PRODUKTHANDBUCH

McAfee Firewall

VERSION 4.0

McAfee SECURITY

Inhalt

Willkommen bei McAfee Firewall 4.0 1

Schützen Sie sich, während Sie online sind, mit den umfassenden Sicherheitsmöglichkeiten von McAfee Firewall. McAfee Firewall ist einfach zu bedienen und doch in hohem Maße konfigurierbar. Dank der Firewall ist Ihr PC bei jeder Verbindung mit dem Internet geschützt, egal ob die Verbindung über DSL, Kabelmodem oder Analogmodem aufgebaut wird. Mit einem Angriffserkennungssystem, farbcodierten Sicherheitswarnungen, anpassbaren akustischen Warnungen, detaillierter Protokollierung und der Analyse von Internet-fähigen Anwendungen bietet McAfee Firewall Ihnen alle erforderlichen Funktionen, die gewährleisten, dass sich bei Ihren Aufenthalten im Internet Sicherheit und Spaß nicht ausschließen müssen.

McAfee Firewall:

- überwacht die Freigabe von Dateien und Druckern.
- zeigt an, wer eine Verbindung mit Ihrem Computer herstellen möchte (wenn Sie den gemeinsamen Zugriff erlauben).
- schützt das Betriebssystem vor eingehenden Floods und anderen Angriffspaketen.
- verhindert, dass nicht vertrauenswürdige Anwendungen Verbindungen über das Netzwerk herstellen.
- bietet detaillierte Informationen über die von Ihnen aufgerufenen Sites und über die Art der Verbindung.
- kann sofort den gesamten Datenverkehr oder nur den Verkehr von einer bestimmten IP-Adresse blockieren.

Verbesserungen und neue Funktionen in dieser Version

- **Firewall-Sicherheitsprüfung:** Untersucht Ihre Sicherheitseinstellungen auf mögliche Schwachstellen.
- **Verbesserte Hacker-Verfolgung:** Durch die Integration von McAfee Visual Trace.
- **Angriffserkennungssystem:** Erkennt übliche Angriffsarten und verdächtige Aktivitäten.

- **PC-Netzwerk-Assistent:** Schützt PCs, die gemeinsam eine Internet-Verbindung verwenden.
- **Assistent zum Erstellen benutzerdefinierter Regeln:** Erstellen Sie benutzerdefinierte Konfigurationen für spezielle Programme.
- **Kennwortschutz:** Verhindern Sie, dass andere Ihre Firewall-Einstellungen ändern, indem Sie sie durch ein Kennwort schützen.
- **Verbesserte Unterstützung von Breitbandverbindungen.**
- **Verbesserungen bei der Bedienung:** McAfee Firewall 4.0 enthält zahlreiche Verbesserungen der Benutzeroberfläche, die Ihnen die Sicherung Ihres Computers erleichtern.

Funktionsweise von McAfee Firewall

McAfee Firewall ist ein einfach zu bedienendes Sicherheitstool, das im Hintergrund arbeitet und die Sicherheit Ihres Computers dynamisch verwaltet.

Setup

Während der Installation werden Ihnen vom Konfigurationsassistenten einige grundlegende Fragen zur Einrichtung von McAfee Firewall gestellt. Damit wird sichergestellt, dass die entsprechenden Tasks an Ihre Erfordernisse angepasst werden (z. B. ob Dateien freigegeben werden oder nicht).

Arbeitsweise

McAfee Firewall filtert den Datenverkehr an den von Ihrem System verwendeten Geräten, z. B. Netzwerkkarten und Modems. Das bedeutet, dass eingehender Verkehr blockiert werden kann, bevor er elementare Funktionen Ihres Computers beeinträchtigen und wertvolle Systemressourcen binden kann.

McAfee Firewall – der Wächter

McAfee Firewall überwacht während der Ausführung vertrauenswürdige und nicht vertrauenswürdige Programme, die eine Verbindung über das Internet herstellen. Im Falle eines vertrauenswürdigen Programms schränkt McAfee Firewall die Funktion des Programms in keinerlei Weise ein. Wenn ein nicht vertrauenswürdiges Programm versucht, eine Verbindung zu oder von Ihrem Computer aufzubauen, blockiert McAfee Firewall den Verbindungsversuch über das Internet.

Konfiguration

Bestimmte Netzwerkverbindungen sind zur Ausführung netzwerkbasierter Services unerlässlich. Diese werden mithilfe benutzerdefinierter Regeln in den Systemeinstellungen von McAfee Firewall verwaltet. Die Standardsystemeinstellungen bieten einen weit reichenden Schutz vor gefährlichen Bedrohungen.

Überblick über dieses Handbuch

In diesem Handbuch finden Sie die wichtigsten Informationen für die Installation und Einrichtung von McAfee Firewall sowie für die ersten Schritte in diesem Programm. Weitere Informationen zum Ausführen von Tasks in McAfee Firewall finden Sie in der Online-Hilfe. Während der Arbeit in den unterschiedlichen Fenstern und Dialogfeldern können Sie die Hilfe jederzeit aufrufen. Darüber hinaus können Sie die Datei Readme.txt lesen, die weitere allgemeine Informationen, bekannte Probleme usw. zu diesem Produkt enthält.

Häufig gestellte Fragen

Im Folgenden finden Sie einige häufig gestellte Fragen, die Sie sich kurz anschauen sollten:

Wie kann mir McAfee Firewall helfen?

McAfee Firewall schützt Ihren PC im Netzwerk. Das Programm fungiert sozusagen als Wächter, der jedes ein- oder ausgehende Datenpaket einzeln überprüft. Dabei dürfen nur die Pakete passieren, die explizit zugelassen sind.

McAfee Firewall ist einfach anzuwenden und bietet gleichzeitig einen hervorragenden Schutz. Wenn Firewall installiert und aktiv ist, werden bekannte Angriffe automatisch abgewehrt. Darüber hinaus können Sie selbst entscheiden, ob die Kommunikation zwischen bestimmten Anwendungen zulässig ist.

Welchen Gefahren ist ein PC im Internet ausgesetzt?

Wenn Sie mit dem Internet verbunden sind, nutzen Sie das Netzwerk gemeinsam mit Millionen anderer Nutzer aus der ganzen Welt. Dies ist eine fantastische Sache, die aber auch Gefahren birgt, da schließlich auch Fremde auf Ihren PC zugreifen können.

Während Sie mit dem Internet verbunden sind, sollten Sie deshalb die entsprechenden Sicherheitsvorkehrungen treffen, um Ihren Computer zu schützen. Beim Einsatz von IRC-Programmen (Internet Relay Chat) sollten Sie besonders Dateien gegenüber misstrauisch sein, die Ihnen von Fremden geschickt werden. Programme zum Remote-Zugriff auf Ihren Computer, z. B. Back Orifice (BO), werden häufig auf diesem Weg verbreitet. Es ist grundsätzlich ratsam, erhaltene Dateien mithilfe eines Antivirenprogramms, z. B. McAfee VirusScan, zu scannen, bevor Sie die Dateien bzw. Dateianhänge öffnen.

Solange Sie mit dem Internet verbunden sind, können Fremde möglicherweise versuchen, auf Ihre freigegebenen Dateien zuzugreifen. Sie sollten deshalb darauf achten, dass freigegebene Dateien nur Ihnen vertrauten Personen zugänglich sind. Ansonsten können Fremde Dateiinhalte auf Ihrem Computer lesen und Dateien löschen.

Welche Schutzmaßnahmen sind darüber hinaus erforderlich?

McAfee Firewall schützt Ihr System auf Netzwerkebene. Weitere wichtige Schutzmechanismen sind z. B.:

- Antivirenprogramme zum Schutz der Anwendungen.
- Anmeldebildschirme und Kennwörter für Bildschirmschoner zum Verhindern unerlaubter Zugriffe.
- Dateiverschlüsselung bzw. Verschlüsselung von Dateisystemen, um die Vertraulichkeit der Daten zu gewährleisten.
- Systemstart-Kennwörter, sodass Ihr PC von niemand anderem gestartet werden kann.
- Schutz des Computers vor physischem Zugriff, z. B. Diebstahlsicherung für Festplatte.

Eine ganz andere, jedoch nicht minder wichtige Schutzmaßnahme besteht darin, den Zugriff auf Informationen, Fehlinformationen und „Datenmüll“, wie er im Internet zuhauf anzutreffen ist, zu kontrollieren. Sie können eine Vielzahl von Diensten oder Programmen einsetzen, z. B. McAfee Internet Security, mit deren Hilfe der Inhalt von Datenpaketen gefiltert und der Zugriff auf bestimmte Sites eingeschränkt werden kann.

Gibt es auch Datenpakete, die McAfee Firewall nicht aufhalten kann?

Eingehende Daten: Nein. Solange McAfee Firewall ein Netzwerkgerät unterstützt und aktiv ist, werden alle eingehenden Pakete abgefangen und anschließend je nach Konfiguration zugelassen oder blockiert. Wenn Sie festgelegt haben, dass alle Daten blockiert werden sollen, dann geschieht dies auch.

Ausgehende Daten: Ja und nein. McAfee Firewall fängt ausgehende Datenpakete bei der Weitergabe an den Netzwerk-Gerätetreiber ab. Nach diesem Prinzip kommunizieren alle gängigen Anwendungen. Bösartige Programme können jedoch unter Umständen andere Wege wählen.

Welche Netzwerkgeräte werden von McAfee Firewall unterstützt?

McAfee Firewall unterstützt Ethernet-Geräte sowie Geräte, die nach dem Ethernet-Prinzip arbeiten. Dazu gehören Einwählverbindungen, ein Großteil der Kabel- und ISDN-Modems sowie die meisten Ethernet-Karten. Nicht unterstützt werden Token Ring, FDDI, ATM, Frame Relay und andere Netzwerke.

Welche Protokolle können von McAfee Firewall gefiltert werden?

McAfee Firewall kann TCP/IP, UDP/IP, ICMP/IP und ARP filtern. Es werden alle Protokolle abgefangen, wobei bestimmte, wie z. B. IPX, entweder zugelassen oder blockiert werden müssen – hierfür erfolgt keine Filterung. Für die Kommunikation im Internet werden IP-Protokolle verwendet. Es werden keine weiteren Protokolle gesendet. Darüber hinaus sind IP-Netzwerke mit Abstand am weitesten verbreitet.

Wie kann das System trotz McAfee Firewall angegriffen werden?

Viele Benutzer schützen sich mithilfe von McAfee Firewall vor Nuke-Angriffen, die die IRC-Verbindungen ihres Systems unterbrechen. Diese Nukes werden von McAfee Firewall abgewehrt. Allerdings gibt es noch andere Möglichkeiten, um die Verbindungen zu unterbrechen.

- **Serverseitige Nukes**: In diesem Fall werden die Nukes nicht an Ihren Computer, sondern direkt an den IRC-Server gesendet, wobei diesem mitgeteilt wird, dass Ihr Computer nicht mehr erreichbar ist. Um dies zu verhindern, benötigt der IRC-Server eine Firewall.
- **Flood-Blockierung einer TCP-Verbindung**: Wenn an Ihr System über eine schnellere Verbindung ein Paket-Flood gesendet wird, kann McAfee Firewall die Pakete zwar stoppen, doch der Flood beansprucht die gesamte Bandbreite der Verbindung. Die Folge ist, dass Ihr System nichts mehr senden kann. Benutzer, die sich über das DFÜ-Netzwerk einwählen, sind durch Angriffe dieser Art besonders gefährdet, da es sich dabei um die langsamste Verbindung handelt.

TIPP

Weitere häufig gestellte Fragen finden Sie in der Datei Readme.txt.

Installation von McAfee Firewall 4.0 2

Mit dem Setup-Programm auf der McAfee Firewall 4.0-Installations-CD können Sie das Programm problemlos auf Ihrem Computer installieren. Nach dem Einlegen der CD-ROM in das CD-ROM-Laufwerk sollte die Installation automatisch starten. Die Informationen im folgenden Abschnitt helfen Ihnen bei der Installation und ersten Verwendung von McAfee Firewall.

Systemanforderungen

Um McAfee Firewall verwenden zu können, benötigen Sie:

- Microsoft Windows XP Home Edition, Windows XP Professional Edition, Windows 2000 Professional, Windows Me, Windows 98 oder Windows 98 SE.
- mindestens Internet Explorer 4.01, Service Pack 2 oder höher, IE 5.01 oder höher wird empfohlen.
- PC mit einem Pentium 100-MHz-Prozessor oder höher.
- 32 MB Arbeitsspeicher.
- 30 MB Festplattenspeicher.
- CD-ROM-Laufwerk.
- Internet-Zugriff für verschiedene Funktionen.

Überblick über Winsock 2

McAfee Firewall verwendet eine API (Application Programming Interface), die von Winsock vor Version 2.0 nicht unterstützt wird. McAfee Firewall überprüft bei der Installation automatisch, ob Winsock 2 vorhanden ist. Wenn dies nicht der Fall ist, wird der Benutzer entsprechend informiert. Wenn der neueste Browser installiert ist (d. h. Internet Explorer 6), ist diese Komponente bereits enthalten, und Sie erhalten diese Meldung nicht. Andernfalls können Sie das Upgrade kostenfrei von der folgenden Website herunterladen: http://www.microsoft.com. Das Upgrade steht auch auf anderen Websites zur Verfügung.

Installationsschritte

Zur Vermeidung von Installationsproblemen sollten Sie vor der Installation von McAfee Firewall alle offenen Programme schließen, einschließlich der Programme, die im Hintergrund laufen, z. B. Bildschirmschoner und Virenscanner.

Nach dem Einlegen der McAfee Firewall 4.0-Installations-CD in das CD-ROM -Laufwerk sollte automatisch ein Autorun-Bildschirm angezeigt werden. Um die McAfee Firewall-Software sofort zu installieren, klicken Sie auf **McAfee Firewall installieren**. Fahren Sie dann mit dem Setup bei Schritt 5 fort.

Führen Sie die folgenden Schritte zur Installation der Software aus.

1. Wenn auf Ihrem Computer Windows 2000 Professional oder Windows XP läuft, melden Sie sich bei dem Computer als Benutzer mit Administratorrechten an. Zur Installation der Software sind Administratorrechte zwingend erforderlich.
2. Legen Sie die McAfee Firewall 4.0-CD in das CD-ROM-Laufwerk ein. Wenn der Installationsassistent nicht automatisch angezeigt wird, gehen Sie zu Schritt 3. Andernfalls wechseln Sie zu Schritt 4.
3. Gehen Sie folgendermaßen vor, wenn das Autorun-Installationsmenü nicht angezeigt wird oder wenn Sie die Software von der McAfee-Website heruntergeladen haben.
    a. Wählen Sie im Windows-Startmenü die Option **Ausführen**. Das Dialogfeld **Ausführen** wird angezeigt.
    b. Geben Sie in das Textfeld „<X>:\SETUP.EXE“ ein, und klicken Sie auf **OK**.
4. <X> steht dabei für den Laufwerksbuchstaben Ihres CD-ROM -Laufwerks bzw. für den Pfad zu dem Ordner, der die entpackten McAfee Firewall-Dateien enthält. Um nach der entsprechenden Datei auf der Festplatte oder CD-ROM zu suchen, klicken Sie auf **Durchsuchen**.
    a. Bevor die Installation fortgesetzt wird, überprüft Setup zuerst, ob das MSI-Dienstprogramm (Microsoft Windows Installer) als Teil der System-Software ausgeführt wird. Wenn auf Ihrem Computer Windows XP läuft, ist die aktuelle Version von MSI bereits vorhanden. Wenn Sie eine ältere Version von Windows verwenden, wurde MSI möglicherweise trotzdem schon von einer anderen Software auf Ihrem Computer installiert. In beiden Fällen zeigt Setup sofort das erste Fenster des Assistenten an. Fahren Sie mit Schritt 5 fort.

b Wenn Setup keine MSI-Version auf Ihrem Computer findet, installiert es die zum Fortsetzen der Installation benötigten Dateien. Sie werden danach aufgefordert, den Computer neu zu starten. Klicken Sie auf **System neu starten**. Nach dem Neustart wird das Setup an der Stelle fortgesetzt, an der es unterbrochen wurde.

5 Folgen Sie den vom Installationsassistenten angezeigten Schritten, um die Installation abzuschließen.

TIPP
Wenn auf Ihrem Computer nicht die entsprechenden Schriftarten zur Anzeige der Endbenutzer-Lizenzvereinbarung (EULA) installiert sind, finden Sie eine korrekt dargestellte EULA-Version auf der McAfee-Installations-CD. Um die Installation abzuschließen, müssen Sie die Bedingungen der Vereinbarung gelesen und akzeptiert haben.

HINWEIS
Bei allen Windows 2000 Professional-Installationen ist für McAfee Firewall ein eindeutiger Treiber erforderlich. Während der Installation werden mehrere Warnmeldungen angezeigt, die Sie darüber informieren, dass Sie versuchen, einen nicht signierten Treiber zu installieren. Klicken Sie jedes Mal auf **OK**, um den Treiber zu installieren, und starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.

Fehlerbehebung für Installationsprobleme

Eine fehlgeschlagene Installation kann zu Software-Problemen führen, die sich schwer zurückverfolgen lassen. Die Hauptursachen für fehlgeschlagene Installationen sind:

- Die Installation wird ausgeführt, während andere Software läuft.
- Temporäre Dateien verhindern die Installation.
- Festplattenfehler.

Führen Sie die folgenden Schritte aus, um die Auswirkungen dieser häufig anzutreffenden Bedingungen für die Installation zu minimieren.

Schritt 1: Schließen anderer Software

Deaktivieren Sie sämtliche Software, die im Hintergrund ausgeführt wird:

1 Halten Sie die Strg- und Alt-Taste gedrückt, und drücken Sie einmal die Entf-Taste. Das Dialogfeld **Anwendung schließen** wird angezeigt.

2 Klicken Sie für alle Einträge außer für den Explorer auf **Task beenden**.

3 Wiederholen Sie die Schritte 2 und 3, bis alle Programme außer dem Explorer geschlossen sind.

4 Wenn im Dialogfeld **Anwendung schließen** nur noch der Explorer angezeigt wird, klicken Sie auf **Abbrechen**.

Schritt 2: Entfernen temporärer Dateien

Löschen Sie den Inhalt des Temp-Ordners in Windows:

1 Doppelklicken Sie auf dem Desktop auf das Symbol **Arbeitsplatz**. Das Fenster **Arbeitsplatz** wird geöffnet. Doppelklicken Sie auf **C:**. Es wird jetzt der Inhalt der Festplatte angezeigt.

2 Doppelklicken Sie auf den Ordner **Windows**.

3 Doppelklicken Sie im Ordner **Windows** auf den Ordner **Temp**.

4 Klicken Sie im Menü **Bearbeiten** auf den Befehl **Alles markieren**. Alle Elemente im Ordner **Temp** sind jetzt markiert.

5 Drücken Sie auf der Tastatur die Entf-Taste, um die Dateien zu löschen. Wenn Sie von Windows aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **Ja**.

6 Klicken Sie in der Windows-Taskleiste auf **Start** und dann auf **Beenden**.

7 Aktivieren Sie im Fenster **Windows beenden** die Option **Neu starten**, und klicken Sie auf **OK**, um den PC neu zu starten.

Schritt 3: Prüfen der Festplatte

Führen Sie die Windows-Festplattendienstprogramme **ScanDisk** und **Defragmentierer** aus, um Fehler auf Ihrer Festplatte zu finden und zu beheben:

1 Klicken Sie auf **Start**, und zeigen Sie nacheinander auf **Programme**, **Zubehör** und **Systemprogramme**. Klicken Sie dann auf **ScanDisk**.

2 Wählen Sie im Fenster **ScanDisk** die Optionen **Standard** und **Fehler automatisch korrigieren**.

3 Klicken Sie auf **Erweitert**. Prüfen Sie, ob im Dialogfeld **Erweiterte ScanDisk-Optionen** die folgenden Einstellungen aktiviert sind:

- Nur bei Fehler
- Protokoll ersetzen
- Löschen
- Freigeben

4 Die anderen Optionen können Sie ignorieren. Klicken Sie auf **OK**. Klicken Sie auf **Starten**. ScanDisk untersucht jetzt Ihre Festplatte auf Fehler. In Abhängigkeit von der Größe der Festplatte kann dieser Vorgang mehrere Minuten dauern.

5 Schließen Sie ScanDisk nach Abschluss des Scan-Vorgangs.

6 Klicken Sie auf **Start**, und zeigen Sie nacheinander auf **Programme**, **Zubehör** und **Systemprogramme**. Klicken Sie dann auf **Defragmentierung**.

7 Klicken Sie auf **OK**, um den Defragmentierer zu starten. In Abhängigkeit von der Geschwindigkeit des Computers und der Größe der Festplatte kann dieser Vorgang mehrere Minuten dauern.

8 Schließen Sie den Defragmentierer, nachdem die Festplatte defragmentiert wurde.

Entfernen oder Ändern der McAfee Firewall-Installation

Wenn auf Ihrem Computer ...

- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional Edition

... läuft, müssen Sie sich beim Computer als Benutzer mit Administratorrechten anmelden.

Gehen Sie anschließend folgendermaßen vor:

1 Starten Sie in der Windows-Systemsteuerung das Applet **Software**.

2 Wählen Sie **McAfee Firewall**, und klicken Sie auf:

   - **Entfernen**, um McAfee Firewall vom Computer zu entfernen.
   - **Ändern**, um die McAfee Firewall-Installation zu ändern.

3 Folgen Sie den vom McAfee Firewall-Installationsassistenten angezeigten Schritten, um die Änderungen abzuschließen.

   Folgen Sie der Setup-Aufforderung, und starten Sie den Computer neu.

Wichtige Informationen zur Windows XP-Migration

Beim Upgrade des Betriebssystems von einer älteren Version auf Windows XP werden alle vor der Migration installierten McAfee-Produkte deaktiviert.

Sie werden auf diesen Sachverhalt beim ersten Starten eines McAfee-Produkts nach der Migration hingewiesen und aufgefordert, das Produkt neu zu installieren.

Dazu müssen Sie alle McAfee-Produkte deinstallieren und anschließend mithilfe der Installations-CD oder der von McAfee heruntergeladenen Software neu installieren.

Erste Schritte mit McAfee Firewall 4.0 3

Nach der Installation müssen Sie McAfee Firewall für den Einsatz konfigurieren. Der Konfigurationsassistent ist Ihnen bei diesem Vorgang behilflich.

Der Konfigurationsassistent

Begrüßungsbildschirm

Der McAfee Firewall-Konfigurationsassistent wird beim ersten Starten von McAfee Firewall angezeigt. Dieser Assistent führt Sie durch das Setup und aktiviert McAfee Firewall auf Ihrem Computer. Mithilfe der Schaltflächen **Zurück**, **Weiter**, **Abbrechen** und **Fertig stellen** können Sie durch die Bildschirme des Konfigurationsassistenten navigieren.

Wenn Sie auf einem beliebigen Bildschirm des Konfigurationsassistenten auf **Abbrechen** klicken, halten Sie den Aktivierungs- und Konfigurationsvorgang an. **Sie müssen den Konfigurationsassistenten beim ersten Mal bis zum Ende ausführen, damit McAfee Firewall aktiviert und einsatzbereit ist.**

Netzwerksteuerungseinstellungen

Über die Netzwerksteuerungseinstellungen legen Sie fest, wie McAfee Firewall reagieren soll, wenn ein Programm versucht, auf das Internet zuzugreifen (eingehend oder abgehend).

1. Wählen Sie auf dem Begrüßungsbildschirm von McAfee Firewall eine der folgenden Optionen für die Netzwerksteuerungseinstellungen.

Tabelle 3-1. Netzwerksteuerungseinstellungen für McAfee Firewall

Einstellung für Internet-Verkehr	Beschreibung
Alles blockieren	Konfiguriert McAfee Firewall so, dass der gesamte eingehende und abgehende Internet-Verkehr auf Ihrem Computer blockiert wird. Dies ist die sicherste Firewall-Einstellung. Die auf dem Computer installierten Programme können in diesem Fall jedoch nicht auf das Internet zugreifen.

Tabelle 3-1. Netzwerksteuerungseinstellungen für McAfee Firewall

Einstellung für Internet-Verkehr	Beschreibung
Alles filtern	Lässt Sie selbst entscheiden, ob eine auf Ihrem Computer installierte Anwendung bzw. ein Programm auf das Internet zugreifen darf. Wenn ein unerkanntes Programm versucht, über das Internet auf Ihren Computer zuzugreifen, können Sie ebenfalls entscheiden, ob Sie den Zugriff gestatten oder verwehren möchten.
Alles zulassen	Konfiguriert McAfee Firewall so, dass der gesamte eingehende und abgehende Internet-Verkehr auf Ihrem Computer zugelassen wird. Alle auf dem Computer installierten Programme dürfen auf das Internet zugreifen. Programme, die versuchen, über das Internet auf Ihren Computer zuzugreifen, werden nicht abgewehrt. Die Option **Alles zulassen** deaktiviert alle McAfee Firewall-Schutzfunktionen und sollte insofern nur zu Diagnosezwecken gewählt werden.

2 Klicken Sie auf **Weiter**.

Programmstart-Optionen

In diesem Bildschirm können Sie auswählen, welche Aktionen McAfee Firewall beim Starten des Computers ausführen soll.

Es gibt verschiedene empfohlene Startoptionen, die bereits vorausgewählt sind.

1 Wählen Sie **McAfee Firewall bei Rechnerstart automatisch starten**, wenn McAfee Firewall zusammen mit dem Computer gestartet werden soll. Wenn McAfee Firewall beim Starten des Computers nicht gestartet werden soll, deaktivieren Sie dieses Kontrollkästchen.

2 Wenn auf dem Windows-Desktop ein McAfee Firewall-Symbol angezeigt werden soll, wählen Sie **McAfee Firewall-Symbol auf dem Desktop platzieren**. Wenn auf dem Windows-Desktop kein Symbol angezeigt werden soll, deaktivieren Sie dieses Kontrollkästchen.

3 Klicken Sie auf **Weiter**.

Zugriff auf Freigaben

Wenn Ihr Computer Teil einer Arbeitsgruppe ist, z. B. eines Heimnetzwerkes, können Sie McAfee Firewall so konfigurieren, dass andere auf die Netzwerkfreigaben Ihres Computers zugreifen können und Sie Zugriff auf die Freigaben anderer Computer haben. **Freigaben** sind Ressourcen, z. B. Laufwerke, Verzeichnisse, Dateien oder Drucker, die einer Arbeitsgruppe oder über ein Heimnetzwerk verbundenen Computern gemeinsam zur Verfügung stehen.

1. **Zugriff auf die Freigaben anderer Computer**: Aktivieren Sie das Kontrollkästchen **Mein Computer soll Zugriff auf die Freigaben fremder Computer haben**, wenn Sie mit Ihrem Computer Zugriff auf freigegebene Laufwerke, Verzeichnisse, Dateien, Drucker usw. anderer Computer in Ihrer Arbeitsgruppe oder im Heimnetzwerk haben möchten.

2. **Zugriff auf eigene Freigaben**: Aktivieren Sie das Kontrollkästchen **Andere Computer sollen Zugriff auf meine Freigaben haben**, wenn Sie anderen Computern in Ihrer Arbeitsgruppe oder im Heimnetzwerk den Zugriff auf Ihre freigegebenen Laufwerke, Verzeichnisse, Dateien, Drucker usw. gestatten möchten.

3. Klicken Sie auf **Weiter**.

Zulässige Anwendungen

Während des Konfigurationsvorgangs hat McAfee Firewall die Festplatte Ihres Computers nach Programmen durchsucht, die auf das Internet zugreifen. Zu diesen Programmen gehören Internet-Browser, Internet-E-Mail-Programme und FTP-Clients (File Transfer Protocol). In diesem Bildschirm legen Sie die Programme fest, denen Sie den Zugriff auf das Internet über McAfee Firewall gestatten.

Wenn Sie für einzelne Programme den Zugriff auf das Internet zulassen möchten, gehen Sie wie folgt vor:

1. Aktivieren Sie auf der in diesem Bildschirm angezeigten Liste die Kontrollkästchen für jene Anwendungen, denen Sie den Zugriff auf das Internet ermöglichen möchten.

   Klicken Sie auf **Alle Laufwerke durchsuchen**, um alle Partitionen, logischen Laufwerke und physischen Festplatten Ihres Computers nach Programmen zu durchsuchen, die Verbindungen zum Internet aufbauen.

Wenn Sie bestimmten oder allen Anwendungen in diesem Bildschirm den Internet-Zugriff nicht gestatten, wird für diese Programme bei jedem Zugriffsversuch eine entsprechende Benachrichtigung ausgegeben, und Sie können entscheiden, ob Sie den Zugriff in diesem Fall gewähren möchten.

2 Klicken Sie nun auf **Fertig stellen**.

Nächster Schritt

Nachdem Sie die Schritte für die erste Konfiguration abgeschlossen haben, werden folgende Aktionen ausgeführt:

1 Der Firewall-Dienst startet.

2 Die McAfee Firewall-Startseite wird geöffnet.

McAfee Firewall ist jetzt einsatzbereit!

TIPP
Bei früheren Versionen von McAfee Firewall konnten Sie den Konfigurationsassistenten nur einmal ausführen. In McAfee Firewall 4.0 können Sie den Assistenten jetzt jederzeit über die leicht zugängliche Verknüpfung auf der McAfee Firewall-Startseite aufrufen.

McAfee Firewall-Startseite

Abbildung 3-1. McAfee Firewall-Startseite

Das Hauptfenster von McAfee Firewall ist Ihr zentraler Einstiegspunkt für alle Tasks, erweiterten Tasks und gemeinsam genutzten Funktionen von McAfee Firewall. Die McAfee Firewall-Oberfläche besteht aus drei Bereichen, die allen McAfee Firewall-Bildschirmen gemeinsam sind.

Titelleiste und Symbolleiste

Titelleiste

Auf der Startseite werden verschiedene Windows-Standardelemente angezeigt:

- Die Titelleiste zeigt den Namen des aktuell ausgeführten Programms an.
- Schaltflächen **Schließen** und **Minimieren**. Die Länge und Breite der Benutzeroberfläche von McAfee Firewall sind unveränderlich. d. h., die Größe des Fensters kann nicht verändert werden.

Symbolleiste

Die Symbolleiste enthält vier browserähnliche Schaltflächen, die auf allen Bildschirmen angezeigt werden.

- **Zurück**: Klicken Sie auf **Zurück**, um zum vorherigen Bildschirm zurückzugelangen.
- **Home**: Klicken Sie auf **Home**, um von einem beliebigen Bildschirm aus zur McAfee Firewall-Startseite zurückzugelangen.
- **Weiter**: Mit den Schaltflächen **Weiter** und **Zurück** können Sie zwischen den Bildschirmen hin- und herwechseln, die Sie im Verlauf der Sitzung angezeigt haben.
- **Hilfe**: Klicken Sie auf **Hilfe**, um das Untermenü für die Hilfe anzuzeigen. Das Untermenü **Hilfe** kann beliebige der folgenden Elemente enthalten.

Untereintrag im Hilfemenü	Funktion
Hilfe auf dieser Seite	Ruft die Online-Hilfe zum aktuellen Bildschirm auf.
Inhalt und Index	Anzeigen der Online-Hilfe zu McAfee Firewall
Hilfe im Internet	Startet Ihren Internet-Browser und führt Sie direkt zur Hilfe-Website von McAfee unter „mcafeehilfe.com“.
McAfee at Home im Internet	Startet Ihren Internet-Browser und führt Sie direkt zu „McAfee-at-home.com/international/germany“.
Überblick über McAfee Firewall	Versionsinformationen zu McAfee Firewall

Statusinformationen

Je nach Konfiguration werden auf der McAfee Firewall-Startseite weitere nützliche Informationen angezeigt, beispielsweise:

- Firewall-Status: **Wird ausgeführt** oder **Gestoppt**. Durch Klicken auf die Verknüpfung unter der Statusinformation können Sie McAfee Firewall starten bzw. stoppen.
- Startseitenbenachrichtigung: Wenn ein Update für Ihre Version von McAfee Firewall zur Verfügung steht, wählen Sie diesen Task aus, um die neue Version herunterzuladen.
- Die Anzahl der momentan aktiven Programme: Klicken Sie auf diesen Task, um die gegenwärtig aktiven Programme anzuzeigen.
- Firewall-Warnhinweise: Wählen Sie diesen Task, um bei Verbindungswarnungen das Protokoll mit den Warnungen anzuzeigen.

Einstellungen für Internet-Verkehr

Im Bereich für die Internet-Verkehr-Einstellungen wird die aktuelle Filtereinstellung angezeigt. Sie können hier eine der folgenden Optionen für den Internet-Verkehr auswählen: **Alles blockieren**, **Alles zulassen** oder **Filtern**. Weitere Informationen zu diesen Einstellungen finden Sie in Tabelle 3-1 auf Seite 17.

Um die Einstellung für den Internet-Verkehr zu ändern, müssen Sie lediglich auf die gewünschte neue Einstellung klicken. Die Änderungen werden in Echtzeit ausgeführt und treten sofort in Kraft.

Status von McAfee Firewall

In diesem Bereich der Startseite wird der aktuelle Status von McAfee Firewall angezeigt. Die Firewall ist entweder aktiviert oder deaktiviert.

Status von McAfee Firewall	Aktion
McAfee Firewall wird ausgeführt	◆ Klicken Sie auf **McAfee Firewall stoppen**, um den Firewall-Schutz zu deaktivieren.
McAfee Firewall wurde gestoppt	◆ Klicken Sie auf **McAfee Firewall starten**, um den Firewall-Schutz zu aktivieren.

Überwachung des Netzwerkverkehrs

Die Überwachung des Netzwerkverkehrs zeigt eine grafische Darstellung der Netzwerkaktivitäten in Echtzeit an. Die Darstellung ist farbcodiert, sodass Sie normalen Netzwerkverkehr, Port-Scans und im schlimmsten Falle Angriffe schnell erkennen können.

- **Grüner Bereich**: In diesem Bereich angezeigte Aktivitäten stellen normalen Netzwerkverkehr dar. Es ist nicht ungewöhnlich, wenn Aktivitäten in diesem Bereich bis in den gelben Bereich reichen.
- **Gelber Bereich**: Bei dieser Zone ist Vorsicht geboten. Sie sollten das Aktivitätsprotokoll anzeigen, um die mit diesem Verkehr verbunden Daten zu überprüfen. Aktivitäten im gelben Bereich können auf einen Port-Scan hindeuten.
- **Roter Bereich**: Aktivitäten im roten Bereich stellen den schlimmsten Fall dar und sind in der Regel auf Angriffe zurückzuführen. Sie können die Details eines Angriffs im McAfee Firewall-Aktivitätsprotokoll einsehen. Wenn die IP-Adresse des Angreifers angezeigt wird, können Sie versuchen, mithilfe der McAfee Firewall-Komponente Visual Trace den Angreifer zurückzuverfolgen.

Task-Bereich

Der Task-Bereich enthält Verknüpfungen, mit denen Sie die **Tasks** und die **erweiterten Tasks** starten können. Je nach Konfiguration zeigt der Task-Bereich eine Task-Liste an. Diese Task-Liste enthält Verknüpfungen, mit denen Sie die Startseite beliebiger anderer auf Ihrem Computer installierten McAfee-Produkte aufrufen können.

Überblick über Tasks

Um einen Task zu starten, müssen Sie lediglich auf die entsprechende Verknüpfung klicken. Die wichtigsten Komponenten von McAfee Firewall können über die Taskliste gestartet werden. Welche Tasks Sie ausführen können, hängt vom Betriebssystem Ihres Computers und dessen Konfiguration ab. Zu den primären Tasks zählen:

- **Internet-Anwendungen überwachen**: Dieser Task erlaubt es, speziellen Anwendungen den Zugriff auf das Internet explizit zu verbieten bzw. zu erlauben.
- **Netzwerkaktivität anzeigen**: Über diesen Task können Sie die Netzwerkaktivitäten (in Echtzeit) und das aktuelle Aktivitätsprotokoll anzeigen.
- **Warneinstellungen festlegen**: Wählen Sie aus, wie McAfee Firewall Sie über eine potenzielle Sicherheitsverletzung benachrichtigen soll.
- **Heimnetzwerk einrichten**: Hilft Ihnen beim Einrichten der Schutzeinstellungen, wenn mehrere PCs eine Internet-Verbindung nutzen.
- **Sicherheitsprüfung durchführen**: Mit diesem Task starten Sie die Sicherheitsüberprüfung von McAfee Firewall.
- **Programmstart-Optionen festlegen**: Wählen Sie aus, wie McAfee Firewall gestartet werden soll.
- **Konfigurationsassistent**: Dieser Task startet den Konfigurationsassistenten.

Überblick über erweiterte Tasks

Ähnlich wie bei der primären Taskliste ist der Umfang der Liste mit den erweiterten Tasks von der Windows-Version, der Konfiguration und anderer eventuell auf Ihrem Computer installierter Software abhängig. Zu den erweiterten Tasks von McAfee Firewall gehören:

- **Erweiterte Optionen und Protokollierung**: Wählen Sie diesen Task, um die Verteidigung gegen Angriffe zu konfigurieren, die automatische Konfiguration von Filterregeln einzurichten und die zu protokollierende Verkehrsart festzulegen.

- **Netzwerkadapter konfigurieren**: Wählen Sie diesen Task, um Ihre aktuellen Netzwerkadapter anzuzeigen und deren Verbindungseinstellungen zu konfigurieren.
- **Einstellungen zur Angriffserkennung**: Über diesen Task legen Sie fest, wie McAfee Firewall auf einen erkannten Angriff reagiert.
- **IP-Adressen blockieren**: Wählen Sie diesen Task, wenn Sie Ihrem Computer den Zugriff auf eine bestimmte IP-Addresse verwehren bzw. wenn Sie den Zugriff auf eine blockierte IP-Adresse zulassen möchten.
- **Kennwort einrichten**: Mit diesem Task können Sie ein Kennwort zum Schutz Ihrer McAfee Firewall-Einstellungen einrichten.
- **Weitere Tasks**: Mit diesem Task wechseln Sie zu einem Bildschirm, in dem Sie die gemeinsam genutzten Funktionen von McAfee Firewall starten können.

Überblick über die McAfee-Liste

Die McAfee-Liste enthält Verknüpfungen, mit denen Sie die Startseiten beliebiger anderer unterstützter McAfee-Produkte aufrufen können.

Andere Funktionen von McAfee Firewall

Sicherheitsprüfung für McAfee Firewall-Einstellungen

Untersucht Ihre Firewall-Sicherheitseinstellungen und ermöglicht Ihnen, unzureichende Einstellungen zu korrigieren, bevor diese Schwachstellen von Hackern ausgenutzt werden. Die Sicherheitsprüfung der McAfee Firewall-Einstellungen markiert Schwachstellen und schlägt Verbesserungen vor, die die optimale Sicherheit Ihres Systems gewährleisten.

Wenn die Sicherheitsprüfung auf ein Problem stößt, können Sie auf **Beheben** klicken. McAfee Firewall hilft Ihnen dann bei der Analyse und Korrektur des potenziellen Problems.

PC-Netzwerk-Assistent

Ein Assistent hilft Ihnen beim Einrichten der Schutzeinstellungen, wenn mehrere PCs eine Internet-Verbindung nutzen.

Alle Netzwerkmedien und -Hardware (z. B. Kabel und Netzwerkadapter) müssen auf jedem Computer installiert sein, damit der Assistent die Computer erkennen kann.

Kennwortschutz

Durch den Kennwortschutz können Sie verhindern, dass andere Personen auf Ihre Firewall-Einstellungen zugreifen und sie verändern können. Außerdem können Sie ausschließen, dass der Firewall-Schutz ohne Eingabe des Kennworts deaktiviert wird.

Überblick über Visual Trace

Visual Trace ist ein vielseitiges Tool, das zum Suchen der benötigten Informationen im Internet und zur Fehlerbehebung bei Verbindungsproblemen verwendet wird.

Auf der einfachsten Ausführungsebene kann mit Visual Trace sichtbar gemacht werden, wie (Daten-)Pakete von Ihrem Computer zu einem anderen Computer im Internet gelangen. Dabei werden alle Knoten (Geräte zur Weiterleitung von Datenverkehr im Internet) zwischen Ihrem Computer und dem Verfolgungsziel angezeigt.

Diese Informationen sind in vielen Situationen von großer Bedeutung. Visual Trace kann zur Fehlerbehebung bei Verbindungsproblemen ebenso eingesetzt werden wie in Fällen, in denen lediglich bestätigt werden soll, dass alle Vorgänge ordnungsgemäß ablaufen. Darüber hinaus erhalten Sie mit Visual Trace zahlreiche nützliche Informationen, z. B. über den Domäneninhaber, über relative Standorte und in vielen Fällen auch über die tatsächlichen Standorte von Knoten.

Neben der Suche nach den Schwachstellen einer Verbindung kann Visual Trace im Rahmen der folgenden Aufgaben eingesetzt werden:

- Feststellen der Ursache für die Unerreichbarkeit einer Site. Liegt der Fehler beim Internet-Dienstanbieter oder in einem entfernteren Bereich des Internets?
- Bestimmen der Position des Netzwerkfehlers, auf Grund dessen die Website nicht erreichbar ist.
- Bestimmen der Standorte von Sites und deren Benutzern, Identifizieren des Besitzers einer Site und Zurückverfolgen des Ursprungs unerwünschter E-Mail-Nachrichten („Spam“).
- Abrufen detaillierter Kontaktinformationen zu Sites in der ganzen Welt (sofern vorhanden).

Aufrufen von Visual Trace

Sie können Visual Trace direkt über das Windows-Startmenü aufrufen. Außerdem können Sie Visual Trace über den Bildschirm **McAfee Firewall – Detailaktivitäten**, das Dialogfeld **IP-Adressen blockieren** und, im Falle eines Angriffs, über die Popup-Benachrichtigung in der Windows-Taskleiste starten.

Weitere Informationen über Visual Trace finden Sie in der Online-Hilfe zu Visual Trace.

McAfee Firewall 4.0 -Konfigurationen 4

Überblick

Die Konfiguration von McAfee Firewall ist in zwei Kategorien eingeteilt: Anwendung (Programm) und System. Bei der Installation werden einige grundlegende Regeln für Systemdienste, z. B. ICMP, DHCP und ARP, eingerichtet (diese werden als Standardeinstellungen betrachtet).

Die Kategorisierung der Programme wird von Ihnen vorgenommen. Immer wenn Sie ein neues Programm ausführen, das versucht, eine Verbindung über das Internet herzustellen, fragt Sie McAfee Firewall, ob Sie das Programm als vertrauenswürdig einstufen möchten.

Geben Sie beispielsweise in Internet Explorer in der Adressleiste eine Internet-Adresse ein (z. B. http://www.mcafee-at-home.com/international/germany/), und drücken Sie die EINGABETASTE. Internet Explorer versucht daraufhin, eine Internet-Verbindung zu der angegebenen Adresse herzustellen. Beim ersten Versuch werden Sie von McAfee Firewall gefragt, ob Sie Internet Explorer „vertrauen". Wenn Sie „Ja" angeben, merkt sich McAfee Firewall, dass Internet Explorer eine zugelassene Anwendung ist. Bei jeder weiteren Verwendung von Internet Explorer erlaubt McAfee Firewall den Verkehr automatisch.

Indem Sie Programmen den Verbindungsaufbau über das Internet gestatten, „erlernt" McAfee Firewall die programmspezifischen Regeln und speichert sie für die spätere Verwendung. Wenn ein trojanisches Pferd versucht, eine Verbindung zum Internet herzustellen, werden Sie in gleicher Weise von McAfee gefragt, ob Sie dem Programm „vertrauen". Sie können so einfach und ohne Zeitverlust verhindern, dass das trojanische Pferd eine Verbindung zum Internet aufbaut.

Programmkonfiguration

Beim ersten Start von McAfee Firewall werden Sie vom Konfigurationsassistenten aufgefordert, jene Programme festzulegen, die über das Internet kommunizieren dürfen. Dabei erstellt McAfee Firewall einen Standardsatz von Kommunikationsregeln für die Programme (Anwendungen). Diese werden als für die Kommunikation **zugelassen** gekennzeichnet.

McAfee Firewall erkennt den Programmtyp, z. B. Internet-Browser, E-Mail-, FTP-, IRC- und Filesharing-Programm, und erstellt einen Standardsatz von Kommunikationsregeln für jedes auf Ihrem Computer installierte Programm. D. h., dass jeder Verbindungsversuch über das Internet entweder blockiert, zugelassen oder gefiltert wird.

Firewall-Kommunikationswarnungen

Eine **McAfee Firewall-Kommunikationswarnung** wird angezeigt, wenn ein nicht erkanntes Programm versucht, eine Verbindung herzustellen. Es kann mehrere Gründe geben, warum ein Programm nicht erkannt wird.

- Wenn Sie ein Programm, das mit dem Internet kommuniziert, nach McAfee Firewall installieren, wird beim ersten Verbindungsversuch eine Warnmeldung angezeigt.
- Auch wenn der Konfigurationsassistent eine sorgfältige Analyse der Programme auf Ihrem Computer durchführt, die mit dem Internet kommunizieren, kann es vorkommen, dass er nicht alle entsprechenden Programme identifizieren kann.

Wenn ein unerkanntes Programm versucht, eine Verbindung herzustellen, wird eine Warnmeldung eingeblendet. In dieser werden Sie aufgefordert, eine der folgenden Optionen zu wählen:

- **Nein, dieses Mal verweigern**: Blockiert den aktuellen und alle zukünftigen Verbindungsversuche durch das Programm. Das aktive Programm wird zur Liste der vertrauenswürdigen Programme mit dem Status „blockiert“ hinzugefügt.
- **Ja, dieses Mal zulassen**: Der aktuelle Versuch zum Herstellen einer Verbindung wird zugelassen. Das Programm wird jedoch nicht zur Liste der vertrauenswürdigen Programme hinzugefügt.
- Wenn Sie das Programm erkennen und in Zukunft keine Warnungen mehr zu diesem Programm erhalten möchten, aktivieren Sie das Kontrollkästchen **Ich erkenne das Programm**.

> **TIPP**
> Auch wenn Sie ein Programm bei der ersten Aufforderung blockieren bzw. zulassen, bietet McAfee Firewall die Möglichkeit diese Einstellung zu ändern und beim nächsten Verbindungsversuch eine andere Option zu wählen. Die vorgenommenen Einstellungen werden beim Beenden von McAfee Firewall automatisch gespeichert und beim nächsten Start des Programms wieder verwendet.

Ändern eines Programmstatus

McAfee Firewall überwacht den Internet-Verkehr, um festzustellen, welche Programme Internet-Verbindungen aufbauen. Je nach Einstellungen wird der Kommunikationsversuch eines Programms zugelassen, blockiert oder gefiltert.

Wenn Sie **Alles zulassen** wählen, können alle auf Ihrem Computer installierten Programme durch die Firewall kommunizieren.

So können Sie die aktuelle Liste der vertrauenswürdigen Programme anzeigen und konfigurieren

1. Wählen Sie in der Taskliste die Option **Internet-Anwendungen überwachen**.
2. Wählen Sie das Programm aus, dessen Filtereinstellungen Sie konfigurieren möchten (oder klicken Sie auf **Durchsuchen**, um ein Programm zur Liste hinzuzufügen).
3. Wählen Sie eine der folgenden Optionen:
   - Internet-Zugriff dieses Programms filtern (empfohlen).
   - Unbegrenzten, filterfreien Internet-Zugriff für dieses Programm zulassen.
   - Internet-Zugriff dieses Programms blockieren.
4. Wenn Sie ein Programm zur Liste hinzufügen möchten, klicken Sie auf **Hinzufügen**, und wählen Sie das gewünschte Programm aus. Um ein Programm aus der Liste zu entfernen, markieren Sie es, und klicken Sie auf **Entfernen**.
5. Klicken Sie auf **Anwenden**.

Anpassen von Filterregeln für ein bestimmtes Programm

Für alle Programme, denen die Option **Filtern** zugewiesen wurde, bietet McAfee Firewall erfahrenen Benutzern die Möglichkeit, eine Reihe benutzerdefinierter Filterregeln zu erstellen.

TIPP
Die Schaltfläche **Anpassen** steht nur zur Verfügung, wenn Sie die Option **Internet-Zugriff dieses Programms filtern** ausgewählt haben.

So erstellen Sie eine benutzerdefinierte Filterregel

1. Wählen Sie im Bildschirm **Internet-Anwendungen überwachen** das Programm aus, für das Sie eine benutzerdefinierte Filterregel erstellen möchten.
2. Wählen Sie das Optionsfeld **Internet-Zugriff dieses Programms filtern (empfohlen)**.
3. Klicken Sie auf **Anpassen**.

   Wenn für das Programm der von McAfee Firewall erstellte Standardregelsatz vorhanden ist, wird das Dialogfeld **Filterregeln anpassen** geöffnet. Wenn für das Programm *kein* Standardregelsatz vorhanden ist, wird das Dialogfeld **Was soll diese Regel tun?** angezeigt.
4. Informationen zum Abschluss der benutzerdefinierten Konfiguration erhalten Sie in den Dialogfeldern zum Anpassen der Filterregeln.

Tabelle 4-2. Schaltflächen im Dialogfeld „Filterregeln anpassen“

Schaltfläche	Beschreibung
Hinzufügen	◆ Klicken Sie auf **Hinzufügen**, um eine neue Regel hinzuzufügen und das Dialogfeld **Was soll diese Regel tun?** anzuzeigen.
Entfernen	◆ Klicken Sie auf **Entfernen**, um die Regel für das ausgewählte Programm zu entfernen. **VORSICHT**: Es gibt keine Funktion, um diesen Vorgang rückgängig zu machen.
Bearbeiten	◆ Klicken Sie auf **Bearbeiten**, um eine Filterregel zu konfigurieren.
Wiederherstellen	◆ Klicken Sie auf **Wiederherstellen**, um wieder die Standardregeln für das ausgewählte Programm zu verwenden. **TIPP**: Wenn Sie eine Filterregel unwiderruflich gelöscht haben, können Sie mit dieser Schaltfläche die Standardregeln auf das ausgewählte Programm anwenden.
OK	◆ Klicken Sie auf **OK**, um das Dialogfeld **Filterregeln anpassen** zu schließen und Ihre Änderungen zu speichern.
Abbrechen	◆ Klicken Sie auf **Abbrechen**, um das Dialogfeld **Filterregeln anpassen** zu schließen, ohne Ihre Änderungen zu speichern.

Primäre Funktionen

Aus der im Dialogfeld **Filterregeln anpassen** angezeigten Liste der primären Funktionen können Sie eine der folgenden Optionen wählen:

Tabelle 4-3. Primäre Funktionen

Option	nach ...
Verbindung zulassen ...	• Protokoll • lokalem Port • Remote-Port
Verbindung blockieren ...	• IP-Adresse • Domänenname • Richtung

Präzisieren der Bedingungen

Nachdem Sie die primäre Funktion für die Regel ausgewählt haben, können Sie die Regel weiter verfeinern, indem Sie die Kontrollkästchen für die gewünschten Kommunikationsmerkmale aktivieren:

Mit ...	verwenden Sie ...
• Richtung	• Protokolle
• Domänennamen	• Remote-Ports
• IP-Adressen	• lokale Ports

In Abhängigkeit von den ausgewählten Kommunikationsmerkmalen werden verschiedene Dialog- und Textfelder eingeblendet. Wenn die benutzerdefinierte Regel beispielsweise lautet „Kommunikation von diesem Programm blockieren, wenn die IP-Adresse xxx ist“, wird ein Textfeld zum Hinzufügen/Bearbeiten einer IP-Adresse angezeigt. Analog dazu wird beim Blockieren eines Programms nach dem Protokoll das Dialogfeld **Protokolle bearbeiten** geöffnet.

Klicken Sie zum Speichern Ihrer Änderungen auf **OK**.

Systemkonfiguration

Das Betriebssystem Ihres Computers kommuniziert auf verschiedenste Arten mit dem Netzwerk, ohne Ihnen dies direkt zu melden. McAfee Firewall ermöglicht das explizite Zulassen oder Blockieren einzelner Systemfunktionen. Die Einstellungen können für jedes Netzwerkgerät unterschiedlich sein, da z. B. ein PC an ein internes Netzwerk angeschlossen sein und zusätzlich eine DFÜ-Verbindung zum Internet haben kann.

Führen Sie die folgenden Schritte zur Überprüfung Ihrer Systemeinstellungen aus.

1. Wählen Sie in der Liste mit den erweiterten Tasks die Option **Netzwerkadapter konfigurieren**.
2. Wählen Sie im Dialogfeld **Netzwerkadapter-Einstellungen konfigurieren** den zu konfigurierenden Adapter aus, und klicken Sie auf **Adaptereinstellungen**, um die Eigenschaften des Adapters anzuzeigen bzw. zu ändern.
   Ergebnis: Die Eigenschaftsseite für den ausgewählten Adapter wird angezeigt.

Sie können jetzt wählen, ob Sie NetBIOS über TCP, Identifizierung, ICMP, ARP, DHCP, RIP, PPTP und andere Protokolle (IP und Nicht-IP) zulassen oder blockieren möchten.

Tabelle 4-4. Standardeinstellungen für Systemaktivitäten

Systemaktivitätstyp	Beschreibung
NetBIOS über TCP: Blockiert	Blockiert generell die Dateifreigabe über TCP und UDP-Broadcasts. Ihr System wird nicht in der Netzwerkumgebung anderer Benutzer angezeigt, und in Ihrer Netzwerkumgebung werden keine Systeme anderer Benutzer angezeigt. Wenn Ihr System NetBIOS andere Protokolle (z. B. IPX oder NetBEUI) unterstützt, kann die Dateifreigabe zugelassen werden, wenn Nicht-IP-Protokolle zugelassen sind (siehe „Andere Protokolle“ weiter unten).
Identifizierung: Blockiert	Dieser Dienst ist häufig für den Empfang von E-Mails erforderlich und wird von den meisten IRC-Servern benötigt.
ICMP: Blockiert	Dieses Protokoll wird häufig zum Beenden der Netzwerkverbindungen anderer Benutzer missbraucht (v. a. bei IRC).
ARP: Zugelassen	ARP ist ein notwendiges Ethernet-Protokoll, es gilt jedoch als gefährlich.

Tabelle 4-4. Standardeinstellungen für Systemaktivitäten

Systemaktivitätstyp	Beschreibung
DHCP: Zugelassen, wenn Ihr System DHCP verwendet.	Das Programm überprüft in der Systemregistrierung, ob eines Ihrer Netzwerkgeräte DHCP verwendet. Wenn dies der Fall ist, wird DHCP für alle diese Geräte zugelassen. Anderenfalls wird DHCP für alle Geräte blockiert. Wenn mehrere Netzwerkgeräte vorhanden sind und eines von ihnen DHCP verwendet, sollten Sie die DHCP-Einstellungen für jedes Gerät einzeln prüfen und nur für das Gerät zulassen, das dieses Protokoll verwendet (i. d. R. Kabel- bzw. ADSL-Modems und bestimmte interne Netzwerke; nicht für DFÜ-Verbindungen).
RIP: Blockiert	Lassen Sie RIP zu, wenn Sie vom Administrator oder ISP dazu aufgefordert werden.
PPTP: Blockiert	Diese Einstellung sollte nur vom Administrator geändert werden.
Sonstige Protokolle: Blockiert	Wenn Sie sich in einem IPX-Netzwerk befinden, sollten Sie „Nicht-IP-Protokolle“ zulassen. Wenn Sie PPTP verwenden, sollten Sie „Sonstige IP-Protokolle“ zulassen. Sprechen Sie sich jedoch mit Ihrem Netzwerkadministrator ab, bevor Sie hieran Änderungen vornehmen.

Angriffserkennungssystem von McAfee Firewall 4.0

5

Überblick über die Angriffserkennung

Im Gegensatz zu anderen Tools zur Angriffserkennung ist das leistungsfähige Angriffserkennungssystem (Intrusion Detection System, IDS) von McAfee Firewall leicht zu konfigurieren und zu aktivieren. Die Benutzer müssen nicht erst alle Einzelheiten über die verschiedenen Angriffsarten erlernen, um eine wirksame „Verteidigungslinie“ gegen Angriffe aufzubauen. Das Entwicklerteam von McAfee Firewall hat ein Tool erstellt, das sich mit einem einzigen Klick auf eine Schaltfläche aktivieren lässt und alle üblichen Angriffstypen und verdächtigen Aktivitäten erkennt.

Ungeschützte Computer werden schnell zu Opfern. Angreifer können beispielsweise mithilfe eines TCP-Port-Scans die auf Ihrem Rechner ausgeführten Dienste identifizieren. Mit diesem Wissen können Sie versuchen, eine Verbindung zu den Diensten herzustellen und Ihren Computer anzugreifen. Wenn ein Angreifer entdeckt, dass Sie einen TELNET-, FTP- oder Webserver-Dienst ausführen, kann er nacheinander jeden Ihrer Ports (1 bis 65535) kontaktieren, bis er einen offenen Port findet, zu dem er eine Verbindung herstellen kann.

Die IDS-Funktion von McAfee Firewall sucht nach bestimmten von Angreifern verwendeten Verkehrsmustern. Dabei prüft McAfee Firewall jedes auf Ihrem Rechner eingehende Paket auf verdächtige oder bekannte Angriffsmuster. Wenn McAfee Firewall beispielsweise ICMP-Pakete findet, überprüft das Programm die Pakete auf verdächtige Verkehrsmuster, indem es den ICMP-Verkehr mit bekannten Angriffsmustern vergleicht. Findet McAfee Firewall Übereinstimmungen, generiert das Programm ein Ereignis, um so vor der möglichen Sicherheitsverletzung zu warnen.

Bei aktivierter Angriffserkennung wird der Datenverkehr durch das Angriffserkennungssystem überprüft. Wenn McAfee Firewall bei aktivierter Angriffserkennung einen Angriff feststellt, können Sie jede weitere Kommunikation von der IP-Adresse des verdächtigen Rechners generell oder für einen bestimmten Zeitraum unterbinden. Über einen erkannten Angriff werden Sie von McAfee Firewall in der Windows-Taskleiste benachrichtigt.

HINWEIS
Da McAfee Firewall Pakete überprüft und nach Paketmustern bestimmter Angriffstypen sucht, kann diese Funktion zu einer leichten Leistungseinbuße des Systems führen.

Konfiguration des Angriffserkennungssystems

Führen Sie die folgenden Schritte aus, um das Angriffserkennungssystem von McAfee Firewall zu konfigurieren:

1. Klicken Sie auf der McAfee Firewall-Startseite auf **Erweiterte Tasks**.
2. Wählen Sie in der Liste mit den erweiterten Tasks die Option **Einstellungen zur Angriffserkennung**.

Hinweise zum Abschluss dieses Tasks erhalten Sie im Dialogfeld **Einstellungen zur Angriffserkennung konfigurieren**.

Häufige vom Angriffserkennungssystem erkannte Angriffe

Die folgende Tabelle enthält die vom McAfee Firewall-Angriffserkennungssystem erkannten Angriffe sowie einen den Angriffen zugeordneten Risikofaktor.

Angriff	Beschreibung	Risikofaktor
1234	Wird auch als Flushot-Angriff bezeichnet. Ein Angreifer sendet ein übergroßes Ping-Paket, mit dem die Netzwerk-Software nicht umgehen kann. In den meisten Fällen stürzt der Computer ab oder arbeitet nur noch langsam. Wenn sich der Computer nicht wieder aktivieren lässt, können ungespeicherte Daten verloren gehen.	Mittel
Back Orifice	Back Orifice ist ein Backdoor-Programm, das von einer Gruppe, die sich selbst „Cult of the Dead Cow“ nennt, für Windows 9x geschrieben wurde. Über diese Hintertür (back door) ist nach der Installation der Remote-Zugriff auf den Rechner möglich, d. h., es können Befehle ausgeführt, Screenshots „geschossen“, die Registrierung bearbeitet und andere Operationen ausgeführt werden. Client-Programme für Back Orifice sind für Windows und UNIX verfügbar.	Hoch
Bonk	Wurde entwickelt, um einen Implementierungsfehler im ersten von Microsoft veröffentlichten Teardrop-Patch auszunutzen. Bei diesem Angriff handelt es sich im Grunde um eine Windows-spezifische Variante des ursprünglichen Teardrop-Angriffs.	Hoch
Fraggle	Dieser Angriff ist eine UDP-Variante des Smurf-Angriffs. Indem gefälschte UDP-Pakete an einen bestimmten Port einer Broadcast-Adresse gesendet werden, reagieren Systeme des „Verstärker“-Netzwerks entweder mit einer UDP-Antwort oder mit einem Paket „ICMP UNREACHABLE“ an den Zielrechner. Diese Flut eingehender Pakete führt zu einem Denial of Service-Angriff gegen den Zielrechner.	Hoch

Angriff	Beschreibung	Risikofaktor
IP Spoofing	IP Spoofing bedeutet, dass Daten mit einer gefälschten Ursprungs-IP -Adresse versendet werden. Prinzipiell stellt die Verwendung einer gefälschten Ursprungs-IP-Adresse keine Gefahr dar, jedoch kann diese Technik zusammen mit anderen eingesetzt werden, z. B. zum TCP-Session-Hijacking oder um die Quelle eines Denial of Service-Angriffs (SYN-Flood, PING-Flood usw.) zu verschleiern.	Mittel
Jolt	Ein Remote-DOS-Angriff, der spezielle ICMP-Paketfragmente verwendet. Der Angriff kann dazu führen, dass das System langsamer arbeitet oder abstürzt.	Hoch
Jolt 2	Ein Remote-DOS-Angriff ähnlich Jolt, der spezielle ICMP- oder UDP-Paketfragmente verwendet. Der Angriff kann dazu führen, dass das System langsamer arbeitet oder abstürzt.	Hoch
Land	Bei diesem Angriff werden TCP-Pakete an einen laufenden Dienst auf dem Ziel-Host gesendet, wobei die Ursprungsadresse mit der des Hosts übereinstimmt. Bei dem TCP-Paket handelt es sich um ein SYN-Paket, das zum Aufbau einer neuen Verbindung verwendet wird. Dieses Paket wird vom selben TCP-Quell-Port gesendet, der auch der Ziel-Port ist. Wenn das Paket vom Ziel-Host angenommen wird, kommt es zu einer Schleife im Betriebssystem, die letztlich zum Absturz des Systems führt.	Hoch
Nestea	Dieser Angriff nutzt einen Fehler beim Berechnen der Größen während des Wiederzusammenführens von Paketfragmenten aus. In der für das Wiederzusammenführen verantwortlichen Routine der angreifbaren Systeme gab es einen Fehler beim Berechnen der Länge des IP-Header-Felds. Durch das Senden speziell präparierter Pakete konnte unter Ausnutzung dieses Fehlers ein angreifbares System zum Absturz gebracht werden.	Hoch
Newtear	Ein DoS-Angriff (Denial of Service), der hauptsächlich Windows NT -basierte Systeme zum Absturz bringt. Der Angriff ist für den Computer selbst nicht gefährlich, die Daten laufender Anwendungen gehen aber mit hoher Wahrscheinlichkeit verloren.	Hoch
Oshare	Ein DoS-Angriff, der durch das Senden einer speziellen Paketstruktur an den Computer verursacht wird. Die Ergebnisse eines solchen Angriffs reichen in Abhängigkeit von Ihrer Rechnerkonfiguration von einem vollständigen Systemabsturz über erhöhte CPU-Auslastung bis zu zeitweisen Verzögerungen. Dieser Angriff betrifft praktisch alle Versionen Windows 98- und NT-basierter Systeme, wobei die Schwere der Auswirkungen von der eingesetzten Hardware abhängt.	Hoch
Ping Flood	Bei diesem Angriff wird eine sehr große Anzhl von „ICMP ECHO“-(PING-)Anforderungen an den angegriffenen Host geschickt. Dieser Angriff ist besonders effektiv, wenn dem Angreifer eine schnellere Netzwerkverbindung zur Verfügung steht als dem Opfer.	Hoch

Angriff	Beschreibung	Risikofaktor
Ping of Death	Dieser Angriff erlaubt einem Remote-Benutzer, Ihr System neu zu starten oder durch das Senden eines übergroßen PING-Pakets zu beeinträchtigen. Dabei wird ein fragmentiertes Paket gesendet, das mehr als 65.536 Byte lang ist und eine fehlerhafte Verarbeitung auf dem Remote-System verursacht. Im Ergebnis wird das Remote-System während der Verarbeitung neu gestartet oder lässt sich nicht mehr kontrollieren.	Hoch
Port-Scannen	Hierbei handelt es sich um keinen Angriff im eigentlichen Sinne. Ein Port-Scan zeigt oft nur an, dass ein Angreifer Ihr System nach potenziellen Schwachstellen durchsucht. Bei einem Port-Scan werden alle TCP- und/oder UDP-Ports überprüft, um festzustellen, welche Dienste (und damit Schwachstellen) vorhanden sind.	Gering
Saihyousen	Der Saihyousen-Angriff kann einige Firewalls zum Absturz bringen. Bei diesem Angriff wird vom Angreifer ein Strom von UDP-Paketen gesendet.	Hoch
Smurf	Bei diesem Angriff wird ein „ICMP ECHO REQUEST“-(PING-)Paket mit einer gefälschten Quelladresse gesendet, die mit dem Zielsystem übereinstimmt. Dieses Paket wird an ein „Verstärker“-Netzwerk geschickt (ein Netzwerk, das das Senden von Paketen an die Broadcast-Adresse erlaubt), sodass jeder Rechner des Verstärkernetzwerks auf die als legitim angesehene Anforderung des Ziels antwortet. Im Ergebnis wird das Zielsystem mit „ICMP ECHO REPLY“-Nachrichten überflutet, was zu einem DoS-Angriff führt.	Hoch
SynDrop	Vom Angreifer werden überlappende, fragmentierte Daten gesendet, die beim Zielcomputer zu Instabilität bzw. zum Absturz führen. Nicht gespeicherte Daten können dabei verloren gehen.	Hoch
Syn Flood	Mit diesem Angriff kann Ihr Netzwerk zum vollständigen Erliegen gebracht werden, indem es mit Verbindungsanforderungen überflutet wird. Dadurch wird die Warteschlange gefüllt, die eine Liste der noch nicht aufgebauten Verbindungen verwaltet. Weitere Verbindungsanforderungen können dann nicht mehr angenommen werden.	Hoch
Teardrop	Dieser Angriff nutzt auf gefährdeten Systemen einen Fehler bei der Wiederzusammenführung fragmentierter Pakete durch den TCP/IP-Stack aus, wobei sämtliche verfügbaren Speicherressourcen in Anspruch genommen werden. Das Senden spezieller IP-Datagramme kann auf vielen Betriebssystemen dazu führen, dass sich das System aufhängt oder neu startet.	Hoch

Angriff	Beschreibung	Risikofaktor
UDP Flood	Ein Remote-DoS-Angriff, der beabsichtigt, den Zielrechner mit mehr Daten zu überfluten, als er verarbeiten kann, und so verhindert, dass zulässige Verbindungen aufgebaut werden. Auf den Rechner kann über TCP/IP nicht mehr zugegriffen werden. Dies geschieht, wenn der Rechner in den Ruhezustand versetzt wurde und anschließend wieder aktiviert wird. Stellen Sie sicher, dass die Option zum bedarfsweisen Laden in der TCP/IP-Systemsteuerung nicht aktiviert ist. TCP/IP ist dann immer geladen, sodass McAfee Firewall auch während des Ruhezustands aktiv ist.	Hoch
Winnuke	Hierbei handelt es sich um einen DoS-Angriff, der bei vielen Windows 95- und Windows NT-Rechnern die Netzwerkfunktionen vollständig deaktiviert. Auch wenn Winnuke nicht notwendigerweise Ihren Rechner beschädigt, kann es doch durch den Angriff zum Verlust aller nicht gespeicherten Daten kommen. Ein Neustart des Rechners sollte zur Wiederherstellung der normalen Betriebsfunktionen führen.	Hoch

Aktualisieren von McAfee Firewall 4.0 6

Überblick über Instant Updater

Da die Technologien, die den McAfee-Software-Produkten zu Grunde liegen, ständig weiterentwickelt werden, bieten wir unseren Kunden in regelmäßigen Abständen Updates an. Sie sollten immer die neueste Version Ihres Produkts verwenden, um ein optimales Maß an Sicherheit zu gewährleisten.

Mithilfe von McAfee Instant Updater können Sie Ihre Software schnell und unkompliziert aktualisieren. Dieser Vorgang erfolgt nahtlos und fast vollständig ohne Ihr Eingreifen.

Instant Updater wird auch verwendet, um Ihre Produkte bei McAfee zu registrieren. Um regelmäßige Produkt-Updates zu erhalten, müssen Sie Ihr Produkt bei McAfee registrieren lassen.

Warum Sie aktualisieren sollten

- Für Ihr McAfee-Produkt könnten neue Funktionen entwickelt worden sein.
- Produktfehler werden in regelmäßigen Abständen behoben.
- Neue Produktinhalte werden regelmäßig bereitgestellt.
- Aktualisierte Virensignaturdateien werden herausgegeben.

So funktioniert der Aktualisierungsvorgang

Instant Updater ermöglicht Ihnen das Herunterladen und Installieren von Updates für McAfee-Produkte, während Sie mit dem Internet verbunden sind. Wenn ein Update vorhanden ist, werden Sie benachrichtigt. Dann können Sie die Updates für Ihre Produkte herunterladen und anwenden.

Funktionen von Instant Updater

- **„Automatisches Update“ ist die Standardeinstellung für Instant Updater**.

  Instant Updater sucht dann im Hintergrund nach Produkt-Updates und wendet diese bei Bedarf an, während Sie mit dem Internet verbunden sind.

  Unter Umständen werden Sie von Instant Updater aufgefordert, Ihren Rechner neu zu starten, damit die Updates wirksam werden können. Mithilfe der Funktion **Automatisches Update** wird täglich nach Updates gesucht, um sicherzustellen, dass das McAfee-Produkt, der Produktinhalt und ähnliche Elemente, wie das Virenscan-Modul und die DAT-Dateien, auf dem aktuellsten Stand sind.

- **Automatische Anfrage**: Wenn die Funktion **Automatische Anfrage** aktiviert ist, werden Sie automatisch benachrichtigt, wenn Sie mit dem Internet verbunden sind und neue Produkt-Updates zur Verfügung stehen. Bei einer langsamen Internet-Verbindung wird diese Funktion nicht empfohlen.

- **Manuelles Update**: Wenn Sie nur selten eine Verbindung zum Internet herstellen, können Sie Ihr McAfee-Produkt mit der Funktion **Manuelles Update** auf den neuesten Stand bringen. Dabei führen Sie manuell eine Aktualisierung aus, während Sie mit dem Internet verbunden sind. Wählen Sie hierfür in dem entsprechenden Produkt die Aktualisierungsfunktion.

  Wenn Sie die Funktion **Manuelles Update** verwenden, behalten Sie die vollständige Kontrolle über den Aktualisierungsvorgang.

Startseitenabfrage

Zu Instant Updater gehört auch die **Startseitenabfrage**. Diese Funktion ermöglicht Ihnen, die Startseite des McAfee-Produkts so zu konfigurieren, dass jedes Mal eine Meldung angezeigt wird, wenn ein Update verfügbar ist. Nach der Installation der McAfee-Software ist die Startseitenabfrage standardmäßig aktiviert.

Konfiguration

Zusätzliche Informationen zu den Einstellungen für die automatische Abfrage und das automatische Update finden Sie in der Online-Hilfe.

Produktsupport und Kundendienst A

Kontaktaufnahme mit dem Kundendienst und dem technischen Support

Produktsupport und Kundendienstleistungen erhalten Sie unter http://www.mcafeehilfe.com. Auf unserer Support-Website finden Sie einen leicht zu bedienenden Antwortassistenten, der Ihnen in drei Schritten rund um die Uhr Antworten auf die häufigsten Fragen gibt. Fortgeschrittenen Benutzern stehen darüber hinaus auch erweiterte Funktionen, wie z. B. eine Schlüsselwortsuche und ein Hilfeverzeichnis, zur Verfügung.

Wenn Sie dennoch keine Lösung zu Ihrem Problem finden, können Sie außerdem rund um die Uhr KOSTENLOS auf unsere Dienste Chat Now! und E-Mail Express! zugreifen. Per Chat und E-Mail können Sie über das Internet schnell einen qualifizierten Support- oder Kundendienstmitarbeiter erreichen, wobei Ihnen keine Kosten entstehen. Informationen zum telefonischen Support können Sie ebenfalls über unsere Website abrufen: http://www.mcafeehilfe.com.

Überblick über „McAfee-at-home.com/international/germany“

McAfee ist für einen engagierten Kundendienst bekannt, in dessen Mittelpunkt stets die Zufriedenheit des Kunden steht. In dieser Tradition haben wir unsere Website zu einer umfassenden Hilfequelle ausgebaut, auf der Sie Antworten auf viele Fragen zu McAfee Consumer-Produkten finden. Bei allen Fragen und Problemen in Zusammenhang mit unseren Produkten sollte http://www.mcafee-at-home.com/international/germany/ Ihre erste Anlaufstelle sein.

Notfallsupport

Wenn Sie ein McAfee-Einzelhandelsprodukt auf Ihrem Computer installiert haben und eine computerbezogene Notfallsituation eintritt, die verhindert, dass Sie eine Verbindung zum Internet herstellen können, können Sie die folgende Telefonnummer anrufen, um telefonischen Support per Rückruf in Anspruch zu nehmen.

Folgende Situationen gelten als Notfälle:

- Ihr Computer kann keine Verbindung zum Internet herstellen.
- Ihr Computer wurde von einem Virus infiziert, und Sie können keine Internet-Verbindung herstellen.
- Ihr Computer reagiert nicht mehr, nachdem Sie ein McAfee-Produkt installiert haben.
- An Stelle eines Einkaufs in unserem eStore möchten Sie mit einem Kundendienstvertreter sprechen, um ein McAfee-Produkt zu erwerben.

Um einen Support-Rückruf zu erhalten, müssen Sie Ihren vollständigen Namen und Ihre Telefonnummer hinterlassen. Ein Vertreter unsers erfahrenen Support- und Kundendienstteams wird Sie so schnell wie möglich zurückrufen.

Halten Sie für unseren Rückruf bitte die folgenden Informationen bereit:

- Die Versionsnummer Ihrer McAfee-Software. Diese Information finden Sie unter **Hilfe > Info**.
- Das Windows-Betriebssystem und die Versionsnummer.
- Umfang des Arbeitsspeichers (RAM).
- Modellname der Festplatte (intern/extern).
- Zusätzliche Karten, Boards oder Hardware.
- Eine vollständige Beschreibung des Problems, z. B. den GENAUEN Wortlaut der Fehlermeldung, die auf dem Bildschirm erscheint, welche Schritte Sie durchgeführt haben, bevor die Fehlermeldung angezeigt wurde, sowie ob der Fehler fortlaufend auftritt und Sie das Problem reproduzieren können.

Kontaktadressen

Network Associates International B.V.
P.O. Box 58326
1040 HH Amsterdam
Niederlande

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

Notfalltelefonnummern:

Land:	Telefonnummer:
Belgien	02 27 50 703
Dänemark	03 5258 321
Deutschland	06 966 404 330
Finnland	09 229 06 000
Frankreich	01 70 20 0 008
Großbritannien	020 794 901 07
Irland	01 601 55 80
Italien	02 45 28 15 10
Luxemburg	040 666 15670
Niederlande	020 504 0586
Norwegen	02 3050420
Österreich	017 908 75 810
Portugal	00 31 20 586 6430 (auf Englisch)
Schweden	08 57 92 9004
Schweiz	022 310 1033
Spanien	901-120 175 (* anteilige Gebühren)

Index

U

W

Weitere Informationen über Produkte,
weltweite Dienstleistungen und
Produktsupport erhalten Sie
von Ihrem autorisierten
McAfee-Vertreter oder unter:

http://www.mcafeehilfe.com

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

www.mcafee-at-home.com

NA-593-0010-GE-1