McAfee®

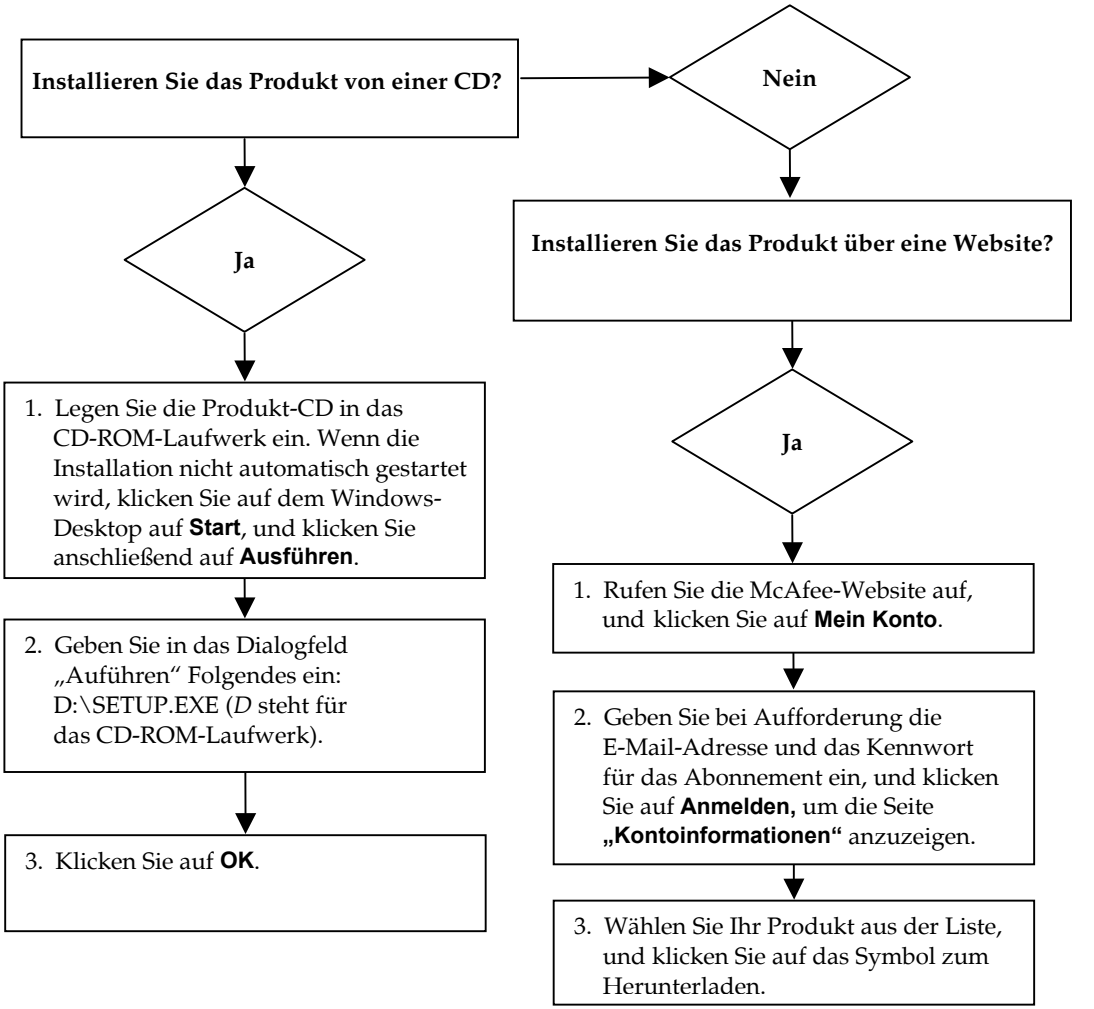
personalfirewallplus

Benutzerhandbuch

McAfee®

Schnellreferenz

Wenn Sie die Installation des Produkts von einer CD oder Website ausführen, sollten Sie diese praktische Referenzseite ausdrucken.



Weitere Informationen

Zum Anzeigen der Benutzerhandbücher auf der Produkt-CD muss Acrobat Reader installiert sein. Andernfalls installieren Sie das Programm jetzt von der McAfee-Produkt-CD.

1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein.
2. Öffnen Sie Windows-Explorer: Klicken Sie auf dem Windows-Desktop auf **Start** und dann auf **Suchen**.
3. Suchen Sie den Ordner mit den Handbüchern (Manuals), und doppelklicken Sie auf die PDF-Datei des gewünschten Benutzerhandbuchs.

Registrierungsvorteile

McAfee empfiehlt, die im Produkt beschriebenen, einfachen Schritte zu befolgen, um Ihre Registrierung direkt an uns zu senden. Durch die Registrierung wird sichergestellt, dass Ihnen im angemessenen Zeitrahmen professionelle technische Unterstützung zur Verfügung steht. Außerdem profitieren Sie von:

- KOSTENLOSEM elektronischen Support
- Updates für Virusdefinitionsdateien (DAT-Dateien) für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der VirusScan-Software

  Preisangaben für ein zusätzliches Jahr Virussignaturen erhalten Sie unter http://www.mcafee.com/.
- Garantie von 60 Tagen für Austausch der Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der SpamKiller-Software

  Preisangaben für ein zusätzliches Jahr Filter-Updates erhalten Sie unter http://www.mcafee.com/.
- McAfee Internet Security Suite-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der MIS-Software

  Preisangaben für ein zusätzliches Jahr Inhalts-Updates erhalten Sie unter http://www.mcafee.com/.

Technischer Support

Technischen Support erhalten Sie unter http://www.mcafeehilfe.com.

Unsere Support-Site ermöglicht Ihnen rund um die Uhr den Zugriff auf einen benutzerfreundlichen Antwort-Assistenten, der Ihnen Antworten auf die häufigsten Fragen gibt.

Die erweiterten Optionen sind für erfahrene Benutzer gedacht. Sie umfassen beispielsweise eine Schlüsselwortsuche und ein Hilfeverzeichnis. Wenn sich keine Lösung findet, können Sie außerdem KOSTENLOS auf unsere Dienste Chat Now! und E-Mail Express! zugreifen. Per Chat und E-Mail können Sie über das Internet schnell und kostenlos einen qualifizierten Support-Mitarbeiter erreichen. Sie können sich auch hier über die telefonischen Support-Möglichkeiten informieren: http://www.mcafeehilfe.com.

Inhalt

Erste Schritte 1

Willkommen bei McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus-Software bietet erweiterten Schutz für Ihren Computer und Ihre persönlichen 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 potentiellen Hacker-Angriffen
- Ergänzung von Anti-Virus-Software
- Überwachung von Internet- und Netzwerkaktivität
- Warnungen bei potentiell schädlichen Ereignissen
- Bereitstellung detaillierter Informationen zu verdächtigem Internetverkehr
- Integration der Funktionalität von HackerWatch.org, einschließlich Ereignismeldung, selbsttestende Tools und die Möglichkeit, gemeldete Ereignisse per E-Mail an andere Online-Behörden zu senden.
- Bereitstellung detaillierter Funktionen zur Verfolgung und Ereignisrecherche

Neue Funktionen

- **Verbesserter Schutz bei Spielen**
  McAfee Personal Firewall Plus schützt Ihren Computer vor versuchtem Eindringen und vor verdächtigen Aktivitäten, während Sie Spiele im Vollbildmodus spielen, kann aber Warnungen ausblenden, wenn ein versuchtes Eindringen oder verdächtige Aktivitäten entdeckt wurden. Nach dem Beenden des Spiels werden dann rote Warnungen angezeigt.

- **Verbesserte Zugriffsverwaltung**
  Mit McAfee Personal Firewall Plus können Sie auf dynamische Art und Weise Anwendungen vorübergehend Zugriff auf das Internet ermöglichen. Für die Anwendung wird der Zugriff nur solange gewährt, wie Sie mit dieser arbeiten. Entdeckt Personal Firewall ein unbekanntes Programm, das versucht, mit dem Internet zu kommunizieren, erhalten Sie über eine rote Warnung die Möglichkeit, die Anwendung vorübergehend auf das Internet zugreifen zu lassen.

- **Umfassendere Sicherheitsprüfung**
  Wenn Sie die Funktion zum Schließen der Verbindung in McAfee Personal Firewall Plus ausführen, können Sie sofort den gesamten eingehenden und ausgehenden Datenverkehr zwischen Ihrem Computer und dem Internet unterbinden. Sie können die Funktion zum Schließen der Verbindung in Personal Firewall auf drei verschiedene Arten aufrufen.

- **Verbesserte Optionen für die Wiederherstellung**
  Mit den Wiederherstellungsoptionen können Sie bei Personal Firewall automatisch die Standardeinstellungen wiederherstellen. Wenn Personal Firewall ungewöhnliches Verhalten aufweist, welches Sie nicht korrigieren können, können Sie die aktuellen Einstellungen aufheben und die Standardeinstellungen der Software wiederherstellen.

- **Schutz für die Internetverbindung**
  Damit ein Benutzer nicht versehentlich die Internetverbindung deaktiviert, wird bei einer blauen Warnung die Option zum Blockieren der Internetadresse nicht angezeigt, wenn Personal Firewall erkannt hat, dass die Internetverbindung von einem DHCP- oder DNS-Server hergestellt wurde. Wenn die eingehenden Daten nicht von einem DHCP- oder DNS-Server stammen, wird die Option angezeigt.

- **Verbesserte HackerWatch.org-Integration**
  Das Melden potentieller Hacker ist einfacher denn je. McAfee Personal Firewall Plus verbessert die Funktionalität von HackerWatch.org. Dies beinhaltet die Übermittlung von potentiell gefährlichen Ereignissen an die Datenbank.

- **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 weitere Aktionen erforderlich wären.

- **Erweiterte Erkennung trojanischer Pferde**
  Personal Firewall vereint die Anwendungsverbindungsverwaltung mit einer erweiterten Datenbank, mit der mehr potentiell bösartige Anwendungen, beispielsweise trojanische Pferde, erkannt und blockiert und somit daran gehindert werden können, auf das Internet zuzugreifen und möglicherweise Ihre persönlichen Daten weiterzugeben.

- **Verbesserte visuelle Verfolgung**
  Visual Trace bietet leicht verständliche grafische Darstellungen, in denen die Quelle der feindlichen Angriffe und des weltweiten Datenverkehrs einschließlich detaillierter Kontakt- bzw. Benutzerinformationen zu den Quell-IP-Adressen angezeigt werden.

- **Verbesserte Benutzerfreundlichkeit**
  McAfee Personal Firewall beinhaltet einen Setup-Assistenten sowie ein Benutzer-Lernprogramm, um Benutzer bei Einrichtung und Verwendung der Firewall zu unterstützen. Obwohl das Produkt zur Verwendung ohne Benutzereingriff entwickelt wurde, stellt McAfee den Benutzern zahlreiche Ressourcen zur Verfügung, um ihnen das Verständnis der Firewall zu erleichtern und deren Nutzen zu verdeutlichen.

- **Erweiterte Eindringungserkennung**
  Das Eindringungserkennungssystem (Intrusion Detection System, IDS) von Personal Firewall erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung prüft jedes Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden und speichert diese im Ereignisprotokoll.

- **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. So können Benutzer Anwendungen, die möglicherweise anfällig für Eindringlinge sind, erkennen und entsprechend reagieren.

Systemanforderungen

- Microsoft® Windows 98, Windows Me, Windows 2000 oder Windows XP
- PC mit Pentium-kompatiblem Prozessor
  Windows 98, 2000: 133 MHz oder höher
  Windows Me: 150 MHz oder höher
  Windows XP (Home und Professional): 300 MHz oder höher
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home und Professional): 128 MB
- 40 MB Festplattenspeicher
- Microsoft® Internet Explorer ab Version 5.5

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 McAfee Personal Firewall Plus-Software 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. Anderenfalls erhalten Sie Ereignismeldungen im Protokoll für eingehende Ereignisse in McAfee Personal Firewall Plus.

Festlegen der Standard-Firewall

McAfee Personal Firewall kann Berechtigungen und Datenverkehr für Internetanwendungen auf Ihrem Computer auch dann verwalten, wenn erkannt wird, dass Windows Firewall auf Ihrem System ausgeführt wird.

Bei der Installation deaktiviert McAfee Personal Firewall automatisch Windows Firewall und richtet sich selbsttätig als standardmäßige Firewall ein. Die gesamte Firewall-Funktionalität und diesbezügliche Meldungen kommen anschließend von McAfee Personal Firewall. Wenn Sie später Windows Firewall über das Windows Security Center oder die Windows-Systemsteuerung aktivieren und auf Ihrem Computer beide Firewalls ausführen sollten, kann die Protokollfunktion in McAfee Firewall teilweise verloren gehen, während Status- und Warnmeldungen möglicherweise doppelt angezeigt werden.

HINWEIS
Wenn beide Firewalls aktiviert sind, zeigt McAfee Personal Firewall nicht alle blockierten IP-Adressen auf der Registerkarte der eingehenden Ereignisse an. Windows Firewall fängt die meisten dieser Ereignisse ab und blockiert sie, wodurch ihre Erkennung und Protokollierung durch McAfee Personal Firewall unterbunden wird. McAfee Personal Firewall kann jedoch auf der Basis anderer Sicherheitsfaktoren zusätzlichen Datenverkehr blockieren. Diese Ereignisse werden protokolliert.

Die Protokollierung ist in Windows Firewall standardmäßig deaktiviert. Wenn Sie jedoch beide Firewalls verwenden möchten, können Sie die Windows Firewall-Protokollfunktion aktivieren. Das Standardprotokoll von Windows Firewall ist C:\Windows\pfirewall.log.

Um sicherzustellen, dass Ihr Computer von mindestens einer Firewall geschützt wird, wird Windows Firewall automatisch erneut aktiviert, sobald McAfee Personal Firewall deinstalliert wird.

Wenn Sie McAfee Personal Firewall deaktivieren oder die Sicherheitseinstellung des Programms auf **Offen** setzen, ohne Windows Firewall manuell zu aktivieren, wird der gesamte Firewall-Schutz, mit Ausnahme der zuvor bereits blockierten Anwendungen, entfernt.

Festlegen der Sicherheitsstufe

Anhand von Sicherheitsoptionen können Sie festlegen, wie Personal Firewall reagieren soll, wenn unerwünschter Datenverkehr erkannt wird. Standardmäßig ist die Sicherheitsstufe **Standardsicherheit** aktiviert. Wenn bei Verwendung der Sicherheitsstufe **Standardsicherheit** eine Anwendung Internetzugriff anfordert und Sie der Anforderung nachkommen, gewähren Sie damit Vollzugriff. Vollzugriff ermöglicht der Anwendung das Senden und Empfangen unaufgeforderter Daten auf Nicht-Systemanschlüssen.

So konfigurieren Sie Sicherheitseinstellungen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen **Optionen**.
2. Klicken Sie auf das Symbol **Sicherheitseinstellungen**.
3. Legen Sie die Sicherheitsstufe fest, indem Sie den Schieberegler in die gewünschte Position bringen.

   Die Sicherheitsstufen rangieren von „Verbindung schließen“ bis „Offen (Kein Filter)“:

   - **Verbindung schließen:** Alle Internetverbindungen Ihres Computers werden geschlossen. Sie können diese Einstellung verwenden, um Anschlüsse zu blockieren, die Sie auf der Seite „Systemdienste“ als offen konfiguriert haben.
   - **Eingeschränkte Sicherheit:** Wenn eine Anwendung eine bestimmte Form des Internetzugriffs erfordert (z. B. „Nur ausgehenden Zugriff“), können Sie die Internetverbindung für diese Anwendung zulassen oder blockieren. Wenn eine Anwendung später Vollzugriff anfordert, können Sie entweder Vollzugriff gewähren oder den Zugriff auf den ausgehenden Datenverkehr beschränkt belassen.
   - **Standardsicherheit (empfohlen):** Wenn eine Anwendung Internetzugriff anfordert und Sie der Anforderung nachkommen, erhält die Anwendung damit Vollzugriff für eingehenden und ausgehenden Datenverkehr.
   - **Vertrauenswürdige Sicherheit:** Allen Anwendungen wird automatisch vertraut, sobald sie versuchen, auf das Internet zuzugreifen. Sie können Personal Firewall jedoch so konfigurieren, dass Sie durch Warnungen über neue Anwendungen auf Ihrem Computer informiert werden. Verwenden Sie diese Einstellung, wenn Sie bemerken, dass bestimmte Spiele oder Streaming Media nicht funktionieren.

- **Offen (Kein Filter):** Ihre Firewall ist deaktiviert. Diese Einstellung lässt den gesamten Datenverkehr ohne Filterung durch Personal Firewall passieren.

  HINWEIS
  Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn die Sicherheitseinstellung der Firewall auf **Offen (Kein Filter)** oder **Verbindung schließen** gesetzt wird. Wenn dies nicht erwünscht ist, können Sie entweder die Berechtigungen der Anwendung auf **Vollzugriff zulassen** setzen oder die Berechtigungsregel **Blockiert** aus der Liste **Internetanwendungen** löschen.

4 Wählen Sie zusätzliche Sicherheitseinstellungen aus:

  HINWEIS
  Wenn auf Ihrem Computer Windows XP ausgeführt wird und mehrere XP-Benutzer hinzugefügt wurden, stehen diese Optionen nur dann zur Verfügung, wenn Sie auf Ihrem Computer als Administrator angemeldet sind.

- **Ereignisse der Eindringungserkennung im Protokoll der eingehenden Ereignisse aufzeichnen:** Wenn Sie diese Option auswählen, werden die von IDS erkannten Ereignisse im Protokoll eingehender Ereignisse angezeigt. Das Eindringungserkennungssystem erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung prüft jedes eingehende und ausgehende Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden. Die Pakete werden mit einer Signaturdatenbank verglichen und automatisch verworfen, wenn sie von dem „schuldigen" Computer kommen.

  IDS sucht nach bestimmten von Angreifern verwendeten Verkehrsmustern. Jedes von Ihrem Computer empfangene Datenpaket wird von IDS überprüft, um verdächtigen Datenverkehr oder Datenverkehr, der bekannten Angriffen gleicht, zu erkennen. Wenn Personal Firewall beispielsweise ICMP-Pakete erkennt, prüft es diese Pakete auf verdächtige Verkehrsmuster, indem es den ICMP-Datenverkehr mit den Mustern bekannter Angriffe vergleicht.

- **ICMP-Ping-Anforderungen akzeptieren:** ICMP-Datenverkehr wird hauptsächlich für Verfolgungen und Ping-Signale verwendet. Ping-Signale wiederum dienen häufig zur Durchführung von kurzen Tests, bevor versucht wird, eine Kommunikation zu initiieren. Wenn Sie ein Peer-to-Peer-File-Sharing-Programm verwenden oder verwendet haben, erhalten Sie möglicherweise eine große Anzahl von Ping-Signalen. Wenn Sie diese Option auswählen, lässt Personal Firewall alle Ping-Anforderungen zu, ohne die Ping-Signale im Protokoll der eingehenden Ereignisse aufzuzeichnen. Wenn Sie die Option nicht auswählen, blockiert Personal Firewall alle Ping-Anforderungen und zeichnet die Ping-Signale im Protokoll der eingehenden Ereignisse auf.

- **Änderung der Personal Firewall-Einstellungen für eine eingeschränkte Anzahl an Benutzern zulassen:** Wenn auf Ihrem Computer Windows XP oder Windows 2000 Professional mit mehreren Benutzern ausgeführt wird, wählen Sie diese Option, damit auch XP-Benutzer mit eingeschränkten Rechten die Einstellungen für Personal Firewall ändern können.

5 Klicken Sie auf **OK**, nachdem Sie die Änderungen vorgenommen haben.

Testen von McAfee Personal Firewall Plus

Sie können Ihre Personal Firewall-Installation auf mögliche Schwachstellen für Eindringlinge und auf verdächtige Aktivitäten testen.

So testen Sie Ihre Personal Firewall-Installation über das McAfee-Taskleistensymbol:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste und wählen **Firewall testen**.

Personal Firewall öffnet Internet Explorer und ruft die Website http://www.hackerwatch.org/ auf, die von McAfee verwaltet wird. Befolgen Sie die Anweisungen auf der Testseite von HackerWatch.org, um Personal Firewall zu testen.

Verwenden von McAfee SecurityCenter

Das 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 auf folgende nützliche Dienste zugreifen:

- Kostenlose Sicherheitsanalyse für Ihren Computer.
- Starten, Verwalten und Konfigurieren aller McAfee-Abonnements über ein einziges Symbol.
- Anzeige fortwährend aktualisierter Viruswarnungen und der neuesten Produktinformationen.
- 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 Dialogfenster **SecurityCenter** auf **Hilfe**.

Wenn SecurityCenter ausgeführt wird und alle auf Ihrem Computer installierten McAfee-Funktionen aktiviert sind, wird das Symbol mit dem roten M 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 starten Sie McAfee SecurityCenter:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol , und wählen Sie anschließend **SecurityCenter öffnen**.

So starten Sie Personal Firewall über McAfee SecurityCenter:

1 In SecurityCenter klicken Sie auf die Registerkarte **Personal Firewall Plus**.

2 Wählen Sie im Menü „Ich möchte…“ einen Task aus.

So starten Sie Personal Firewall von Windows aus:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste und zeigen dann auf **Personal Firewall**.

2 Wählen Sie einen Task.

Verwenden von McAfee Personal Firewall Plus

2

So öffnen Sie Personal Firewall:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend einen Task aus.

Info zur Zusammenfassung

Die Personal Firewall-Zusammenfassung enthält vier Zusammenfassungsseiten:

- Hauptübersicht
- Anwendungsübersicht
- Ereignisübersicht
- HackerWatch-Zusammenfassung

Die Zusammenfassungsseiten enthalten 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.

So öffnen Sie die Hauptübersicht in Personal Firewall:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Zusammenfassung anzeigen** (Abbildung 2-1).

Abbildung 2-1. Hauptübersicht

Klicken Sie auf die folgenden Steuerelemente, um zu den verschiedenen Zusammenfassungen zu navigieren:

Objekt	Beschreibung
Ansicht ändern	Klicken Sie auf **Ansicht ändern**, um eine Zusammenfassungsliste zu öffnen. Von dieser Liste aus können Sie die gewünschte Zusammenfassung zur Ansicht auswählen.
Pfeil nach rechts	Klicken Sie auf den Pfeil nach rechts, um die nächste Zusammenfassung anzuzeigen.
Pfeil nach links	Klicken Sie auf den Pfeil nach links, um die vorherige Zusammenfassung anzuzeigen.
Home	Klicken Sie auf das Home-Symbol, um zur **Hauptübersicht** zurückzukehren.

Die Seite mit der Hauptübersicht enthält folgende Informationen:

Objekt	Beschreibung
Sicherheitseinstellung	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	Hier wird die Anzahl der Ereignisse angezeigt, die am aktuellen Tag blockiert wurden. Klicken Sie auf den Link, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Änderungen von Anwendungsregeln	Hier wird die Anzahl der Anwendungsregeln angezeigt, die in letzter Zeit geändert wurden. Klicken Sie auf den Link, um die Liste der zugelassenen und blockierten Anwendungen anzuzeigen und 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 letzten eingehenden Ereignisse angezeigt. Klicken Sie auf einen Link, um den Ablauf des betreffenden Ereignisses zu verfolgen oder die IP-Adresse als vertrauenswürdig einzustufen. Von einer vertrauenswürdigen IP-Adresse gelangt der gesamte Datenverkehr auf Ihren Computer.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf den Link, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen aufgeführt, die zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um anzuzeigen, mit welchen IP-Adressen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf Personal Firewall-Seiten die Aktivitäten der Firewall anzuzeigen bzw. Tasks durchzuführen.

So öffnen Sie die Seite „Anwendungsübersicht“:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Zusammenfassung anzeigen**.
2. Klicken Sie auf **Ansicht ändern** und wählen dann **Anwendungsübersicht**.

Diese Seite enthält die folgenden Informationen:

Objekt	Beschreibung
Datenverkehrsmonitor	Der **Datenverkehrsmonitor** zeigt eingehende und ausgehende Internetverbindungen der vergangenen 15 Minuten. Klicken Sie auf das Diagramm, um Details zum Datenverkehr 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. **Regel erstellt am**: 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 zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um anzuzeigen, mit welchen IP-Adressen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf Personal Firewall-Seiten den Anwendungsstatus anzuzeigen bzw. anwendungsbezogene Tasks durchzuführen.

So öffnen Sie die Seite „Ereignisübersicht“:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Zusammenfassung anzeigen.**
2. Klicken Sie auf **Ansicht ändern** und wählen dann **Ereignisübersicht**.

Diese Seite enthält die folgenden Informationen:

Objekt	Beschreibung
Anschlussvergleich	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 auf der Seite der eingehenden Ereignisse aufgeführte Details dazu anzuzeigen. Außerdem können Sie eine Beschreibung des Anschlusses anzeigen, indem Sie den Mauszeiger über die Anschlussnummer bewegen.
Hauptverursacher	**Hauptverursacher** zeigt die am häufigsten blockierten IP-Adressen und für jede Adresse den Zeitpunkt des letzten eingehenden Ereignisses sowie die Gesamtzahl der eingehenden Ereignisse pro Adresse für die letzten dreißig Tage. Klicken Sie auf ein Ereignis, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf eine Zahl, um Ereignisdetails aus dem Protokoll der eingehenden Ereignisse anzuzeigen.
Letztes Ereignis	Unter **Letztes Ereignis** werden die letzten eingehenden Ereignisse angezeigt. Klicken Sie auf einen Link, um den Ablauf des betreffenden Ereignisses zu verfolgen oder die IP-Adresse als vertrauenswürdig einzustufen. Von einer vertrauenswürdigen IP-Adresse gelangt der gesamte Datenverkehr auf Ihren Computer.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf den Personal Firewall-Seiten Details zu Ereignissen anzuzeigen bzw. ereignisbezogene Tasks durchzuführen.

So öffnen Sie die Seite „HackerWatch-Zusammenfassung“:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Zusammenfassung anzeigen**.
2. Klicken Sie auf **Ansicht ändern** und wählen anschließend **HackerWatch-Zusammenfassung**.

Diese Seite enthält die folgenden Informationen:

Objekt	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.
Ereignisverfolgung	Unter **Ereignisverfolgung** wird die Anzahl der eingehenden Ereignisse angegeben, die an HackerWatch.org übermittelt wurden.
Globale Anschlussaktivität	Unter **Globale Anschlussaktivität** werden die Anschlüsse angegeben, die innerhalb der letzten fünf Tage offensichtlich am häufigsten eine Bedrohung dargestellt haben. Klicken Sie auf einen Anschluss, um die Anschlussnummer und die Anschlussbeschreibung anzuzeigen.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den HackerWatch.org-Seiten zu gelangen, auf denen Sie ausführlichere Informationen zur weltweiten Hackeraktivität erhalten.

Info zur Seite mit den Internetanwendungen

Mithilfe der Seite mit den Internetanwendungen können Sie die Liste der zugelassenen und blockierten Anwendungen anzeigen:

So starten Sie die Seite mit den Internetanwendungen:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Anwendungen** (Abbildung 2-2).

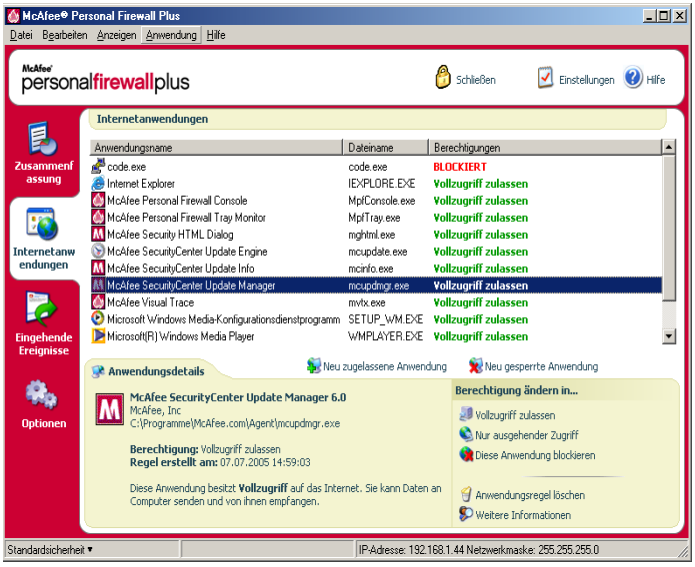


Abbildung 2-2. Seite mit Internetanwendungen

Diese Seite enthält folgende Informationen:

- Anwendungsname
- Dateiname
- Aktuelle Berechtigungsstufen
- Anwendungsdetails: Anwendungsname und -version, Name des Unternehmens, Pfadname, Berechtigung, Zeitstempel und Erläuterungen der Berechtigungsarten.

Ändern von Anwendungsregeln

Mit Personal Firewall können Sie die Zugriffsregeln für Anwendungen ändern.

So ändern Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Internetanwendungen** aus.
2. In der Liste der **Internetanwendungen** klicken Sie mit der rechten Maustaste auf die Anwendungsregel einer Anwendung und wählen eine andere Zugriffsstufe aus:
   - **Vollzugriff zulassen:** Lässt eingehende und ausgehende Internetverbindungen für die Anwendung zu.
   - **Nur ausgehender Zugriff:** Lässt nur ausgehende Internetverbindungen für die Anwendung zu.
   - **Diese Anwendung blockieren:** Lässt keinerlei Internetzugriff dieser Anwendung zu.

     HINWEIS
     Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn die Firewall auf die Sicherheitseinstellung **Offen (Kein Filter)** oder **Verbindung schließen** gesetzt wird. Wenn dies nicht erwünscht ist, können Sie entweder die Zugriffsregel der Anwendung auf **Vollzugriff zulassen** setzen oder die Berechtigungsregel **Blockiert** aus der Liste **Internetanwendungen** löschen.

So löschen Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Internetanwendungen**.
2. In der Liste der **Internetanwendungen** klicken Sie mit der rechten Maustaste auf die Anwendungsregel, und wählen Sie dann **Anwendungsregel löschen** aus.

Wenn die Anwendung das nächste Mal Internetzugriff anfordert, können Sie ihre Berechtigungsstufe erneut festlegen, um sie der Liste wieder hinzuzufügen.

Zulassen und Blockieren von Internetanwendungen

So ändern Sie die Liste der zugelassenen und blockierten Internetanwendungen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Internetanwendungen**.
2. Auf der Seite mit den Internetanwendungen klicken Sie auf eine der folgenden Optionen:
   - **Neu zugelassene Anwendung:** Hiermit gewähren Sie einer Anwendung vollen Internetzugriff.
   - **Neu gesperrte Anwendung:** Hiermit sperren Sie den Internetzugriff einer Anwendung.
   - **Anwendungsregel löschen:** Hiermit entfernen Sie eine Anwendungsregel.

Info zur Seite mit den eingehenden Ereignissen

Über die Seite für eingehende Ereignisse können Sie das Protokoll eingehender Ereignisse anzeigen, das erstellt wird, wenn Personal Firewall unaufgeforderte Internetverbindungen blockiert.

So starten Sie die Seite für eingehende Ereignisse:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse** (Abbildung 2-3).

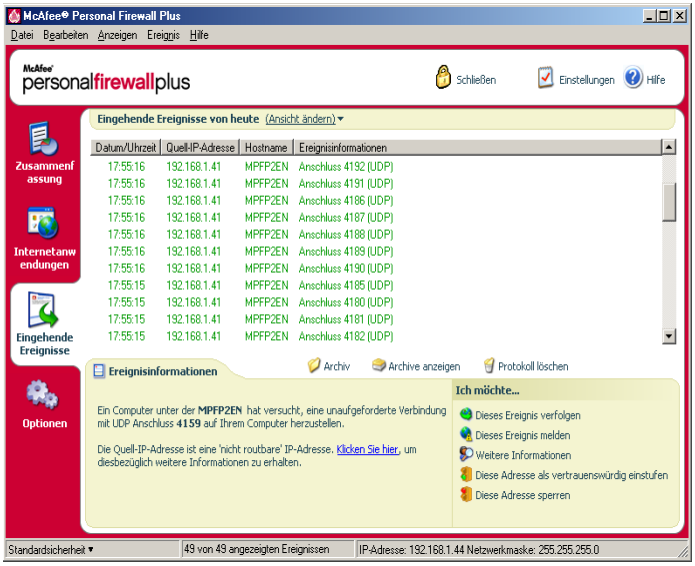


Abbildung 2-3. Seite mit eingehenden Ereignissen

Die Seite mit den eingehenden Ereignissen enthält folgende Informationen:

- Zeitstempel
- Quell-IP-Adressen
- Hostnamen
- Dienst- oder Anwendungsnamen
- Ereignisdetails: Verbindungstypen, Verbindungsanschlüsse, Hostnamen oder IP-Adresse und Erläuterungen zu Anschlussereignissen

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.

IP-Adresstypen

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. Wird dieser Adresstyp erkannt, weist Personal Firewall darauf hin, dass der Datenverkehr eine leere IP-Adresse verwendet hat. Häufig ist dies ein Hinweis darauf, dass der Absender absichtlich die Quelle des Datenverkehrs verschleiert. 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. Beispielsweise ist 0.0.0.0 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 besteht darin, 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 die Situation eintreten, dass diese Pakete als Ereignis gemeldet werden.

Die zweite Ursache besteht darin, dass die Quell-IP-Adresse gefälscht wurde. Gefälschte Pakete können ein Anzeichen dafür sein, dass jemand Ihren Computer auf Trojaner überprüft. Personal Firewall blockiert diese Aktivitäten, so dass Ihr Computer geschützt ist.

Ereignisse von 127.0.0.1

Ereignisse geben manchmal die Quell-IP-Adresse 127.0.0.1 an. Dies wird als Loopback-Adresse oder „localhost“ bezeichnet.

Viele legitime Programme verwenden die Loopback-Adresse für die Kommunikation zwischen Komponenten. Sie können beispielsweise viele persönliche E-Mail- oder Webserver über eine Weboberfläche konfigurieren. Um die Weboberfläche aufzurufen, geben Sie „http://localhost/“ in Ihren Webbrowser ein.

Personal Firewall lässt Datenverkehr von diesen Programmen zu. Wenn also 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 weisen in der Regel darauf hin, dass Ihr Computer von einem anderen auf Trojaner überprüft wird. Personal Firewall blockiert dieses versuchte Eindringen, so dass Ihr Computer geschützt ist.

Für einige Programme, insbesondere 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 ermitteln 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. Wenn jedoch bei einem Programm (wie Netscape) Probleme auftreten, fügen Sie 127.0.0.1 zur Liste der vertrauenswürdigen IP-Adressen in Personal Firewall hinzu.

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 jedoch die Gefahr verringert, dass Angriffe mit gefälschten Adressen ausgeführt werden.

Ereignisse von Computern in Ihrem lokalen Netzwerk (LAN)

Ereignisse können auch von Computern in Ihrem LAN (Local Area Network) generiert werden. Um anzuzeigen, dass diese Ereignisse durch Ihr Netzwerk erzeugt werden, werden sie in Personal Firewall grün dargestellt.

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 kann Ihr „lokales“ Netzwerk genauso gefährlich sein wie das Internet; insbesondere, wenn Ihr Computer an ein Netzwerk mit einer hohen Bandbreite, beispielsweise DSL oder Kabelmodem, angeschlossen ist. Wählen Sie in diesem Fall nicht die Option **Alle Computer in meinem LAN als vertrauenswürdig einstufen**. Nehmen Sie stattdessen die IP-Adressen der lokalen Computer manuell in die Liste der vertrauenswürdigen IP-Adressen auf.

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-Adressen bezeichnet. Diese IP-Adressen sollten niemals Ihr Netzwerk verlassen und können in der Regel als vertrauenswürdig angesehen werden.

Der Block 192.168.xxx.xxx 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 Trojanern 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

Das Protokoll der eingehenden Ereignisse zeigt Ereignisse in unterschiedlicher Form an. 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 mit identischen Ereignisinformationen anzuzeigen.

Um Informationen zu einem Ereignis anzuzeigen, klicken Sie auf das Ereignis und zeigen die Informationen im Bereich **Ereignisinformationen** an.

Anzeigen der Ereignisse von heute

Verwenden Sie diese Option, um die Ereignisse des heutigen Tags anzuzeigen.

So zeigen Sie die Ereignisse von heute an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Ereignisse von heute anzeigen**.

Anzeigen der Ereignisse aus dieser Woche

Verwenden Sie diese Option, um die Ereignisse dieser Woche anzuzeigen.

So zeigen Sie die Ereignisse aus dieser Woche an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Ereignisse aus dieser Woche anzeigen**.

Anzeigen des vollständigen Protokolls eingehender Ereignisse

Verwenden Sie diese Option, um alle Ereignisse dieser Woche anzuzeigen.

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 **Inbound Events**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Vollständiges Protokoll anzeigen**.

   Das Protokoll der eingehenden Ereignisse zeigt alle Ereignisse an.

Anzeigen von Ereignissen eines bestimmten Tags

Verwenden Sie diese Option, um die Ereignisse eines bestimmten Tags anzuzeigen.

So zeigen Sie die Ereignisse eines bestimmten Tags an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse des ausgewählten Tages anzeigen**.

Anzeigen von Ereignissen einer bestimmten Internetadresse

Verwenden Sie diese Option, um andere Ereignisse anzuzeigen, die von einer bestimmten Internetadresse stammen.

So zeigen Sie Ereignisse von einer bestimmten Internetadresse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und klicken auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse mit der ausgewählten Internetadresse anzeigen**.

Anzeigen von Ereignissen, die über identische gemeinsame Ereignisinformationen verfügen

Verwenden Sie diese Option, wenn Sie wissen möchten, ob das Protokoll der eingehenden 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 Dienst hervor, das bzw. der diesen Anschluss verwendet.

So zeigen Sie Ereignisse an, die über identische gemeinsame Ereignisinformationen verfügen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und klicken auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse mit identischen Ereignisinformationen anzeigen**.

Reagieren auf eingehende Ereignisse

Zusätzlich zur Überprüfung von Details zu Ereignissen im Protokoll eingehender Ereignisse 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.

So verfolgen Sie ein ausgewähltes Ereignis:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen **Eingehende Ereignisse**.
2. Im Protokoll der eingehenden Ereignisse klicken Sie mit der rechten Maustaste auf das zu verfolgende Ereignis und klicken dann auf **Ausgewähltes Ereignis verfolgen**. Sie können auch auf ein Ereignis doppelklicken, um eine Ereignisverfolgung durchzuführen.

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

Abrufen von Ratschlägen von HackerWatch.org

So rufen Sie Ratschläge von HackerWatch.org ab:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse**.
2. Wählen Sie den Ereigniseintrag auf der Seite der eingehenden Ereignisse, und klicken Sie dann im Bereich **Ich möchte…** auf **Weitere Informationen**.

Ihr Standard-Webbrowser wird gestartet und öffnet die Seite HackerWatch.org, um Informationen zum Ereignistyp abzurufen und zu ermitteln, ob das Ereignis gemeldet werden sollte.

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 in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen **Eingehende Ereignisse**.
2. Klicken Sie auf das zu meldende Ereignis und danach im Bereich **Ich möchte…** auf **Dieses Ereignis melden**.

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

Anmelden bei HackerWatch.org

Beim ersten Öffnen der Zusammenfassungsseite kontaktiert Personal Firewall HackerWatch.org, um Ihre eindeutige Benutzer-ID zu generieren. Wenn Sie 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 Maßnahmen 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

Sie können die Seite der eingehenden Ereignisse dazu verwenden, eine IP-Adresse zur Liste der vertrauenswürdigen IP-Adresse hinzuzufügen, um eine permanente Verbindung zuzulassen.

Wenn auf der Seite 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.

So fügen Sie eine IP-Adresse zur Liste der vertrauenswürdigen IP-Adressen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen **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 **Quell-IP-Adresse als vertrauenswürdig einstufen**.

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 zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.

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

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Optionen** aus.
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 aktiviert in der Liste der vertrauenswürdigen IP-Adressen angezeigt.

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, den Zugriff unterbinden zu müssen.

Wenn auf der Seite der eingehenden Ereignisse ein Ereignis angezeigt wird, das eine zu sperrende IP-Adresse enthält, können Sie Personal Firewall so konfigurieren, dass Verbindungen mit dieser Adresse in jedem Fall unterbunden werden.

Sie können die Seite der eingehenden Ereignisse, auf der die IP-Adressen des gesamten eingehenden Datenverkehrs aufgeführt werden, dazu verwenden, eine IP-Adresse zu sperren, die vermutlich die Quelle verdächtiger oder unerwünschter Internetaktivität bildet.

So fügen Sie eine IP-Adresse zur Liste der gesperrten IP-Adressen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Die Seite der eingehenden Ereignisse listet die IP-Adressen des gesamten eingehenden Internetdatenverkehrs auf. Wählen Sie eine IP-Adresse aus und wählen Sie eine der folgenden Vorgehensweisen:
   - Klicken Sie mit der rechten Maustaste auf die IP-Adresse, und wählen Sie dann **Quell-IP-Adresse sperren**.
   - Klicken Sie im Menü **Ich möchte…** auf die Option **Diese Adresse sperren**.

3 Verwenden Sie im Dialogfeld zum Hinzufügen einer gesperrten IP-Adressregel eine der folgenden Einstellungen zur Konfiguration einer Regel für gesperrte IP-Adressen:

- **Eine einzelne IP-Adresse:** Die zu sperrende IP-Adresse. Standardmäßig ist die IP-Adresse eingetragen, die Sie auf der Seite der eingehenden Ereignisse ausgewählt haben.
- **Ein IP-Adressbereich:** Die IP-Adressen zwischen der Adresse in „Von IP-Adresse“ und der Adresse in „An IP-Adresse“.
- **Ablaufdatum für diese Regel festlegen auf:** Datum und Uhrzeit, zu der die gesperrte IP-Adresse abläuft. Wählen Sie die gewünschten Werte für Datum und Uhrzeit aus dem Aufklappmenü.
- **Beschreibung:** Bei Bedarf beschreiben Sie die neue Regel.
- Klicken Sie auf **OK**.

4 Klicken Sie im Dialogfeld auf **Ja**, um Ihre Einstellungen zu bestätigen. Klicken Sie auf **Nein**, um zum Dialogfeld zum Hinzufügen einer gesperrten IP-Adressregel zurückzukehren.

Wenn Personal Firewall ein Ereignis von einer gesperrten Internetverbindung erkennt, wird eine Warnung entsprechend der angegebenen Methode auf der Seite „Warneinstellungen“ ausgegeben.

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

1 Klicken Sie auf die Registerkarte **Optionen**.

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 aktiviert 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 der eingehenden Ereignisse archivieren, um sämtliche protokollierte eingehende Ereignisse einschließlich Datum und Uhrzeit, Hostnamen, Anschlüssen und Ereignisinformationen zu speichern. Sie sollten Ihr Protokoll eingehender Ereignisse regelmäßig archivieren, damit das Protokoll nicht zu groß wird.

So archivieren Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Archiv**.
3. Klicken Sie im Dialogfeld „Protokoll archivieren“ auf **Ja**, um den Archivierungsvorgang fortzusetzen.
4. Klicken Sie auf **Speichern**, um das Archiv im Standardspeicherort zu speichern, oder navigieren Sie zu dem Speicherort, an dem das Archiv gespeichert werden soll.

Hinweis: Standardmäßig archiviert Personal Firewall automatisch das Protokoll eingehender Ereignisse. Aktivieren oder deaktivieren Sie die Option **Protokollierte Ereignisse automatisch archivieren** auf der Seite der Ereignisprotokolleinstellungen, indem Sie das Häkchen setzen oder entfernen.

Anzeigen des archivierten Protokolls eingehender Ereignisse

Sie können zuvor archivierte Protokolle eingehender Ereignisse anzeigen. Das gespeicherte Archiv enthält Datum und Uhrzeit, Quell-IP-Adressen, Hostnamen, Anschlüsse und Ereignisinformationen zu den Ereignissen.

So zeigen Sie das archivierte Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Archive anzeigen**.
3. Suchen bzw. wählen Sie den Dateinamen des Archivs, und klicken Sie auf **Öffnen**.

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.

So löschen Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse**.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Protokoll löschen**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das Protokoll zu löschen.

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.

So kopieren Sie Ereignisse in die Zwischenablage:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis im Protokoll eingehender Ereignisse.
3. Klicken Sie auf **Ausgewähltes Ereignis in Zwischenablage kopieren**.
4. Starten Sie Editor.
   - Geben Sie `notepad` in die Befehlszeile ein, oder klicken Sie auf die Windows-Schaltfläche **Start**, zeigen auf **Programme**, dann auf **Zubehör**. Wählen Sie **Editor** aus.
5. Klicken Sie auf **Bearbeiten**, und klicken Sie anschließend auf „Einfügen“. Der Ereignistext wird in Editor angezeigt. Wiederholen Sie diesen Schritt so oft, bis Sie alle erforderlichen Ereignisse in Editor eingefügt haben.
6. Speichern Sie die Editor-Datei an einem sicheren Ort.

Löschen von ausgewählten Ereignissen

Sie können Ereignisse aus dem Protokoll eingehender Ereignisse löschen.

So löschen Sie Ereignisse aus dem Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen auf **Personal Firewall** und wählen anschließend **Eingehende Ereignisse**.
2. Klicken Sie auf der Seite eingehender Ereignisse auf den zu löschenden Ereigniseintrag.
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 zusätzlich angegebenen Empfehlungen angezeigt werden sollen, klicken Sie auf die Registerkarte **Optionen**, 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** aus.

Rote Warnungen

Rote Warnungen enthalten wichtige Informationen, und es ist ein sofortiges Eingreifen Ihrerseits erforderlich:

- **Internetanwendung blockiert:** Diese Warnung wird angezeigt, wenn Personal Firewall eine Anwendung daran hindert, auf das Internet zuzugreifen. Wenn beispielsweise eine Warnung zu einem Trojaner 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.
- **Die Anwendung wurde geändert:** Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung, der Sie zuvor Zugriff auf das Internet gewährt haben, geändert wurde. Falls Sie die Anwendung nicht kürzlich aktualisiert haben, gehen Sie mit Bedacht vor, wenn Sie ihr Zugriff auf das Internet gewähren.
- **Die 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.

HINWEIS
Die Standardeinstellung für automatische Updates von Windows XP SP2 lädt Updates für das Windows-Betriebssystem und andere auf Ihrem Rechner ausgeführte Microsoft-Programme herunter und installiert diese, ohne dass Sie darüber benachrichtigt werden. Wenn eine Anwendung durch ein solches stilles Windows-Update geändert wurde, zeigt McAfee Personal Firewall bei der nächsten Ausführung der betreffenden Microsoft-Anwendung eine Meldung an.

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

Warnung „Internetanwendung blockiert“

Wenn eine Warnung zu einem Trojaner angezeigt wird (Abbildung 2-4), verweigert Personal Firewall diesem Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer nach Viren zu durchsuchen. Wenn McAfee VirusScan nicht installiert ist, starten Sie McAfee SecurityCenter.

Abbildung 2-4. Warnung „Internetanwendung blockiert“

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 zur Seite mit den eingehenden Ereignissen* auf Seite 24).
- Klicken Sie auf **Launch McAfee VirusScan (McAfee VirusScan starten)**, um den Computer nach Viren zu durchsuchen.

- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Abgehenden Zugriff gewähren**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).

Warnung „Die Anwendung möchte auf das Internet zugreifen“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-5) aus, wenn Internet- oder Netzwerkverbindungen für neue oder geänderte Anwendungen erkannt werden.

Abbildung 2-5. Warnung „Die Anwendung möchte auf das Internet zugreifen“

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 für die automatische Verwendung von Empfehlungen konfiguriert wurde.

McAfee erkennt das Programm, das auf das Internet zugreifen möchte, möglicherweise nicht (Abbildung 2-6).

Abbildung 2-6. Warnung bei nicht erkannter Anwendung

Deshalb kann McAfee nicht empfehlen, wie Sie mit dem Programm verfahren sollen. Sie können McAfee dieses Programm melden, indem Sie auf **Informieren Sie McAfee über dieses Programm** klicken. Es wird eine Webseite angezeigt, auf der Sie nach Informationen zu dem Programm gefragt werden. Übermitteln Sie so viele Informationen wie möglich.

Die übermittelten Informationen werden von unseren HackerWatch-Mitarbeitern in Verbindung mit anderen Tools verwendet, um festzustellen, ob ein Programm in unsere Datenbankliste der bekannten Programme aufgenommen werden soll, und wenn ja, wie Personal Firewall damit umgehen soll.

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

- Klicken Sie auf **Zugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Zugriff einmal gewähren**, um eine temporäre Internetverbindung der Anwendung zuzulassen. Für die Anwendung wird der Zugriff nur solange gewährt, wie Sie mit dieser arbeiten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf **Abgehenden Zugriff gewähren**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren.

Warnung „Die Anwendung wurde geändert“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-7) aus, wenn eine Anwendung geändert wurde, der Sie zuvor den Internetzugriff gewährt haben. Falls Sie die fragliche Anwendung nicht erst kürzlich aktualisiert haben, gehen Sie mit Bedacht vor, wenn Sie ihr Zugriff auf das Internet gewähren.

Abbildung 2-7. Warnung „Die Anwendung wurde geändert“

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

- Klicken Sie auf **Zugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Zugriff einmal gewähren**, um eine temporäre Internetverbindung der Anwendung zuzulassen. Für die Anwendung wird der Zugriff nur solange gewährt, wie Sie mit dieser arbeiten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf **Abgehenden Zugriff gewähren**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren.

Warnung „Die Anwendung fordert Serverzugriff an“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-8) aus, wenn erkannt wird, dass eine Anwendung, der Sie zuvor den Zugriff auf das Internet gewährt haben, den Internetzugriff als Server angefordert hat.

Abbildung 2-8. Warnung „Die Anwendung fordert Serverzugriff an“

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 **Zugriff einmal gewähren**, um einen temporären Internetzugriff der Anwendung zuzulassen. Für die Anwendung wird der Zugriff nur solange gewährt, wie Sie mit dieser arbeiten.
- Klicken Sie auf **Serverzugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken**, um eingehende Internetverbindungen zu verhindern.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren. Grüne Warnungen

Grüne Warnungen

Grüne Warnungen benachrichtigen Sie bei Ereignissen in Personal Firewall, wenn beispielsweise einer Anwendung automatisch Internetzugriff gewährt wurde.

Das Programm darf auf das Internet zugreifen: Diese Warnung wird angezeigt, wenn Personal Firewall automatisch allen neuen 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.

Warnung „Programm darf auf das Internet zugreifen“

Wenn Sie in den Optionen für die Sicherheitseinstellungen die Einstellung **Vertrauenswürdig** ausgewählt haben, gewährt Personal Firewall automatisch allen neuen Anwendungen Internetzugriff, und informiert Sie anschließend in Form einer Warnung (Abbildung 2-9).

Abbildung 2-9. 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 über das Internetanwendungsprotokoll Details zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite mit den Internetanwendungen* auf Seite 21).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um die Anzeige dieses Warnungstyps zu unterdrücken.

- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.

Warnung „Die Anwendung wurde geändert“

Wenn Sie in den Optionen für die Sicherheitseinstellungen die Einstellung **Vertrauenswürdig** ausgewählt haben, gewährt Personal Firewall automatisch allen neuen und geänderten Anwendungen Internetzugriff. 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 zur Seite mit den Internetanwendungen* auf Seite 21).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um die Anzeige dieses Warnungstyps zu unterdrücken.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.

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 die Sicherheitseinstellung **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 2-10) aus, wenn unerwünschter Internet- oder Netzwerkverkehr blockiert wird.

Abbildung 2-10. 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 über das Protokoll eingehender Ereignisse von Personal Firewall Details zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite mit den eingehenden Ereignissen* auf Seite 24).
- 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.

Index

S

T

V

W

Z