BENUTZERHANDBUCH

McAfee® Personal Firewall Plus™

McAfee SECURITY

Inhalt

Erste Schritte 1

Willkommen bei McAfee Personal Firewall Plus!

Die Software McAfee Personal Firewall Plus bietet erweiterten Schutz für Ihren Computer und persönliche Daten. Personal Firewall baut eine Barriere zwischen Ihrem Computer und dem Internet auf. Dabei wird der Internetverkehr im Hintergrund auf verdächtige Aktivitäten hin überwacht.

Das Programm umfasst folgende Funktionen:

- Abwehr von potenziellen Hacker-Angriffen
- Ergänzung von Antivirus-Software
- Überwachung von Internet- und Netzwerkaktivität
- Warnungen bei potenziell schädlichen Ereignissen
- Gibt detaillierte Informationen zu verdächtigem Internetverkehr aus
- Integriert Funktionalität von Hackerwatch.org, einschließlich Ereignismeldung, selbsttestende Tools und die Möglichkeit, gemeldete Ereignisse per E-Mail an andere Onlinebehörden zu senden.
- Bietet umfangreiche Funktionen zur Verfolgung und Ereignisprüfung

Neue Funktionen

Verbesserte HackerWatch.org-Integration

Noch nie war es einfacher, potentielle Hacker zu melden. McAfee Personal Firewall Plus verbessert die Funktionalität von HackerWatch.org, die die Möglichkeit bietet, Ereignisse potentiell gefährlicher Aktivitäten an eine Datenbank zu senden.

Erweiterter Intelligenter Umgang mit Anwendungen

Wenn eine Anwendung Internetzugriff anfordert, prüft Personal Firewall zuerst, ob es die Anwendung als vertrauenswürdig oder bösartig einstuft. Gilt die Anwendung als vertrauenswürdig, gewährt Personal Firewall ihr automatisch den Zugriff auf das Internet, ohne dass Sie etwas dazu tun müssen. Diese Datenbank wurde verbessert und bietet den Benutzern nun detailliertere Informationen über Anwendungen, die eine Verbindung zum Internet herstellen.

- **Erweiterte Erkennung von trojanischen Pferden**
  McAfee Personal Firewall Plus vereint die Anwendungsverbindungsverwaltung mit einer verbesserten Datenbank zu Erkennung und Sperrung des Internetzugriffs von potentiell gefährlichen Anwendungen, wie beispielsweise trojanischen Pferden. So wird verhindert, dass Ihre vertraulichen Daten weitergegeben werden.

- **Verbesserte visuelle Verfolgung**
  McAfee Personal Firewall Plus enthält Visual Trace, ein aktualisiertes Tool zur Eindringungserkennung. Visual Trace verfügt über leicht verständliche graphische Darstellungen, in denen der Ursprung gefährlicher Angriffe und der weltweite Datenverkehr angezeigt werden. Sie erhalten detaillierte Kontakt- und Eigentümerinformationen über die Ursprungs-IP-Adresse und zu allen nachfolgenden Schritten auf Ihrem Computer. In McAfee Personal Firewall Plus wurden der Funktion Visual Trace weitere geographische Daten hinzugefügt. Dadurch können Standortdetails besser angezeigt und die Standorte der Eindringlinge genauer visuell identifiziert werden. Mit Hilfe von Visual Trace können Benutzer visuell verfolgen, wo der Ursprung von Eindringungsversuchen liegt. Mit diesen neuen Daten können Benutzer eine verbesserte graphische Darstellung ihrer Suchvorgänge anzeigen.

- **Verbesserte Benutzerfreundlichkeit**
  McAfee Personal Firewall Plus enthält einen Setup-Assistenten und ein Benutzer-Lernprogramm, das die Benutzer durch den Setup-Vorgang für die Firewall führt. Obgleich das Produkt so gestaltet wurde, dass es ohne Interaktion seitens des Benutzers verwendet werden kann, bietet McAfee zahlreiche Ressourcen, die verdeutlichen, wie eine Firewall funktioniert und welchen Schutz sie bietet.

- **Verbesserte Eindringungsabwehr**
  McAfee Personal Firewall Plus schützt Ihre Privatsphäre dank der Eindringungsabwehr gegen mögliche Bedrohungen aus dem Internet besser als je zuvor. Durch die Verwendung einer Heuristik-ähnlichen Funktion bietet McAfee eine dritte Schutzstufe, da Objekte blockiert werden, die Symptome von Angriffen oder Merkmale von Hacker-Versuchen aufweisen.

- **Verbesserte Datenverkehr-Analyse**
  McAfee Personal Firewall Plus bietet dem Benutzer eine Anzeige der eingehenden und ausgehenden Daten des Computers und zeigt Anwendungsverbindungen sowie Anwendungen an, die aktiv nach offenen Verbindungen suchen. Dadurch können Anwendungen, die anfällig sind für Angriffe, angezeigt und entsprechende Maßnahmen ergriffen werden.

Dokumentation

Die Dokumentation für Personal Firewall Plus umfasst dieses Benutzerhandbuch und eine Online-Hilfe-Datei. Das Benutzerhandbuch ist ein Teil der Online-Hilfe. Vollständige Informationen und Anweisungen zur Verwendung von Personal Firewall Plus finden Sie in der Online-Hilfe. Nach der Installation von Personal Firewall Plus können Sie die Online-Hilfe aufrufen, indem Sie Personal Firewall Plus öffnen und anschließend auf das Symbol für die **Hilfe** im oberen Fensterbereich oder auf die Schaltfläche **Hilfe** klicken, die in einigen Dialogfeldern angezeigt wird.

Systemanforderungen

- Microsoft® Windows 98, Windows Me, Windows 2000 oder Windows XP
- PC mit mindestens 486er Prozessor (empfohlen wird Pentium)
- 8 MB freier Festplattenspeicher für die Installation
- Microsoft® Internet Explorer 5.01 oder höher

HINWEIS
Sie können die neueste Version von Internet Explorer von der Microsoft-Website unter *http://www.microsoft.com/worldwide/* herunterladen.

Deinstallation anderer Firewalls

Bevor Sie die Software McAfee Personal Firewall Plus installieren, müssen Sie alle anderen Firewall-Programme auf Ihrem Computer deinstallieren. Befolgen Sie hierzu die Deinstallationsanweisungen zu Ihrem Firewall-Programm.

HINWEIS
Wenn Sie Windows XP verwenden, müssen Sie die integrierte Firewall vor der Installation von McAfee Personal Firewall Plus nicht zwingend deaktivieren. Wir empfehlen jedoch, die integrierte Firewall dennoch zu deaktivieren. Tun Sie dies nicht, erhalten Sie Ereignismeldungen im Protokoll für eingehende Ereignisse in McAfee Personal Firewall Plus.

Installation von McAfee® Personal Firewall Plus™

McAfee stellt die Software McAfee Personal Firewall Plus in zwei Formaten zur Verfügung:

- Auf CD-ROM
- Als Download-Datei auf der McAfee-Website

Personal Firewall Plus wird im Ordner für McAfee unter „Programme“ installiert. Nachdem Sie Personal Firewall Plus installiert und eingerichtet haben, werden Sie aufgefordert, den Computer neu zu starten. Sie müssen den Computer neu starten, bevor Sie Personal Firewall Plus verwenden können.

So installieren Sie Personal Firewall Plus:

1 Wenn Sie Personal Firewall Plus von der McAfee-Website heruntergeladen haben, wird der Installationsassistent angezeigt. Fahren Sie fort mit Schritt 2.

   Oder

   Wenn Sie eine Personal Firewall Plus-CD erworben haben, legen Sie die Software-CD für Personal Firewall Plus in das CD-ROM-Laufwerk des Computers ein. Die Lizenzvereinbarung wird angezeigt.

   Wenn der Installationsassistent nicht automatisch gestartet wird, ist die Autorun-Funktion Ihres Computers möglicherweise deaktiviert. Aktivieren Sie die Autorun-Funktion.

   a Wählen Sie ein Land aus, um die Sprache anzugeben, in der die Lizenzvereinbarung angezeigt werden soll.

   b Wenn Sie die Lizenzvereinbarung gelesen haben, klicken Sie auf **Akzeptieren**, um die Bestimmungen dieser Vereinbarung zu akzeptieren.

      Der Installationsassistent für McAfee Personal Firewall Plus wird angezeigt.

2 Befolgen Sie die Anweisungen im Installationsassistenten, um die Installation abzuschließen.

Am Ende der Installation wird der Setup-Assistent für Personal Firewall Plus angezeigt. (Abbildung 1-1).

Abbildung 1-1. Setup-Assistent

Verwendung des Setup-Assistenten

Da Personal Firewall bereits so konfiguriert ist, dass der Schutz Ihres Computers sofort gewährleistet ist, ist eine Verwendung des Setup-Assistenten nicht unbedingt erforderlich. Der Setup-Assistent unterstützt Sie dabei, Ihren Computer nach Viren zu durchsuchen und Folgendes zu konfigurieren:

- Gewünschte Alarmtypen
- Die Art der Netzwerkverbindung
- Empfohlene Anwendungseinstellungen

Sie haben jederzeit die Möglichkeit, auf **Abbrechen** zu klicken, um die Standardeinstellungen zu akzeptieren. Sie können die Einstellungen von Personal Firewall jederzeit ändern.

> **HINWEIS**
> Wenn Sie auf eine neue Version von Personal Firewall aufrüsten und Ihre aktuellen Firewall-Einstellungen beibehalten möchten, klicken Sie auf **Abbrechen**.

Nach der Verwendung des Setup-Assistenten müssen Sie den Computer neu starten, um den Installationsvorgang abzuschließen.

So verwenden Sie den Setup-Assistenten:

1. Klicken Sie auf **Weiter**.
2. Befolgen Sie die Anweisungen, die in den Dialogfeldern angezeigt werden.
3. Klicken Sie auf **Fertig stellen**, wenn Sie die Vorgänge im Setup-Assistenten abgeschlossen haben.

   Sie werden zum Neustart des Computers aufgefordert. Klicken Sie auf **OK**, um den Computer jetzt neu zu starten, oder klicken Sie auf **Abbrechen**, um den Computer zu einem späteren Zeitpunkt neu zu starten. Sie müssen den Computer neu starten, bevor Sie Personal Firewall verwenden können.

Testen von McAfee® Personal Firewall Plus™

So testen Sie Personal Firewall:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  , wählen Sie **Personal Firewall** aus, und klicken Sie auf **Firewall testen**.
2. Personal Firewall öffnet den Internet Explorer und ruft die Website http://www.hackerwatch.org/ auf, die von McAfee Security geführt wird. Befolgen Sie die Anweisungen auf der Testseite von Hacherwatch.org, um Personal Firewall zu testen.

   HINWEIS
   Wenn Sie eine Internetverbindung über einen Proxy-Server oder Netzwerkadressübersetzungs-Server herstellen, was in den meisten Unternehmensnetzwerken (LANs) der Fall ist, wird der Lesevorgang nicht ordnungsgemäß ausgeführt. Das Firewall-Testprogramm von Hackerwatch.org überprüft, welcher Computer eine Anfrage bezüglich des Firewall-Tests gesendet hat, und testet diesen Computer. Wenn Sie eine Verbindung über einen Proxy- oder NAT-Server herstellen, leitet dieser Server die Anforderung Ihres Computers bezüglich des Firewall-Tests lediglich weiter, und Hackerwatch.org testet den falschen Computer. Sie gehören dem Proxy-Server an und nicht Ihrem Computer.

Verwenden von McAfee® SecurityCenter™

McAfee SecurityCenter stellt Ihre Anlaufstelle für alle Sicherheitsbelange dar und ist über das Symbol auf der Windows-Taskleiste oder dem Windows-Desktop zugänglich. Mit diesem Programm können Sie die folgenden nützlichen Aufgaben ausführen:

- Kostenlose Sicherheitsanalyse für Ihren Computer
- Starten, Verwalten und Konfigurieren aller McAfee-Abonnements über ein einziges Symbol
- Anzeige fortwährend aktualisierter Viruswarnungen und der neuesten Produktinformationen
- Bezug kostenloser Testabonnements, in deren Rahmen Sie Testversionen mit Hilfe unseres patentierten Softwareübertragungsverfahrens direkt von McAfee herunterladen und installieren können
- Direkte Links zu häufig gestellten Fragen und Antworten sowie Kontoinformationen auf der McAfee-Website

HINWEIS
Um weitere Informationen zu den Funktionen anzuzeigen, klicken Sie im Dialogfeld **SecurityCenter** auf **Hilfe**.

Wenn SecurityCenter ausgeführt wird und alle auf Ihrem Computer installierten McAfee-Funktionen aktiviert sind, wird das SecurityCenter-Symbol  auf der Windows-Taskleiste angezeigt. Dieser Bereich, der auch die Systemuhr enthält, befindet sich in der Regel unten rechts auf dem Windows-Desktop.

Wenn auf Ihrem Computer installierte McAfee-Anwendungen deaktiviert sind, wird das McAfee-Symbol schwarz dargestellt  .

So öffnen Sie McAfee SecurityCenter:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  .
2. Klicken Sie auf **SecurityCenter öffnen**.

So greifen Sie auf eine Funktion von McAfee Personal Firewall Plus zu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  .
2. Zeigen Sie auf **Personal Firewall**, und klicken Sie auf die zu verwendende Funktion.

Verwenden von McAfee® Personal Firewall Plus™ 2

So öffnen Sie Personal Firewall:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Zusammenfassung anzeigen**, **Internetanwendungen**, **Eingehende Ereignisse** oder **Dienstprogramme**.

Info zur Zusammenfassung

Die Personal Firewall-Zusammenfassung enthält vier Zusammenfassungen: Hauptübersicht, Anwendungsübersicht, Ereignis-Zusammenfassung und HackerWatch-Zusammenfassung. Die Zusammenfassung enthält unterschiedliche Berichte zu kürzlich eingegangenen Ereignissen, dem Anwendungsstatus sowie der von HackerWatch.org gemeldeten weltweiten Eindringaktivität. Außerdem finden Sie hier Links zu Tasks, die in Personal Firewall häufig ausgeführt werden.

Wenn Sie die Personal Firewall-Zusammenfassungen anzeigen möchten, klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Zusammenfassung anzeigen**. Die Seite mit der Hauptübersicht wird eingeblendet (Abbildung 2-1).

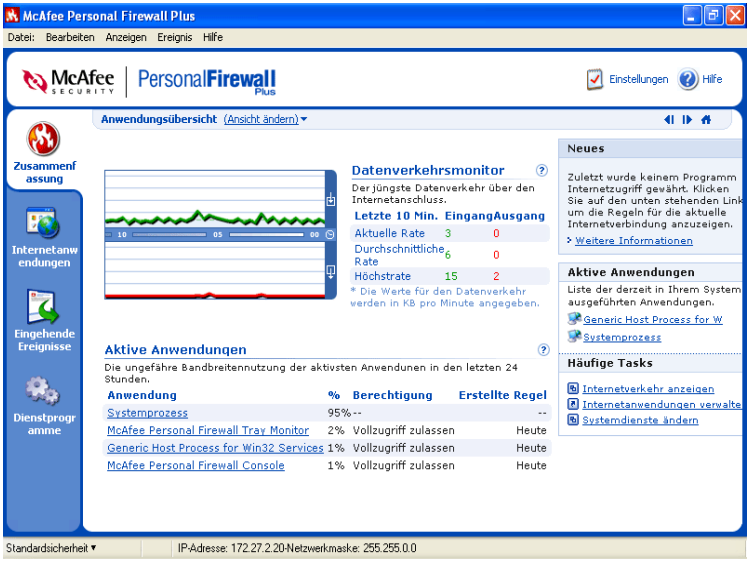

Abbildung 2-1. Seite mit der Hauptübersicht

Klicken Sie auf Folgendes, um zu unterschiedlichen Zusammenfassungen zu gelangen:

Artikel	Beschreibung
Ansicht ändern	Klicken Sie auf **Ansicht ändern**, um eine Liste mit Zusammenfassungen zu öffnen. Wählen Sie in der Liste die anzuzeigende Zusammenfassung aus.
 Rechtspfeil	Klicken Sie auf den Rechtspfeil, um die nächste Zusammenfassung anzuzeigen.
 Linkspfeil	Klicken Sie auf den Linkspfeil, um die vorherige Zusammenfassung anzuzeigen.
 Home	Klicken Sie auf das Home-Symbol, um zur **Hauptübersicht** zurückzukehren.

Die Seite mit der Hauptübersicht enthält folgende Informationen:

Artikel	Beschreibung
Sicherheits-einstellung	Aus dem Status der Sicherheitseinstellung geht hervor, auf welche Sicherheitsstufe die Firewall eingestellt ist. Klicken Sie auf den Link, um die Sicherheitsstufe zu ändern.
Blockierte Ereignisse	Aus dem Status der blockierten Ereignisse geht hervor, wie viele Ereignisse heute blockiert wurden. Klicken Sie auf den Link, um Ereignisdetails von der Seite für eingehende Ereignisse anzuzeigen.
Änderungen von Anwen-dungsregeln	Aus dem Status der Anwendungsregeln geht hervor, wie viele Anwendungsregeln in der letzten Zeit geändert wurden. Klicken Sie auf den Link, um die Liste zugelassener und blockierter Anwendungen einzublenden und um Anwendungsberechtigungen zu ändern.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Letztes Ereignis	Unter **Letztes Ereignis** werden die aktuellen eingehenden Ereignisse angezeigt. Sie können auf einen Link klicken, um das Ereignis zu verfolgen oder um der IP-Adresse zu vertrauen. Wenn Sie einer IP-Adresse vertrauen, wird der Empfang von Datenverkehr von dieser IP-Adresse auf Ihrem Computer ermöglicht.
Täglicher Bericht	Unter **Täglicher Bericht** wird angegeben, wie viele eingehende Ereignisse Personal Firewall heute, diese Woche und diesen Monat blockiert hat. Klicken Sie auf den Link, um Ereignisdetails von der Seite für eingehende Ereignisse anzuzeigen.

Artikel	Beschreibung
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen aufgeführt, die derzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um die IP-Adressen anzuzeigen, mit denen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den Personal Firewall-Seiten zu gelangen, auf denen Sie die Firewall-Aktivität anzeigen und Tasks ausführen können.

Wenn Sie die Anwendungsübersicht anzeigen möchten, klicken Sie auf **Ansicht ändern**, und wählen Sie dann **Anwendungsübersicht**. Die Anwendungsübersicht enthält folgende Informationen:

Artikel	Beschreibung
Datenverkehrs-monitor	Aus dem **Datenverkehrsmonitor** geht der eingehende und abgehende Datenverkehr über die Internetverbindung innerhalb der letzten zehn Minuten hervor. Klicken Sie auf das Diagramm, um Details zur Datenverkehrsüberwachung anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** wird die Bandbreitennutzung der aktivsten Anwendungen des Computers in den letzten 24 Stunden angegeben. **Anwendung** – Die Anwendung, die auf das Internet zugreift. **%** – Der Prozentsatz der Bandbreite, der von der Anwendung genutzt wird. **Berechtigung** – Die Art von Internetzugriff, die für die Anwendung zulässig ist. **Erstellte Regel** – Der Erstellungszeitpunkt der Anwendungsregel.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen aufgeführt, die derzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um die IP-Adressen anzuzeigen, mit denen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den Personal Firewall-Seiten zu gelangen, auf denen Sie den Anwendungsstatus anzeigen und anwendungsbezogene Tasks ausführen können.

Wenn Sie die Ereignis-Zusammenfassung anzeigen möchten, klicken Sie auf **Ansicht ändern**, und wählen Sie dann **Ereignis-Zusammenfassung**. Die Seite mit der Ereignis-Zusammenfassung enthält folgende Informationen:

Artikel	Beschreibung
Anschluss-vergleich	Unter **Anschlussvergleich** wird ein Kreisdiagramm der Anschlüsse auf Ihrem Computer angezeigt, auf die in den letzten 30 Tagen am häufigsten versucht wurde zuzugreifen. Sie können auf einen Anschlussnamen klicken, um Details von der Seite für eingehende Ereignisse anzuzeigen. Sie können den Mauszeiger auch über der Anschlussnummer platzieren, um eine Beschreibung des Anschlusses einzublenden.
Haupt-verursacher	Unter **Hauptverursacher** wird angegeben, welche IP-Adressen am häufigsten blockiert wurden, wann das letzte eingehende Ereignis für die einzelnen Adressen auftrat und wie viele eingehende Ereignisse in den letzten dreißig Tagen für die einzelnen Adressen insgesamt aufgetreten sind. Klicken Sie auf ein Ereignis, um Ereignisdetails von der Seite für eingehende Ereignisse anzuzeigen.
Täglicher Bericht	Unter **Täglicher Bericht** wird angegeben, wie viele eingehende Ereignisse Personal Firewall heute, diese Woche und diesen Monat blockiert hat. Klicken Sie auf eine Zahl, um Ereignisdetails von der Seite für eingehende Ereignisse anzuzeigen.
Letztes Ereignis	Unter **Letztes Ereignis** werden die aktuellen eingehenden Ereignisse angezeigt. Sie können auf einen Link klicken, um das Ereignis zu verfolgen oder um der IP-Adresse zu vertrauen. Wenn Sie einer IP-Adresse vertrauen, wird der Empfang von Datenverkehr von dieser IP-Adresse auf Ihrem Computer ermöglicht.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den Personal Firewall-Seiten zu gelangen, auf denen Sie Ereignisdetails anzeigen und ereignisbezogene Tasks ausführen können.

Wenn Sie die HackerWatch-Zusammenfassung anzeigen möchten, klicken Sie auf **Ansicht ändern**, und wählen Sie dann **HackerWatch-Zusammenfassung**. Die Seite mit der HackerWatch-Zusammenfassung enthält folgende Informationen:

Artikel	Beschreibung
Weltweite Aktivität	Unter **Weltweite Aktivität** wird auf einer Weltkarte die kürzlich blockierte Aktivität angezeigt, die von HackerWatch.org überwacht wird. Klicken Sie auf die Karte, um die Karte von HackerWatch.org zu öffnen, auf der die globale Bedrohung analysiert wird.
Ereignisumfang	Unter **Ereignisumfang** wird die Anzahl eingehender Ereignisse angegeben, die an HackerWatch.org übermittelt wurden.
Globale Anschluss-aktivität	Unter **Globale Anschlussaktivität** werden die Anschlüsse angegeben, die innerhalb der letzten fünf Tage anscheinend am häufigsten eine Bedrohung dargestellt haben. Klicken Sie auf einen Anschluss, um die Anschlussnummer und die Anschluss-beschreibung anzuzeigen.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den HackerWatch.org-Seiten zu gelangen, auf denen Sie aufführlichere Informationen zur weltweiten Hackeraktivität erhalten.

Info zu Internetanwendungen

Mit Hilfe der Seite **Internetanwendungen** können Sie die Liste der zugelassenen und blockierten Anwendungen anzeigen:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Internetanwendungen**. Die Seite mit den Internetanwendungen wird eingeblendet (Abbildung 2-2).

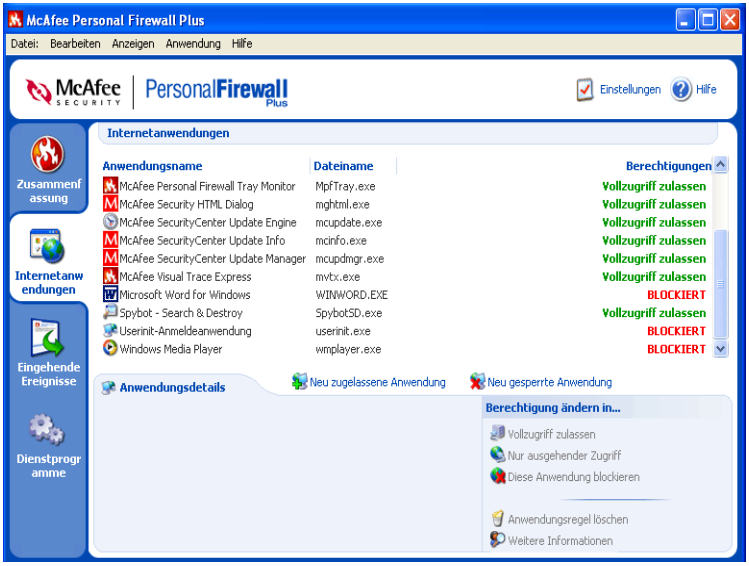

Abbildung 2-2. Seite mit Internetanwendungen

Sie enthält die folgenden Informationen:

- Anwendungsname
- Dateinamen
- Aktuelle Berechtigungsstufen
- Anwendungsdetails: Pfadnamen, Berechtigungszeitstempel und Erklärungen der Berechtigungsarten

Ändern von Berechtigungen

In Personal Firewall können Sie die Berechtigungsstufe für jede Anwendung festlegen, die einen Internetzugriff anfordert.

So ändern Sie eine Berechtigungsstufe:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Internetanwendungen**.
2. Klicken Sie mit der rechten Maustaste in der Liste **Berechtigungen** auf die Berechtigungsstufe einer Anwendung, und wählen Sie eine andere Stufe:
   - Klicken Sie auf **Vollzugriff zulassen**, um zuzulassen, dass die Anwendung Daten sendet und empfängt.
   - Klicken Sie auf **Nur ausgehenden Zugriff**, um zu verhindern, dass die Anwendung Daten empfängt.
   - Klicken Sie auf **Diese Anwendung blockieren**, um zu verhindern, dass die Anwendung Daten sendet oder empfängt.

So löschen Sie eine Berechtigungsstufe:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Internetanwendungen**.
2. Klicken Sie mit der rechten Maustaste in der Liste **Berechtigungen** auf die Berechtigungsstufe einer Anwendung, und klicken Sie auf **Anwendungsregel löschen**.

Wenn die Anwendung das nächste Mal Internetzugriff anfordert, können Sie ihre Berechtigungsstufe so festlegen, dass sie der Liste erneut hinzugefügt wird.

Ändern von Anwendungen

So ändern Sie die Liste der zugelassenen und blockierten Internetanwendungen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Internetanwendungen**.
2. Fügen Sie der Liste **Anwendungsname** Anwendungen hinzu, oder entfernen Sie Anwendungen aus ihr:
   - Um eine neue zugelassene Anwendung hinzuzufügen, klicken Sie auf **Neu zugelassene Anwendung**, wählen die zuzulassende Anwendung aus und klicken auf **Öffnen**.
   - Um eine neue gesperrte Anwendung hinzuzufügen, klicken Sie auf **Neu gesperrte Anwendung**, wählen die zu sperrende Anwendung aus und klicken auf **Öffnen**.
   - Zum Entfernen einer Anwendung aus der Liste klicken Sie auf **Anwendungsregel löschen**.

Info zu eingehenden Ereignissen

Über die Seite für eingehende Ereignisse können Sie das Protokoll eingehender Ereignisse anzeigen, das erzeugt wird, wenn Personal Firewall unaufgeforderten Internetverkehr blockiert.

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Eingehende Ereignisse**. Die Seite mit den eingehenden Ereignissen wird eingeblendet (Abbildung 2-3).

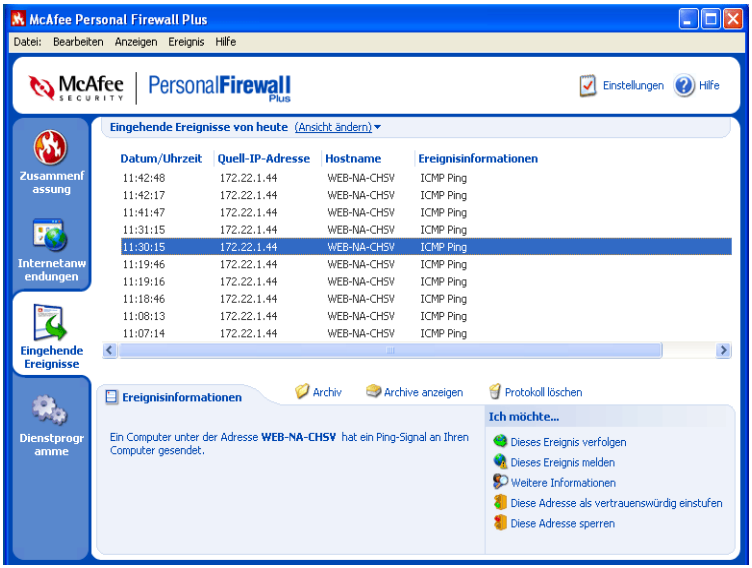

Abbildung 2-3. Seite mit eingehenden Ereignissen

Die Seite mit den eingehenden Ereignissen enthält folgende Informationen:

- Zeitstempel
- Quell-IP-Adressen
- Hostnamen
- Dienst- oder Anwendungsnamen
- Ereignisdetails: Verbindungstypen, Verbindungsanschlüsse und Erklärungen der Anschlussereignisse

Erläuterungen zu Ereignissen

Info zu IP-Adressen

IP-Adressen bestehen aus Zahlen, genauer gesagt aus vier verschiedenen Zahlenblöcken zwischen 0 und 255. Diese Zahlen identifizieren einen bestimmten Ort, an den der Datenverkehr im Internet weitergeleitet werden kann.

Spezielle IP-Adressen

Einige IP-Adressen sind aus unterschiedlichen Gründen ungewöhnlich:

Nicht routbare IP-Adressen – Diese stellen einen privaten IP-Adressraum dar. Diese IP-Adressen können im Internet nicht verwendet werden. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x–172.31.x.x und 192.168.x.x.

Loopback-IP-Adressen – Loopback-Adressen werden zu Testzwecken verwendet. Datenverkehr, der an diesen IP-Adressblock gesendet wird, kehrt sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da das Gerät niemals verlassen wird, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block lautet 127.x.x.x.

Null-IP-Adresse – Dies ist eine ungültige Adresse. Eine Null-IP-Adresse weist darauf hin, dass im Datenverkehr eine leere IP-Adresse verwendet wurde und der Absender den Ursprung des Datenverkehrs nicht preisgeben möchte. Der Absender kann keine Antwort auf den Datenverkehr erhalten, es sei denn, das Paket geht bei einer Anwendung ein, die den Paketinhalt, d. h. die anwendungsspezifischen Anweisungen, erkennt. Jede Adresse, die mit 0 (0.x.x.x) beginnt, ist eine Null-Adresse. 0.0.0.0 ist beispielsweise eine Null-IP-Adresse.

Ereignisse von 0.0.0.0

Wenn Ereignisse mit der IP-Adresse 0.0.0.0 angezeigt werden, gibt es hierfür zwei mögliche Ursachen. Die erste und häufigste Ursache ist die, dass Ihr Computer ein fehlerhaftes Paket erhalten hat. Das Internet ist nicht zu 100 % zuverlässig, und es ist immer möglich, dass fehlerhafte Pakete eingehen. Da Personal Firewall die Pakete vor der TCP/IP-Validierung erkennt, kann es passieren, dass diese Pakete als Ereignis gemeldet werden.

Die zweite Ursache ist die, dass die Quell-IP-Adresse gefälscht wurde. Gefälschte Pakete sind möglicherweise ein Anzeichen dafür, dass jemand auf Ihrem Computer nach einem trojanischen Pferd gesucht hat. Da Personal Firewall diesen Versuch blockiert hat, ist Ihr Computer sicher.

Ereignisse von 127.0.0.1

Ereignisse geben manchmal die Quell-IP-Adresse 127.0.0.1 an. Hierbei ist zu beachten, dass es sich um eine spezielle IP-Adresse handelt, die auch Loopbackadresse genannt wird.

Ganz gleich, welchen Computer Sie verwenden, die Adresse 127.0.0.1 bezieht sich immer Sie selbst. Diese Adresse wird auch Localhost genannt, weil der Computername „Localhost“ immer die IP-Adresse 127.0.0.1 auflöst.

Bedeutet dies, dass der Computer einen Angriff auf sich selbst ausübt? Wird Ihr Computer von einem trojanischen Pferd oder von Spyware angegriffen? Dies ist sehr unwahrscheinlich. Viele legitime Programme verwenden die Loopbackadresse für die Kommunikation zwischen den Komponenten. Zahlreiche persönliche E-Mail- oder Webserver lassen sich beispielsweise über eine Weboberfläche konfigurieren, auf die über die Adresse „http://localhost/“ (oder eine vergleichbare Adresse) zugegriffen werden kann.

Personal Firewall lässt Datenverkehr von diesen Programmen zu. Wenn Ereignisse mit der IP-Adresse 127.0.0.1 angezeigt werden, bedeutet dies in der Regel, dass die Quell-IP-Adresse gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Da Personal Firewall diesen Versuch blockiert hat, ist Ihr Computer sicher. Demzufolge ist es wenig sinnvoll, von der IP-Adresse 127.0.0.1 stammende Ereignisse zu melden.

Für einige Programme, vor allem Netscape ab Version 6.2, gilt jedoch, dass die Adresse 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen aufgenommen werden muss. Die Komponenten dieser Programme kommunizieren so miteinander, dass Personal Firewall nicht bestimmen kann, ob es sich um einen lokalen Datenverkehr handelt oder nicht.

Für den Beispielfall Netscape 6.2 gilt: Wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen, können Sie Ihre Buddyliste nicht verwenden. Wenn Sie folglich Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr bedenkenlos blockieren. Sollte jedoch ein Programm (wie Netscape) Probleme haben, nehmen Sie die Adresse 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen in Personal Firewall auf, und ermitteln Sie anschließend, ob das Problem behoben ist.

Wird das Problem durch die Aufnahme von 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen behoben, müssen Sie Ihre Entscheidungsmöglichkeiten abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, es besteht jedoch die Gefahr, dass Angriffe mit gefälschten Adressen ausgeführt werden. Wenn Sie diese Adresse nicht als vertrauenswürdig einstufen, funktioniert das Programm nicht. Es wird in diesem Fall jedoch die Gefahr verringert, dass Angriffe mit gefälschten Adressen ausgeführt werden.

Ereignisse von Computern in Ihrem LAN

Ereignisse können auch von Computern in Ihrem LAN (Local Area Network) generiert werden. Wenn diese Ereignisse aus dem „näheren Bereich“ stammen, werden sie grün angezeigt.

In der Regel empfiehlt es sich für die Einstellungen eines Unternehmens-LANs, im Dialogfeld **Vertrauenswürdige IP-Adressen** das Kontrollkästchen **Alle Computer in meinem LAN als vertrauenswürdig einstufen** zu aktivieren.

In einigen Situationen ist das lokale Netzwerk jedoch sogar noch gefährlicher als ein öffentliches Netzwerk. Dies gilt besonders dann, wenn Sie ein öffentliches Netzwerk mit einer hohen Bandbreite, beispielsweise DSL oder Kabelmodems, verwenden. In diesem Fall sollte das Kontrollkästchen **Alle Computer in meinem LAN als vertrauenswürdig einstufen** nicht aktiviert werden.

Wenn Sie in einem privaten Netzwerk mit Breitbandanschluss arbeiten, sollten Sie stattdessen die IP-Adressen der lokalen Computer manuell in die Liste der vertrauenswürdigen IP-Adressen aufnehmen. Beachten Sie, dass Sie mit Hilfe von .255-Adressen einen gesamten Block als vertrauenswürdig kennzeichnen können. So können Sie Ihr gesamtes ICS-Netzwerk als vertrauenswürdig einstufen, indem Sie die IP-Adresse 192.168.255.255 in die Liste der vertrauenswürdigen IP-Adressen aufnehmen.

Ereignisse von privaten IP-Adressen

IP-Adressen im Format 192.168.xxx.xxx, 10.xxx.xxx.xxx und 172.16.0.0 - 172.31.255.255 werden als nicht routbare oder private IP-Adresen bezeichnet. Diese IP-Adressen sollten niemals Ihr Netzwerk verlassen und können in der Regel als vertrauenswürdig gelten.

Der Block 192.168 wird in Zusammenhang mit Microsoft Internet Connection Sharing (ICS) verwendet. Wenn Sie ICS verwenden und Ereignisse von diesem IP-Block angezeigt werden, können Sie die IP-Adresse 192.168.255.255 in die Liste der vertrauenswürdigen IP-Adressen aufnehmen. Dadurch wird der Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie nicht in einem privaten Netzwerk arbeiten und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die Quell-IP-Adresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Da Personal Firewall diesen Versuch blockiert hat, ist Ihr Computer sicher.

Da private IP-Adressen (je nach Netzwerk) auf unterschiedliche Computer verweisen, müssen derartige Ereignisse nicht gemeldet werden.

Anzeigen von Ereignissen im Ereignisprotokoll

Über das Protokoll eingehender Ereignisse können Ereignisse auf mehrere Arten komfortabel angezeigt werden. In der Standardansicht werden nur Ereignisse des aktuellen Tags angezeigt. Sie können auch die Ereignisse anzeigen, die in der vergangenen Woche aufgetreten sind. Auch das gesamte Protokoll kann eingeblendet werden.

Des Weiteren ermöglicht Personal Firewall es Ihnen, eingehende Ereignisse von bestimmten Tagen, bestimmten Internetadressen (IP-Adressen) bzw. Ereignisse anzuzeigen, die identische Ereignisinformationen enthalten.

Für weitere Informationen zu einem Ereignis klicken Sie auf das jeweilige Ereignis. Die Informationen werden am unteren Rand der Seite der eingehenden Ereignisse im Bereich **Ereignisinformationen** angezeigt.

Anzeigen der Ereignisse von heute

So zeigen Sie nur die Ereignisse an, die heute aufgetreten sind:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Ereignisse von heute anzeigen**.

   Im Protokoll eingehender Ereignisse werden nur die Ereignisse angezeigt, die heute aufgetreten sind.

Anzeigen der Ereignisse aus dieser Woche

So zeigen Sie die Ereignisse an, die in der vergangenen Woche aufgetreten sind:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Ereignisse aus dieser Woche anzeigen**.

   Im Protokoll eingehender Ereignisse werden die Ereignisse angezeigt, die diese Woche aufgetreten sind.

Anzeigen des vollständigen Protokolls eingehender Ereignisse

So zeigen Sie alle Ereignisse im Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Vollständiges Protokoll anzeigen**.

   Im Protokoll eingehender Ereignisse werden alle Ereignisse aus dem Protokoll eingehender Ereignisse angezeigt, mit Ausnahme der Archive.

Ausschließliches Anzeigen von Ereignissen des ausgewählten Tages

Diese Option empfiehlt sich, wenn Sie nur die Ereignisse eines bestimmten Tags anzeigen möchten. Alle anderen Ereignisse werden ausgeblendet.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Nur Ereignisse des ausgewählten Tages anzeigen**.

   Im Protokoll eingehender Ereignisse werden die Ereignisse des heutigen Tags angezeigt.

Anzeigen von Ereignissen mit der ausgewählten Internetadresse

Diese Option empfiehlt sich, wenn Sie weitere Ereignisse anzeigen möchten, die von einer bestimmten Internetadresse stammen. Alle anderen Ereignisse werden ausgeblendet.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Nur Ereignisse mit der ausgewählten Internetadresse anzeigen**.

   Im Protokoll eingehender Ereignisse werden nur die Ereignisse angezeigt, die von der ausgewählten Internetadresse stammen.

Anzeigen von Ereignissen mit identischen Ereignisinformationen

Diese Option ist hilfreich, wenn Sie wissen möchten, ob das Protokoll eingehender Ereignisse weitere Ereignisse enthält, die in der Spalte **Ereignisinformationen** dieselben Informationen aufweisen wie das von Ihnen ausgewählte Ereignis. Sie können auf diese Weise ermitteln, wie oft dieses Ereignis stattgefunden hat, und überprüfen, ob die Ereignisse von derselben Quelle stammen. Aus der Spalte **Ereignisinformationen** geht eine Beschreibung des Ereignisses und, falls bekannt, das gängige Programm bzw. der gängige Service hervor, das bzw. der diesen Anschluss verwendet.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Ansicht** auf **Nur Ereignisse mit identischen Ereignisinformation anzeigen**.

   Im Protokoll eingehender Ereignisse werden Ereignisse mit identischen Ereignisinformationen angezeigt.

Reagieren auf eingehende Ereignisse

Außer Details zu Ereignissen im Protokoll eingehender Ereignisse anzuzeigen, können Sie eine visuelle Verfolgung der IP-Adressen zu Ereignissen im Protokoll eingehender Ereignisse durchführen oder Ereignisdetails auf der Website der Anti-Hacker-Online-Community HackerWatch.org anzeigen.

Verfolgen eines ausgewählten Ereignisses

Sie können versuchen, eine visuelle Verfolgung der IP-Adresse für ein Ereignis im Protokoll eingehender Ereignisse durchzuführen.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie auf das gewünschte Ereignis und anschließend auf **Ausgewähltes Ereignis verfolgen**.

   Sie können auch auf ein Ereignis doppelklicken, um eine Verfolgung durchzuführen.

   Standardmäßig beginnt Personal Firewall eine visuelle Verfolgung mit Hilfe des integrierten Visual Trace-Programms.

Abrufen von Ratschlägen von HackerWatch.org

Weitere Informationen zu einem Ereignis können Sie von der Anti-Hacker-Online-Community HackerWatch.org erhalten. Gehen Sie dazu wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Suchen Sie das Ereignis, zu dem Sie weitere Informationen benötigen, und klicken Sie darauf.
3. Klicken Sie im Menü **Ereignis** auf **Weitere Informationen zum Ereignis**.

Der Webbrowser wird geöffnet und wechselt zur Website von HackerWatch.org unter http://www.hackerwatch.org/. Dort erhalten Sie detaillierte Informationen zu dem Ereignistyp und Ratschläge dazu, ob Sie das Ereignis melden sollen.

Melden eines Ereignisses

Um ein Ereignis zu melden, das Ihrer Meinung nach einen Angriff auf Ihren Computer darstellte, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie auf das zu meldende Ereignis und danach im unteren rechten Bereich auf **Dieses Ereignis melden**.

   Personal Firewall meldet das Ereignis unter Ihrer eindeutigen ID an die Website von HackerWatch.org.

Anmelden bei HackerWatch.org

Wenn Sie zum ersten Mal die Zusammenfassung öffnen, kontaktiert Personal Firewall HackerWatch.org, damit eine eindeutige ID für Sie erzeugt wird. Wenn Sie bereits ein eingetragener Benutzer sind, wird Ihre Anmeldung automatisch überprüft. Sind Sie ein neuer Benutzer, müssen Sie einen Spitznamen sowie eine E-Mail-Adresse angeben und in der Bestätigungs-E-Mail von HackerWatch.org auf den Überprüfungs-Link klicken, damit Sie auf der Website die Funktionen zum Filtern und Senden von Ereignissen verwenden können.

Sie können Ereignisse auch ohne Überprüfung Ihrer Benutzer-ID an HackerWatch.org melden. Um Ereignisse zu filtern und als E-Mail an einen Freund zu senden, müssen Sie sich jedoch für den Dienst anmelden.

Durch die Anmeldung für den Dienst können wir Ihre Angaben überwachen und Sie benachrichtigen, wenn HackerWatch.org weitere Informationen oder Vorgehensweisen benötigt. Eine Anmeldung ist außerdem erforderlich, da wir alle eingegangenen Informationen bezüglich ihres Wertes bestätigen müssen.

E-Mail-Adressen werden von HackerWatch.org vertraulich behandelt. Wenn ein ISP weitere Informationen anfordert, wird die Anfrage über HackerWatch.org weitergeleitet. Ihre E-Mail-Adresse wird niemals bekannt gegeben.

Einstufen einer Adresse als vertrauenswürdige Adresse

Wenn im Protokoll eingehender Ereignisse ein Ereignis angezeigt wird, das eine zuzulassende IP-Adresse enthält, können Sie festlegen, dass Personal Firewall Verbindungen mit dieser Adresse in jedem Fall ermöglicht:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis, dessen IP-Adresse als vertrauenswürdig eingestuft werden soll, und klicken Sie anschließend auf **Der Quell-IP-Adresse vertrauen**.
3. Überprüfen Sie, ob die in der Bestätigungsmeldung **Diese Adresse als vertrauenswürdig einstufen** angegebene IP-Adresse korrekt ist, und klicken Sie anschließend auf **OK**.

   Die IP-Adresse wird der Liste der vertrauenswürdigen IP-Adressen hinzugefügt.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1. Klicken Sie auf die Registerkarte **Dienstprogramme**.
2. Klicken Sie auf das Symbol für **Vertrauenswürdige & Gesperrte IP-Adressen**, und klicken Sie dann auf die Registerkarte **Vertrauenswürdige IP-Adressen**.

   Die IP-Adresse wird in die Liste **Vertrauenswürdige IP-Adressen** aufgenommen.

Sperren einer Adresse

Wenn eine IP-Adresse in Ihrem Protokoll eingehender Ereignisse angezeigt wird, bedeutet dies, dass Datenverkehr von dieser Adresse blockiert wurde. Folglich stellt das Sperren einer Adresse keinen zusätzlichen Schutz dar, es sei denn, der Computer verfügt über Anschlüsse, die über die Systemdienste-Funktion absichtlich geöffnet werden, bzw. der Computer weist eine Anwendung auf, die für den Empfang von Datenverkehr berechtigt ist.

Fügen Sie der Liste gesperrter IP-Adressen nur dann eine IP-Adresse hinzu, wenn Sie über einen oder mehrere Anschlüsse verfügen, die absichtlich geöffnet sind, und Sie Grund zu der Annahme haben, dass Sie den Zugriff dieser Adresse auf die geöffneten Anschlüsse unterbinden müssen.

Wenn im Protokoll eingehender Ereignisse ein Ereignis angezeigt wird, das eine zu sperrende IP-Adresse enthält, können Sie festlegen, dass Personal Firewall Verbindungen mit dieser Adresse in jedem Fall unterbindet:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis, dessen IP-Adresse gesperrt werden soll, und klicken Sie anschließend auf **Quell-IP-Adresse sperren**.
3. Überprüfen Sie, ob die in der Bestätigungsmeldung **Diese Adresse sperren** angegebene IP-Adresse korrekt ist, und klicken Sie anschließend auf **OK**.

   Die IP-Adresse wird der Liste der gesperrten IP-Adressen hinzugefügt.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1. Klicken Sie auf die Registerkarte **Dienstprogramme**.
2. Klicken Sie auf das Symbol für **Vertrauenswürdige & Gesperrte IP-Adressen**, und klicken Sie dann auf die Registerkarte **Gesperrte IP-Adressen**.

   Die IP-Adresse wird in der Liste der gesperrten IP-Adressen angezeigt.

Verwalten des Protokolls eingehender Ereignisse

Auf der Seite mit den eingehenden Ereignissen können Sie die Ereignisse im Protokoll eingehender Ereignisse verwalten, das erzeugt wird, wenn Personal Firewall unaufgeforderten Internetverkehr blockiert:

Archivieren des Protokolls eingehender Ereignisse

Sie können das aktuelle Protokoll eingehender Ereignisse in einer Datei auf der Festplatte archivieren. Es wird empfohlen, das Ereignisprotokoll in regelmäßigen Abständen zu archivieren, da es relativ umfangreich werden kann.

So archivieren Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Datei** auf **Protokoll archivieren**.
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.
4. Klicken Sie auf **Speichern**, um das Archiv im Standardspeicherort zu speichern, oder navigieren Sie zu dem Speicherort, in dem das Archiv gespeichert werden soll.

Anzeigen des archivierten Protokolls eingehender Ereignisse

Sie können zuvor archivierte Protokolle eingehender Ereignisse anzeigen.

> **WARNUNG**
> Bevor Sie die Archive anzeigen, müssen Sie Ihr aktuelles Protokoll eingehender Ereignisse archivieren. Wenn Sie diesen Vorgang nicht ausführen, wird der Inhalt des aktuellen Protokolls eingehender Ereignisse gelöscht, sobald Sie ein Archiv anzeigen.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Datei** auf **Archivierte Protokolle anzeigen**.
3. Klicken Sie auf den Namen der Archivdatei (eventuell müssen Sie zunächst zum Dateispeicherort navigieren) und anschließend auf **Öffnen**.

   Die archivierten Daten werden im Protokoll eingehender Ereignisse angezeigt.

Löschen des Inhalts des Protokolls eingehender Ereignisse

Sie können alle Informationen aus dem Protokoll eingehender Ereignisse löschen.

> **WARNUNG**
> Wenn Sie den Inhalt des Protokolls eingehender Ereignisse löschen, kann dieser nicht wiederhergestellt werden. Wenn Sie davon ausgehen, dass Sie das Ereignisprotokoll zukünftig noch benötigen, sollten Sie es stattdessen archivieren.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Datei** auf **Protokoll löschen**.
3. Klicken Sie in der Bestätigungsmeldung zum Löschen des Protokolls auf **Ja**.

   Das Ereignisprotokoll ist nun leer.

Exportieren angezeigter Ereignisse

Falls die Daten Ihrem ISP, dem technischen Support oder einer Behörde bereitgestellt werden müssen, können Sie Ihr Ereignisprotokoll in eine Textdatei exportieren.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Menü **Datei** auf **Angezeigte Ereignisse exportieren**.
3. Navigieren Sie zu dem Verzeichnis, in dem Sie die Ereignisse speichern möchten.
4. Benennen Sie die Datei gegebenenfalls um, und klicken Sie anschließend auf **Speichern**.

   Die Ereignisse werden in dem angegebenen Verzeichnis in einer TXT-Datei gespeichert.

Kopieren von Ereignissen in die Zwischenablage

Sie können ein Ereignis in die Zwischenablage kopieren, um es von dort aus in eine Textdatei im Windows-Editor einzufügen.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll eingehender Ereignisse auf das zu exportierende Ereignis.
3. Klicken Sie im Menü **Bearbeiten** auf **Ausgewähltes Ereignis in Zwischenablage kopieren**.
4. Öffnen Sie den Windows-Editor:

   Klicken Sie auf der Windows-Taskleiste auf die Schaltfläche **Start**. Zeigen Sie auf **Programme**, dann auf **Zubehör**, und klicken Sie anschließend auf **Editor**.
5. Klicken Sie im Menü **Bearbeiten** auf **Einfügen**. Das Ereignis wird im Editor angezeigt. Wiederholen Sie diesen Schritt so oft, bis alle erforderlichen Ereignisse enthalten sind.
6. Speichern Sie die Datei an einem sicheren Ort.

Löschen von ausgewählten Ereignissen

Sie können Ereignisse aus dem Protokoll eingehender Ereignisse löschen.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll eingehender Ereignisse auf das zu löschende Ereignis.
3. Klicken Sie im Menü **Bearbeiten** auf **Ausgewähltes Ereignis löschen**.

   Das Ereignis wird aus dem Protokoll eingehender Ereignisse gelöscht.

Info zu Warnungen

Es wird Ihnen dringend empfohlen, sich mit den Warntypen vertraut zu machen, auf die Sie bei der Verwendung von Personal Firewall stoßen. Lesen Sie die folgenden Informationen über vorhandene Warntypen sowie mögliche Reaktionen, damit Sie sicher mit Warnungen umgehen können.

> **HINWEIS**
> Empfehlungen zu Warnungen unterstützen Sie bei der richtigen Handhabung einer Warnung. Wenn Warnungen mit Empfehlungen versehen angezeigt werden sollen, klicken Sie auf die Registerkarte **Dienstprogramme**, klicken Sie dann auf das Symbol **Warneinstellungen** und wählen Sie dann in der Liste **Empfehlungen** entweder **Empfehlungen automatisch verwenden** (die Standardeinstellung) oder **Nur Empfehlungen anzeigen**.

Rote Warnungen

Rote Warnungen enthalten wichtige Informationen, und es ist ein sofortiges Eingreifen Ihrerseits erforderlich. Es gibt folgende rote Warnungen:

- **Internetanwendung blockiert!** – Diese Warnung wird angezeigt, wenn Personal Firewall eine Anwendung daran hindert, auf das Internet zuzugreifen. Wenn beispielsweise eine Warnung zu einem trojanischen Pferd angezeigt wird, verweigert McAfee diesem Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer nach Viren zu durchsuchen.
- **Die Anwendung möchte auf das Internet zugreifen –** Diese Warnung wird angezeigt, wenn Personal Firewall Internet- oder Netzwerkverkehr bei neuen Anwendungen erkennt. („Standard“ oder „Eingeschränkte Sicherheit“)

- **Die Anwendung wurde geändert –** Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung geändert wurde, der Sie zuvor Zugriff auf das Internet gewährt haben. Wenn Sie die fragliche Anwendung vor kurzem aktualisiert haben, sollten Sie vorsichtig vorgehen, wenn Sie ihr Zugriff auf das Internet gewähren. („Vertrauenswürdig“, „Standard“, oder „Eingeschränkte Sicherheit“)

- **Anwendung fordert Serverzugriff an –** Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung, der Sie zuvor Zugriff auf das Internet gewährt haben, Internetzugriff als Server anfordert. (Eingeschränkte Sicherheit)

Grüne Warnungen

Grüne Warnungen informieren Sie über Änderungen, die an Personal Firewall vorgenommen wurden. Über grüne Warnungen können Sie beispielsweise über Anwendungen informiert werden, denen Personal Firewall automatisch Internetzugriff gewährt hat. Auf diese Weise können Sie auch auf neue Anwendungsregeln hingewiesen werden.

Programm darf auf das Internet zugreifen – Diese Warnung wird angezeigt, wenn Personal Firewall automatisch allen neuen oder geänderten Anwendungen Internetzugriff gewährt und Sie anschließend informiert (Sicherheitseinstellung Vertrauenswürdig). Ein Beispiel für eine geänderte Anwendung ist eine Anwendung mit geänderten Regeln, durch die der Anwendung automatisch der Internetzugriff erlaubt wird.

Blaue Warnungen

Blaue Warnungen enthalten Informationen, es ist jedoch keine Reaktion Ihrerseits erforderlich.

- **Versuch, eine Verbindung herzustellen, wurde blockiert –** Diese Warnung wird angezeigt, wenn Personal Firewall unerwünschten Internet- oder Netzwerkverkehr blockiert. („Vertrauenswürdig“, „Standard“, oder „Eingeschränkte Sicherheit“)

Versuch, eine Verbindung herzustellen, wurde blockiert

Wenn Sie als Sicherheitseinstellung **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-4) aus, wenn unerwünschter Internet- oder Netzwerkverkehr blockiert wird.

Abbildung 2-4. Versuch, eine Verbindung herzustellen, wurde blockiert

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Ereignisprotokoll anzeigen**, um Details über das Protokoll eingehender Ereignisse von Personal Firewall zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zu eingehenden Ereignissen* auf Seite 20).
- Klicken Sie auf **Diese Adresse verfolgen**, um eine visuelle Verfolgung der IP-Adressen dieses Ereignisses durchzuführen.
- Klicken Sie auf **Diese Adresse sperren**, um zu verhindern, dass diese Adresse auf Ihren Computer zugreift. Die Adresse wird der Liste der gesperrten IP-Adressen hinzugefügt.
- Klicken Sie auf **Diese Adresse als vertrauenswürdig einstufen**, um dieser IP-Adresse den Zugriff auf Ihren Computer zu gewähren.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.

Internetanwendung blockiert!

Wenn eine Warnung zu einem trojanischen Pferd angezeigt wird (Abbildung 2-5), verweigert Personal Firewall diesem Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer nach Viren zu durchsuchen.

Abbildung 2-5. Internetanwendung blockiert-Warnung

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Weitere Informationen**, um über das Protokoll eingehender Ereignisse Details zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zu eingehenden Ereignissen* auf Seite 20).
- Klicken Sie auf **McAfee VirusScan Online starten**, um den Computer nach Viren zu durchsuchen.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.

Die Anwendung möchte auf das Internet zugreifen

Wenn Sie in den Optionen der Sicherheitsteinstellungen **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-6) aus, wenn Internet- oder Netzwerkverkehr für neue oder geänderte Anwendungen erkannt wird.

Abbildung 2-6. Die Anwendung möchte auf das Internet zugreifen-Warnung

Wenn eine Warnung eingeblendet wird, die zur Vorsicht hinsichtlich der Gewährung von Internetzugriff für die Anwendung rät, können Sie auf **Klicken Sie hier, um weitere Informationen anzuzeigen** klicken, um weitere Informationen über die Anwendung zu erhalten. Diese Option wird nur dann in der Warnung angezeigt, wenn Personal Firewall zur automatischen Verwendung von Empfehlungen konfiguriert wurde.

McAfee erkennt die Anwendung, die auf das Internet zuzugreifen versucht, möglicherweise nicht (Abbildung 2-7).

Abbildung 2-7. McAfee erkennt diese Anwendungswarnung nicht

Folgich kann McAfee keine Empfehlung hinsichtlich der Anwendung aussprechen. Sie können McAfee diese Anmeldung melden, indem Sie auf **Informieren Sie McAfee über dieses Programm**. Daraufhin wird eine Webseite angezeigt, auf der Sie gebeten werden, anwendungsbezogene Angaben zu machen. Machen Sie möglichst detaillierte Angaben.

Die von Ihnen übermittelten Informationen werden von unserem HackerWatch -Team gemeinsam mit anderen Forschungstools verwendet, um zu ermitteln, ob eine Anwendung in unsere Datenbank bekannter Anwendungen aufgenommen wird und wie sie in diesem Fall von Personal Firewall gehandhabt werden soll.

- Klicken Sie auf **Zugriff gewähren**, um der Anwendung das Senden und Empfangen unaufgeforderter Daten auf Nicht-Systemanschlüssen zu erlauben.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um zu verhindern, dass die Anwendung Daten sendet oder empfängt.

WICHTIG
Anwendungen, die Internetzugriff für Online-Produktupdates benötigen (z. B. McAfee-Sicherheitsdienste), müssen Sie den Zugriff gewähren, um sie auf dem neuesten Stand zu halten.

Die Anwendung wurde geändert

Wenn Sie in den Optionen der Sicherheitseinstellungen **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-8) aus, wenn eine Anwendung geändert wurde, der Sie zuvor den Internetzugriff gewährt haben. Falls Sie die fragliche Anwendung vor kurzem aktualisiert haben, gehen Sie mit Bedacht vor, wenn Sie ihr Zugriff auf das Internet gewähren.

Abbildung 2-8. Die Anwendung wurde geändert-Warnung

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Zugriff gewähren**, um der Anwendung das Senden und Empfangen unaufgeforderter Daten auf Nicht-Systemanschlüssen zu erlauben.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um zu verhindern, dass die Anwendung Daten sendet oder empfängt.

Anwendung fordert Serverzugriff an

Wenn Sie in den Optionen der Sicherheitseinstellungen **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-9) aus, wenn erkannt wird, dass eine Anwendung, der Sie zuvor den Zugriff auf das Internet gewährt haben, den Internetzugriff als Server angefordert hat.

Abbildung 2-9. Anwendung fordert Serverzugriff an-Warnung

Beispielsweise wird eine Warnung eingeblendet, wenn MSN Messenger Serverzugriff anfordert, um im Rahmen eines Chats eine Datei zu senden.

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Serverzugriff gewähren**, um zuzulassen, dass die Anwendung Daten sendet und empfängt.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken**, um zu verhindern, dass die Anwendung Daten empfängt.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um zu verhindern, dass die Anwendung Daten sendet oder empfängt.

Programm darf auf das Internet zugreifen

Wenn Sie in den Optionen für die Sicherheitseinstellungen **Vertrauenswürdig** ausgewählt haben, gewährt Personal Firewall automatisch allen neuen oder geänderten Anwendungen Internetzugriff, und informiert Sie anschließend in Form einer Warnung (Abbildung 2-10).

Abbildung 2-10. Programm darf auf das Internet zugreifen

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Anwendungsprotokoll anzeigen**, um Details über das Internetanwendungsprotokoll zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zu Internetanwendungen* auf Seite 17).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um die Anzeige dieses Warnungstyps zu unterdrücken.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.

Index

T

V

W

Z