die Protokollierung:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.
3. Deaktivieren Sie beide für die Protokollfunktion angebotenen Optionen.
4. Klicken Sie auf „Speichern“.

Struktur der Protokolldatei

Die Protokolldatei ist eine Textdatei, die das Tabulatorzeichen als Begrenzungszeichen verwendet und unter dem Namen „Norton Personal Firewall Log“ im Ordner „Preferences“ abgelegt wird. Sie wird im erweiterten WebSTAR-Protokollformat erstellt und kann mit jedem Tabellenkalkulations- oder Textverarbeitungsprogramm und mit vielen Analyseprogrammen für Log- oder Protokolldateien gelesen werden.

Zugriffsversuche werden mit folgenden Merkmalen protokolliert; (sie werden in die Zeile !!LOG_FORMAT aufgenommen, wenn Norton Personal Firewall gestartet oder eine neue Protokolldatei erstellt wird):

DATE, TIME	Datum und Uhrzeit des Zugriffs im WebSTAR-Standardformat
RESULT	Angabe ‚OK‘ für einen zugelassenen und ‚ERR!‘ für einen verweigerten Zugriff
HOSTNAME	IP-Adresse des Clients, der den Zugriff über den angegebenen Port versuchte
SERVER_PORT	Port, über den der angegebene Client den Zugriffsversuch unternahm
METHOD	Angabe des für den Zugriffsversuch verwendeten Protokolls (TCP oder UDP)

Wenn Sie die Protokolldatei in ein Tabellenkalkulationsprogramm exportieren und die Daten darin sortieren, können Sie Regelmäßigkeiten, die auf ein potentielles Sicherheitsrisiko hindeuten, unter Umständen leichter erkennen. Beispiele:

- Sortieren Sie die Daten nach der Spalte RESULT und danach nach der Spalte HOSTNAME. Achten Sie bei Zeilen mit der Angabe ‚ERR!‘ in der Spalte RESULT darauf, ob in der Spalte HOSTNAME wiederholt dieselbe IP-Adresse protokolliert wurde. Eine große Anzahl von ‚ERR!‘-Zeilen für eine bestimmte einzelne IP-Adresse können das Indiz für eine versuchte Schutzverletzung sein.

- Sortieren Sie die Daten nach der Spalte RESULT und danach nach den Spalten HOSTNAME und SERVER_PORT. Achten Sie bei Zeilen mit der Angabe ‚ERR!‘ in der Spalte RESULT und mit derselben IP-Adresse in der Spalte HOSTNAME darauf, ob in der Spalte SERVER_PORT aufeinander folgende Portnummern erscheinen. Zeilen mit aufeinander folgenden Portnummern, die dieselbe IP-Adresse als Ausgangspunkt nennen, können das Indiz für eine Port-Suche sein.

Weitere Informationen über eine IP-Adresse in der Protokolldatei (oder in der Warnmeldung der Benachrichtigungsfunktion) können Sie im Fenster „Zugriffsverlauf“ abrufen. Weitere Informationen zum Anzeigen des Fensters „Zugriffsverlauf“ finden Sie im Abschnitt „So zeigen Sie das Fenster „Zugriffsverlauf“ an:“ auf Seite 34.

K A P I T E L 5

Firewall-Schutz anpassen

Für die Arbeit mit Norton Personal Firewall ist es unter Umständen erforderlich, die Zugriffseinstellungen zu ändern. Dies ist zum Beispiel der Fall, wenn Sie einem Kollegen, der an einem anderen Ort arbeitet, per File Sharing den Zugriff auf Ihren Computer ermöglichen wollen. Möglicherweise verwenden Sie auch einen Dienst auf Ihrem Computer, der nicht in der Liste der geschützten Dienste enthalten ist. Sie können in diesem Fall für diesen Dienst einen Eintrag zu der Liste hinzufügen. Sie können den Schutz außerdem auch auf die UDP-Ports Ihres Computers ausweiten.

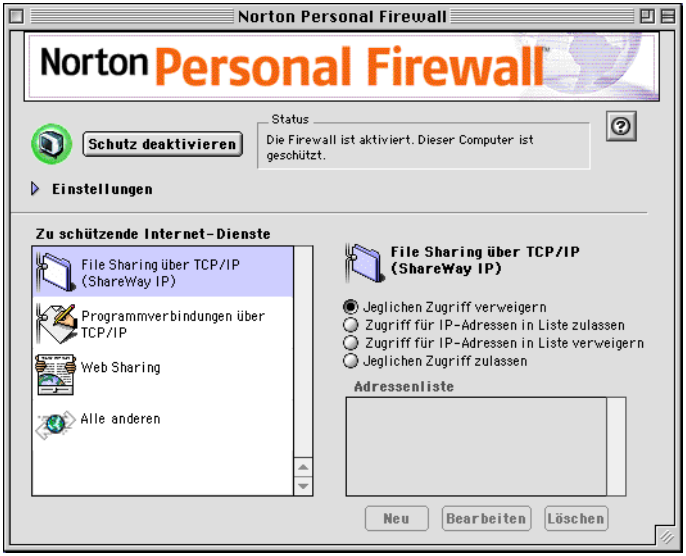
Änderungen an den Zugriffseinstellungen haben keine Auswirkung auf Computer, die mit Ihrem Computer verbunden sind, während Sie die Änderungen vornehmen. Die Änderungen werden erst wirksam, wenn die Verbindung beendet wurde. Wenn Sie beispielsweise den Zugriff auf den Dienst ‚File Sharing' auf Ihrem Computer verweigern, solange ein anderer Computer mit diesem Dienst verbunden ist, bleibt die Verbindung bestehen, bis sich der betreffende Benutzer abmeldet oder Sie die Verbindung explizit trennen.

Vordefinierter Schutz für Internet-Standardverbindungen

Die in das Macintosh OS integrierten Internet-Dienste sind bereits im Fenster „Setup" von Norton Personal Firewall vordefiniert. Für Dienste ohne eigenen Eintrag in der Liste gilt der Schutz, der in der Zeile „Alle anderen" definiert ist. Standardmäßig gilt für ‚alle anderen' Dienste, dass jeglicher Zugriff verweigert wird. Sie können die Schutzeinstellungen für jeden der aufgelisteten Dienste ändern.

So öffnen Sie das Fenster „Setup“:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wird das Fenster „Setup“ nicht direkt angezeigt, wählen Sie „Setup“ aus dem Menü „Fenster“.
3. Wenn nicht das komplette Fenster „Setup“ angezeigt wird, klicken Sie auf „Einstellungen“, um es zu erweitern.



Wenn Sie das Fenster „Setup“ zum ersten Mal öffnen, werden die Schutzeinstellungen rechts im Fenster nicht angezeigt. Klicken Sie in der Liste links auf einen Dienst, um die Einstellungen für diesen Dienst anzuzeigen.

Für jeden im Fenster „Setup“ aufgeführten Dienst können Sie folgende Einstellungen vornehmen:

- Jeglichen Zugriff verweigern.
- Den Zugriff nur für die aufgelisteten IP-Adressen zulassen.
- Den Zugriff nur für die aufgelisteten IP-Adressen verweigern.
- Jeglichen Zugriff zulassen.

Die Reihenfolge der Einstellungen reflektiert den Grad der Beschränkung von weitgehend beschränkt bis weitgehend unbeschränkt. Wenn Sie den Zugriff auf einen Dienst zulassen oder verweigern wollen, klicken Sie auf den betreffenden Dienst und legen Sie die gewünschte Einstellung fest.

Wenn Sie den Zugriff für eine oder mehrere IP-Adressen zulassen oder verweigern wollen, klicken Sie auf den betreffenden Dienst und anschließend auf die entsprechende Einstellung und geben Sie danach in der Liste rechts unten die IP-Adressen an, für die die Beschränkung bzw. Freigabe gelten soll.

So definieren Sie die IP-Adresse(n), für die der Zugriff zugelassen oder verweigert werden soll:

1. Wählen Sie den Internet-Dienst, für den Sie die Zugriffseinstellungen festlegen wollen.
2. Geben Sie an, ob für die definierten IP-Adressen der Zugriff zugelassen oder verweigert werden soll, indem Sie die entsprechende Option aktivieren.
3. Klicken Sie auf „Neu“, um eine Adresse oder einen Adressbereich für die Liste zu definieren.

   Daraufhin erscheint das Fenster „Neue Adresse“.

IP-Adressen hinzufügen

Mit den beiden ersten Optionen im Fenster „Neue Adresse“ können Sie eine einzelne Adresse oder einen IP-Bereich definieren, für die/den der Zugriff zugelassen bzw. verweigert werden soll.

So fügen Sie eine einzelne Adresse hinzu:

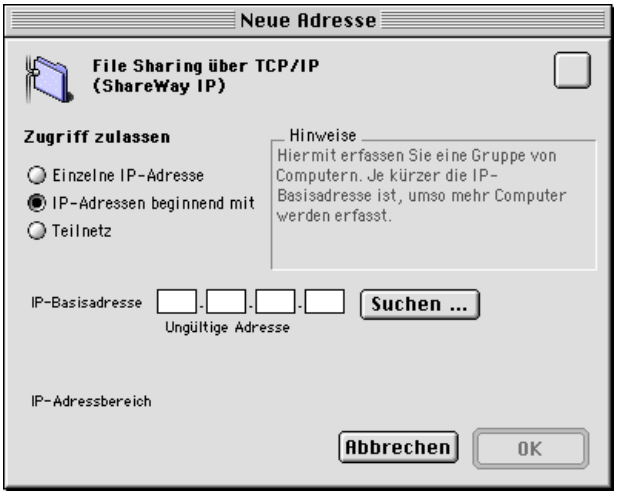
1. Aktivieren Sie im Fenster „Neue Adresse“ die Option „Einzelne IP-Adresse“.

2 Geben Sie im Feld „IP-Adresse“ die betreffende IP-Adresse ein.

3 Klicken Sie auf „OK“.

So fügen Sie einen Adressbereich hinzu:

1 Aktivieren Sie im Fenster „Neue Adresse“ die Option „IP-Adressen beginnend mit“.



2 Geben Sie im Bereich „IP-Basisadresse“ so viele Ziffern ein, wie zur eindeutigen Definition des gewünschten Adressbereichs nötig sind.

Wenn Sie im Feld „IP-Basisadresse“ eine Ziffer eingeben, ermittelt Norton Personal Firewall automatisch das jeweilige Ende des Bereichs und zeigt das ermittelte Ergebnis im Bereich „IP-Adressbereich“ unten im Fenster „Neue Adresse“ an.

3 Klicken Sie auf „OK“.

Suchen von IP-Adressen

Wenn Sie eine einzelne IP-Adresse oder einen IP-Adressbereich definieren wollen, können Sie auch einen Hostnamen eingeben, um die zugehörige IP-Adresse zu ermitteln.

So suchen Sie eine IP-Adresse:

1 Klicken Sie im Fenster „Neue Adresse“ auf „Suchen“.

2 Geben Sie im Fenster „IP-Adresse suchen“ den Hostnamen ein.

3 Klicken Sie auf „Suchen“.

4 Klicken Sie auf „OK“, um die im Fenster „IP-Adresse suchen“ gefundene Adresse in das Fenster „Neue Adresse“ zu übernehmen.

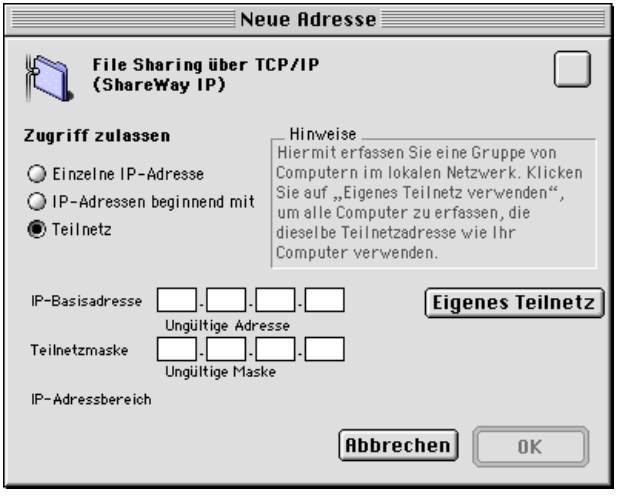
Teilnetzadressen hinzufügen

Sie können den Zugriff auf Ihren Computer auch für Teilnetze zulassen oder verweigern. Im Basismodus können Sie die Einstellungen nur für Ihr eigenes Teilnetz festlegen. Im erweiterten Modus können Sie Ihr eigenes oder ein anderes Teilnetz einstellen.

Die Anleitung zum Wechseln in den erweiterten Modus finden Sie im Abschnitt „So wechseln Sie in den erweiterten Modus:“ auf Seite 28.

So fügen Sie Adressen für Ihr eigenes Teilnetz hinzu:

1 Aktivieren Sie im Fenster „Neue Adresse“ die Option „Teilnetz“.



2 Klicken Sie auf „Eigenes Teilnetz“.

Die IP-Basisadresse und die *Teilnetzmaske* für Ihr Teilnetz werden automatisch in die entsprechenden Felder eingetragen. Die Teilnetzmaske legt fest, wie viele Ziffern einer IP-Adresse zur Identifizierung des Teilnetzes nötig sind.

3 Klicken Sie auf „OK“.

So fügen Sie Adressen für ein anderes Teilnetz hinzu:

1 Aktivieren Sie im Fenster „Neue Adresse“ die Option „Teilnetz“.

2 Geben Sie die IP-Basisadresse und die Teilnetzmaske für das gewünschte Teilnetz in die dafür vorgesehenen Felder ein.

3 Klicken Sie auf „Mein Teilnetz“, wenn Sie die Werte für Ihr eigenes Teilnetz verwenden wollen.

   Norton Personal Firewall trägt in diesem Fall die entsprechenden Werte automatisch in den Feldern ein.

4 Klicken Sie auf „OK“.

Schutzdefinition für eigenen Dienst

Wenn Sie die Zugriffseinstellungen für einen Dienst festlegen wollen, der nicht im Fenster „Setup“ aufgelistet ist, müssen Sie den betreffenden Dienst zunächst in Norton Personal Firewall definieren. Für diesen Vorgang müssen Sie den erweiterten Modus aktivieren.

Die Anleitung zum Wechseln in den erweiterten Modus finden Sie im Abschnitt „So wechseln Sie in den erweiterten Modus:“ auf Seite 28.

So definieren Sie einen zusätzlich zu schützenden Dienst:

1 Aktivieren Sie die Liste der Dienste und klicken Sie auf „Neu“.

2 Wählen Sie einen Port für den Dienst.

3 Geben Sie den Namen des Diensts ein.

   Wenn Sie eine Portnummer aus der Liste wählen, wird der Name des jeweiligen Diensts automatisch ergänzt.

   Für den Dienst wird automatisch ein Symbol angezeigt.

4 Durch Kopieren und Einfügen können Sie das Symbol, das im Fenster „Neuer Dienst“ angezeigt wird, durch ein Symbol Ihrer Wahl ersetzen.

5 Klicken Sie auf „OK“.

Der neu hinzugefügte Dienst erscheint nun im Fenster „Setup“ in der Liste der Dienste. Sie können nun die Zugriffseinstellungen für diesen Dienst festlegen.

Weitere Informationen finden Sie im Abschnitt „Vordefinierter Schutz für Internet-Standardverbindungen“ auf Seite 41.

Einen eigenen Dienst ändern oder löschen

Anders als vordefinierte Dienste, die Sie weder bearbeiten noch löschen können, können Sie einen Dienst, den Sie selbst hinzugefügt haben, jederzeit bearbeiten oder löschen.

So bearbeiten Sie einen eigenen Dienst:

1. Wählen Sie den gewünschten Dienst im Fenster „Setup“.
2. Klicken Sie auf „Bearbeiten“.
3. Ändern Sie im Dialogfenster „Dienst bearbeiten“ den Namen oder (durch Ausschneiden und Einfügen) das Symbol des Diensts.
4. Wenn Sie die Portnummer ändern wollen, müssen Sie den Dienst löschen und einen neuen Eintrag mit der gewünschten neuen Portnummer erstellen.
5. Klicken Sie auf „OK“.

So löschen Sie einen eigenen Dienst:

1. Wählen Sie den gewünschten Dienst im Fenster „Setup“.
2. Klicken Sie auf „Löschen“.
3. Klicken Sie im Fenster „Warnung“, das daraufhin angezeigt wird, erneut auf „Löschen“, um zu bestätigen, dass Sie den Dienst wirklich löschen wollen.

Schutzeinstellungen ändern

Sie können auf zwei Ebenen Änderungen an den Schutzeinstellungen für einen Dienst vornehmen. Sie können den Grad der Zugriffsbeschränkung ändern (zum Beispiel von „Jeglichen Zugriff verweigern“ in „Zugriff durch IP-Adressen in Liste zulassen“) oder die Adressen in der Liste bearbeiten, die der jeweiligen Schutzoption zugeordnet ist. Diese Änderungen können Sie direkt im Fenster „Setup“ vornehmen.

Grad der Zugriffsbeschränkung ändern

Sie können den Grad der Zugriffsbeschränkung immer nur für jeweils einen Dienst ändern.

So ändern Sie den Grad der Zugriffsbeschränkung:

1. Wählen Sie den gewünschten Dienst im Fenster „Setup“.
2. Aktivieren Sie die gewünschte neue Schutzoption:
   - Wenn Sie eine der beiden Schutzoptionen aktivieren, die mit einer Liste von IP-Adressen gekoppelt sind, müssen Sie diese Liste erstellen.

     Informationen über das Erstellen einer IP-Adressliste finden Sie im Abschnitt „Vordefinierter Schutz für Internet-Standardverbindungen“ auf Seite 41.
   - Wenn Sie eine mit einer IP-Adressliste gekoppelte Option durch eine der beiden Optionen „Jeglichen Zugriff zulassen“ oder „Jeglichen Zugriff verweigern“ ersetzen, müssen Sie die zugeordneten Adressen nicht eigens löschen. Sie sind im Fenster „Setup“ weiterhin zu sehen, werden aber abgeblendet.

IP-Adressliste ändern

Für jede der beiden mit einer IP-Adressliste gekoppelten Schutzoptionen können Sie neue Adressen in die Liste aufnehmen sowie die in der Liste enthaltenen Adressen bearbeiten oder löschen.

Klicken Sie, bevor Sie Änderungen an einer Liste vornehmen, auf den Dienst, für den die Änderungen gelten sollen, damit auch wirklich die richtige Adressliste angezeigt wird.

So fügen Sie der Liste eine oder mehrere neue Adressen hinzu:

1. Klicken Sie im Fenster „Setup“ auf „Neu“.
2. Fügen Sie die neue(n) IP-Adresse(n) hinzu.
3. Klicken Sie auf „OK“.

Weitere Informationen über das Hinzufügen von IP-Adressen finden Sie im Abschnitt „IP-Adressen hinzufügen“ auf Seite 43. Weitere Informationen über das Hinzufügen von Teilnetzadressen finden Sie im Abschnitt „Teilnetzadressen hinzufügen“ auf Seite 45.

So bearbeiten Sie eine Adresse oder einen Adressbereich in der Liste:

1 Wählen Sie im Fenster „Setup“ die gewünschte Adresse oder den gewünschten Adressbereich.

2 Klicken Sie auf „Bearbeiten“.

3 Nehmen Sie im Fenster „Adresse bearbeiten“ die gewünschten Änderungen vor.

4 Klicken Sie auf „OK“.

So löschen Sie eine Adresse oder einen Adressbereich aus der Liste:

1 Wählen Sie im Fenster „Setup“ die gewünschte Adresse oder den gewünschten Adressbereich.

2 Klicken Sie auf „Löschen“.

3 Klicken Sie im Fenster „Warnung“, das daraufhin angezeigt wird, erneut auf „Löschen“, um Ihre Anforderung zu bestätigen.

Schutz für UDP-Ports einrichten

User Datagram Protocol (UDP) ist ein vergleichsweise einfaches Protokoll, das für Internet-Operationen verwendet wird. UDP wird zum Beispiel von DNS (Domain Name System) verwendet, um Hostnamen in IP-Adressen umzusetzen.

Es besteht daher wenig Grund, UDP-Ports zu schützen. Trotzdem kann es in bestimmten Situationen wünschenswert oder erforderlich sein, einen UDP-Port zu schützen. Lassen Sie beim Schutz dieser Ports aber besondere Vorsicht walten, da der verweigerte Zugriff auf einen UDP-Dienst zu Problemen beim Zugang zum Internet führen kann.

In den meisten Fällen genügt es, den Schutz nur für die UDP-Ports bis 1023 zu aktivieren; diese niedrigen UDP-Portnummern werden für Standarddienste verwendet wie *DHCP* (Dynamic Host Configuration Protocol, mit dem in der Regel die IP-Adresse eines Computers abgerufen wird) und NTP (Network Time Protocol, das vom Kontrollfeld „Datum & Uhrzeit“ verwendet werden kann). Ports mit höheren Nummern werden von UDP-Diensten wie DNS dynamisch verwendet. Wenn Sie den Zugriff auf Ports mit hohen Nummern verweigern, können die entsprechenden Dienste nicht mehr ausgeführt werden, da nicht mehr geklärt werden kann, welche Ports von einem bestimmten Dienst verwendet werden.

So aktivieren Sie den Schutz für UDP-Ports:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.
3. Aktivieren Sie die Option „Erweiterte Kontrolle über Dienste aktivieren“.
4. Aktivieren Sie die Option „Schutz für UDP und TCP aktivieren“.
5. Geben Sie den Nummernbereich der Ports an, die geschützt werden sollen.
6. Klicken Sie auf „Speichern“.

Funktionsweise des UDP-Schutzes

Nachdem Sie den UDP-Schutz aktiviert haben, funktioniert er gleich wie der TCP-Schutz. Norton Personal Firewall verwendet für den UDP- und den TCP-Schutz dieselbe Liste von Diensten. Im Normalfall verwendet ein Dienst nur entweder den TCP- oder den UDP-Port; Norton Personal Firewall schützt aber die Ports beider Typen für den jeweiligen Dienst (sofern der UDP-Schutz für den betreffenden Port aktiv ist).

Ein Unterschied zwischen UDP- und TCP-Schutz hängt mit der Tatsache zusammen, dass UDP ein *verbindungsloses Protokoll* ist (das zum Senden einer Nachricht keine bestehende Verbindung benötigt), während es sich bei TCP um ein *verbindungsabhängiges Protokoll* handelt (das zum Senden einer Nachricht eine bestehende Verbindung benötigt). Bei TCP kann Norton Personal Firewall nur den Verbindungsversuch zulassen oder verweigern, nicht aber die Informationen, die auf den Versuch folgen. Bei UDP muss Norton Personal Firewall im Gegensatz dazu jede an einen bestimmten Dienst gerichtete Informationseinheit einzeln zulassen oder verweigern. Aus diesem Grund ist es nicht möglich, nur eingehende Verbindungsversuche abzublocken; es kann nur die komplette Kommunikation für einen Dienst abgeblockt werden.

Weitere Abweichungen bei UDP ergeben sich bei den Funktionen für die Protokollierung und die Benachrichtigung. Bei TCP wird Norton Personal Firewall auch dann über Zugriffsversuche informiert (und kann sie entsprechend protokollieren), wenn auf dem betreffenden Port kein Dienst aktiv ist. Anders verhält es sich bei UDP; hier wird Norton Personal Firewall über Zugriffsversuche auf Ports, die nicht aktiv sind, im Normalfall nicht informiert. Daher erfolgt keine Benachrichtigung für diese Versuche, und die Versuche werden weder protokolliert noch im Fenster „Zugriffsverlauf“ angezeigt.

Da UDP ein verbindungsloses Protokoll ist, protokolliert und meldet Norton Personal Firewall jedes UDP-Paket, das an einen geschützten UDP-Port gerichtet wird (sofern die entsprechenden Optionen konfiguriert wurden). Es ist nicht ratsam, bei aktivem UDP-Schutz die zugelassenen Zugriffe zu protokollieren, da in sehr kurzer Zeit sehr viele Protokolleinträge generiert werden können. Da beispielsweie DNS einen UDP-Port verwendet, würde für jede Verbindung zu einer Website ein Eintrag im Protokoll generiert.

Selbst wenn Sie nur die UDP-Ports mit niedrigen Nummern schützen, sollten Sie spezielle Einträge für die einzelnen Dienste erstellen. Wenn Ihr Computer zum Beispiel die eigene IP-Adresse über DHCP abruft, sollten Sie für den Dienst DHCP an Port 68 die Einstellung „Jeglichen Zugriff zulassen“ verwenden (bzw. die Einstellung „Zugriff für IP-Adressen in Liste zulassen“ aktivieren und die IP-Adresse des DHCP-Servers eingeben). Beim Aktivieren des UDP-Schutzes wird von Norton Personal Firewall automatisch ein solcher Eintrag für den Dienst DHCP generiert. Um den maximalen Schutz sicherzustellen, gilt für diesen Dienst anfangs die Einstellung „Jeglichen Zugriff verweigern“.

K A P I T E L 6

Problemlösungen

Häufig gestellte Fragen (FAQs)

Wie kann ich den Firewall-Schutz deaktivieren?

Sie können den Firewall-Schutz an zwei Stellen deaktivieren: im Fenster „Setup“ oder mit der Kontrollleiste (bei Macintosh OS 8.5 oder höher).

So deaktivieren Sie den Firewall-Schutz im Fenster „Setup“:

1. Doppelklicken Sie auf das Programmsymbol von **Norton Personal Firewall**.
2. Wird das Fenster „Setup“ nicht direkt angezeigt, wählen Sie „Setup“ aus dem Menü „Fenster“.
3. Wählen Sie „Schutz deaktivieren“.

So deaktivieren Sie den Firewall-Schutz mit dem Menü des Moduls in der Kontrollleiste:

1. Klicken Sie in der Kontrollleiste auf das Modul von **Norton Personal Firewall**, um das zugehörige Menü zu öffnen.
2. Wählen Sie „Firewall-Schutz deaktivieren“.

Sie können das Kontrollleistenmenü auch dazu verwenden, den Schutz durch Norton Personal Firewall für eine bestimmte Zeitdauer auszusetzen.

So deaktivieren Sie Norton Personal Firewall für eine bestimmte Zeitdauer:

1. Klicken Sie in der Kontrollleiste auf das Modul von **Norton Personal Firewall**, um das zugehörige Menü zu öffnen.
2. Wählen Sie „Firewall-Schutz vorübergehend deaktivieren“.

3 Geben Sie an, nach wie vielen Minuten der Schutz durch Norton Personal Firewall wieder gestartet werden soll.

4 Klicken Sie auf „OK“.

Weshalb kann ich von einer Website keine Dateien herunterladen?

Möglicherweise verwenden Sie FTP für den Transfer der Dateien. Viele Funktionen des FTP-Protokolls hängen davon ab, dass der FTP-Server eine TCP-Verbindung zurück zu Ihrem Computer öffnet und diese Verbindung als Daten-Port verwendet, um Daten von Ihrem Computer zu erhalten. Das Problem besteht nun darin, dass die Nummer für den Daten-Port nach dem Zufallsprinzip ausgewählt wird und es daher schwierig ist, den Zugriff auf den FTP-Server vorzeitig zuzulassen.

Führen Sie einen der folgenden Schritte aus, um diese FTP-Probleme zu lösen:

- Wählen Sie „Firewall-Schutz vorübergehend deaktivieren“ aus dem Menü des Kontrollleistenmoduls.

  Norton Personal Firewall muss nur zu dem Zeitpunkt deaktiviert sein, an dem die Dateiübertragung gestartet wird. Wenn Sie mehrere Dateien in einem Arbeitsgang übertragen wollen, müssen Sie sicherstellen, dass Norton Personal Firewall deaktiviert bleibt, bis die Übertragung der letzten Datei gestartet wurde. Wenn Sie einen Computer mit Macintosh OS 8.1 verwenden, können Sie Norton Personal Firewall im Fenster „Setup“ deaktivieren und aktivieren.
- Richten Sie den Eintrag für ‚alle anderen‘ Dienste so ein, dass der Zugriff durch den FTP-Server zugelassen wird; (verwenden Sie dabei die IP-Adresse, die im Fenster „Zugriffsverlauf“ angezeigt wird).
- Wenn Ihre FTP-Client-Anwendung die Möglichkeit bietet, einen Daten-Port anzugeben, erstellen Sie einen Eintrag für den Port, den Sie verwenden wollen, und lassen Sie den Zugriff durch den FTP-Server auf diesen Port zu.
- Unterstützt Ihre FTP-Client-Anwendung den FTP-Datentransfer im passiven Modus (so dass kein Daten-Port benötigt wird), machen Sie davon Gebrauch. Vergewissern Sie sich (bei Macintosh OS 8.5 und höher), dass im Kontrollfeld „Internet“ auf der Seite „Erweitert“ die Option „FTP Passive Mode (PASV) verwenden“ aktiviert ist.

Weshalb kann ich auf keine Website zugreifen?

Sie haben möglicherweise den UDP-Schutz aktiviert und dabei einen Dienst mit einer niedrigen Portnummer beeinflusst, den Ihr Computer für routinemäßige Internet-Aktivitäten benötigt. Mögliche Ursachen sind:

- DHCP: Prüfen Sie im Kontrollfeld „TCP/IP“, ob Ihr Computer so konfiguriert ist, dass er die eigene IP-Adresse über DHCP erhält. Ist dies der Fall, wurde von Norton Personal Firewall ein Eintrag für den Dienst DHCP generiert. Bearbeiten Sie diesen Eintrag so, dass der DHCP-Server auf Ihren Computer zugreifen kann. Verwenden Sie für die Bearbeitung die IP-Adresse des DHCP-Servers, die im Fenster „Zugriffsverlauf“ angezeigt wird.
- DNS: Fast alle Internet-Operationen, die von Ihrem Computer ausgehen, verwenden DNS, um Hostnamen in IP-Adressen umzusetzen. Vergewissern Sie sich, dass die für DNS dynamisch zugeordneten Ports (in der Regel die Ports ab 32768) nicht blockiert werden.

Hinweise dazu, wie Sie prüfen können, welche Portnummern blockiert sind, finden Sie im Abschnitt „Zugriffsverlauf anzeigen“ auf Seite 33. Informationen darüber, wie Sie einen Eintrag bearbeiten, um den Zugriff auf den entsprechenden Dienst zuzulassen, finden Sie im Abschnitt „IP-Adressen hinzufügen“ auf Seite 43.

Weshalb funktioniert mein FTP-Server nicht?

Wenn Sie einen FTP-Server auf Ihrem Computer ausführen, kann es geschehen, dass bestimmte Benutzer Probleme beim Verbindungsaufbau zum Server haben, obwohl Sie den Zugriff auf Port 21 zulassen. Verwendet eine Client-Software den passiven FTP-Modus (PASV), kann der Client dynamisch eine zweite Verbindung zum Server für den Daten-Port öffnen. Veranlassen Sie in diesem Fall, dass der Client nicht den passiven Modus verwendet, oder räumen Sie dem Client den Zugriff auf den neuen, vom Server geöffneten Port ein.

Informationen darüber, wie Sie den Zugriff auf einen Port zulassen, finden Sie im Abschnitt „Schutzdefinition für eigenen Dienst“ auf Seite 46.

Weshalb funktioniert mein Drucker nicht?

Möglicherweise haben Sie AppleTalk deaktiviert, als Sie gewarnt wurden, dass AppleTalk denselben Port verwendet wie Ihre Internet-Verbindung. Schalten Sie in diesem Fall AppleTalk wieder ein, wenn Sie drucken wollen.

Welcher Dienst verbirgt sich hinter einer Portnummer?

In der folgenden Tabelle sind die Nummern von TCP- und UDP-Ports zusammengestellt, die von Macintosh Diensten häufig verwendet werden.

TCP-Ports

Port	Verwendung	Hinweise
20	FTP-Daten	Nur als Quell-Port verwendet
21	FTP-Steuerung	
23	Telnet	Häufiger Angriffspunkt
25	SMTP (E-Mail)	
53	DNS	Verwendet i. d. R. UDP, nicht TCP
70	Gopher	
79	Finger	
80	HTTP (Web)	
88	Kerberos	
105	PH (Verzeichnis)	
106	Poppass (Kennwort ändern)	
110	POP3 (E-Mail)	
111	Remote Procedure Call (RPC)	Verwendet für Java
113	AUTH	
119	NNTP (News)	
139	NETBIOS-Sitzung	Windows-Zugriff (ASIP 6)
143	IMAP (Neue E-Mail)	
311	AppleShare Web Admin	ASIP 6.1 und höher
384	ARNS (Tunneling)	
387	AURP (Tunneling)	
389	LDAP (Verzeichnis)	

Port	Verwendung	Hinweise
407	Timbuktu 5.2 oder höher	Frühere Versionen nutzen andere Ports
427	SLP (Service Location)	Verwendet TCP nur für große Antwortpakete
443	SSL (HTTPS)	
497	Retrospect	UDP zum Suchen von Clients
510	FirstClass Server	
515	LPR (Drucken)	
548	AFP (AppleShare)	
554	RTSP (QuickTime Server)	Verwendet auch UDP 6970+
591	FileMaker Pro Web	Empfohlene Alternative: 80
626	IMAP Admin	Apple Systemerweiterung in ASIP 6
660	ASIP Remote Admin	ASIP 6.3 und höher
666	Now Contact Server	Verstößt gegen tatsächliche Port-Zuordnung
687	ASIP Shared U&G Port	ASIP 6.2 und höher
1080	WebSTAR Admin	WebSTAR Portnummer plus 1000
1417	Timbuktu Control (vor 5.2)	Logon erfolgt über UDP-Port 407
1418	Timbuktu Observe (vor 5.2)	Logon erfolgt über UDP-Port 407
1419	Timbuktu Send Files (vor 5.2)	Logon erfolgt über UDP-Port 407
1420	Timbuktu Exchange (vor 5.2)	Logon erfolgt über UDP-Port 407
1443	WebSTAR/SSL Admin	WebSTAR Portnummer plus 1000
3031	Programmverbindungen (Apple Ereignisse)	Macintosh OS 9 und höher
4000	Now Public Event Server	
4199	EIMS Admin	
4347	LANsurveyor Responders	Verwendet auch UDP

Port	Verwendung	Hinweise
5003	FileMaker Pro	Direkter Zugriff, nicht über Web; UDP für Host-Liste
5190	AOL Instant Messenger	
5498	Hotline Tracker	UDP-Port 5499 zum Suchen von Servern
5500	Hotline Server	
5501	Hotline Server	
6699	Napster/Macster Client	Im Firewall-Modus des Servers verwendet
7070	Real Player	Verwendet auch UDP-Ports 6970-7170
7648	CuSeeMe (Video)	Client-Verbindungen; UDP für Audio/Video
7649	CuSeeMe (Video)	Verbindungsaufbau
19813	4D Server	Bisher 14566 (6.0 und höher)

UDP-Ports

Port	Verwendung	Hinweise
53	DNS	Verwendet manchmal TCP
68	Dynamic Host Configuration Protocol (DHCP)	Oft zum Abrufen der IP-Adresse eines Computers verwendet
69	Trivial File Transfer Protocol (TFTP)	
123	Network Time Protocol	
137	Windows Name Service	
138	Windows Datagram Service	
161	Simple Network Management Protocol (SNMP)	

Port	Verwendung	Hinweise
407	Timbuktu	Nur Handshaking, vor Version 5.2
458	QuickTime TV	
497	Retrospect	Zum Suchen von Clients im Netzwerk
514	Syslog	
554	Real Time Streaming Protocol (QuickTime)	
2049	Network File System (NFS)	
3283	Apple Network Assistant	
5003	FileMaker Pro	Zum Abrufen der Host-Liste
6970 +	QuickTime und RealPlayer	
7070	RTSP Alternate (RealPlayer)	

Wie erstelle ich eine neue Protokolldatei?

Wenn Ihre Protokolldatei aufgrund Ihrer Größe unhandlich wird, können Sie eine neue Protokolldatei erstellen und verwenden. Sie müssen dazu die bisherige Protokolldatei nicht löschen; Sie können sie archivieren.

Wenn Sie die Protokollfunktion nicht deaktivieren, bevor Sie Ihre bisherige Protokolldatei umbenennen oder verschieben, schreibt Norton Personal Firewall die Protokolldaten in die bisherige Datei, bis Sie die Protokollfunktion deaktivieren oder Ihren Computer neu starten; erst danach wird die neue Datei erstellt und verwendet.

So erstellen Sie eine neue Protokolldatei:

1. Doppelklicken Sie auf das Programmsymbol „Norton Personal Firewall“ oder wählen Sie „Norton Personal Firewall öffnen“ aus dem Menü des Kontrollleistenmoduls, um Norton Personal Firewall zu starten.
2. Wählen Sie „Voreinstellungen“ aus dem Menü „Bearbeiten“.
3. Deaktivieren Sie die Protokollfunktion.

4 Benennen Sie die Protokolldatei um (sie hat den Namen „Norton Personal Firewall Log“) oder verschieben Sie sie aus dem Ordner „Preferences“ in einen anderen Ordner.

5 Aktivieren Sie nun wieder die Protokollfunktion.

Norton Personal Firewall erstellt automatisch eine neue Protokolldatei im Ordner „Preferences“.

Weshalb wird Norton Personal Firewall nicht geladen?

Wenn Sie sehr viele Systemerweiterungen verwenden und den virtuellen Speicher deaktiviert haben, liegt möglicherweise ein Konflikt mit einer anderen Systemerweiterung vor. Aktivieren Sie versuchsweise den virtuellen Speicher oder entfernen Sie nicht benötigte Systemerweiterungen.

Weshalb funktioniert File Sharing nicht?

Möglicherweise haben Sie File Sharing über TCP/IP aktiviert. Standardmäßig wird für alle TCP/IP-Dienste jeglicher Zugriff verweigert. Sie müssen den Zugriff auf den Dienst ‚File Sharing‘ zulassen, damit dieser Dienst wieder verfügbar ist.

Fragen zu lokalen Netzwerken

Wie kann ich alle Computer in meinem lokalen Netzwerk schützen?

Installieren Sie eine Kopie von Norton Personal Firewall nur auf Computern mit Zugang zum Internet. Für andere Computer im Netzwerk, die keinen Zugang zum Netzwerk haben, ist Norton Personal Firewall nicht nötig.

Sie sollten aber eine Kopie von Norton Personal Firewall auf allen Computern mit Airport Anbindung installieren.

Wie wird der Zugriff für einen Computer mit dynamisch zugeordneter IP-Adresse eingerichtet?

Computer, die ihre eigene IP-Adresse über DHCP (Dynamic Host Configuration Protocol) abrufen, haben im Normalfall bei jeder Verbindung mit einem Netzwerk eine andere IP-Adresse. Allerdings liegen diese verwendeten IP-Adressen in einem bestimmten Bereich. Sie können diesen Bereich ermitteln, indem Sie im Fenster „Zugriffsverlauf“ nach Einträgen mit verweigerten Zugriffen für den betreffenden Computer suchen und sich die jeweils verwendeten IP-Adressen notieren. Danach können Sie einen IP-Adressbereich für den Dienst definieren, auf den der Computer zugreifen soll.

Weitere Informationen über das Fenster „Zugriffsverlauf“ finden Sie im Abschnitt „So zeigen Sie das Fenster „Zugriffsverlauf“ an:“ auf Seite 34. Informationen über das Definieren eines IP-Adressbereichs finden Sie im Abschnitt „So fügen Sie einen Adressbereich hinzu:“ auf Seite 44.

Wie wirkt sich die Firewall auf das File Sharing und auf gemeinsam genutzte Drucker aus?

Norton Personal Firewall schützt TCP/IP-Verbindungen. Die Software hat keinen Einfluss auf AppleTalk Verbindungen. Wenn Sie wollen, dass andere Computer per File Sharing über TCP/IP auf Ihren Computer zugreifen können, müssen Sie die IP-Adressen dieser anderen Computer in die Liste der für den Dienst ‚File Sharing‘ zugriffsberechtigten IP-Adressen aufnehmen.

Informationen darüber, wie Sie den Zugriff auf einen Dienst zulassen, finden Sie im Abschnitt „IP-Adressen hinzufügen“ auf Seite 43.

A N H A N G

A

Programmdateien aktualisieren

LiveUpdate hilft Ihnen, Ihre Programmdateien stets auf dem neuesten Stand zu halten. Wenn Sie über einen Internet-Zugang verfügen, ist LiveUpdate die effizienteste Methode zum Aktualisieren Ihrer Dateien.

Wenn Sie America Online (AOL) als Internet Service Provider (ISP) verwenden, müssen Sie sich bei AOL anmelden, bevor Sie LiveUpdate verwenden können. Weitere Informationen finden Sie im Abschnitt „LiveUpdate mit America Online verwenden“ auf Seite 69.

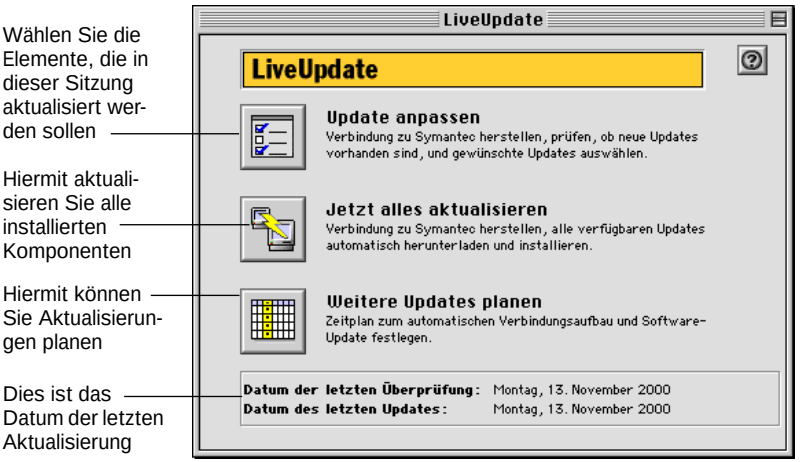
Info über LiveUpdate

Symantec ermöglicht Ihnen mit Ihrem Abonnement den Online-Zugang zu aktualisierten Programmdateien.

LiveUpdate verwendet Ihren vorhandenen Internet-Zugang, um eine Verbindung zum LiveUpdate-Server von Symantec herzustellen, sieht nach, ob neue Virusdefinitionen und Programm-Updates vorhanden sind, lädt diese automatisch herunter und installiert sie auf Ihrem Computer.

Programmdateien aktualisieren

Sie können bestimmen, dass LiveUpdate in einem Arbeitsgang nach Updates für alle Dateien suchen soll, die Auswahl für die Update-Funktion anpassen oder ein Ereignis für eine künftige LiveUpdate-Sitzung planen.



LiveUpdate lädt die verfügbaren Updates herunter und installiert sie auf Ihrem Computer. In einem Dialogfenster wird der Verlauf der Dateiübertragung angezeigt.

Die Dateiübertragung dauert einige Minuten. Wenn sie beendet ist, werden Sie von LiveUpdate informiert.

Sie werden ebenfalls informiert, wenn Ihre Dateien aktualisiert wurden.

So aktualisieren Sie Ihre Programmdateien mit LiveUpdate:

1. Klicken Sie im Hauptfenster von Norton Personal Firewall auf „LiveUpdate“.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf „Jetzt alles aktualisieren“, wenn Sie alle Dateien aktualisieren wollen.
   - Klicken Sie auf „Update anpassen“, um anzugeben, was in dieser Sitzung aktualisiert werden soll.

     Weitere Informationen finden Sie im Abschnitt „So passen Sie eine LiveUpdate-Sitzung an:“ auf Seite 67.
   - Klicken Sie auf „Weitere Updates planen“, um LiveUpdate Scheduler zu starten und LiveUpdate-Ereignisse zu planen.

     Weitere Informationen finden Sie im Abschnitt „So planen Sie ein LiveUpdate-Ereignis:“ auf Seite 68.
3. Klicken Sie auf „Schließen“.
4. Klicken Sie auf „Neustart“, wenn Sie von LiveUpdate zum Neustarten Ihres Computers aufgefordert werden.
5. Wählen Sie „Beenden“ aus dem Menü „Ablage“.

Papierkorb nach der Verwendung von LiveUpdate leeren

Nachdem Sie Ihre Programmdateien mit LiveUpdate aktualisiert haben, befinden sich einige Objekte im Papierkorb. LiveUpdate verschiebt ältere, nicht mehr benötigte Dateien in den Papierkorb. Leeren Sie den Papierkorb. Wenn Sie nach der Installation der Anwendung noch keinen Neustart durchgeführt haben, wird eventuell die Meldung angezeigt, dass diese Dateien gerade verwendet werden. Nach einem Neustart können Sie den Papierkorb leeren.

Datei „What's New“ für LiveUpdate

LiveUpdate legt auf dem Schreibtisch die Datei „What's New“ ab. Sie enthält Informationen über die Dateien, die von LiveUpdate aktualisiert wurden.

So lesen Sie die Datei „What's New“:

- Doppelklicken Sie auf die Datei „What's New“, um die Informationen über die aktualisierten Dateien zu lesen.

  Die Datei wird in SimpleText geöffnet.

So schließen Sie die Datei „What's New“:

- Drücken Sie **Befehlstaste-Q**, um SimpleText zu beenden.

So löschen Sie die Datei „What's New“:

- Ziehen Sie die Datei auf den Papierkorb.

Versionsnummern und Datumsangaben überprüfen

Sie werden von LiveUpdate mit Versionsnummern und Statusangaben darüber informiert, ob Ihre Programmdateien auf dem aktuellen Stand sind. Das Datum der Programmdatei wird auch im Fenster „Über“ angezeigt, das Sie über das Menü „Apple“ öffnen können.

So zeigen Sie das Dialogfenster „Über“ für eine Anwendung an:

1 Starten Sie Norton Personal Firewall.

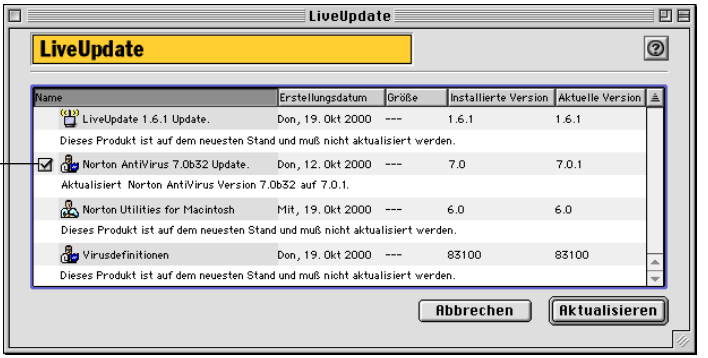
2 Wählen Sie „Über Norton Personal Firewall“ aus dem Menü „Ablage“.

Im Dialogfenster „Über“ werden die Versionsnummer und die Datumsangaben für das Copyright angezeigt.

3 Klicken Sie auf „OK“, um das Fenster „Über“ wieder zu schließen.

LiveUpdate-Sitzungen anpassen

Mit LiveUpdate können Sie einzelne Elemente aktualisieren und alle Elemente auslassen, die nicht aktualisiert werden sollen.



Wählen Sie die Elemente, die in dieser Sitzung aktualisiert werden sollen

So passen Sie eine LiveUpdate-Sitzung an:

1 Klicken Sie im Fenster von LiveUpdate auf „Update anpassen“.

LiveUpdate ermittelt daraufhin die Anwendungen, die auf Ihrem Volume installiert sind, und zeigt eine Liste der dafür verfügbaren Updates an.

2 Wählen Sie die Elemente, die in dieser Sitzung aktualisiert werden sollen.

LiveUpdate berücksichtigt die nicht ausgewählten Elemente nicht. Wenn Ihre Dateien bereits auf dem aktuellen Stand sind, können keine Elemente ausgewählt werden.

3 Klicken Sie auf „Aktualisieren“.

Die Dateiübertragung dauert einige Minuten. Wenn sie beendet ist, werden Sie von LiveUpdate informiert.

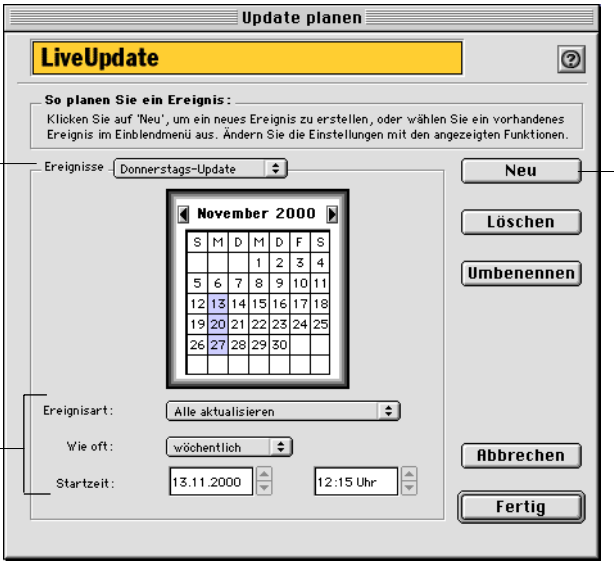
Sie werden ebenfalls informiert, wenn Ihre Dateien aktualisiert wurden.

LiveUpdate-Ereignisse planen

Sie können automatische LiveUpdate-Sitzungen zum Aktualisieren Ihrer Programmdateien planen. Verwenden Sie dazu LiveUpdate Scheduler; mit dieser Komponente können Sie Ereignisse planen, die zum vorgegebenen Zeitpunkt automatisch ausgeführt werden.

So planen Sie ein LiveUpdate-Ereignis:

1 Klicken Sie im Hauptfenster von LiveUpdate auf „Weitere Updates planen“.



Wählen Sie einen Ereignisnamen

Hiermit fügen Sie ein neues Ereignis hinzu

Wählen Sie hier Art, Zeitpunkt und Häufigkeit für das Ereignis

2 Klicken Sie im Dialogfenster „Update planen“ auf „Neu“.

3 Geben Sie den Namen für das Ereignis ein.

4 Klicken Sie auf „OK“.

5 Geben Sie die Ereignisart an und legen Sie fest, wie oft das Ereignis ausgeführt werden soll und wann es das erste Mal ausgeführt werden soll.

Die Tage, an denen Updates bereitgestellt werden, sind im Kalender hervorgehoben. Die Tage für andere geplante Ereignisse sind unterstrichen.

6 Geben Sie nun die geplante Zeit und das Datum für die Aktualisierung ein.

- Klicken Sie auf das **Stundenfeld** und stellen Sie mit den Pfeiltasten die gewünschte Stunde ein.
- Klicken Sie danach auf das **Minutenfeld** und stellen Sie die Minuten ein.

Damit das geplante LiveUpdate-Ereignis ausgeführt werden kann, muss Ihr Computer zum vorgesehenen Zeitpunkt eingeschaltet sein. Ist Ihr Computer zum bewussten Zeitpunkt nicht eingeschaltet, wird LiveUpdate gestartet, wenn Sie Ihren Computer das nächste Mal starten.

7 Klicken Sie auf „Fertig“.

LiveUpdate mit America Online verwenden

Wenn Sie America Online (AOL) als Internet Service Provider (ISP) verwenden, müssen Sie sich eventuell erst bei AOL anmelden, bevor Sie LiveUpdate verwenden können.

So verwenden Sie LiveUpdate mit AOL:

1 Melden Sie sich bei AOL an.

2 Klicken Sie auf der Begrüßungsseite von AOL auf den AOL Internet-Browser.

3 Starten Sie LiveUpdate.

4 Führen Sie die Schritte im Abschnitt „So aktualisieren Sie Ihre Programmdateien mit LiveUpdate:“ auf Seite 65 aus.

5 Beenden Sie AOL, wenn die LiveUpdate-Sitzung zu Ende ist.

Wenn Sie von LiveUpdate zu einem Neustart Ihres Computers aufgefordert werden, trennen Sie die Verbindung zu AOL, bevor Sie den Neustart veranlassen.

G L O S S A R

Die folgenden Begriffe werden bei ihrem ersten Auftreten im Text durch *Kursivschrift.* hervorgehoben.

AppleTalk	Ein Protokoll, das von bestimmten Geräten in einem Netzwerk (z. B. Drucker und Server) für die Kommunikation verwendet wird.
DHCP	Dynamic Host Configuration Protocol. Ein Dienst, mit dem IP-Adressen den Geräten in einem Netzwerk dynamisch zugeordnet werden.
Domain Name System (DNS)	Ein Dienst, der Hostnamen in IP-Adressen umsetzt.
Firewall	Ein Filter, der Verbindungen und Datenübertragungen über das Internet blockiert oder zulässt.
FTP	File Transfer Protocol. Ein Anwendungsprotokoll, das für die Übertragung von Dateien zwischen Computern verwendet wird.
Hacker	Eine Person, die sich unbefugt Zugang zu Fremdcomputern mit dem Ziel verschafft, in den Besitz der Informationen auf diesen Computern zu kommen oder Schaden auf diesen Computern anzurichten.
Hostname	Ein Name, der einen Computer in einem Netzwerk identifiziert. Der Hostname der Website von Symantec lautet z. B. ‚www.symantec.com'. Hostnamen werden mit DNS in IP-Adressen umgesetzt.
Internet	Ein dezentralisiertes, weltweites Netzwerk, über das Millionen von Computern miteinander verbunden sind.
Internet-Protocol-Adresse (IP-Adresse)	Eine Zahl, die einen Computer im Internet eindeutig identifiziert.
PPP	Point-to-Point Protocol. Ein Verfahren für Verbindungen zum Internet, das Funktionen für die Fehlerprüfung bereitstellt.
Protokoll	Ein Regelwerk für die Kommunikation und die Datenübertragung zwischen Computern. Beispiele für Protokolle sind HTTP und FTP.

Proxy-Server	Ein Server, der eine von einem Client an einen anderen Server gerichtete Anforderung für diesen anderen Server zu erfüllen versucht. Kann die Anforderung nicht erfüllt werden, wird sie an den eigentlichen Zielserver weitergeleitet. Proxy-Server werden eingesetzt, um die Geschwindigkeit im Web zu erhöhen und um Anforderungen an das Web zu filtern.
TCP/IP	Transmission Control Protocol/Internet Protocol. Ein Sammelbegriff für Protokolle, die im Auftrag des US-Verteidigungsministeriums für die Errichtung weltweiter Netzwerke entwickelt wurden. TCP wird für eingesetzt, um Fehler bei der Datenübertragung zu erkennen und zu korrigieren; IP wird für die Datenübertragung verwendet.
Teilnetz	Ein lokales Netzwerk, das Bestandteil eines größeren Intranet oder des Internet ist.
Teilnetzmaske	Ein Code in Form einer IP-Adresse, mit der Computer feststellen können, wie viele Teile einer IP-Adresse für die Identifikation eines Teilnetzes und wie viele Teile für die Identifikation eines einzelnen Computers innerhalb dieses Teilnetzes erforderlich sind.
Trojanisches Pferd	Ein Programm, das getarnt als attraktives Angebot (z. B. als legale Kopie eines Softwareprogramms) bei einem bestimmten auslösenden Ereignis unerwartete Vorgänge auf einem Computer startet.
UDP	User Datagram Protocol. Ein einfaches Protokoll, mit dem Informationen ohne Empfangsbestätigung und ohne Zustellgarantie ausgetauscht werden.
Verbindungsabhängiges Protokoll	Ein Protokoll, das eine bestehende Verbindung für die Übertragung eines Informationspakets erfordert.
Verbindungsloses Protokoll	Ein Protokoll, das ein Datenpaket an eine Zieladresse in einem Netzwerk sendet, ohne zuvor die Verbindung herzustellen.
Virus	Ein kleines Programm, das entwickelt wurde, sich zu replizieren und zu verbreiten, in der Regel ohne Wissen des Benutzers.
Webserver	Ein Computer mit einer Serversoftware, der angeforderte Web-Inhalte an Ihren Browser sendet.

I N D E X

H

I

K

L

M

N

P

R

S

T

U

V

W

Z

Symantec-Lösungen für Service und Unterstützung

Symantec bemüht sich weltweit um ausgezeichnete Serviceleistungen. Unser Ziel ist, Ihnen professionelle Hilfestellung bei der Anwendung unserer Software zu leisten und professionelle Dienste anzubieten – ganz gleich, in welchem Land.

Die Angebote für Service und Unterstützung sind von Land zu Land unterschiedlich. Wenn Sie Fragen zu den unten beschriebenen Dienstleistungen haben, lesen Sie bitte den Abschnitt „Alle Kontaktinformationen auf einen Blick“ am Ende dieses Kapitels.

Wenn Sie dieses Produkt zusammen mit Ihrem Computer erworben haben, erhalten Sie unter Umständen auch Unterstützung vom dem entsprechenden Computer-Hersteller.

Registrierung Ihres Symantec-Produkts

Die Registrierung Ihres Symantec-Produkts berechtigt Sie, die technische Unterstützung zu beanspruchen, Ersatzkopien von Datenträgern und Handbüchern anzufordern sowie andere wertvolle Serviceleistungen zu nutzen. Sie können Ihr Symantec-Produkt auf eine der folgenden Weisen registrieren:

- Füllen Sie das Online-Registrierformular von Symantec aus:

  http://www.symantec.com/region/de/techsupp/forms/register_form.html
- Während des Installationsvorgangs (wenn Ihr Symantec-Produkt über diese Funktion verfügt).
- Sie können sich telefonisch durch einen Anruf beim Kundenservice-Center von Symantec registrieren. Die Telefonnummern werden am Ende dieses Kapitels unter „Alle Kontaktinformationen auf einen Blick“ aufgeführt.
- Wenn Ihrem Produkt eine Registrierkarte beiliegt, füllen Sie diese bitte aus und senden Sie sie an die angegebene Adresse.
- Sollte sich Ihre Adresse ändern, können Sie Symantec davon verständigen, indem Sie das Online-Adreßänderungsformular an folgender Stelle ausfüllen:

  http://www.symantec.com/region/de/techsupp/forms/change_address_form.html.

Sie können Ihre neuen Adreßangaben dem Kundenservice von Symantec auch telefonisch mitteilen.

Virendefinitions-Updates

Wenn Ihr Softwareprogramm über die Funktion „LiveUpdate“ verfügt, können Sie auf die Schaltfläche „LiveUpdate“ klicken, um Virusdefinitionen automatisch herunterzuladen und zu installieren. Virusdefinitionsdateien sind ebenfalls im Internet an folgender Adresse erhältlich:

http://www.symantec.com/avcenter/index.html

Gehen Sie folgendermaßen vor, um Ihre Virendefinitionen zu aktualisieren:

- Klicken Sie auf die Grafik „Definitions Updates“, oder klicken Sie in der Liste „Sections“ auf „Download Updates“.
- Klicken Sie unten auf der Seite auf „Download Virus Definition Updates“.
- Wählen Sie Ihre Sprache und das Produkt aus.
- Wählen Sie den entsprechenden Dateinamen für Ihr Produkt aus.
- Geben Sie einen Verzeichnispfad auf Ihrer Festplatte an, in dem die heruntergeladene Datei gespeichert werden soll.
- Wenn das Download abgeschlossen ist, navigieren Sie im Windows Explorer zu der Datei, und doppelklicken Sie darauf.

Nach Abschluss des Updates befinden sich Ihre Virendefinitionen auf dem neuesten Stand.

Erneuern des Abonnements für Virendefinitions-Updates

Wenn Sie es vorziehen, können Sie sich Updates von Virusdefinitionen auch von Symantec per Post zuschicken lassen. Um diesen Service zu abonnieren, wenden Sie sich bitte an das örtliche Symantec-Kundenservice-Center. Die Nummern für Ihr Kundenservice-Center finden Sie am Ende dieses Kapitels unter „Alle Kontaktinformationen auf einen Blick“.

Der Kauf von Norton AntiVirus berechtigt Sie ein Jahr lang zum Bezug kostenloser Virendefinitionen über das Internet. Nach diesem Zeitraum können Sie über die Symantec-Website ein Jahresabonnement für eine nominale Gebühr erstehen. Die Symantec-Website können Sie nachstehend unter „Regionale Sites“ nachschlagen. Nachdem Sie diese Site aufgerufen haben, klicken Sie auf „Shop Symantec“ und wählen Sie „Virus-Update-Abonnement“.

Informationen zu anderen Kaufmethoden erhalten Sie über Ihr örtliches Symantec-Kundenservice-Center . Die Telefonnummern für Ihr Kundenservice-Center finden Sie am Ende dieses Kapitels unter „Alle Kontaktinformationen auf einen Blick“.

Ältere Versionen von Symantec-Produkten

Wenn auf Ihrem Rechner ein Norton 2000-Produkt installiert ist, wird die LiveAdvisor-Schaltfläche in der Menüleiste bei der Installation eines Norton 2001-Produkts entfernt. Da LiveAdvisor nicht länger zur Übermittlung von Informationen verwendet wird, geht Ihnen dadurch jedoch keine Funktionalität verloren. Wie Ihnen in den endgültigen LiveAdvisor-Nachrichten mitgeteilt wurde, hat Symantec die LiveAdvisor-Übermittlungsmethode durch Informationen an den folgenden Stellen ersetzt:

Symantec-Websites:

AntiVirus Research Center

www.symantec.com/avcenter/index.html

Regionale Sites:

- **Europa/Englisch:** www.symantec.com/eusupport/
- **Deutschland:** www.symantec.de/desupport/
- **Schweiz:** www.symantec.ch/chsupport/

Produktspezifische Newsbulletins:

US/Englisch:
http://www.symantec.com/techsupp/bulletin/index.html

Service und Unterstützung

Symantec bietet eine Reihe technischer und nicht-technischer Optionen für Unterstützung, die auf Ihre individuellen Anforderungen zugeschnitten sind und Ihnen helfen, Ihre Software bestmöglich zu nutzen. Kostenloser Support ist auf den Symantec-Webseiten für Service und Unterstützung sowie durch das Faxabrufsystem von Symantec erhältlich.

World Wide Web und FTP

Auf Symantecs Internet-Site haben Sie uneingeschränkten Zugriff auf technische und nicht-technische Informationen sowie auf Informationen über unser Unternehmen und unsere Produkte. Die Website bietet Ihnen folgendes:

- Im Abschnitt „Häufig gestellte Fragen (FAQs)“ finden Sie eine Zusammenstellung häufig auftretender Fragen zu Symantec-Produkten und die entsprechenden Antworten.
- Durchsuchen Sie die technischen und nicht-technischen Unterstützungsdatenbanken (Knowledge Bases – Online-Zusammenstellungen technischer und nicht-technischer Fragen und der jeweiligen Antworten).
- Senden Sie eine Nachricht an eine der Diskussionsgruppen, bei denen technische Fragen eingereicht werden können. Ein technischer Mitarbeiter von Symantec wird innerhalb eines Arbeitstages antworten.

Weiterhin haben Sie die Möglichkeit, den Service- und Unterstützungsassistenten zu verwenden, mit dem Sie leicht an die gewünschten Informationen gelangen können.

Bitte schlagen Sie am Ende dieses Kapitels unter „Alle Kontaktinformationen auf einen Blick“ die Adressen für die Symantec-Website „Service und Unterstützung“ nach.

Wenn Ihr Softwareprogramm über die Funktion „LiveUpdate“ verfügt, können Sie auf die Schaltfläche „LiveUpdate“ klicken, um Software-Updates und Virusdefinitionen automatisch herunterzuladen und zu installieren. Zugriff auf Produkt-Updates und Virusdefinitionen kann auch über die Website für Service und Unterstützung erfolgen, oder Sie können sich direkt zu unserer FTP-Site begeben, um dort technische Hinweise und Software-Patches herunterzuladen:

ftp.symantec.com

Faxabrufsystem (FOD: Fax On Demand)

Das Faxabrufsystem von Symantec kann 24 Stunden täglich benutzt werden, um allgemeine Produktinformationen oder technische Hinweise mit Ihrem Faxgerät zu empfangen. Die für Ihr Land gültige Faxabrufnummer finden Sie im Abschnitt „Alle Kontaktinformationen auf einen Blick“ am Ende dieses Kapitels.

Telefon-Support

Symantec bietet gebührenpflichtige telefonische Unterstützung für Konsumerprodukte an. Kunden können auf einer Pro-Anfrage-Basis Unterstützung direkt von einem Mitarbeiter des technischen Supports oder auf der Basis eines Jahresabonnements über den Kundenservice erhalten.

Bitte wenden Sie sich für Informationen und Beratung bezüglich des Symantec-Serviceangebots an das Kundenservice-Center von Symantec. Die Telefonnummer Ihres lokalen Kundenservice-Centers können Sie dem Abschnitt „Alle Kontaktinformationen auf einen Blick“ am Ende dieses Kapitels entnehmen.

Unterstützung für ältere oder eingestellte Versionen

Nachdem eine neue Version (Upgrade) eines Produkts auf den Markt kommt, ist für eine begrenzten Zeitraum nach dem Erscheinen der neuen Version weiterhin technische Unterstützung für die Vorgängerversion erhältlich. Technische Informationen sind eventuell noch über die Symantec-Website und das Faxabrufsystem zu erhalten.

Wenn Symantec bekannt gibt, daß ein Produkt nicht mehr vermarktet oder verkauft wird, steht der gebührenpflichtige technische Support dafür nur noch 60 Tage zur Verfügung. Weitere Unterstützung zu ausgelaufenden Produkten können Sie danach nur noch über das Faxabrufsystem oder Dokumente auf der Website von Symantec erhalten.

Kundenservice

Das Symantec-Kundenservice-Center hilft Ihnen bei nicht-technischen Anfragen, beispielsweise:

- Allgemeine Produktinformationen (z. B. Leistungsmerkmale, Preise, Sprachverfügbarkeit, Händler in Ihrer Nähe usw.)
- Hilfe bei einfachen Problemen, z. B. wie Sie Ihre Versionsnummer überprüfen können
- Neueste Informationen zu Produkt-Updates und -Upgrades
- Wie Sie Ihr Produkt aktualisieren oder eine neue Version (Upgrade) installieren können
- Versand von Produktliteratur oder Testversionen
- Ersatz fehlender oder defekter CDs, Handbücher, usw.

- Aktualisierung Ihrer Registrierungsdaten bei Adreß- oder Namensänderungen
- Bestellung von Norton AntiVirus-Abonnements
- Informationen zu den Optionen für technische Unterstützung durch Symantec
- Beratung zu den Optionen der technische Unterstützung von Symantec
- Bestellung von Abonnements für technische Unterstützung für Konsumerprodukte

Ausführliche Kundenservice-Informationen können Sie auf der Symantec-Website für Service und Unterstützung nachschlagen oder durch einen Anruf beim Kundenservice-Center von Symantec erhalten. Bitte schlagen Sie die Webadressen und die Nummer Ihres lokalen Kundenservice-Centers im Abschnitt „Alle Kontaktinformationen auf einen Blick“ am Ende dieses Kapitels nach.

Alle Kontaktinformationen auf einen Blick

Symantec-Websites für Service und Unterstützung

- **Europa/Englisch:** www.symantec.com/eusupport/
- **Deutschland:** www.symantec.de/desupport/
- **Schweiz:** www.symantec.com/chsupport/
- **Symantec FTP:** ftp.symantec.com
  (Herunterladen von technischen Hinweisen und neuesten Patches)

Besuchen Sie „Symantec Service und Unterstützung“ im Web. Dort können Sie die Datenbank des technischen und nicht-technischen Supports durchsuchen, häufig gestellte Fragen (FAQs) zu Produkten lesen, Ihre Frage an eine der Diskussionsgruppen senden und vieles mehr. Mit dem Service- und Unterstützungsassistenten können Sie schnell und einfach die gewünschten Informationen finden. Verwenden Sie die Übersicht, wenn Sie bereits wissen, wo sich die gewünschten Informationen befinden. Aus praktischen Gründen sind die Optionen in der Übersicht in technische und nicht-technische Kategorien aufgeteilt.

Technische Unterstützung von Symantec

Symantec bietet KOSTENLOSEN technischen Support über die Website für Service und Unterstützung. Bitte beachten Sie, daß es sich bei der technischen Unterstützung per Telefon um einen gebührenpflichtigen Service handelt.

Utilities-Produkte	Lokale Telefonnummern (für andere Länder siehe unter „Desktop-Unterstützung“)
Norton SystemWorks Norton CleanSweep Norton CrashGuard Norton Utilities für DOS/ Win 3.1, Win95, NT, MAC Norton Commander Win95/NT Norton Ghost (Endbenutzer)	Deutschland: + (49) 69 6641 0371 Großbritannien: + (44) 20 7744 0061 Frankreich: + (33) 1 64 53 80 73 Holland: + (31) 71 408 3958

Norton Internet Security und andere, oben nicht aufgeführte Utilities werden nur über das Web unterstützt.

AntiVirus	Lokale Telefonnummern (für andere Länder siehe unter „Desktop-Unterstützung“)
Norton AntiVirus Win 98/95, NT, Win3.1/DOS, Macintosh	Deutschland: + (49) 69 6641 0353 Großbritannien: + (44) 20 7616 5813 Frankreich: + (33) 1 64 53 80 63 Holland: + (31) 71 408 3952

Remote-Produktivitätslösungen	Lokale Telefonnummern (für andere Länder siehe unter „Desktop-Unterstützung“)
WinFax/TalkWorks pcAnywhere for 95/NT pcAnywhere DOS, Win 3.1, CE	Deutschland: + (49) 69 6641 0350 Großbritannien: + (44) 20 7616 5803 Frankreich: + (33) 1 64 53 80 60 Holland: + (31) 71 408 3951

Desktop-Unterstützung, andere Länder

Österreich: + 43 (1) 501375023	Norwegen: + 47 23053330
Belgien: + 32 (2) 7131701	Polen: 0-0800 311 1269
Dänemark: + 45 35 445720	Südafrika: + (27) 11 7849856
Finnland: + 358 (9) 22 930417	Spanien: + (34) 91 6625255
Irland: + 353 (1) 6011901	Schweden: + (46) 8 7355024
Israel: 1-800-9453805	Schweiz: + (41) 1 2121847
Italien: + 39 054228062	Türkei: 90 212 213 42 65

Faxabrufsystem

Über das Faxabrufsystem (FOD: Fax On Demand) von Symantec können Sie menügesteuert Produktliteratur anfordern. Wenn Sie die entsprechende Nummer für Ihr Land anrufen, werden Sie durch ein Menü von Optionen geführt, die über die Telefontastatur gewählt werden können. Die ausgewählten Informationen werden automatisch an Ihr Faxgerät übermittelt.

Belgien	+ (32) 2 7131710
Dänemark	+ 45 35 445710
Deutschland	+ (49) 69 6641 0310
Finnland	+ (358) 9 22 930411
Frankreich	+ (33) 1 64 53 80 52
Großbritannien	+ (44) 20 7616 5710
Italien	+ 39 024827 0010
Luxemburg	+ (352) 29 84 795022
Niederlande	+ (31) 71 4083790
Norwegen	+ 47 23 053310
Österreich	+ (43) 1 50 137 5022
Schweden	+ (46) 751 5681
Schweiz	+ (41) 1 2126267
Spanien	+ (34) 91 662 4021

Symantec-Kundenservice

Bietet mehrsprachige nichttechnische Informationen und Beratung per Telefon.

Belgien	+ (32) 2 7131700
Dänemark	+ 45 35 44 57 00
Deutschland	+ (49) 69 6641 0300
Finnland	+ (358) 9 22 930410
Frankreich	+ (33) 1 64 53 80 50
Großbritannien:	+ (44) 20 7616 5600
Irland	+ (353) 1 811 8032
Italien	+ 39 02 48270000
Luxemburg	+ 352 29 84 79 50 20
Niederlande	+ (31) 20 5040565
Norwegen	+ 47 23 05 33 00
Österreich	+ (43) 1 50 137 5020
Schweden	+ (46) 8 703 9615
Schweiz	+ (41) 1 2126262
Spanien	+ (34) 91 6624413
Südafrika	+ (27) 11 784 9855
Andere Länder (nur englischsprachige Dienste)	+ (353) 1 811 8032

Symantec-Kundenservice – Postanschrift

Symantec Ltd.

Customer Service Centre

Europe, Middle East and Africa (EMEA)

PO Box 5689

Dublin 15

Irland

Für Südafrika

Symantec SA (Pty) Ltd

PO Box 1998

Gallo Manor, Sandton

2052 South Africa

Wir haben uns um größtmögliche Genauigkeit der Informationen in diesem Dokument bemüht. Diese Informationen unterliegen jedoch gelegentlichen Veränderungen. Symantec Corporation behält sich das Recht vor, solche Änderungen ohne vorherige Ankündigung vorzunehmen.