McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Benutzerhandbuch

Inhalt

KAPITEL 1

Einleitung

McAfee VirusScan Plus Suite schützt Ihren Computer und Ihre Dateien vor Viren, Spyware und Hackern. Sie können sicher und unbeschwert im Internet surfen und Dateien herunterladen, weil Sie wissen, dass McAfee immer aktiv ist, immer aktualisiert wird und Sie somit immer schützt. Der zuverlässige Schutz von McAfee blockiert Bedrohungen und hält Hacker automatisch ab, so dass Ihr Computer "gesund" und sicher bleibt. McAfee ermöglicht außerdem die einfache Kontrolle Ihres Sicherheitsstatus sowie das einfache Überprüfen auf Viren und Spyware und gewährleistet, dass Ihre Produkte dank dem neu gestalteten McAfee SecurityCenter stets auf dem neuesten Stand sind. Zusätzlich erhalten Sie automatisch mit Ihrem Abonnement die neueste McAfee-Software und die neuesten Updates.

VirusScan Plus enthält folgende Programme:

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (nur Lizenz für 3 Benutzer)
- SiteAdvisor

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter ist eine benutzerfreundliche Umgebung, in der McAfee-Benutzer ihre Sicherheitsabonnements starten, verwalten und konfigurieren können.

SecurityCenter dient außerdem als Informationsquelle für Viruswarnungen, Produktinformationen, Support und Abonnementinformationen sowie als schnelle Verbindung zu den Tools und News auf der McAfee-Website.

In diesem Kapitel

Funktionen

McAfee SecurityCenter bietet folgende neue Funktionen und Vorteile:

Neu entworfener Sicherheitsstatus

Vereinfacht es, den Sicherheitsstatus Ihres Computers zu prüfen, nach Updates zu suchen und potentielle Sicherheitsrisiken zu beseitigen.

Ständige Updates und Upgrades

Installiert automatisch tägliche Updates. Wenn eine neue Version von McAfee verfügbar wird, erhalten Sie diese während der Laufzeit Ihres Abonnements automatisch, so dass gewährleistet wird, dass Sie stets über den aktuellsten Schutz verfügen.

Warnungen in Echtzeit

Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

Umfassender Schutz

Eine Vielzahl von Erneuerungsoptionen, so dass Ihr McAfee-Schutz stets auf dem aktuellsten Stand ist.

Leistungs-Tools

Entfernt nicht verwendete Dateien, defragmentiert verwendete Dateien und verwendet die Systemwiederherstellung, um Ihren Computer auf höchstem Leistungsniveau zu halten.

Echte Online-Hilfe

Unterstützung von Experten für Computer-Sicherheit von McAfee über den Internet-Chat, per E-Mail oder das Telefon.

Schutz für sicheres Surfen

Das McAfee SiteAdvisor-Browser-Plugin hilft Ihnen, sofern installiert, sich vor Spyware, Spam, Viren und Online-Bedrohungen zu schützen, indem es Websites klassifiziert, die Sie besuchen, oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie erhalten ausführliche Sicherheitsklassifizierungen, die belegen, wie eine Site beim Test der E-Mail-Praktiken, Downloads, Online-Zugehörigkeiten und Störungen, z. B. Popups und Nachverfolgungs-Cookies von Fremdherstellern, abgeschnitten hat.

KAPITEL 3

Verwenden von SecurityCenter

SecurityCenter wird über das McAfee SecurityCenter-Symbol im Windows-Benachrichtigungsbereich rechts neben der Taskleiste oder über Ihren Windows-Desktop gestartet.

Wenn Sie SecurityCenter öffnen, wird im Bereich "Home" der Schutzstatus Ihres Computers angezeigt, und Sie erhalten schnellen Zugriff auf Update-, Scan (falls McAfee VirusScan installiert ist) und andere häufig auftretende Tasks:

Header

Hilfe

Anzeigen der Hilfedatei zur Anwendung

Linke Spalte

Aktualisieren

Aktualisieren Sie Ihr Produkt, um zu gewährleisten, dass Ihr Computer vor den neuesten Bedrohungen geschützt ist.

Scannen

Falls McAfee VirusScan installiert ist, können Sie einen manuellen Scan Ihres Computers durchführen.

Häufige Tasks

Führen Sie häufig vorkommende Tasks aus, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

Komponenten installiert

Hier sehen Sie, welche Sicherheitsdienste die Sicherheit Ihres Computers schützen.

Hauptbereich

Sicherheitsstatus

Unter **Bin ich geschützt** finden Sie die allgemeine Ebene für den Schutzstatus Ihres Computers. Darunter können Sie Details zu diesem Status nach der Schutzkategorie und dem Schutztyp anzeigen.

SecurityCenter-Informationen

Zeigen Sie an, wann die letzte Aktualisierung Ihres Computers stattgefunden hat, wann der letzte Scan durchgeführt wurde (falls McAfee VirusScan installiert ist) und wann Ihr Abonnement abläuft.

In diesem Kapitel

Erläuterungen zu den SecurityCenter-Symbolen

In Ihrem Windows-Benachrichtigungsbereich werden SecurityCenter-Symbole rechts neben der Taskleiste angezeigt. Verwenden Sie diese Symbole, um zu erkennen, ob Ihr Computer umfassend geschützt ist, ob gerade ein Scan durchgeführt wird (falls McAfee VirusScan installiert ist), ob Updates vorliegen, um kürzlich aufgetretene Ereignisse anzuzeigen, Ihren Computer zu warten und Support von der McAfee-Website zu erhalten.

Öffnen von SecurityCenter und Verwenden der zusätzlichen Funktionen

Wenn SecurityCenter ausgeführt wird, wird das SecurityCenter M-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So öffnen Sie SecurityCenter und verwenden die zusätzlichen Funktionen:

- Klicken Sie mit der rechten Maustaste auf das Hauptsymbol von SecurityCenter, und klicken Sie anschließend auf eine der folgenden Optionen:
  - SecurityCenter öffnen
  - Updates
  - Direkte Links

    Das Untermenü enthält Links zu "Home", "Kürzlich aufgetretene Ereignisse", "Netzwerk verwalten", "Computer warten" und "Datensicherung" (falls installiert).
  - Abonnement überprüfen

    (Dieses Element wird angezeigt, wenn mindestens ein Produkt-Abonnement abgelaufen ist.)
  - Upgrade Center
  - Kundendienst

Prüfen Ihres Schutzstatus

Wenn Ihr Computer nicht umfassend geschützt ist, wird das Symbol für den Schutzstatus rechts neben der Taskleiste im Windows-Systembereich angezeigt. Das Symbol kann je nach dem Schutzstatus rot oder gelb sein.

So prüfen Sie Ihren Schutzstatus:

- Klicken Sie auf das Symbol für den Schutzstatus, um SecurityCenter zu öffnen und etwaige Probleme zu beheben.

Prüfen des Status Ihrer Updates

Wenn Sie auf Updates prüfen, wird das Updates-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So prüfen Sie den Status Ihrer Updates:

- Zeigen Sie auf das Updates-Symbol, um den Status Ihrer Updates als Quickinfo anzuzeigen.

Erläuterungen zum Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme. Wenn ein Problem mehr als eine Schutzkategorie betrifft, kann das Beheben dieses Problems dazu führen, dass mehrere Kategorien wieder den Status für umfassenden Schutz erreichen.

Zu den Faktoren für den Schutzstatus zählen externe Sicherheitsbedrohungen, die auf dem Computer installierten Sicherheitsprodukte, Produkte mit Zugriff auf das Internet sowie deren Konfiguration.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten.

Bin ich geschützt?

Informationen zur Gesamtebene des Schutzstatus Ihres Computers finden Sie unter **Bin ich geschützt** in SecurityCenter.

- **Ja** wird angezeigt, wenn Ihr Computer umfassend geschützt ist (grün).
- **Nein** wird angezeigt, wenn Ihr Computer teilweise geschützt (gelb) oder nicht geschützt (rot) ist.

Um die meisten Sicherheitsprobleme automatisch zu lösen, klicken Sie neben dem Schutzstatus auf **Beheben**. Wenn jedoch ein oder mehrere Probleme weiterhin bestehen und Ihre Reaktion erfordern, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

Erläuterungen zu den Schutzkategorien und -typen

Unter **Bin ich geschützt** in SecurityCenter können Sie Details zum Status anzeigen, aufgeschlüsselt nach den folgenden Schutzkategorien und -typen:

- Computer und Dateien
- Internet und Netzwerk
- E-Mail und IM
- Parental Controls

Die in SecurityCenter angezeigten Schutztypen hängen davon ab, welche Produkte installiert sind. Wenn beispielsweise der PC Health-Schutztyp angezeigt wird, ist die McAfee-Datensicherungssoftware installiert.

Wenn in einer Kategorie keine Sicherheitsprobleme vorliegen, ist der Status "grün". Wenn Sie auf eine grüne Kategorie klicken, wird rechts eine Liste der aktivierten Schutztypen angezeigt, gefolgt von einer Liste der bereits ignorierten Probleme. Wenn keine Probleme vorliegen, wird eine Virushinweis statt der Probleme angezeigt. Sie können auch auf **Konfigurieren** klicken, um Ihre Optionen für diese Kategorie zu ändern.

Wenn alle Schutztypen in einer Kategorie den Status "grün" aufweisen, ist der Status der Kategorie insgesamt "grün". Wenn alle Schutzkategorien den Status "grün" aufweisen, ist der Schutzstatus insgesamt "grün".

Wenn eine der Schutzkategorien den Status "gelb" oder "rot" aufweist, können Sie die Sicherheitsprobleme lösen, indem Sie sie beheben oder ignorieren, wodurch sich der Status in "grün" ändert.

Erläuterungen zum Schutz von Computer und Dateien

Die Schutzkategorie "Computer und Dateien" umfasst die folgenden Schutztypen:

- **Virenschutz**: Der Echtzeit-Scan-Schutz schützt Ihren Computer vor Viren, Würmern, Trojanern, verdächtigen Skripts, Hybridangriffen und anderen Bedrohungen. Das Programm führt automatische Scans durch und versucht, die Dateien zu säubern (einschließlich komprimierter .exe-Dateien, des Boot-Sektors, des Speichers und wichtiger Dateien), wenn Sie oder Ihr Computer darauf zugreifen.
- **Spyware-Schutz**: Der Spyware-Schutz dient zur raschen Erkennung, Blockierung und Entfernung von Spyware, Adware und anderen potentiell unerwünschten Programmen, die Ihre persönlichen Daten sammeln und ohne Ihre Zustimmung weiterleiten.
- **SystemGuards**: SystemGuards erkennt Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Sie können diese Änderungen prüfen und entscheiden, ob Sie sie erlauben möchten.
- **Windows-Schutz**: Der Windows-Schutz gibt den Status des Windows-Updates auf Ihrem Computer an. Wenn McAfee VirusScan installiert ist, steht außerdem der Pufferüberlaufschutz zur Verfügung.

Einer der Faktoren für den Schutz von Computer und Dateien sind externe Virusbedrohungen. Schützt beispielsweise Ihre Antivirensoftware Ihren Computer, wenn ein Virenausbruch stattfindet? Zu den weiteren Faktoren gehören die Konfiguration Ihrer Antivirensoftware und ob Ihre Software fortlaufend mit den neuesten Erkennungssignaturdateien aktualisiert wird, damit der Schutz Ihres Computers vor den neuesten Bedrohungen gewährleistet bleibt.

Öffnen des Konfigurationsbereichs für "Computer und Dateien"

Wenn unter **Computer & Dateien** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Computer und Dateien":

1. Klicken Sie im Home-Bereich auf **Computer & Dateien**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Schutz von Internet und Netzwerk

Die Schutzkategorie "Internet und Netzwerk" umfasst die folgenden Schutztypen:

- **Firewall-Schutz**: Der Firewall-Schutz schützt Ihren Computer vor Intrusionen und unerwünschtem Netzwerkverkehr. Gewährt alle eingehenden und ausgehenden Internetverbindungen.
- **Drahtloser Schutz**: Der drahtlose Schutz schützt Ihr privates drahtloses Netzwerk vor Intrusionen und Datenabfang. Wenn Sie jedoch derzeit mit einem externen drahtlosen Netzwerk verbunden sind, variiert Ihr Schutz in Abhängigkeit der Sicherheitsebene dieses Netzwerks.
- **Web-Browsing-Schutz**: Der Web-Browsing-Schutz verhindert, dass auf Ihrem Computer Werbung, Popups und Web-Bugs ausgeführt werden, während Sie im Internet surfen.
- **Phishing-Schutz**: Der Phishing-Schutz hilft dabei, betrügerische Websites zu blockieren, die über Hyperlinks in E-Mails und Instant Messages, Popups und anderen Quellen persönliche Informationen abrufen.
- **Personal Information Protection**: Personal Information Protection blockiert die Veröffentlichung wichtiger und vertraulicher Daten im Internet.

Öffnen des Konfigurationsbereichs für "Internet und Netzwerk"

Wenn unter **Internet & Netzwerk** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Internet und Netzwerk":

1. Klicken Sie im Home-Bereich auf **Internet & Netzwerk**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zu E-Mail- und IM-Schutz

Die Schutzkategorie "E-Mail- und IM-Schutz" umfasst die folgenden Schutztypen:

- **E-Mail-Schutz**: Der E-Mail-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden und ausgehenden E-Mail-Nachrichten und -Anhängen zu säubern.
- **Spam-Schutz**: Der Spam-Schutz hilft Ihnen, Ihren E-Mail-Posteingang frei von unerwünschten E-Mails zu halten.
- **IM-Schutz**: Der Instant Messaging (IM)-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden Instant Messaging-Nachrichten zu säubern. Das Programm verhindert außerdem, dass Instant Messaging-Clients unerwünschte Inhalte oder persönliche Informationen über das Internet austauschen.
- **Schutz für sicheres Surfen**: Falls installiert, hilft das McAfee SiteAdvisor-Browser-Plugin dabei, Ihren Computer vor Spyware, Spam, Viren und Online-Scams zu schützen, indem es Websites bewertet, die Sie besuchen oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie können detaillierte Sicherheitsbewertungen anzeigen, aus denen hervorgeht, wie eine Site auf E-Mail-Praktiken, Downloads, Online-Partnerschaften und störende Praktiken, wie Popups und Verfolgungs-Cookies von Drittanbietern, getestet wird.

Öffnen des Konfigurationsbereichs für "E-Mail und IM"

Wenn unter **E-Mail & IM** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "E-Mail und IM"

1. Klicken Sie im Home-Bereich auf **E-Mail & IM**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Parental Controls-Schutz

Die Schutzkategorie "Parental Controls" umfasst die folgenden Schutztypen:

- **Parental Controls**: Die Inhaltsblockierung verhindert, dass Benutzer unerwünschte Internet-Inhalte anzeigen, indem potentiell schädliche Websites blockiert werden. Die Internetaktivitäten und die -nutzung der Benutzer können außerdem überwacht und eingeschränkt werden.

Öffnen des Konfigurationsbereichs für "Parental Controls"

Wenn unter **Parental Controls** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Parental Controls":

1. Klicken Sie im Home-Bereich auf **Parental Controls**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden. Wenn ein oder mehrere Probleme dennoch weiterhin vorliegen, müssen Sie sie lösen.

Automatisches Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden.

So beheben Sie Sicherheitsprobleme automatisch:

- Klicken Sie neben dem Schutzstatus auf **Beheben**.

Manuelles Beheben von Sicherheitsproblemen

Wenn ein oder mehrere Probleme nicht automatisch behoben werden, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

So beheben Sie Sicherheitsprobleme manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Wenn innerhalb der letzten 30 Tage kein vollständiger Scan Ihres Computers durchgeführt wurde, klicken Sie links neben dem HauptSchutzstatus auf **Scannen**, um einen manuellen Scan durchzuführen. (Dieses Element wird angezeigt, wenn McAfee VirusScan installiert ist.)
  - Wenn Ihre Virusdefinitionsdateien (DAT) veraltet sind, klicken Sie links neben dem HauptSchutzstatus auf **Update**, um Ihren Schutz zu aktualisieren.
  - Wennn ein Programm nicht installiert ist, klicken Sie für die Installation auf **Erhalten Sie vollständigen Schutz**.
  - Wenn Komponenten für ein Programm fehlen, installieren Sie es erneut.
  - Wenn ein Programm registriert sein muss, um vollständigen Schutz zu erhalten, klicken Sie zur Registrierung auf **Jetzt registrieren**. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)
  - Wenn ein Programm abgelaufen ist, klicken Sie auf **Mein Abonnement jetz überprüfen**, um Ihren Kontostatus zu prüfen. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)

Anzeigen der SecurityCenter-Informationen

Im unteren Teil des Schutzstatusbereichs bieten Ihnen die SecurityCenter-Informationen Zugriff auf SecurityCenter-Optionen. Sie sehen hier außerdem, wann das letzte Update sowie der letzte Scan durchgeführt wurden (falls McAfee VirusScan installiert ist) und wann die Abonnements für Ihre McAfee-Produkte ablaufen.

Öffnen des SecurityCenter-Konfigurationsbereichs

Sie können den SecurityCenter-Konfigurationsbereich öffnen, um Ihre Optionen im Home-Bereich zu ändern.

So öffnen Sie den SecurityCenter-Konfigurationsbereich:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.

Anzeigen von Informationen zum installierten Produkt

Sie können eine Liste der installierten Produkte anzeigen, in der Sie die Versionsnummer des Produkts und den Zeitpunkt der letzten Aktualisierung sehen.

So zeigen Sie Ihre McAfee-Produktinformationen an:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Details anzeigen**, um das Fenster mit Produktinformationen zu öffnen.

Verwenden des Menüs "Erweitert"

Wenn Sie SecurityCenter zum ersten Mal öffnen, wird in der linken Spalte das Menü "Grundlagen" angezeigt. Wenn Sie ein erfahrener Benutzer sind, können Sie auf das Menü **Erweitert** klicken, um ein detaillierteres Menü mit Befehlen an dieser Stelle anzuzeigen. Das zuletzt verwendete Menü wird angezeigt, wenn Sie SecurityCenter das nächste Mal verwenden.

Das Menü "Erweitert" umfasst die folgenden Elemente:

- Home
- Berichte und Protokolle (umfasst die Liste "Zuletzt aufgetretene Ereignisse" und Protokolle für die letzten 30, 60 und 90 Tage nach dem Typ geordnet)
- Konfigurieren
- Wiederherstellen
- Extras

KAPITEL 4

Konfigurieren von SecurityCenter-Optionen

SecurityCenter zeigt den Schutzstatus Ihres Computers insgesamt, ermöglicht Ihnen das Erstellen von McAfee-Benutzerkonten, installiert automatisch die neuesten Produkt-Updates und benachrichtigt Sie automatisch mit Warnmeldungen und -signalen bei öffentlichen Virenausbrüchen, Sicherheitsbedrohungen und Produkt-Updates.

Im SecurityCenter-Konfigurationsbereich können Sie Ihre SecurityCenter-Optionen für die folgenden Funktionen ändern:

- Schutzstatus
- Benutzer
- Automatische Updates
- Warnungen

In diesem Kapitel

Konfigurieren des Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

Konfigurieren ignorierter Probleme

Sie können Probleme als Teil des Schutzstatus Ihres Computers insgesamt in die Nachverfolgung aufnehmen oder davon ausschließen. Wenn ein Sicherheitsproblem von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

So konfigurieren Sie ignorierte Probleme:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Schutzstatus**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Führen Sie im Bereich "Ignorierte Probleme" einen der folgenden Schritte aus:
   - Um zuvor ignorierte Probleme in den Schutzstatus mit aufzunehmen, aktivieren Sie die entsprechenden Kontrollkästchen.
   - Um Probleme aus dem Schutzstatus auszuschließen, wählen Sie die entsprechenden Kontrollkästchen aus.
4. Klicken Sie auf **OK**.

Konfigurieren von Benutzeroptionen

Wenn Sie Programme von McAfee ausführen, für die Benutzerberechtigungen erforderlich sind, entsprechen diese Berechtigungen standardmäßig den Windows-Benutzerkonten auf diesem Computer. Um die Benutzerverwaltung für diese Programme einfacher zu gestalten, können Sie jederzeit dazu übergehen, McAfee-Benutzerkonten zu verwenden.

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfigurierung anderer McAfee-Benutzerkonten beginnen.

Übergehen zur Verwendung von McAfee-Benutzerkonten

Standardmäßig werden Windows-Benutzerkonten verwendet. Beim Wechseln zu McAfee-Benutzerkonten ist das Erstellen von zusätzlichen Windows-Benutzerkonten jedoch nicht mehr erforderlich.

So gehen Sie zur Verwendung von McAfee-Benutzerkonten über:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Um McAfee-Benutzerkonten zu verwenden, klicken Sie auf **Wechseln**.

Wenn Sie zum ersten Mal McAfee-Benutzerkonten verwenden, müssen Sie ein Administratorkonto erstellen (Seite 26).

Erstellen eines Administratorkontos

Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, werden Sie aufgefordert, ein Administratorkonto zu erstellen.

So erstellen Sie ein Administratorkonto:

1. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
2. Wählen Sie aus der Liste eine Frage zur Wiederbeschaffung des Kennworts aus, und geben Sie die Antwort auf die geheime Frage in das Kästchen **Antwort** ein.
3. Klicken Sie auf **Übernehmen**.

   Wenn Sie fertig sind, wird der Benutzerkontotyp im entsprechenden Feld mit den bestehenden Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm aktualisiert, falls zutreffend. Wenn Sie zum ersten Mal Benutzerkonten konfigurieren, wird der Bereich "Benutzer verwalten" angezeigt.

Konfigurieren von Benutzeroptionen

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfiguration anderer McAfee-Benutzerkonten beginnen.

So konfigurieren Sie Benutzeroptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **Benutzerkonten** auf **Hinzufügen**.
4. Geben Sie in das Feld **Benutzername** einen Benutzernamen ein.
5. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
6. Wählen Sie das Kontrollkästchen **Startbenutzer** aus, wenn Sie diesen neuen Benutzer als Startbenutzer festlegen möchten, wenn SecurityCenter gestartet wird.
7. Wählen Sie unter **Benutzerkontotyp** einen Kontotyp für diesen Benutzer aus, und klicken Sie anschließend auf **Erstellen**.

   Hinweis: Nach dem Erstellen des Benutzerkontos müssen Sie unter "Parental Controls" die Einstellungen für einen Benutzer mit eingeschränkten Rechten konfigurieren.

8. Um das Kennwort eines Benutzers, die automatische Anmeldung oder den Kontotyp zu ändern, wählen Sie einen Benutzernamen aus der Liste aus, und klicken Sie auf **Bearbeiten**.
9. Klicken Sie auf **Übernehmen**.

Abrufen des Administratorkennworts

Wenn Sie das Administratorkennwort vergessen, können Sie es abrufen.

So rufen Sie das Administratorkennwort ab:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort vergessen**.
3. Geben Sie die Antwort auf die von Ihnen bei der Erstellung des Administratorkontos angegebene geheime Frage ein.
4. Klicken Sie auf **Senden**.

   Ihr vergessenes Administratorkennwort wird angezeigt.

Ändern des Administratorkennworts

Wenn Sie sich nicht an Ihr Administratorkennwort erinnern oder vermuten, dass es missbraucht worden sein könnte, können Sie es ändern.

So ändern Sie das Administratorkennwort:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort ändern**.
3. Geben Sie im Feld **Altes Kennwort** Ihr bestehendes Kennwort ein.
4. Geben Sie im Feld **Kennwort** das neue Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
5. Klicken Sie auf **OK**.

Konfigurieren der Update-Optionen

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates für Ihre gesamten McAfee-Dienste. Die neuesten Produkt-Updates werden anschließend automatisch installiert. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Automatisches Prüfen auf Updates

Das Bestehen einer Internetverbindung vorausgesetzt, sucht SecurityCenter Online automatisch alle vier Stunden nach neuen Updates. Sie können SecurityCenter auch so konfigurieren, dass Sie benachrichtigt werden, bevor Updates heruntergeladen oder installiert werden.

So prüfen Sie automatisch auf Updates:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Update-Optionen" einen der folgenden Schritte aus:
   - Updates automatisch installieren und benachrichtigen, wenn das Produkt aktualisiert wurde (empfohlene Einstellung) (Seite 30)
   - Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist (Seite 31)
   - Vor dem Herunterladen von Updates benachrichtigen (Seite 32)
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 32).

Automatisches Herunterladen und Installieren von Updates

Wenn Sie in den SecurityCenter-Update-Optionen die Option **Updates automatisch installieren und benachrichtigen, wenn meine Dienste aktualisiert werden (empfohlene Einstellung)** auswählen, werden Updates automatisch von SecurityCenter heruntergeladen und installiert.

Automatisches Herunterladen von Updates

Wenn Sie in den Update-Optionen die Option **Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist** auswählen, lädt SecurityCenter Updates automatisch herunter und benachrichtigt Sie, wenn ein Update installiert werden kann. Sie können dann entscheiden, ob Sie das Update installieren oder die Installation auf einen späteren Zeitpunkt verschieben möchten (Seite 33).

So installieren Sie ein automatisch heruntergeladenes Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.

   Bei entsprechender Aufforderung müssen Sie sich auf der Website anmelden, damit Ihr Abonnement verifiziert werden kann. Der Download erfolgt erst nach der Verifizierung.

2. Nach der Verifizierung Ihres Abonnements klicken Sie im Bereich "Updates" auf **Update**, um das Update herunterzuladen und zu installieren. Wenn Ihr Abonnement abgelaufen ist, klicken Sie in dem diesbezüglichen Warnhinweis auf **Abonnement erneuern** und folgen dann den Eingabeaufforderungen.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Benachrichtigen vor dem Herunterladen von Updates

Wenn Sie im Bereich "Update-Optionen" **Benachrichtigen vor dem Herunterladen von Updates** aktiviert haben, werden Sie vor dem Herunterladen von Updates von SecurityCenter benachrichtigt. Sie können dann selbst entscheiden, ob Sie ein Update Ihrer Sicherheitsdienste herunterladen und installieren und damit die Gefahr eines Angriffs eliminieren möchten.

So laden und installieren Sie ein Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.
2. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden.

   Das Update wird automatisch heruntergeladen.
3. Klicken Sie nach Abschluss der Update-Installation in der Warnung auf **OK**.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Deaktivieren von automatischen Updates

Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatische Aktualisierung deaktivieren.

Hinweis: Prüfen Sie mindestens ein Mal wöchentlich, ob Updates verfügbar sind (Seite 34). Wenn Sie keine Updates installieren, sind die Sicherheitsmechanismen zum Schutz Ihres Computers nicht auf dem aktuellen Stand.

So deaktivieren Sie die automatische Aktualisierung:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern.
3. Klicken Sie auf **Aus**.
4. Bestätigen Sie die Änderung, indem Sie auf **Ja** klicken.

   Der Status wird im Header aktualisiert.

Wenn Sie nach sieben Tagen nicht manuell prüfen, ob Updates zur Verfügung stehen, werden Sie durch eine Warnmeldung daran erinnert.

Verschieben von Updates auf einen späteren Zeitpunkt

Wenn Sie beim Empfang der Benachrichtigung zu beschäftigt sind, Ihre Sicherheitsdienste zu aktualisieren, können Sie wählen, ob Sie zu einem späteren Zeitpunkt daran erinnert werden möchten, oder die Nachricht ignorieren.

So verschieben Sie ein Update auf einen späteren Zeitpunkt:

- Führen Sie einen der folgenden Vorgänge aus:
  - Klicken Sie in der Warnung auf **Später erinnern** und anschließend auf **OK**.
  - Klicken Sie auf **Warnung schließen** und anschließend auf **OK**, um die Warnung zu schließen und keine Aktionen zu ergreifen.

Manuelles Prüfen auf Updates

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates und installiert anschließend die neuesten Produkt-Updates. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Windows-Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 32).

So prüfen Sie manuell auf Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste mit der rechten Maustaste auf das SecurityCenter M-Symbol und klicken Sie anschließend auf **Aktualisierungen**.

   Während SecurityCenter nach Updates sucht, können Sie weiterhin andere Aufgaben damit durchführen.

   Es wird in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste ein animiertes Symbol angezeigt. Wenn SecurityCenter den Vorgang abgeschlossen hat, wird das Symbol automatisch wieder ausgeblendet.
3. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden, um Ihr Abonnement zu verifizieren.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Konfigurieren von Alarmoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

Konfigurieren von Warnoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

So konfigurieren Sie Warnoptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Warnoptionen" einen der folgenden Schritte aus:
   - **Bei einem öffentlichen Virusausbruch oder einer öffentlichen Sicherheitsbedrohung benachrichtigen**
   - **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**
   - **Akustisches Signal bei Warnungen ausgeben**
   - **Splash-Bildschirm von McAfee beim Starten von Windows anzeigen**
4. Klicken Sie auf **OK**.

Hinweis: Damit zukünftig keine informativen Warnmeldungen von der Warnung selbst mehr anzeigt werden, klicken Sie auf **Diese Warnung nicht mehr anzeigen**. Sie können diese Warnmeldungen später im Bereich "Informationswarnungen" erneut aktivieren.

Konfigurieren von Informationswarnungen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die Ihr unmittelbares Eingreifen nicht erforderlich machen. Wenn Sie informative Warnmeldungen von der Warnung selbst für die Zukunft deaktivieren, können Sie sie später im Bereich "Informationswarnungen" erneut aktivieren.

So konfigurieren Sie Informationswarnungen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **SecurityCenter-Konfiguration** auf die Option **Informationswarnungen**.
4. Deaktivieren Sie das Kontrollkästchen **Informationswarnungen verbergen**, und deaktivieren Sie anschließend die Kontrollkästchen für Warnungen, die Sie anzeigen möchten, in der Liste.
5. Klicken Sie auf **OK**.

KAPITEL 5

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

In diesem Kapitel

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Wartens Ihres Computers und des Verwaltens Ihres Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Sicherns Ihrer Daten (falls McAfee Datensicherung installiert ist).

So führen Sie häufig vorkommende Tasks aus:

- Führen Sie im Menü "Grundlagen" unter **Häufige Tasks** einen der folgenden Schritte aus:
  - Um zum Home-Bereich zurückzukehren, klicken Sie auf **Home**.
  - Um kürzlich aufgetretene, von Ihrer Sicherheitssoftware erkannte Ereignisse anzuzeigen, klicken Sie auf **Zuletzt aufgetretene Ereignisse**.
  - Um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen, klicken Sie auf **Computer warten**.
  - Um Ihr Computer-Netzwerk zu verwalten, klicken Sie auf einem Computer mit Verwaltungskapazitäten für dieses Netzwerk auf **Netzwerk verwalten**.

Der Network Manager überwacht PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen, damit Sie Sicherheitsprobleme im Netzwerk einfach identifizieren können.

- Um Sicherungskopien Ihrer Dateien zu erstellen, klicken Sie auf **Datensicherung**, wenn McAfee Datensicherung installiert ist.

  Automatische Sicherungen speichern Kopien Ihrer wichtigsten Dateien, wann immer Sie möchten, so dass Ihre Dateien auf einem CD-/DVD-, USB- oder einem externen oder Netzwerklaufwerk verschlüsselt und gespeichert werden.

Tipp: Sie können häufig vorkommende Tasks von zwei weiteren Orten aus durchführen (unter **Home** im Menü "Erweitert" und im Menü **QuickLinks** des SecurityCenter M-Symbols ganz rechts auf der Taskleiste). Sie können unter **Berichte und Protokolle** im Menü "Erweitert" auch kürzlich aufgetretene Ereignisse und umfassende Protokolle nach Typ geordnet anzeigen.

Zuletzt aufgetretene Ereignisse anzeigen

Kürzlich aufgetreten Ereignisse werden protokolliert, wenn Änderungen an Ihrem Computer vorgenommen werden. Die Beispiele umfassen das Aktivieren oder Deaktivieren eines Schutztyps, das Entfernen einer Bedrohung sowie das Blockieren eines Versuchs, eine Internetverbindung herzustellen. Sie können die 20 am häufigsten aufgetretenen Ereignisse sowie die Details dazu anzeigen.

Details zu diesen Ereignissen finden Sie in der Hilfedatei des jeweiligen Produkts.

So zeigen Sie die zuletzt aufgetretenen Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Aktuelle Ereignisse anzeigen**.

   Sämtliche kürzlich aufgetretenen Ereignisse werden in der Liste angezeigt, zusammen mit dem Datum und einer kurzen Beschreibung.

2. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** ein Ereignis aus, um weitere Informationen im Detailbereich anzuzeigen.

   Unter **Ich möchte** werden alle verfügbaren Aktionen angezeigt.

3. Um eine umfassendere Liste mit Ereignissen anzuzeigen, klicken Sie auf **Protokoll anzeigen**.

Automatisches Warten Ihres Computers

Um wertvollen Speicherplatz auf Ihrer Festplatte frei zu machen und die Leistung Ihres Computers zu optimieren, können Sie QuickClean- oder Defragmentierungs-Task so planen, dass sie in regelmäßigen Zeitabständen ausgeführt werden. Diese Tasks umfassen das Löschen, Shreddern und Defragmentieren von Dateien und Ordnern.

So warten Sie Ihren Computer automatisch:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie auf **Taskplaner** auf **Start**.
3. Wählen Sie in der Vorgangsliste **QuickClean** oder **Defragmentierungsprogramm** aus.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Um einen bestehenden Task zu verändern, wählen Sie den Task aus und klicken dann auf **Ändern**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen neuen Task zu erstellen, geben Sie den Namen in das Feld **Taskname** ein und klicken anschließend auf **Erstellen**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen Task zu löschen, wählen Sie ihn aus und klicken dann auf **Löschen**.
5. Zeigen Sie unter **Task-Zusammenfassung** an, wann der Task zuletzt ausgeführt wurde, wann er zum nächsten Mal ausgeführt wird sowie welchen Status er hat.

Manuelles Warten Ihres Computers

Sie können manuelle Wartungs-Tasks ausführen, um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen.

So warten Sie Ihren Computer manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Um QuickClean zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten** und anschließend auf **Start**.
  - Um das Defragmentierungsprogramm zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten**, und anschließend auf **Analysieren**.
  - Um die Systemwiederherstellung im Menü "Erweitert" zu verwenden, klicken Sie auf **Tools**, klicken Sie anschließend auf **Systemwiederherstellung** und dann auf **Start**.

Entfernen nicht verwendeter Dateien und Ordner

Verwenden Sie QuickClean, um wertvollen Speicherplatz frei zu machen und die Leistung Ihres Computers zu optimieren.

So entfernen Sie nicht verwendete Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **QuickClean** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Defragmentieren von Dateien und Ordnern

Die Dateifragmentierung findet statt, wenn Dateien und Ordner gelöscht und neue Dateien hinzugefügt werden. Durch die Fragmentierung wird der Festplattenzugriff verlangsamt und die Gesamtleistung Ihres Computers herabgesetzt, wenn normalerweise auch nicht sehr stark.

Verwenden Sie das Defragmentierungsprogramm, um Teile einer Datei auf aufeinanderfolgenden Sektoren auf einer Festplatte zu schreiben, um die Geschwindigkeit von Zugriff und Abruf zu erhöhen.

So defragmentieren Sie Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **Defragmentierungsprogramm** auf **Analysieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Zurücksetzen Ihres Computers auf die vorherigen Einstellungen

Wiederherstellungspunkte sind Kurzübersichten über Ihren Computer, die Windows in regelmäßigen Abständen speichert sowie wenn wichtige Ereignisse stattfinden (beispielsweise wenn ein Programm oder Treiber installiert wird). Sie können jdeoch auch jederzeit Ihre eigenen Wiederherstellungspunkte erstellen und diese benennen.

Verwenden Sie Wiederherstellungspunkte, um schädliche Änderungen an Ihrem Computer rückgängig zu machen und diesen auf die vorherigen Einstellungen zurückzusetzen.

So setzen Sie Ihren Computer auf die vorherigen Einstellungen zurück:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Systemwiederherstellung**.
2. Klicken Sie unter **Systemwiederherstellung** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Verwalten Ihres Netzwerks

Wenn Ihr Computer über Verwaltungskapazitäten für Ihr Netzwerk verfügt, können Sie Network Manager verwenden, um PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen zu überwachen, damit Sie Sicherheitsprobleme einfach identifizieren können.

Wenn der Schutzstatus Ihres Computers in diesem Netzwerk nicht überwacht wird, ist Ihr Computer entweder nicht Teil dieses Netzwerks, oder es handelt sich um ein nicht verwaltetes Mitglied dieses Netzwerks. Weitere Details hierzu finden Sie in der Hilfedatei zu Network Manager.

So verwalten Sie Ihr Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Netzwerk verwalten**.
2. Klicken Sie auf das Symbol, das in der Netzwerkkarte für diesen Computer steht.
3. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Weitere Informationen zu Viren

Verwenden Sie die Vireninformationsbibliothek und die Virus Map, um folgende Aktionen durchzuführen:

- Erfahren Sie mehr zu den neuesten Viren, E-Mail-Virus-Hoaxes und anderen Bedrohungen.
- Erhalten Sie kostenlose Tools zur Virenentfernung, die Ihnen dabei helfen, Ihren Computer zu reparieren.
- Hier erfahren Sie aus der Vogelperspektive in Echtzeit, an welchen Orten der Welt derzeit PCs von Viren angegriffen werden.

So erhalten Sie weitere Informationen zu Viren:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Virusinformationen**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Untersuchen von Viren mithilfe der McAfee-Virusinformationsbibliothek
   - Untersuchen von Viren mithilfe der World Virus Map auf der McAfee-Website

KAPITEL 6

McAfee QuickClean

Beim Surfen im Internet sammelt sich viel Müll auf Ihrem Computer an. Schützen Sie Ihre Privatsphäre und löschen Sie Müll aus dem Internet und E-Mails, die Sie nicht benötigen, mit QuickClean. QuickClean identifiziert und löscht Dateien, die sich beim Internetsurfen angesammelt haben, einschließlich unerwünschter Cookies, E-Mails, Downloads und des Verlaufs - Daten, die persönliche Informationen über Sie enthalten. Es schützt Ihre Privatsphäre durch das sichere Löschen dieser sensiblen Informationen.

QuickClean löscht außerdem unerwünschte Programme. Legen Sie fest, welche Dateien eliminiert werden sollen, und sorgen Sie für Ordnung, ohne dabei wesentliche Informationen zu löschen.

In diesem Kapitel

Erläuterungen zu den QuickClean-Funktionen

In diesem Abschnitt werden die Funktionen von QuickClean beschrieben.

Funktionen

QuickClean bietet einen Satz an effizienten und leicht zu verwendenden Tools, mit denen digitale Überschussdaten sicher gelöscht werden können. Sie können wertvollen Festplattenspeicherplatz frei geben und die Leistung Ihres Computers optimieren.

KAPITEL 7

Bereinigen Ihres Computers

Mit QuickClean können Sie Dateien und Ordner sicher löschen.

Wenn Sie im Internet surfen, kopiert Ihr Browser jede Internetseite und die darin enthaltenen Graphiken in einen Ordner im Zwischenspeicher auf Ihrer Festplatte. Der Browser kann die Seite dann schnell herunterladen, wenn Sie auf diese Seite zurückkehren. Das Zwischenspeichern von Dateien ist nützlich, wenn Sie wiederholt dieselben Internetseiten besuchen und sich ihr Inhalt nicht häufig ändert. Meistens sind die zwischengespeicherten Dateien jedoch nicht hilfreich und können gelöscht werden.

Sie können verschiedene Elemente mit den folgenden Cleanern löschen.

- Papierkorb-Cleaner: Leert Ihren Windows-Papierkorb.
- Cleaner für temporäre Dateien: Löscht Dateien, die in temporären Ordner gespeichert sind.
- Kurzbefehls-Cleaner: Löscht unterbrochene Kurzbefehle und Kurzbefehle mit einem verknüpften Programm.
- Cleaner für verlorene Dateifragmente: Löscht verlorene Dateifragmente von Ihrem Computer.
- Registrierungs-Cleaner: Löscht Windows-Registrierungsinformationen für Programme, die von Ihrem Computer gelöscht wurden.
- Cache Cleaner: Entfernt Dateien aus dem Zwischenspeicher, die beim Browsen im Internet anfallen. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert.
- Cookie Cleaner: Löscht Cookies. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert. Cookies sind kleine Dateien, die Ihr Webbrowser auf Anfrage eines Webservers auf Ihrem Computer speichert. Wenn Sie danach erneut eine Seite dieser Website vom Webserver laden, sendet Ihr Browser das Cookie zurück an den Webserver. Diese Cookies können wie Tags fungieren, mit denen der Webserver nachverfolgen kann, welche Seiten wie oft aufgerufen wurden.
- Browser-Verlaufs-Cleaner: Löscht Ihren Browser-Verlauf.
- Outlook Express und Outlook E-Mail Cleaner für gelöschte und gesendete Elemente: Löscht E-Mails aus Ihren Ordnern für gesendete und gelöschte Outlook-E-Mails.
- Cleaner für zuletzt verwendete Dateien: Löscht kürzlich verwendete Elemente, die auf Ihrem Computer gespeichert sind, wie Microsoft Office-Dokumente.

- ActiveX und Plugin Cleaner: Löscht ActiveX-Steuerelemente und -Plugins.
  ActiveX ist eine Technologie, die für die Implementierung von Steuerelementen in ein Programm verwendet wird. Ein ActiveX-Steuerlement kann eine Schaltfläche zur Oberfläche eines Programms hinzufügen. Die meisten dieser Steuerelemente sind harmlos. Einige Personen verwenden jedoch die ActiveX-Technologie, um Informationen von Ihrem Computer zu sammeln.
  Plugins sind kleine Softwareprogramme, die eine Verbindung zu größeren Anwendungen herzustellen, um weitere Funktionen verfügbar zu machen. Plugins ermöglichen es dem Webbrowser, auf Dateien zuzugreifen und diese auszuführen, die in HTML-Dokumente eingebettet sind, die Formate aufweisen, die der Browser normalerweise nicht erkennen würde (beispielsweise Animations-, Video- und Audiodateien).
- Cleaner für Systemwiederherstellungspunkte: Löscht alte Systemwiederherstellungspunkte von Ihrem Computer.

In diesem Kapitel

Verwenden von QuickClean

In diesem Abschnitt wird beschrieben, wie QuickClean verwendet wird.

Säubern Ihres Computers

Sie können nicht verwendete Dateien und Ordner löschen, Festplattenspeicher freigeben und die Leistung Ihres Computers optimieren.

So säubern Sie Ihren Computer:

1. Klicken Sie im Menü "Erweitert" auf **Tools**.
2. Klicken Sie auf **Computer warten**, und klicken Sie anschließend unter **McAfee QuickClean** auf **Start**.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um die in der Liste ausgewählten Standard-Cleaner zu übernehmen.
   - Wählen Sie die gewünschten Cleaner aus, und klicken Sie anschließend auf **Weiter.** Für den Cleaner für zuletzt verwendete Dateien können Sie auf **Eigenschaften** klicken, um die Programme zu löschen, deren Listen Sie nicht säubern möchten.
   - Klicken Sie auf **Standardwerte wiederherstellen**, um die Standard-Cleaner wiederherzustellen, und klicken Sie anschließend auf **Weiter**.
4. Klicken Sie nach Durchführung der Analyse auf **Weiter**, um das Löschen der Dateien zu bestätigen. Sie können diese Liste erweitern, um die Dateien anzuzeigen, die gesäubert werden, und deren Speicherort.
5. Klicken Sie auf **Weiter**.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um den Standardwert **Nein, ich möchte meine Dateien mithilfe der Standardlöschung von Windows löschen** zu übernehmen.
   - Klicken Sie auf **Ja, ich möchte meine Dateien mit Shredder sicher löschen**, und geben Sie die Anzahl an Durchläufen an. Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden.
7. Klicken Sie auf **Fertig stellen**.
8. Zeigen Sie unter **Zusammenfassung von QuickClean** die Anzahl an gelöschten Registrierungsdateien an sowie die Menge an Festplattenspeicher, der nach der Säuberung der Festplatte und der Internetdateien wieder zur Verfügug stand.

KAPITEL 8

McAfee Shredder

Gelöschte Dateien lassen sich auch nach dem Leeren des Papierkorbs wiederherstellen. Wenn eine Datei gelöscht wird, markiert Windows den betreffenden Speicherplatz auf dem Laufwerk als nicht mehr in Gebrauch, die Datei selbst ist jedoch noch vorhanden. Mit forensischen Computer-Tools können Steuererklärungen, Lebensläufe oder andere Dokumente, die von Ihnen gelöscht wurden, wiederhergestellt werden. Shredder schützt Ihre Privatsphäre, indem es unerwünschte Dateien permanent löscht.

Um eine Datei dauerhaft zu löschen, müssen Sie die vorhandene Datei wiederholt mit neuen Daten überschreiben. Microsoft(R) Windows löscht Dateien nicht sicher, da ansonsten sämtliche Dateivorgänge sehr langsam wären. Auch durch das Vernichten eines Dokuments wird nicht immer verhindert, dass das Dokument wiederhergestellt werden kann, da einige Programme temporäre verborgene Kopien geöffneter Dokumente erstellen. Wenn Sie nur die Dateien vernichten, die im Windows(R)-Explorer angezeigt werden, sind möglicherweise noch temporäre Kopien jener Dokumente irgendwo vorhanden.

Hinweis: Für vernichtete Dateien gibt es keine Sicherungskopien. Sie können von Shredder gelöschte Dateien nicht wiederherstellen.

In diesem Kapitel

Erläuterungen zu den Funktionen von Shredder

In diesem Abschnitt werden die Funktionen von Shredder beschrieben.

Funktionen

Shredder ermöglicht es Ihnen, den Inhalt Ihres Papierkorbs, temporäre Internetdateien, den Website-Verlauf, Dateien, Ordner und Datenträger wiederherzustellen.

KAPITEL 9

Vernichten unerwünschter Dateien mit Shredder

Shredder schützt Ihre persönlichen Daten, indem er unerwünschte Dateien, wie den Inhalt Ihres Papierkorbs, temporäre Internetdateien und den Website-Verlauf sicher und dauerhaft löscht. Sie können zu vernichtende Dateien und Ordner auswählen oder nach diesen suchen.

In diesem Kapitel

Verwenden von Shredder

In diesem Abschnitt wird beschrieben, wie Shredder verwendet wird.

Vernichten von Dateien, Ordnern und Datenträgern

Dateien können auf Ihrem Computer verbleiben, auch nachdem Sie Ihren Papierkorb geleert haben. Wenn Sie jedoch Dateien vernichten, werden Ihre Daten dauerhaft gelöscht, und Hacker können nicht darauf zugreifen.

So vernichten Sie Dateien, Ordner und Datenträger:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Shredder**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Dateien und Ordner löschen**, um Dateien und Ordner zu vernichten.
   - Klicken Sie auf **Die Daten eines ganzen Datenträgers löschen**, um einen Datenträger zu vernichten**.**
3. Wählen Sie eine der folgenden Vernichtungsstufen aus:
   - **Schnell**: Vernichtet die ausgewählten Elemente in einem Durchlauf.
   - **Umfassend**: Vernichtet die ausgewählten Elemente in sieben Durchläufen.
   - **Benutzerdefiniert**: Vernichtet die ausgewählten Elemente in bis zu zehn Durchläufen. Eine hohe Anzahl an Vernichtungsdurchläufen erhöht Ihre Stufe für die sichere Dateientfernung.
4. Klicken Sie auf **Weiter**.
5. Führen Sie einen der folgenden Vorgänge aus:
   - Wenn Sie Dateien vernichten, klicken Sie in der Liste **Zu vernichtende Dateien auswählen** auf **Inhalt des Papierkorbs**, **Temporäre Internet-Dateien** oder **Website-Verlauf**. Wenn Sie einen Datenträger vernichten möchten, klicken Sie auf den Datenträger.
   - Klicken Sie auf **Durchsuchen**, navigieren Sie zu den zu vernichtenden Dateien, und wählen Sie sie aus.
   - Geben Sie den Pfad zu den zu vernichtenden Dateien in der Liste **Zu vernichtende Dateien auswählen** ein.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.

8 Klicken Sie auf **Fertig**.

KAPITEL 10

McAfee Network Manager

McAfee(R) Network Manager stellt eine graphische Ansicht der Computer und Komponenten dar, die Ihr Home-Netzwerk bilden. Sie können Network Manager verwenden, um den Schutzstatus jedes verwalteten Computers in Ihrem Netzwerk remote zu überwachen und gemeldete Sicherheitslücken auf diesen verwalteten Computern remote zu beheben.

Bevor Sie mit der Verwendung von Network Manager beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Network Manager.

In diesem Kapitel

Funktionen

Network Manager bietet die folgenden Funktionen:

Graphische Netzwerkzuordnung

Die Netzwerkzuordnung von Network Manager bietet eine graphische Übersicht des Sicherheitsstatus der Computer und der Komponenten, aus denen Ihr privates Netzwerk besteht. Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), erkennt die Netzwerkübersicht diese Änderungen. Sie können die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Remote-Verwaltung

Verwenden Sie die Netzwerkübersicht von Network Manager zur Verwaltung des Sicherheitsstatus der Computer, aus denen Ihr privates Netzwerk besteht. Sie können einen Computer einladen, dem verwalteten Netzwerk beizutreten, den Schutzstatus des verwalteten Computers überwachen und bekannte Sicherheitslücken bei einem Remote-Computer im Netzwerk beheben.

Erläuterung der Network Manager-Symbole

Die folgende Tabelle erläutert die häufig auf der Network Manager-Netzwerkzuordnung verwendeten Symbole.

-Symbol	Beschreibung
	Steht für einen verwalteten Computer, der online ist.
	Steht für einen verwalteten Computer, der offline ist.
	Steht für einen unverwalteten Computer, auf dem die McAfee 2007-Sicherheits-Software installiert ist.
	Steht für einen unverwalteten Computer, der offline ist.
	Steht für einen Computer, der online ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät.
	Steht für einen Computer, der offline ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät, das offline ist.
	Bedeutet, dass das entsprechende Element geschützt und verbunden ist.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf und keine Verbindung besteht.
	Steht für einen drahtlosen Home-Router.
	Steht für einen standardmäßigen Home-Router.
	Steht für das Internet, falls eine Verbindung besteht.
	Steht für das Internet, falls keine Verbindung besteht.

KAPITEL 11

Erstellen eines verwalteten Netzwerks

Sie erstellen ein verwaltetes Netzwerk, indem Sie mit den Elementen auf Ihrer Netzwerkzuordnung arbeiten und Mitglieder (Computer) zum Netzwerk hinzufügen.

In diesem Kapitel

Arbeiten mit der Netzwerkzuordnung

Jedes Mal, wenn Sie von einem Computer eine Verbindung zum Netzwerk herstellen, analysiert Network Manager den Status des Netzwerks, um festzustellen, ob Mitglieder vorliegen (verwaltet oder unverwaltet), welche Router-Attribute es gibt und wie der Internetstatus lautet. Wenn keine Mitglieder gefunden werden, nimmt Network Manager an, dass der derzeit verbundene Computer der erste Computer im Netzwerk ist, und macht den Computer automatisch zu einem verwalteten Mitglied mit Administratorrechten. Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Sie können das Netzwerk jederzeit umbenennen.

Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), können Sie die Netzwerkmappe an Ihre Bedürfnisse anpassen. Sie können beispielsweise die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Zugreifen auf die Netzwerkzuordnung

Sie können auf Ihre Netzwerkzuordnung zugreifen, indem Sie Network Manager über die SecurityCenter-Liste der häufigen Tasks starten. Die Netzwerkzuordnung bietet eine graphische Darstellung des Computers und der Komponenten, die Ihr Home-Netzwerk ausmachen.

So greifen Sie auf die Netzwerkzuordnung zu:

- Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
  Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.

Hinweis: Wenn Sie das erste Mal auf die Netzwerkübersicht zugreifen, werden Sie gefragt, ob die anderen Computern im Netzwerk vertrauenswürdig sind, bevor die Netzwerkübersicht angezeigt wird.

Netzwerkzuordnung aktualisieren

Sie können die Netzwerkzuordnung jederzeit aktualisieren, beispielsweise wenn ein anderer Computer dem verwalteten Netzwerk beitritt.

So aktualisieren Sie die Netzwerkzuordnung:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerkzuordnung aktualisieren**.

Hinweis: Der Link **Netzwerkzuordnung aktualisieren** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Netzwerk umbenennen

Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Wenn dieser Name nicht passt, können Sie ihn ändern.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerk umbenennen**.
3. Geben Sie im Feld **Netzwerk umbenennen** den Namen des Netzwerks ein.
4. Klicken Sie auf **OK**.

Hinweis: Der Link **Netzwerk umbenennen** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Anzeigen oder Verbergen von Elementen in der Netzwerkzuordnung

Standardmäßig werden alle Computer und Komponenten in Ihrem Home-Netzwerk in der Netzwerkzuordnung angezeigt. Wenn Sie jedoch Elemente ausgeblendet haben, können Sie sie jederzeit wieder anzeigen. Nur unverwaltete Elemente können ausgeblendet werden, verwaltete Computer können nicht ausgeblendet werden.

Ziel	Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**, und führen Sie anschließend die folgenden Schritte aus...
Verbergen eines Elements aus der Netzwerkzuordnung	Klicken Sie in der Netzwerkzuordnung auf ein Element, und klicken Sie anschließend unter **Ich möchte** auf **Dieses Element verbergen**. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.
Anzeigen verborgener Elemente in der Netzwerkzuordnung	Klicken Sie unter **Ich möchte** auf **Verborgene Elemente anzeigen**.

Anzeigen der Elementdetails

Sie können detaillierte Informationen zu einer beliebigen Komponente in Ihrem Netzwerk anzeigen, indem Sie die Komponente in der Netzwerkzuordnung auswählen. Diese Informationen umfassen den Komponentennamen, seinen Schutzstatus und andere Informationen, die für die Verwaltung der Komponente erforderlich sind.

So zeigen Sie Details zu einem Element an:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** die Informationen zu diesem Element an.

Anmelden am verwalteten Netzwerk

Bevor ein Computer remote verwaltet wird oder ihm Zugriff auf die Remote-Verwaltung anderer Computer im Netzwerk gewährt werden kann, muss er ein vertrauenswürdiges Mitglied des Netzwerks werden. Die Netzwerkmitgliedschaft wird neuen Computern von bestehenden Netzwerkmitgliedern (Computern) mit Administratorrechten gewährt. Um sicherzustellen, dass sich nur vertrauenswürdige Computer am Netzwerk anmelden, müssen sowohl Benutzer des gewährenden als auch des anzumeldenden Computers sich gegenseitig authentifizieren.

Wenn ein Computer dem Netzwerk beitritt, wird er aufgefordert, seinen McAfee-Schutzstatus für die anderen Computer im Netzwerk sichtbar zu machen. Wenn ein Computer zustimmt und seinen Schutzstatus sichtbar macht, wird er ein *verwaltetes* Mitglied des Netzwerks. Wenn ein Computer ablehnt und seinen Schutzstatus nicht sichtbar macht, wird er ein *unverwaltetes* Mitglied des Netzwerks. Unverwaltete Mitglieder des Netzwerks sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- oder Druckerfreigabe).

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder EasyNetwork), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer in Network Manager zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Anmelden an einem verwalteten Netzwerk

Wenn Sie eine Einladung erhalten, einem verwalteten Netzwerk beizutreten, können Sie diese entweder annehmen oder ablehnen. Sie können auch bestimmen, ob Sie möchten, dass dieser und andere Computer im Netzwerk gegenseitig ihre Sicherheitseinstellungen überwachen (beispielsweise ob die Virenschutzdienste eines Computers auf dem neuesten Stand sind).

So melden Sie sich an einem verwalteten Netzwerk an:

1. Aktivieren Sie im Dialogfeld für die Einladung das Kontrollkästchen **Es diesem und anderen Computern erlauben, gegenseitig ihre Sicherheitseinstellungen zu überwachen**, um es anderen Computern im verwalteten Netzwerk zu erlauben, die Sicherheitseinstellungen Ihres Computers zu überwachen.
2. Klicken Sie auf **Anmelden**.
   Wenn Sie die Einladung annehmen, werden zwei Spielkarten angezeigt.
3. Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden.
4. Klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Einladen eines Computers, sich am verwalteten Netzwerk anzumelden

Wenn ein Computer dem verwalteten Netzwerk hinzugefügt wird oder ein anderer unverwalteter Computer im Netzwerk vorliegt, können Sie diesen Computer einladen, sich am verwalteten Netzwerk anzumelden. Nur Computer mit Administratorrechten für das Netzwerk können andere Computer dazu einladen, sich am Netzwerk anzumelden. Wenn Sie die Einladung senden, können Sie auch die Berechtigungsstufe angeben, die Sie dem anzumeldenden Computer zuweisen möchten.

So laden Sie einen Computer ein, sich am verwalteten Netzwerk anzumelden:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.
3. Klicken Sie im Dialogfeld "Einen Computer einladen, diesem verwalteten Netzwerk beizutreten" auf eine der folgenden Optionen:
   - **Zugriff als Gast gewähren**
     Der Gastzugriff erlaubt dem Computer den Zugriff auf das Netzwerk.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem vollständigen Zugriff (wie mit dem Gastzugriff) können Computer auf das Netzwerk zugreifen.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem administrativen Zugriff können Computer mit Administratorrechten auf das Netzwerk zugreifen. Dieser Zugriff erlaubt es dem Computer außerdem, anderen Computern Zugriff zu gewähren, die sich am verwalteten Netzwerk anmelden möchten.

4 Klicken Sie auf **Einladen**.
Es wird eine Einladung, dem verwalteten Netzwerk beizutreten, an den Computer gesendet. Wenn der Computer die Einladung annimmt, werden zwei Spielkarten angezeigt.

5 Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden.

6 Klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Wenn Sie es dem Computer erlauben, sich am Netzwerk anzumelden, werden dadurch andere Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Zugriff verweigern**.

Computer im Netzwerk nicht mehr als vertrauenswürdig einstufen

Wenn Sie fälschlicherweise zustimmen, den anderen Computern im Netzwerk zu vertrauen, so können Sie diese Auswahl auch wieder aufheben.

So erklären Sie Computer in diesem Netzwerk als nicht mehr vertrauenswürdig:

- Klicken Sie unter **Ich möchte** auf **Computern in diesem Netzwerk nicht mehr vertrauen**.

Hinweis: Der Link **Computern in diesem Netzwerk nicht mehr vertrauen** ist nur verfügbar, wenn sich keine anderen verwalteten Computer am Netzwerk angemeldet haben.

KAPITEL 12

Remote-Verwaltung des Netzwerks

Nachdem Sie Ihr verwaltetes Netzwerk eingerichtet haben, können Sie Network Manager verwenden, um die Computer und Komponenten, die sich in Ihrem Netzwerk befinden, remote zu verwalten. Sie können den Status und die Berechtigungsstufen der Computer und Komponenten überwachen und Sicherheitslücken remote beheben.

In diesem Kapitel

Überwachen des Status und der Berechtigungen

Ein verwaltetes Netzwerk hat zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht. Unverwaltete Mitglieder sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- und Druckerfreigabe). Ein unverwalteter Computer kann jederzeit von einem anderen verwalteten Computer im Netzwerk eingeladen werden, ein verwalteter Computer zu werden. Ebenso kann ein verwalteter Computer jederzeit ein unverwalteter Computer werden.

Verwalteten Computern sind entweder administrative, vollständige oder Gastberechtigungen zugewiesen. Administrative Berechtigungen erlauben es dem verwalteten Computer, den Schutzstatus aller anderen verwalteten Computer im Netzwerk zu verwalten und anderen Computern die Mitgliedschaft im Netzwerk zu gewähren. Vollständige und Gastberechtigungen erlauben es einem Computer nur, auf das Netzwerk zuzugreifen. Sie können die Berechtigungsstufe eines Computers jederzeit ändern.

Da ein verwaltetes Netzwerk auch aus Geräten besteht (z. B. Routern), können Sie Network Manager auch für die Verwaltung dieser Geräte verwenden. Sie können auch die Anzeigeeigenschaften eines Geräts in der Netzwerkzuordnung konfigurieren und verändern.

Überwachen des Schutzstatus eines Computers

Wenn der Schutzstatus eines Computers nicht im Netzwerk überwacht wird (entweder, weil der Computer kein Mitglied des Netzwerks ist, oder weil der Computer ein unverwaltetes Mitglied des Netzwerks ist), können Sie eine Anfrage für die Überwachung stellen.

So überwachen Sie den Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Stoppen der Überwachung des Schutzstatus eines Computers

Sie können die Überwachung des Schutzstatus eines verwalteten Computers in Ihrem privaten Netzwerk stoppen. Der Computer wird dann zu einem unverwalteten Computer.

So stoppen Sie die Überwachung des Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer nicht mehr überwachen**.
3. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

Ändern der Berechtigungen eines verwalteten Computers

Sie können die Berechtigungen eines verwalteten Computers jederzeit ändern. Dadurch können Sie angeben, welche Computer den Schutzstatus (Sicherheitseinstellungen) anderer Computer im Netzwerk überwachen können.

So ändern Sie die Berechtigungen eines verwalteten Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Berechtigungen für diesen Computer ändern**.
3. Aktivieren oder Deaktivieren Sie im Dialogfeld zum Ändern der Berechtigungen das Kontrollkästchen, das angibt, ob dieser Computer und andere Computer im verwalteten Netzwerk den Schutzstatus der anderen Computer überwachen können.
4. Klicken Sie auf **OK**.

Verwalten eines Geräts

Sie können ein Gerät verwalten, indem Sie von Network Manager aus auf ihre Verwaltungs-Website zugreifen.

So verwalten Sie ein Gerät:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Dieses Gerät verwalten**. Es wird ein Webbrowser geöffnet, der die Verwaltungs-Webseite des Geräts anzeigt.
3. Geben Sie in Ihrem Webbrowser Ihre Anmeldeinformationen ein, und konfigurieren Sie die Sicherheitseinstellungen des Geräts.

Hinweis: Wenn es sich bei dem Gerät um einen durch Wireless Network Security geschützten drahtlosen Router oder Zugriffspunkt handelt, müssen Sie Wireless Network Security verwenden, um die Sicherheitseinstellungen eines Geräts zu konfigurieren.

Ändern der Anzeigeeigenschaften eines Geräts

Wenn Sie die Anzeigeeigenschaften eines Geräts verändern, können Sie den Anzeigenamen eines Geräts in der Netzwerkzuordnung ändern und angeben, ob es sich bei diesem Gerät um einen drahtlosen Router handelt.

So ändern Sie die Anzeigeeigenschaften eines Geräts:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Geräteeigenschaften ändern**.
3. Um den Anzeigenamen des Geräts anzugeben, geben Sie einen Namen in das Feld **Name** ein.
4. Zum Angeben des Gerätetyps klicken Sie auf eine der folgenden Optionen:
   - **Router**
     Diese Option steht für einen standardmäßigen Home-Router.
   - **Drahtloser Router**
     Diese Option steht für einen drahtlosen Home-Router.
5. Klicken Sie auf **OK**.

Beheben von Sicherheitslücken

Verwaltete Computer mit Administratorrechten können den McAfee-Schutzstatus anderer verwalteter Computer im Netzwerk überwachen und sämtliche gemeldeten Sicherheitslücken remote beheben. Wenn beispielweise der McAfee-Schutzstatus eines verwalteten Computers angibt, dass VirusScan deaktiviert ist, kann ein anderer verwalteter Computer mit Administratorrechten diese Sicherheitslücke *beheben*, indem er VirusScan remote aktiviert.

Wenn Sie Sicherheitslücken remote beheben, repariert Network Manager automatisch die meisten gemeldeten Probleme. Einige Sicherheitslücken erfordern jedoch möglicherweise ein manuelles Eingreifen auf dem lokalen Computer. In diesem Fall behebt Network Manager diejenigen Probleme, die remote repariert werden können, und fordert Sie dann auf, die übrigen Probleme zu beheben, indem Sie sich auf dem betreffenden Computer bei SecurityCenter anmelden und die angegebenen Empfehlungen befolgen. In einigen Fällen lautet der Vorschlag, dass die McAfee 2007-Sicherheits-Software auf dem Remote-Computer oder den Computern in Ihrem Netzwerk installiert werden sollte.

Sicherheitslücken schließen

Sie können Network Manager verwenden, um automatisch die meisten Sicherheitslücken auf verwalteten Remote-Computern zu beheben. Wenn beispielsweise VirusScan auf einem Remote-Computer deaktiviert ist, können Sie für die automatische Aktivierung Network Manager verwenden.

So beheben Sie Sicherheitslücken:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** den Schutzstatus eines Elements an.
3. Klicken Sie unter **Ich möchte** auf **Sicherheitslücken schließen**.
4. Klicken Sie auf **OK**, nachdem die Sicherheitslücken geschlossen wurden.

Hinweis: Auch wenn Network Manager die meisten Sicherheitslücken automatisch schließt, erfordert das Beheben einiger Probleme möglicherweise das Starten von SecurityCenter auf dem betroffenen Computer und das Befolgen der angegebenen Empfehlungen.

Installieren der McAfee-Sicherheits-Software auf Remote-Computern

Wenn auf einem oder meheren Computern in Ihrem Netzwerk die McAfee 2007-Sicherheits-Software nicht ausgeführt wird, kann ihr Schutzstatus nicht remote überwacht werden. Wenn Sie diese Computer remote überwachen möchten, müssen Sie zu jedem Computer gehen und die McAfee 2007-Sicherheits-Software installieren.

So installieren Sie die McAfee-Sicherheits-Software auf einem Remote-Computer:

1. Besuchen Sie in einem Browser auf dem Remote-Computer die Seite http://download.mcafee.com/us/.
2. Befolgen Sie die Bildschirmanweisungen für die Installation der McAfee 2007-Sicherheits-Software auf dem Computer.

KAPITEL 13

McAfee VirusScan

VirusScan bietet umfassenden, verlässlichen und aktuellen Schutz vor Viren und Spyware. Unterstützt durch die preisgekrönte McAfee-Scantechnologie schützt VirusScan vor Viren, Würmern, Trojanern, verdächtigen Skripts, Root-Kits, Pufferüberläufen, Hybridangriffen, Spyware, potentiell unerwünschten Programmen und anderen Bedrohungen.

In diesem Kapitel

Funktionen

Diese Version von VirusScan umfasst folgende Funktionen:

Virenschutz

Beim Echtzeit-Scan werden Dateien untersucht, wenn Sie oder Ihr Computer darauf zugreifen.

Scannen

Durchsucht Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen. Sie können außerdem mit der rechten Maustaste auf ein Element klicken, um es zu untersuchen.

Erkennung von Spyware und Adware

VirusScan identifiziert und entfernt Spyware, Adware und andere Programme, die Ihre Privatsphäre verletzen und die Leistung Ihres Computers beeinträchtigen können.

Automatische Updates

Automatische Updates schützen Sie vor den neuesten identifizierten und nicht identifizierten Computerbedrohungen.

Schnelles Scannen im Hintergrund

Schnelle, im Hintergrund ausgeführte Scans identifizieren und beseitigen Viren, Trojaner, Spyware, Adware, Dialer und andere Bedrohungen, ohne Sie bei der Arbeit zu unterbrechen.

Echtzeit-Sicherheitswarnungen

Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

Erkennen und Säubern an den am meisten gefährdeten Stellen

VirusScan führt die Überwachung und Säuberung an den Haupteintrittspunkten des Computers durch: E-Mails, Instant Messaging-Anlagen und Internetdownloads.

Überwachung von E-Mails auf Aktivitäten, die auf einen Wurm hinweisen.

WormStopper™ blockiert Trojaner, die versuchen, Würmer per E-Mail an andere Computer zu senden, und fragt nach, bevor unbekannte E-Mail-Programme E-Mail-Nachrichten an andere Computer senden.

Überwachen von Skripts auf Aktivitäten, die auf einen Wurm hinweisen.

ScriptStopper™ blockiert bekannte, schädliche Skripts, so dass diese auf Ihrem Computer nicht ausgeführt werden.

McAfee X-Ray für Windows

McAfee X-Ray erkennt und entfernt Rootkits und andere Programme, die sich vor Windows verstecken.

Pufferüberlaufschutz

Der Pufferüberlaufschutz schützt Sie vor Pufferüberläufen. Pufferüberläufe passieren, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (temporärer Speicher) zu speichern, als Ihr Computer zulässt, wodurch gültige Daten in nahe gelegenen Puffern beschädigt oder überschrieben werden.

McAfee SystemGuards

SystemGuards untersucht Ihren Computer auf bestimmte Verhaltensweisen, die auf Viren, Spyware oder Hacker-Aktivitäten hinweisen können.

KAPITEL 14

Verwalten des Virenschutzes

Sie können den Echtzeit-Viren-, Spyware-, SystemGuards- und Skriptschutz verwalten. Sie können beispielsweise das Scannen deaktivieren oder die zu scannenden Dateien angeben.

Die erweiterten Optionen können nur von Benutzern mit Administratorrechten geändert werden.

In diesem Kapitel

Verwenden des Virenschutzes

Wenn der Virenschutz (Echtzeit-Scannen) gestartet wird, überwacht er Ihrem Computer kontinuierlich auf Virusaktivitäten. Beim Echtzeit-Scannen werden alle Dateien gescannt, auf die Sie oder Ihr Computer zugreifen. Wenn der Virenschutz eine infizierte Datei erkennt, versucht er, die Infektion zu säubern oder zu entfernen. Wenn eine Datei nicht gesäubert oder entfernt werden kann, werden Sie in einer Warnmeldung zum Ausführen weiterer Maßnahmen aufgefordert.

Verwandte Themen

- Grundlegendes zu Sicherheitswarnungen (Seite 111)

Virenschutz deaktivieren

Wenn Sie den Virenschutz deaktivieren, wird Ihr Computer nicht mehr laufend auf Virenaktivitäten überprüft. Falls Sie den Virenschutz jedoch deaktivieren müssen, vergewissern Sie sich, dass keine Verbindung mit dem Internet besteht.

Hinweis: Durch die Deaktivierung des Virenschutzes wird auch der Spyware-, E-Mail- und Instant Messaging-Echtzeitschutz deaktiviert.

So deaktivieren Sie den Virenschutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Aus**.
4. Führen Sie im Dialogfeld für die Bestätigung eine der folgenden Aktionen durch:
   - Wenn der Virenschutz nach einer bestimmten Zeit wieder aktiviert werden soll, aktivieren Sie das Kontrollkästchen **Echtzeit-Scan wieder aktivieren nach** und wählen Sie im Menü eine Uhrzeit aus.
   - Wenn der Virenschutz nicht nach einer bestimmten Zeit wieder aktiviert werden soll, deaktivieren Sie das Kontrollkästchen **Echtzeit-Scan wieder aktivieren nach**.

5 Klicken Sie auf **OK**.

Wenn der Echtzeitschutz so konfiguriert ist, dass er beim Start von Windows automatisch ausgeführt wird, ist Ihr Computer nach einem Neustart wieder geschützt.

Verwandte Themen

- Konfiguration des Echtzeitschutzes (Seite 82)

Aktivieren des Virenschutzes

Der Virenschutz überwacht Ihren Computer kontinuierlich auf Virusaktivitäten.

So aktivieren Sie den Virenschutz:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Ein**.

Konfigurieren des Echtzeit-Schutzes

Sie haben die Möglichkeit, den Echzeit-Virenschutz zu ändern. Sie können beispielsweise nur Programmdateien und -dokumente überprüfen lassen oder das Echtzeit-Scannen beim Starten von Windows deaktivieren (nicht empfohlen).

Konfiguration des Echtzeitschutzes

Sie können den Echtzeit-Virenschutz bearbeiten. Sie können beispielsweise festlegen, dass nur Programmdateien und Dokumente untersucht werden oder dass Echtzeit-Scans beim Starten von Windows deaktiviert werden (nicht empfohlen).

So konfigurieren Sie den Echtzeitschutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Mithilfe von Heuristik auf unbekannte Viren prüfen**: Dateien werden mit Signaturen bekannter Viren verglichen, um Anzeichen nicht identifizierter Viren zu erkennen. Diese Option bietet die gründlichste Überprüfung, ist aber meist zeitaufwändiger als ein normaler Scan.
   - **Diskettenlaufwerk beim Herunterfahren prüfen**: Beim Herunterfahren Ihres Computers wird Ihr Diskettenlaufwerk untersucht.
   - **Auf Spyware und potentiell unerwünschte Programme prüfen**: Spyware, Adware und andere Programme, die potentiell ohne Ihre Erlaubnis Daten sammeln und übermitteln, werden erkannt und entfernt.
   - **Nachverfolgungs-Cookies suchen und entfernen**: Cookies, die potentiell ohne Ihre Erlaubnis Daten sammeln und übermitteln, werden erkannt und entfernt. Ein Cookie identifiziert Benutzer, wenn diese eine Webseite besuchen.
   - **Netzlaufwerke scannen**: Laufwerke, die mit Ihrem Netzwerk verbunden sind, werden gescannt.
   - **Pufferüberlaufschutz aktivieren**: Wenn eine Pufferüberlaufaktivität erkannt wird, wird sie blockiert, und Sie werden benachrichtigt.
   - **Echtzeit-Scans starten, wenn Windows gestartet wird (empfohlen)**: Der Echtzeitschutz wird bei jedem Start Ihres Computers aktiviert, auch wenn Sie ihn für eine Sitzung deaktivieren.

5 Klicken Sie auf eine der folgenden Schaltflächen:

- **Alle Dateien (empfohlen)**: Alle Dateitypen, die Ihr Computer verwendet, werden gescannt. Mit dieser Option erhalten Sie die gründlichste Überprüfung.
- **Nur Programmdateien und Dokumente**: Nur Programmdateien und Dokumente werden gescannt.

6 Klicken Sie auf **OK**.

Verwenden des Spyware-Schutzes

Der Spyware-Schutz entfernt Spyware, Adware und andere potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten.

Deaktivieren des Spyware-Schutzes

Wenn Sie den Spyware-Schutz deaktivieren, werden potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, nicht erkannt.

So deaktivieren Sie den Spyware-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Spyware-Schutz** auf **Aus**.

Aktivieren des Spyware-Schutzes

Der Spyware-Schutz entfernt Spyware, Adware und andere potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten.

So aktivieren Sie den Spyware-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Spyware-Schutz** auf **Ein**.

Verwenden von SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Anschließend können Sie diese Änderungen prüfen und entscheiden, ob Sie sie zulassen oder nicht.

SystemGuards ist wie folgt kategorisiert.

Programm

SystemGuards für Programme erkennt Änderungen an Startdateien, Erweiterungen und Konfigurationsdateien.

Windows

SystemGuards für Windows erkennt Änderungen an Ihren Internet Explorer-Einstellungen, einschließlich der Browserattribute und Sicherheitseinstellungen.

Browser

SystemGuards für Browser erkennt Änderungen an Windows-Diensten, Zertifikaten und Konfigurationsdateien.

Deaktivieren von SystemGuards

Wenn Sie SystemGuards deaktivieren, werden nicht autorisierte Änderungen an Ihrem Computer nicht erkannt.

So deaktivieren Sie alle SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard** auf **Aus**.

Aktivieren von SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus.

So aktivieren Sie SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard** auf **Ein**.

Konfigurieren von SystemGuards

Sie haben die Möglichkeit, SystemGuards zu konfigurieren. Sie können für jede erkannte Änderung festlegen, ob Sie benachrichtigt werden möchten und das Ereignis protokolliert, nur das Ereignis protokolliert oder SystemGuard deaktiviert werden soll.

Konfigurieren von SystemGuards

Sie haben die Möglichkeit, SystemGuards zu konfigurieren. Sie können für jede erkannte Änderung festlegen, ob Sie benachrichtigt werden möchten und das Ereignis protokolliert, nur das Ereignis protokolliert oder SystemGuard deaktiviert werden soll.

So konfigurieren Sie SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard-Schutz** auf **Erweitert**.
4. Klicken Sie in der SystemGuards-Liste auf eine Kategorie, um eine Liste der zugeordneten SystemGuards und deren Status anzuzeigen.
5. Klicken Sie auf den Namen eines SystemGuard.
6. Unter **Details** finden Sie Informationen zu SystemGuard.
7. Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:
   - Klicken Sie auf **Warnungen anzeigen**, wenn Sie benachrichtigt werden möchten, wenn eine Änderung eintritt und das Ereignis protokolliert wird.
   - Klicken Sie auf **Änderungen nur protokollieren**, wenn beim Erkennen einer Änderung keine Aktion ausgeführt werden soll. Die Änderung wird nur protokolliert.
   - Klicken Sie auf **Diesen SystemGuard deaktivieren**, um den SystemGuard zu deaktivieren. Sie werden im Fall einer Änderung weder benachrichtigt, noch wird das Ereignis protokolliert.
8. Klicken Sie auf **OK**.

Grundlegendes zu SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Anschließend können Sie diese Änderungen prüfen und entscheiden, ob Sie sie zulassen oder nicht.

SystemGuards ist wie folgt kategorisiert.

Programm

SystemGuards für Programme erkennt Änderungen an Startdateien, Erweiterungen und Konfigurationsdateien.

Windows

SystemGuards für Windows erkennt Änderungen an Ihren Internet Explorer-Einstellungen, einschließlich der Browserattribute und Sicherheitseinstellungen.

Browser

SystemGuards für Browser erkennt Änderungen an Windows-Diensten, Zertifikaten und Konfigurationsdateien.

Allgemeines zu SystemGuards für Programme

SystemGuards für Programme erkennt folgende Elemente:

ActiveX-Installationen

Erkennt ActiveX-Programme, die über Internet Explorer heruntergeladen wurden. ActiveX-Programme werden von Websites heruntergeladen und auf dem Computer im Verzeichnis "C:\Windows\Downloaded Program Files" oder "C:\Windows\Temp\Temporary Internet Files" gespeichert. Zudem werden Sie in der Registrierung anhand ihrer CLSID (die lange Zahlenfolge zwischen den geschweiften Klammern) identifiziert.

Internet Explorer verwendet viele legitime ActiveX-Programme. Wenn Sie ein ActiveX-Programm nicht für vertrauenswürdig halten, können Sie es löschen, ohne dass dies Folgen für den Betrieb des Computers hat. Wenn Sie dieses Programm zu einem späteren Zeitpunkt wieder benötigen, lädt Internet Explorer es beim nächsten Mal herunter, wenn Sie eine Website öffnen, für die das Programm erforderlich ist.

Startelemente

Überwacht Änderungen an den Start-Registrierungschlüsseln und -ordnern. In den Start-Registrierungsschlüsseln der Windows-Registrierung und in den Startordnern im Startmenü werden die Pfade zu Programmen auf Ihrem Computer gespeichert. Die dort aufgeführten Programme werden beim Start von Windows geladen. Spyware oder andere potenziell unerwünschte Programme versuchen häufig zu starten, wenn Windows gestartet wird.

Windows Shell Execute Hooks

Überwacht Änderungen an der Liste der Programme, die in "explorer.exe" geladen werden. Ein Shell Execute Hook ist ein Programmm, das sich in die Windows-Shell von "explorer.exe" lädt. Ein Shell Execute Hook-Programm empfängt alle auf einem Computer ausgeführten Befehle. Jedes in die explorer.exe-Shell geladene Programm kann vor dem tatsächlichen Start eines weiteren Programms einen zusätzlichen Task ausführen. Spyware oder andere potenziell unerwünschte Programme können Shell Execute Hooks verwenden, um das Ausführen von Sicherheitsprogrammen zu verhindern.

Shell Service Object Delay Load

Überwacht Änderungen an Dateien, die im Registrierungsschlüssel "ShellServiceObjectDelayLoad" aufgelistet sind. Diese Dateien werden beim Starten des Computers von der Datei "explorer.exe" geladen. Da "explore.exe" die Shell des Computers ist, wird sie immer gestartet und lädt die unter diesem Registrierungsschlüssel aufgelisteten Dateien. Diese Dateien werden beim Startvorgang so frühzeitig geladen, dass der Benutzer nicht eingreifen kann.

Info zu Windows SystemGuards

Windows SystemGuards finden die folgenden Elemente:

Kontextmenü-Handler

Verhindert nicht genehmigte Änderungen der Windows-Kontextmenüs. Mittels dieser Menüs können Sie mit einem Klick der rechten Maustaste bestimmte Aktionen für diese Datei ausführen.

AppInit DLLs

Verhindert nicht genehmigte Änderungen oder Erweiterungen der AppInit.DLLs von Windows. Der Registrierungswert AppInit_DLLs enthält eine Liste der Dateien, die beim Laden der Datei user32.dll geladen werden. Dateien im Wert AppInit_DLLs werden ganz am Anfang der Windows-Startroutine geladen, wodurch möglicherweise schädliche DLLs verborgen werden, bevor ein Eingriff durch den Benutzer möglich ist.

Windows-Hostsdatei

Überwacht Änderungen an der Hostsdatei Ihres Computers. Ihre Hostsdatei wird zur Umleitung bestimmter Domänennamen an bestimmte IP-Adressen verwendet. Wenn Sie beispielsweise die Website www.beispiel.com besuchen, prüft der Browser die Hostsdatei, findet einen Eintrag für beispiel.com und verweist auf die IP-Adresse dieser Domäne. Einige Spyware-Programme versuchen, die Hostsdatei zu ändern, um den Browser zu einer anderen Website weiterzuleiten oder um zu verhindern, dass Software ordnungsgemäß aktualisiert wird.

Winlogon-Shell

Überwacht die Winlogon-Shell. Diese Shell wird automatisch geladen, wenn sich ein Benutzer bei Windows anmeldet. Bei dieser Shell handelt es sich um die Hauptbenutzeroberfläche (UI), die zur Verwaltung von Windows verwendet wird. In der Regel handelt es sich hierbei um den Windows-Explorer (explorer.exe). Die Windows-Shell kann jedoch leicht so geändert werden, dass sie auf ein anderes Programm verweist. In diesem Fall wird jedes Mal, wenn sich ein Benutzer anmeldet, ein anderes Programm als die Windows-Shell gestartet.

Windows-Anmeldung - Benutzerinitialisierung

Überwacht Änderungen an den Benutzereinstellungen der Windows-Anmeldung. Der Schlüssel HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit legt fest, welches Programm gestartet wird, sobald sich ein Benutzer bei Windows anmeldet. Das Standardprogramm stellt das Profil, die Schriftarten, die Farben und andere Einstellungen für den Benutzernamen wieder her. Spyware und andere potentiell unerwünschte Programme können versuchen, sich selbst zu starten, indem sie sich selbst zu diesem Schlüssel hinzufügen.

Windows-Protokolle

Überwacht Änderungen an den Netzwerkprotokollen. Einige Spyware-Programme oder andere potentiell unerwünschte Programme übernehmen die Steuerung darüber, wie der Computer Informationen sendet und empfängt. Dies wird über die Windows-Protokollfilter und -handler erreicht.

Aufgesetzte Winsock-Dienstanbieter

Überwacht Layered Service Providers (LSPs), die Ihre Daten über das Netzwerk abrufen und sie ändern oder umleiten können. Legitime LSPs umfassen Software für Kindersicherungen, Firewalls und andere Sicherheitsprogramme. Spyware kann LSPs verwenden, um Ihre Internetaktivitäten zu überwachen und Ihre Daten zu bearbeiten. Um die Neuinstallation des Betriebssystems zu vermeiden, sollten Sie McAfee-Programme für das automatische Entfernen von Spyware und schadhaften LSPs verwenden.

Windows-Shell-Öffnungsbefehle

Verhindert Änderungen an den Öffnungsbefehlen der Windows-Shell (explore.exe). Shellöffnungsbefehle ermöglichen es einem bestimmten Programm, jedes Mal ausgeführt zu werden, wenn ein bestimmter Dateityp ausgeführt wird. Ein Wurm kann beispielsweise versuchen, jedes Mal ausgeführt zu werden, wenn eine EXE-Anwendung ausgeführt wird.

Gemeinsam verwendeter Taskplaner

Überwacht den Registrierungsschlüssel für den gemeinsam verwendeten Taskplaner, der eine Liste mit Programmen enthält, die beim Starten von Windows ausgeführt werden. Einige Spyware-Programme oder andere potentiell unerwünschte Programme ändern diesen Schlüssel und fügen sich ohne Ihre Erlaubnis selbst zur Liste hinzu.

Windows Messenger-Dienst

Überwacht den Windows Messenger-Dienst, der eine nicht dokumentierte Funktion von Windows Messenger ist, mit der Benutzer Popupmeldungen senden können. Einige Spyware-Programme oder andere potentiell unerwünschte Programme versuchen, den Dienst zu aktivieren und unerwünschte Werbung zu senden. Der Dienst kann auch durch Ausnutzen einer bekannten Sicherheitslücke bei remote ausgeführtem Code missbraucht werden.

Windows-Datei Win.ini

Die Datei Win.ini ist eine textbasierte Datei, die eine Liste der Programme enthält, die nach dem Starten von Windows ausgeführt werden sollen. Die Syntax zum Laden dieser Programme dient in dieser Datei zur Unterstützung älterer Windows-Versionen. Die meisten Programme verwenden zum Laden von Programmen nicht die Datei Win.ini: Einige Spyware-Programme oder andere potentiell unerwünschte Programme sind jedoch so konzipiert, dass sie sich diese Legacysyntax zunutze machen und beim Starten von Windows selbst laden.

Info zu Browser-SystemGuards

Windows SystemGuards finden die folgenden Elemente:

Browserhilfsobjekte

Überwacht Zusätze zu Browserhilfsobjekten (BHOs). Bei BHOs handelt es sich um Programme, die als Internet Explorer-Plugins fungieren. Spyware und Programme, die Ihren Browser missbrauchen, verwenden BHOs häufig, um Werbung anzuzeigen oder um Ihre Surfgewohnheiten zu verfolgen. BHOs werden auch von vielen legitimen Programmen verwendet, wie z. B. von gewöhnlichen Symbolleisten zum Suchen.

Internet Explorer-Leisten

Überwacht Änderungen, die an der Programmliste der Internet Explorer-Leiste vorgenommen werden. Bei Explorer-Leisten handelt es sich um Bereiche wie beispielsweise die Such-, Favoriten- oder Verlaufsbereiche, die in Internet Explorer (IE) oder Windows-Explorer angezeigt werden.

Internet Explorer-Plugins

Verhindert, dass Spyware Internet Explorer-Plugins installiert. Bei Internet Explorer-Plugins handelt es sich um Software-Addons, die beim Starten von Internet Explorer geladen werden. Spyware verwendet Internet Explorer-Plugins häufig, um Werbung anzuzeigen oder um Ihre Surfgewohnheiten zu verfolgen. Legitime Plugins fügen Funktionen zu Internet Explorer hinzu.

Internet Explorer-ShellBrowser

Überprüft Änderungen an Ihrer Internet Explorer-ShellBrowser-Instanz. Der Internet Explorer-ShellBrowser enthält Informationen und Einstellungen über eine Instanz von Internet Explorer. Falls diese Einstellungen geändert werden oder ein neuer ShellBrowser hinzugefügt wird, kann dieser ShellBrowser die Steuerung von Internet Explorer vollständig übernehmen und Funktionen wie beispielsweise Symbolleisten, Menüs und Schaltflächen hinzufügen.

Internet Explorer-Webbrowser

Überprüft Änderungen an Ihrer Internet Explorer-Webbrowser-Instanz. Der Internet Explorer-Webbrowser enthält Informationen und Einstellungen über eine Instanz von Internet Explorer. Falls diese Einstellungen geändert werden oder ein neuer Webbrowser hinzugefügt wird, kann dieser Webbrowser die Steuerung von Internet Explorer vollständig übernehmen und Funktionen wie beispielsweise Symbolleisten, Menüs und Schaltflächen hinzufügen.

Internet Explorer-URL-Suchhooks

Überwacht Änderungen, die am Internet Explorer-URL-Suchhook vorgenommen werden. URL-Suchhooks werden verwendet, wenn Sie eine Adresse im Adressfeld des Browsers ohne Verwendung von Protokollen (z. B. http:// oder ftp://) eingeben. Wenn Sie eine solche Adresse eingeben, kann der Browser URL-Suchhooks zum Durchsuchen des Internets nach der von Ihnen eingegebenen Adresse verwenden.

Internet Explorer-URLs

Überwacht Änderungen an den voreingestellten URLs von Internet Explorer. Dadurch wird verhindert, dass Spyware oder andere potentiell unerwünschte Programme Ihre Browser-Einstellungen ohne Ihre Zustimmung ändern.

Internet Explorer-Beschränkungen

Überwacht Internet Explorer-Beschränkungen, die es dem Computeradministrator ermöglichen, Benutzer daran zu hindern, die Startseite bzw. andere Optionen in Internet Explorer zu ändern. Diese Optionen sollten nur aktiviert sein, wenn sie der Administrator absichtlich festgelegt hat.

Internet Explorer-Sicherheitszonen

Überwacht Internet Explorer-Sicherheitszonen. Internet Explorer verfügt über vier vordefinierte Sicherheitszonen: Internet, lokales Intranet, vertrauenswürdige Sites und eingeschränkte Sites. Jede Sicherheitszone besitzt ihre eigene Sicherheitseinstellung, die vordefiniert ist oder vom Benutzer angepasst werden kann. Sicherheitszonen sind ein Ziel von einigen Spyware-Programmen oder anderen potentiell unerwünschten Programmen, da diese Programme durch das Herabsetzen der Sicherheitsstufe Sicherheitswarnungen umgehen und unerkannt handeln können.

Internet Explorer - Vertrauenswürdige Sites

Überwacht die vertrauenswürdigen Sites von Internet Explorer. Die Liste der vertrauenswürdigen Sites ist ein Verzeichnis der Websites, die Sie als vertrauenswürdig eingestuft haben. Diese Liste ist das Ziel von einigen Spyware-Programmen oder anderen potentiell unerwünschten Programmen, da verdächtige Sites damit ohne Ihre Erlaubnis im Vorhinein als vertrauenswürdig eingestuft werden können.

Internet Explorer-Richtlinie

Überwacht die Internet Explorer-Richtlinien. Diese Einstellungen werden normalerweise von Systemadministratoren verwendet, können aber durch Spyware missbraucht werden. Änderungen können verhindern, dass Sie eine andere Startseite festlegen, oder bewirken, dass Registerkarten im Dialogfeld "Internetoptionen" im Menü "Extras" nicht angezeigt werden.

Verwenden von Skriptprüfungen

Ein Skript kann Dateien erstellen, kopieren oder löschen. Es kann zudem die Windows-Registrierung öffnen.

Die Skriptprüfung verhindern automatisch, dass gefährliche Skripts auf Ihrem Computer ausgeführt werden.

Skriptprüfungen deaktivieren

Wenn Sie Skriptprüfungen deaktivieren, wird das Ausführen verdächtiger Skripts nicht erkannt.

So deaktivieren Sie Skriptprüfungen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Skriptptüfung** auf **Aus**.

Prüfskripte aktivieren

Die Skriptptüfung gibt eine Warnmeldung aus, wenn die Ausführung eines Skripts dazu führt, dass Dateien erstellt, kopiert oder gelöscht werden, oder dass Ihre Windows-Registrierung geöffnet wird.

So aktivieren Sie Skriptprüfungen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Skriptptüfung** auf **Ein**.

Verwenden des E-Mail-Schutzes

Der E-Mail-Schutz erkennt und blockiert Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen. Dazu gehören Viren, Trojaner, Würmer, Spyware, Adware und andere Bedrohungen.

E-Mail-Schutz deaktivieren

Wenn Sie den E-Mail-Schutz deaktivieren, werden potenzielle Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen nicht erkannt.

So deaktivieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Aus**.

E-Mail-Schutz aktivieren

Der E-Mail-Schutz erkennt Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen.

So aktivieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Ein**.

E-Mail-Schutz konfigurieren

Mit Hilfe der Optionen für den E-Mail-Schutz können sie ein- und ausgehende Nachrichten und Würmer prüfen. Würmer replizieren und verbrauchen Systemressourcen, wodurch die Leistung reduziert bzw. Tasks verlangsamt werden. Würmer können Kopien von sich selbst über E-Mail-Nachrichten verbreiten. Sie können beispielsweise versuchen, E-Mail-Nachrichten an Personen in Ihrem Adressbuch weiterzuleiten.

E-Mail-Schutz konfigurieren

Mit Hilfe der Optionen für den E-Mail-Schutz können sie ein- und ausgehende Nachrichten und Würmer prüfen.

So konfigurieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Erweitert**.
4. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Eingehende E-Mail-Nachrichten überprüfen** Eingehende (POP3) Nachrichten werden auf potenzielle Bedrohungen geprüft.
   - **Ausgehende E-Mail-Nachrichten überprüfen**: Ausgehende (SMTP) Nachrichten werden auf potenzielle Bedrohungen geprüft.
   - **WormStopper aktivieren**: WormStopper blockiert Würmer in E-Mail-Nachrichten.
5. Klicken Sie auf **OK**.

Verwenden des Instant Messaging-Schutzes

Der Instant Messaging-Schutz erkennt Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten.

Instant Messaging-Schutz deaktivieren

Wenn Sie den Instant Messaging-Schutz deaktivieren, werden Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten nicht erkannt.

So deaktivieren Sie den Instant Messaging-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Instant Messaging-Schutz** auf **Aus**.

Instant Messaging-Schutz aktivieren

Der Instant Messaging-Schutz erkennt Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten.

So aktivieren Sie den Instant Messaging-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Instant Messaging-Schutz** auf **Ein**.

KAPITEL 15

Manuelles Prüfen des Computers

Sie können Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen durchsuchen. Wenn VirusScan eine verdächtige Datei findet, versucht es automatisch, die Datei zu bereinigen, sofern es sich dabei nicht um ein potenziell unerwünschtes Programm handelt. Wenn VirusScan die Datei nicht bereinigen kann, können Sie die Datei isolieren oder löschen.

In diesem Kapitel

Manuelles Scannen

Sie können die Überprüfung jederzeit manuell ausführen. Wenn Sie VirusScan beispielsweise gerade installiert haben, können Sie eine Überprüfung ausführen, um sicherzustellen, dass auf Ihrem Computer keine Viren oder andere Bedrohungen vorhanden sind. Wenn Sie die Echtzeit-Überprüfung deaktiviert haben, können Sie eine Überprüfung durchführen, um sicherzustellen, dass Ihr Computer noch sicher ist.

Überpüfung unter Verwendung der Einstellungen für das manuelle Prüfen

Bei diesem Scantyp werden die von Ihnen festgelegten Einstellungen für die manuelle Prüfung verwendet. VirusScan prüft den Inhalt komprimierter Dateien (.zip, .cab usw.), zählt eine komprimierte Datei jedoch als eine Datei. Die Anzahl der durchsuchten Dateien kann auch variieren, wenn Sie seit der letzten Überprüfung Ihre temporären Internetdateien gelöscht haben.

So führen Sie die Überpüfung unter Verwendung der Einstellungen für das manuelle Prüfen aus:

1. Klicken Sie im Menü "Grundlagen" auf **Scannen**. Wenn das Scannen abgeschlossen ist, werden in einer Zusammenfassung die Anzahl der geprüften und erkannten Elemente sowie der Zeitpunkt der letzten Prüfung angezeigt.
2. Klicken Sie auf **Fertig stellen**.

Verwandte Themen

- Konfigurieren manueller Prüfungen (Seite 102)

Scan ohne Verwendung Ihrer Einstellungen für manuelle Scans

Dieser Scan verwendet nicht die von Ihnen festgelegten Einstellungen für manuelle Scans. VirusScan scannt den Inhalt komprimierter Dateien (.zip, .cab etc.), und zählt dabei eine komprimierte Datei als eine Datei. Die Anzahl der durchsuchten Dateien kann auch variieren, wenn Sie seit der letzten Überprüfung Ihre temporären Internetdateien gelöscht haben.

So führen Sie einen Scan ohne Verwendung Ihrer Einstellungen für manuelle Scans durch:

1. Klicken Sie im Menü "Erweitert" auf **Home**.
2. Klicken Sie im Home-Bereich auf **Prüfen**.
3. Aktivieren Sie unter **Zu scannende Bereiche** die Kontrollkästchen neben den Dateien, Ordnern und Laufwerken, die gescannt werden sollen.
4. Aktivieren Sie unter **Optionen** die Kontrollkästchen neben den Dateitypen, die gescannt werden sollen.
5. Klicken Sie auf **Jetzt scannen**. Wenn der Scan beendet ist, wird eine Zusammenfassung angezeigt, in der die Anzahl der gescannten und erkannten Elemente sowie die Anzahl der gesäuberten Elemente und das Datum des letzten Scan angezeigt werden.
6. Klicken Sie auf **Fertig stellen**.

Hinweis: Diese Optionen werden nicht gespeichert.

Scannen in Windows Explorer

Sie können ausgewählte Dateien, Ordner oder Laufwerke in Windows Explorer auf Viren und andere Bedrohungen hin überprüfen.

So durchsuchen Sie Dateien im Windows Explorer:

1. Öffnen Sie Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll, und klicken Sie dann auf **Scannen**. Zur Gewährleistung einer umfassenden Prüfung sind alle Standard-Prüfoptionen ausgewählt.

Konfigurieren manueller Prüfungen

Bei der manuellen oder geplanten Prüfung können Sie die zu prüfenden Dateitypen, die zu prüfenden Speicherorte und den Zeitpunkt der Prüfungen festlegen.

Konfigurieren der zu prüfenden Dateitypen

Sie können die zu prüfenden Dateitypen konfigurieren.

So konfigurieren Sie die zu prüfenden Dateitypen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.
5. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Mithilfe der Heuristik auf unbekannte Viren prüfen**: Die Dateien werden mit Signaturen bekannter Viren verglichen, um Hinweise auf nicht identifizierte Viren zu erkennen. Diese Option bietet die gründlichste Überprüfung, ist aber meist zeitaufwendiger als eine normale Überprüfung.
   - **ZIP-Dateien und anderen Archivdateien prüfen**: Erkennt und entfernt Viren in .zip- und anderen Archivdateien. Manchmal werden Viren in eine ZIP-Datei eingesetzt und diese ZIP-Datei anschließend in eine andere ZIP-Datei eingefügt, um Anti-Virus-Scanner zu umgehen.
   - **Auf Spyware und potenziell unerwünschte Programme prüfen**: Spyware, Adware und andere Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, werden erkannt und entfernt.
   - **Nachverfolgungs-Cookies suchen und entfernen**: Cookies, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, werden erkannt und entfernt. Ein Cookie identifiziert Benutzer, wenn diese eine Webseite besuchen.
   - **Auf Rootkits und andere Stealth-Programme prüfen**: Erkennt und entfernt alle Rootkit- und andere Programme, die sich vor Windows verbergen.
6. Klicken Sie auf eine der folgenden Schaltflächen:
   - **Alle Dateien (empfohlen)**: Jeder aus dem Computer verwendete Dateityp wird geprüft. Mit dieser Option erhalten Sie die gründlichste Überprüfung.
   - **Nur Programmdateien und Dokumente**: Es werden nur Programmdateien und Dokumente geprüft.

7 Klicken Sie auf **OK**.

Konfigurieren der zu prüfenden Speicherorte

Sie können die zu prüfenden Speicherorte für manuelle oder geplante Prüfungen konfigurieren.

So konfigurieren Sie den zu prüfenden Speicherort:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Erweitert**.

4 Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.

5 Wählen Sie unter **Zu prüfender Standard-Speicherort** die zu prüfenden Dateien, Ordner und Laufwerke aus.

   Um eine möglichst umfassende Prüfung zu gewährleisten, wählen Sie die Option **Kritische Dateien**.

6 Klicken Sie auf **OK**.

Planen von Prüfungen

Sie können Prüfungen planen, um Ihren Computer zu festgelegten Intervallen umfassend auf Viren und andere Bedrohungen zu prüfen.

So planen Sie eine Prüfung:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Erweitert**.

4 Klicken Sie im Fenster "Virenschutz" auf **Geplanter Scan**.

5 Stellen Sie sicher, dass **Planmäßige Überprüfung aktivieren** ausgewählt ist.

6 Aktivieren Sie das Kontrollkästchen neben dem Wochentag, an dem die Prüfung ausgeführt werden soll.

7 Klicken Sie zum Angeben einer Startzeit in der Liste der Startzeiten auf einen Wert.

8 Klicken Sie auf **OK**.

Tipp: Um den Standardzeitplan zu verwenden, klicken Sie auf **Zurücksetzen.**

KAPITEL 16

Verwalten von VirusScan

Sie können Elemente aus den Listen mit vertrauenswürdigen Elementen löschen, unter Quarantäne gestellte Programme, Cookies und Dateien verwalten, Ereignisse und Protokolle anzeigen und McAfee verdächtige Aktivitäten melden.

In diesem Kapitel

Verwalten vertrauenswürdiger Listen

Wenn Sie einem SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm vertrauen, wird das Element einer Liste vertrauenswürdiger Elemente hinzugefügt, so dass das Element nicht mehr erkannt wird.

Wenn Sie einem Programm versehentlich vertrauen oder wenn ein Programm erkannt werden soll, müssen Sie es aus dieser Liste entfernen.

Verwalten vertrauenswürdiger Listen

Wenn Sie einem SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm vertrauen, wird das Element einer Liste vertrauenswürdiger Elemente hinzugefügt, so dass das Element nicht mehr erkannt wird.

Wenn Sie einem Programm versehentlich vertrauen oder wenn ein Programm erkannt werden soll, müssen Sie es aus dieser Liste entfernen.

So entfernen Sie Elemente aus den Listen mit vertrauenswürdigen Elementen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Virenschutz" auf **Listen mit vertrauenswürdigen Elementen**.
5. Wählen Sie in der Liste ein vertrauenswürdiges Objekt des Typs SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm aus, um dessen Elemente und ihren Vertrauensstatus anzuzeigen.
6. Unter **Details** finden Sie Informationen zu diesem Element.
7. Klicken Sie unter **Ich möchte** auf eine Aktion.
8. Klicken Sie auf **OK**.

Verw. isolierter Programme, Cookies und Dateien

Unter Quarantäne gestellte Programme, Cookies und Dateien können wiederhergestellt, gelöscht oder zur Analyse an McAfee gesendet werden.

Wiederherstellen von unter Quarantäne gestellten Programmen, Cookies und Dateien

Falls erforderlich, können Sie Programme, Cookies und Dateien, die unter Quarantäne gestellt wurden, wiederherstellen.

So stellen Sie unter Quarantäne gestellte Programme, Cookies und Dateien wieder her:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die wiederhergestellt werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **Wiederherstellen**.

Entfernen von unter Quarantäne gestellten Programmen, Cookies und Dateien

Sie können unter Quarantäne gestellte Programme, Cookies und Dateien entfernen.

So entfernen Sie unter Quarantäne gestellte Programme, Cookies und Dateien:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die wiederhergestellt werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **Entfernen**.

Unter Quarantäne gestellte Programme, Cookies und Dateien an McAfee senden

Sie können unter Quarantäne gestellte Programme, Cookies und Dateien zur Analyse an McAfee senden.

Hinweis: Wenn die unter Quarantäne gestellte Datei, die Sie senden möchten, die maximal zulässige Größe überschreitet, kann die Datei abgelehnt werden. In den meisten Fällen ist dies jedoch nicht der Fall.

So senden Sie unter Quarantäne gestellte Programme oder Dateien an McAfee:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die an McAfee gesendet werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **An McAfee senden**.

Anzeigen zuletzt aufg. Ereignisse und Protokolle

Unter "Zuletzt aufgetretene Ereignisse" und "Protokolle" werden Ereignisse zu allen installierten McAfee-Produkten angezeigt.

Unter "Zuletzt aufgetretene Ereignisse" können Sie die letzten 30 signifikanten Ereignisse sehen, die auf Ihrem Computer aufgetreten sind. Sie können blockierte Programme wiederherstellen, die Echtzeitprüfung neu aktivieren und Pufferüberläufen vertrauen.

Außerdem können sie Protokolle anzeigen, in denen alle Ereignisse der letzten 30 Tage aufgezeichnet werden.

Ereignisse anzeigen

Unter "Zuletzt aufgetretene Ereignisse" können Sie die letzten 30 signifikanten Ereignisse sehen, die auf Ihrem Computer aufgetreten sind. Sie können blockierte Programme wiederherstellen, die Echtzeitprüfung neu aktivieren und Pufferüberläufen vertrauen.

So zeigen Sie Ereignisse an:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Zuletzt aufgetretene Ereignisse**.
3. Wählen Sie das Ereignis aus, das Sie sich ansehen möchten.
4. Unter **Details** finden Sie Informationen zu diesem Ereignis.
5. Klicken Sie unter **Ich möchte** auf eine Aktion.

Protokolle anzeigen

In Protokollen werden alle Ereignisse aufgezeichnet, die in den letzten 30 Tagen aufgetreten sind.

So zeigen Sie Protokolle an:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Zuletzt aufgetretene Ereignisse**.
3. Klicken Sie im Fenster "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
4. Wählen Sie den Protokoll aus, den Sie sich ansehen möchten, und wählen Sie anschließend ein Protokoll aus.
5. Unter **Details** finden Sie Informationen zu diesem Protokoll.

Autom. Melden anonymer Informationen

Sie können Viren, potenziell unerwünschte Programme und Hacker-Informationen anonym an McAfee senden. Diese Option ist nur während der Installation verfügbar.

Es werden keine Informationen gesammelt, anhand derer Sie persönlich identifiziert werden können.

Bei McAfee melden

Sie können Viren, potenziell unerwünschte Programme und Hacker-Informationen an McAfee senden. Diese Option ist nur während der Installation verfügbar.

So melden Sie anonyme Informationen automatisch:

1. Übernehmen Sie bei der Installation von VirusScan die Vorgabe **Anonyme Informationen übermittteln**.
2. Klicken Sie auf **Weiter**.

Grundlegendes zu Sicherheitswarnungen

Wenn die Echtzeitprüfung eine Bedrohung erkennt, wird eine Warnung angezeigt. Bei den meisten Viren, Trojanern und Würmern versucht die Echtzeitprüfung automatisch, die Datei zu bereinigen, und zeigt eine Warnung an. Bei potenziell unerwünschten Programmen und SystemGuards wird die Datei oder Änderung von der Echtzeitprüfung ermittelt, automatisch blockiert und eine Warnung angezeigt. Bei Pufferüberlauf, Nachverfolgungs-Cookies und Skriptaktivitäten blockiert die Echtzeitprüfung die Aktivität automatisch und benachrichtigt Sie.

Diese Warnungen können in drei Grundarten eingeteilt werden.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Sie können anschließend festlegen, wie mit erkannten Dateien, E-Mails, verdächtigen Skripts, potenziellen Würmern, potenziell unerwünschten Programmen, SystemGuards oder Pufferüberläufen verfahren werden soll.

Verwalten von Warnungen

McAfee bietet mehrere Warnungen, um Sie bei der Verwaltung der Sicherheit zu unterstützen. Diese Warnungen können in drei Grundarten eingeteilt werden.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Rote Warnungen

Bei einer roten Warnung ist ein Eingreifen Ihrerseits erforderlich. In einigen Fällen kann McAfee nicht ermitteln, wie es automatisch auf eine bestimmte Aktivität reagieren soll. In diesen Fällen wird die entsprechende Aktivität in einer roten Warnung beschrieben und Sie haben mehrere Optionen zur Auswahl.

Gelbe Warnungen

Eine gelbe Warnung ist eine nicht-kritische Benachrichtigung, bei der in der Regel kein Eingreifen Ihrerseits erforderlich ist. Die entsprechende Aktivität wird in einer gelben Warnung beschrieben und Sie haben mehrere Optionen zur Auswahl.

Grüne Warnungen

In den meisten Fällen enthalten grüne Warnungen allgemeine Angaben zu einem Ereignis und es ist kein Eingreifen Ihrerseits erforderlich.

Konfigurieren von Warnoptionen

Wenn Sie nicht möchten, dass eine Warnung noch einmal angezeigt wird und dies später ändern möchten, haben Sie die Möglichkeit, dies entsprechend zu konfigurieren. Weitere Informationen zum Konfigurieren von Warnoptionen finden Sie in der SecurityCenter-Dokumentation.

KAPITEL 17

Zusätzliche Hilfe

In diesem Kapitel werden die häufig gestellte Fragen und Fehlerbehebungsszenarios beschrieben.

In diesem Kapitel

Fragen und Antworten (FAQs)

Dieser Abschnitt enthält Antworten zu den am häufigsten gestellten Fragen.

Eine Bedrohung wurde erkannt. Wie soll ich vorgehen?

McAfee verwendet Warnungen, um Ihre Sicherheit zu verwalten. Diese Warnungen lassen sich in drei allgemeine Typen aufteilen.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Sie können anschließend festlegen, wie erkannte Dateien, entdeckte E-Mails, verdächtige Skripts, potentielle Würmer, potentiell unerwünschte Programme, SystemGuards oder Pufferüberläufe verwaltet werden sollen.

Weitere Informationen zur Verwaltung bestimmter Bedrohungen finden Sie in der Virus-Informationsbibliothek unter: http://us.mcafee.com/virusInfo/default.asp?affid=.

Verwandte Themen

- Grundlegendes zu Sicherheitswarnungen (Seite 111)

Kann ich VirusScan mit den Browsern "Netscape", "Firefox" und "Opera" verwenden?

Sie können Netscape, Firefox oder Opera als Standardbrowser verwenden, müssen jedoch auch Microsoft Internet Explorer ab Version 6.0 auf Ihrem Computer installiert haben.

Ist zur Ausführung einer Prüfung eine Internetverbindung erforderlich?

Zum Ausführen einer Prüfung müssen Sie nicht mit dem Internet verbunden sein. Sie sollten aber mindestens einmal wöchentlich eine Verbindung zum Internet herstellen, damit McAfee-Aktualisierungen empfangen werden können.

Überprüft VirusScan E-Mail-Anlagen?

Wenn Sie die Echtzeitprüfung und den E-Mail-Schutz aktiviert haben, werden beim Eingang der E-Mail-Nachricht alle Anhänge geprüft.

Überprüft VirusScan auch komprimierte Dateien?

VirusScan prüft .ZIP-Dateien und andere Archivdateien.

Warum treten bei der Prüfung ausgehender E-Mails Fehler auf?

Bei der Prüfung ausgehender E-Mail-Nachrichten können folgende Fehlertypen auftreten:

- Protokollfehler. Der E-Mail-Server hat eine E-Mail-Nachricht abgelehnt.
  Wenn ein Protokoll- oder Systemfehler auftritt, werden die verbleibenden E-Mail-Nachrichten für die entsprechende Sitzung weiter verarbeitet und an den Server gesendet.
- Verbindungsfehler. Eine Verbindung zum E-Mail-Server wurde abgebrochen.
  Wenn ein Verbindungsfehler auftritt, vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist, und versuchen Sie, die Nachricht über die Liste der **gesendeten** Nachrichten Ihres E-Mail-Programms erneut zu senden.
- Systemfehler. Es ist ein Filehandling- bzw. ein anderer Systemfehler aufgetreten.
- Fehler mit verschlüsselter SMTP-Verbindung. Es wurde eine verschlüsselte SMTP-Verbindung mit Ihrem E-Mail-Programm festgestellt.
  Wenn ein Fehler mit der verschlüsselten SMTP-Verbindung auftritt, deaktivieren Sie die verschlüsselte SMTP-Verbindung in Ihrem E-Mail-Programm, um sicherzustellen, dass Ihre E-Mail-Nachrichten überprüft werden.

Wenn beim Senden von E-Mail-Nachrichten Zeitüberschreitungen auftreten, deaktivieren Sie die Überprüfung ausgehender E-Mail-Nachrichten oder deaktivieren Sie die verschlüsselte SMTP-Verbindung in Ihrem E-Mail-Programm.

Verwandte Themen

- E-Mail-Schutz konfigurieren (Seite 97)

Problembehandlung

Dieser Abschnitt enthält Hilfe zu allgemeinen Problemen, die auftreten können.

Ein Virus kann nicht bereinigt oder gelöscht werden

Einige Viren müssen Sie manuell vom Computer entfernen. Versuchen Sie, Ihren Computer neu zu starten und die Prüfung erneut auszuführen.

Wenn der Computer einen Virus nicht selbständig bereinigen oder löschen kann, verwenden Sie die Virus Information Library unter: http://us.mcafee.com/virusInfo/default.asp?affid=.

Weitere Unterstützung erhalten Sie vom McAfee-Kundendienst auf der McAfee-Website.

Hinweis: Viren können nicht von CD-ROMs, DVDs oder schreibgeschützten Disketten entfernt werden.

Ein Element kann auch nach dem Neustart nicht entfernt werden

In einigen Fällen ist es erforderlich, dass Sie Ihren Computer nach dem Prüfen und Entfernen von Elementen neu starten.

Wenn das Element nach dem Neustart des Computers nicht entfernt werden kann, senden Sie die Datei an McAfee.

Hinweis: Viren können nicht von CD-ROMs, DVDs oder schreibgeschützten Disketten entfernt werden.

Verwandte Themen

- Verwalten von unter Quarantäne gestellten Programmen, Cookies und Dateien (Seite 107)

Komponenten fehlen oder sind beschädigt

Einige Situationen können zu einer fehlerhaften Installation von VirusScan führen:

- Es ist nicht genügend Festplattenplatz oder Arbeitsspeicher auf Ihrem Computer verfügbar. Stellen Sie sicher, dass Ihr Computer den Systemanforderungen der Software entspricht.
- Der Internetbrowser ist nicht richtig konfiguriert.
- Ihre Internetverbindung ist fehlerhaft. Überprüfen Sie Ihre Verbindung oder versuchen Sie später noch einmal, eine Verbindung herzustellen.
- Dateien fehlen oder die Installation schlägt fehl.

Versuchen Sie, potenzielle Probleme zu beheben, und installieren Sie VirusScan anschließend erneut.

KAPITEL 18

McAfee Personal Firewall

Personal Firewall bietet erweiterten Schutz für Ihren Computer und Ihre persönlichen Daten. Personal Firewall errichtet eine Barriere zwischen Ihrem Computer und dem Internet. Dabei wird der Internetverkehr im Hintergrund auf verdächtige Aktivitäten überwacht.

In diesem Kapitel

Funktionen

Personal Firewall bietet Schutz bei ein- und ausgehenden Verbindungen, vertraut automatisch bekannten gutartigen Programmen und hilft dabei, Spyware, Trojaner und Keylogger-Programme zu blockieren. Mit Firewall können Sie Hacker-Angriffe abwehren, die Internet- und Netzwerkaktivität überwachen, sich über feindliche oder verdächtige Ereignisse benachrichtigen lassen, detaillierte Informationen zum Internetverkehr anzeigen und Antivirus-Abwehrstrategien ergänzen.

Standardmäßige und benutzerdefinierte Sicherheitsstufen

Schützen Sie sich mit Hilfe der standardmäßigen Einstellungen von Firewall vor Intrusion-Angriffen und verdächtigen Aktivitäten oder passen Sie Firewall an Ihre Sicherheitsanforderungen an.

Empfehlungen in Echtzeit

Lassen Sie sich dynamisch Empfehlungen zukommen, um zu ermitteln, ob Programmen Internetzugriff gewährt werden oder Netzwerkverkehr als vertrauenswürdig eingestuft werden soll.

Intelligente Zugriffsverwaltung für Programme

Im Firewall-Fenster "Programmberechtigungen" verwalten Sie den Internetzugriff für Programme über Warnungen und Ereignisprotokolle oder Sie konfigurieren Zugriffsberechtigungen für bestimmte Programme.

Gaming-Schutz

Sie können verhindern, dass Warnungen zu Einbruchsversuchen und verdächtigen Aktivitäten während des Spielens im Vollbildmodus angezeigt werden, und Firewall so konfigurieren, dass die Warnungen nach Abschluss des Computerspiels angezeigt werden.

Schutz beim Computer-Start

Bevor Windows gestartet wird, schützt Firewall Ihren Computer vor Einbruchsversuchen sowie vor unerwünschten Programmen und unerwünschtem Netzwerkverkehr.

Kontrolle des Systemdienstanschlusses

Systemdienstanschlüsse können ein Sicherheitsrisiko für Ihren Computer darstellen. Mit Firewall können Sie die für einige Programme erforderlichen offenen und geschlossenen Systemdienstanschlüsse erstellen und verwalten.

Verwalten von Computer-Verbindungen

Sie können Remote-Verbindungen und IP-Adressen, die eine Verbindung zu Ihrem Computer herstellen, als vertrauenswürdig einstufen oder blockieren.

Integration von HackerWatch-Informationen

HackerWatch ist ein Sicherheitsinformations-Hub, der globale Hacking- und Intrusion-Muster verfolgt und die aktuellsten Informationen zu Programmen auf Ihrem Computer zur Verfügung stellt. Außerdem haben Sie die Möglichkeit, globale Sicherheitsereignisse und Statistiken zu Internetanschlüssen anzuzeigen.

Firewall sperren

Des Weiteren können Sie den gesamten ein- und ausgehenden Netzwerkverkehr zwischen Ihrem Computer und dem Internet sofort sperren.

Sicherheitseinstellungen für Firewall wiederherstellen

Sie können die ursprünglichen Sicherheitseinstellungen für Firewall wiederherstellen. Wenn sich Personal Firewall nicht so verhält, wie Sie es wünschen, haben Sie die Möglichkeit, Ihre aktuellen Einstellungen rückgängig zu machen und die Standardeinstellungen des Produkts wiederherzustellen.

Erweiterte Erkennung von Trojanern

Personal Firewall verwaltet Programmverbindungen mit einer erweiterten Datenbank, mit der mehr potenziell bösartige Anwendungen, beispielsweise Trojaner, erkannt und blockiert und somit daran gehindert werden können, auf das Internet zuzugreifen und möglicherweise Ihre persönlichen Daten weiterzugeben.

Ereignisprotokollierung

Legen Sie fest, ob die Protokollierung aktiviert oder deaktiviert werden soll, und, wenn sie aktiviert wird, welche Ereignistypen protokolliert werden sollen. Mit der Ereignisprotokollierung können Sie zuletzt aufgetretende ein- oder ausgehende Ereignisse anzeigen. Außerdem haben Sie die Möglichkeit, Ereignisse anzuzeigen, die auf Einbruchsversuche hindeuten.

Überwachen des Internetverkehrs

Sie können einfach zu lesende grafische Karten prüfen, auf der die Quelle von feindlichen Angriffen und Datenverkehr weltweit angezeigt werden. Zudem werden detaillierte Eigentümerinformationen und geografische Daten für Ursprungs-IP-Adressen bereitgestellt. Des Weiteren können Sie ein- und ausgehenden Verkehr analysieren sowie die Programmbandbreite und die Programmaktivität überwachen.

Eindringschutz

Schützt Ihre Privatsphäre, indem Eindringschutz gegen mögliche Bedrohungen aus dem Internet zur Verfügung gestellt wird. Durch die Verwendung Heuristik-ähnlicher Funktionen bietet McAfee eine dritte Schutzstufe, da alle Objekte blockiert werden, die Angriffssymptome oder Eigenschaften von Hacker-Angriffen aufweisen.

Intelligente Datenverkehrsanalyse

Prüft sowohl ein- als auch ausgehenden Internetverkehr und Programmverbindungen, einschließlich derer, die aktiv offene Verbindungen überwachen. Dies ermöglicht Ihnen, Programme zu erkennen, die möglicherweise ein Risiko darstellen, und entsprechende Gegenmaßnahmen zu treffen.

Firewall starten

Schon direkt nach der Installation von Firewall ist Ihr Computer vor Intrusionsversuchen und unerwünschtem Internetdatenverkehr geschützt. Darüber hinaus können Sie mit Firewall Warnungen erhalten sowie den Zugriff auf eingehende und ausgehende Internetverbindungen bekannter und unbekannter Programme verwalten. Empfehlungen und Standardsicherheit sind automatisch aktiviert.

Sie können Firewall zwar im Bereich "Internet & Netzwerkkonfiguration" deaktivieren, jedoch ist Ihr Computer dann nicht mehr gegen Intrusionsversuche und unerwünschten Internetdatenverkehr geschützt. Außerdem sind Sie dann nicht mehr in der Lage, eingehende und ausgehende Internetverbindungen effektiv zu verwalten. Daher sollten Sie den Firewall-Schutz nur vorübergehend und nur wenn absolut notwendig deaktivieren. Sie können Firewall auch im Bereich "Internet & Netzwerkkonfiguration" aktivieren.

Firewall deaktiviert automatisch die Windows® Firewall und richtet sich selbsttätig als standardmäßige Firewall ein.

Hinweis: Öffnen Sie zum Konfigurieren von Firewall das Fenster "Netzwerk- & Internetkonfiguration".

Firewall-Schutz aktivieren

Das Aktivieren der Firewall schützt Ihren Computer vor Intrusionsversuchen und unerwünschtem Internetdatenverkehr. Damit können außerdem eingehende und ausgehende Internetverbindungen verwaltet werden.

So aktivieren Sie den Firewall-Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Firewall-Schutz** auf **Ein**.

Firewall-Schutz deaktivieren

Durch das Deaktivieren des Firewall-Schutzes wird Ihr Computer anfällig gegenüber Intrusionsversuchen und unerwünschtem Internetdatenverkehr. Außerdem können Sie ohne den Firewall-Schutz keine eingehenden und ausgehenden Internetverbindungen verwalten.

So deaktivieren Sie den Firewall-Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Firewall-Schutz** auf **Aus**.

Mit Warnungen arbeiten

Firewall unterstützt Sie mit verschiedenen Warnungen bei der Verwaltung Ihrer Sicherheit. Diese Warnungen lassen sich in vier allgemeine Typen aufteilen.

- Warnung "Trojaner blockiert"
- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Warnungen können auch Empfehlungen enthalten, wie Benutzer bei angezeigten Warnungen vorgehen sollten. In anderen Warnungen werden Benutzer darauf hingewiesen, wie Sie weitere Informationen zu den auf Ihrem Computer ausgeführten Programmen erhalten können.

Allgemeines zu Warnungen

Firewall verfügt über vier allgemeine Warnungstypen. Einige Warnungen enthalten Hinweise, wie sie weitere Informationen zu den auf Ihrem Computer ausgeführten Programmen erhalten können.

Warnung "Trojaner blockiert"

Trojaner tarnen sich als legale Programme und können zu Schäden an Ihrem Computer sowie zu Systemabstürzen führen. Außerdem können sie Unbefugten Zugriff auf Ihren Computer gewähren. Die Warnung "Trojaner blockiert" wird angezeigt, wenn Firewall einen Trojaner auf Ihrem Computer erkennt und dann blockiert. Sie sollten Ihr System in jedem Fall nach weiteren Bedrohungen scannen. Diese Warnung wird bei jeder Sicherheitsstufe angezeigt, außer bei der Sicherheitsstufe "Offen" oder wenn die Option "Empfehlungen" deaktiviert ist.

Rote Warnungen

Der häufigste Warnungstyp ist die rote Warnung. Er erfordert im Allgemeinen ein Eingreifen durch den Benutzer. Da Firewall in einigen Fällen die notwendigen Aktionen für eine Programmaktivität bzw. ein Netzwerkereignis nicht automatisch feststellen kann, beschreibt die Warnung zunächst die aktuelle Programmaktivität (bzw. das Netzwerkereignis) und führt dann eine oder mehrere Optionen auf, auf die Sie reagieren müssen. Wenn die Option "Empfehlungen" aktiviert ist, werden Programme zum Bereich "Programmberechtigungen" hinzugefügt.

Folgende Warnmeldungen treten am häufigsten auf:

- **Das Programm fordert Zugriff auf das Internet an**: Firewall hat ein Programm erkannt, das versucht, eine Verbindung zum Internet herzustellen.
- **Das Programm wurde geändert**: Firewall hat eine Änderung an einem Programm erkannt. Dabei kann es sich eventuell um das Ergebnis einer Onlineaktualisierung handeln.
- **Programm blockiert**: Firewall blockiert ein Programm, da es im Bereich "Programmberechtigungen" aufgeführt ist.

In Abhängigkeit Ihrer Einstellungen und der Programmaktivität bzw. des Netzwerkereignisses werden die folgenden Optionen am häufigsten angezeigt:

- **Zugriff gewähren**: Gewährt einem Programm auf Ihrem Computer den Zugriff auf das Internet. Diese Regel wird dem Bereich "Programmberechtigungen" hinzugefügt.
- **Zugriff einmal gewähren**: Gestattet einem Programm auf Ihrem Computer temporären Zugriff auf das Internet. Ein einmaliger Zugriff auf das Internet ist beispielsweise bei der Installation eines neuen Programms erforderlich.
- **Zugriff blockieren**: Verhindert, dass ein bestimmtes Programms auf das Internet zugreift.
- **Nur ausgehenden Zugriff gewähren**: Gestattet einem bestimmten Programm nur den Zugriff auf eine ausgehende Internetverbindung. Diese Warnung wird in der Regel nur dann angezeigt, wenn die Sicherheitsstufen "Eingeschränkt" und "Stealth" eingestellt sind.
- **Diesem Netzwerk vertrauen**: Gestattet eingehenden und ausgehenden Datenverkehr von einem Netzwerk. Das Netzwerk wird dem Bereich "Vertrauenswürdige IP-Adressen" hinzugefügt.
- **Diesem Netzwerk derzeit nicht vertrauen**: Blockiert eingehenden und ausgehenden Datenverkehr von einem Netzwerk.

Gelbe Warnung

Bei gelben Warnungen handelt es sich um nichtkritische Benachrichtigungen, die Sie über von Firewall erkannte Netzwerkereignisse informieren. Beispielsweise wird die Warnung **Neues Netzwerk gefunden** angezeigt, wenn Firewall das erste Mal ausgeführt wird oder wenn ein Computer, auf dem Firewall installiert ist, mit einem neuen Netzwerk verbunden wird. Sie können entscheiden, ob das Netzwerk vertrauenswürdig oder nicht vertrauenswürdig ist. Wenn das Netzwerk vertrauenswürdig ist, gestattet Firewall den Datenverkehr von anderen Computern in diesem Netzwerk, und das Netzwerk wird dem Bereich "Vertrauenswürdige IP-Adressen" hinzugefügt.

Grüne Warnung

In den meisten Fällen enthalten grüne Warnungen allgemeine Informationen zu einem Ereignis. Auf grüne Warnungen muss nicht reagiert werden. Grüne Warnungen treten in der Regel nur dann auf, wenn die Sicherheitsstufen "Standardsicherheit", "Eingeschränkte Sicherheit", "Stealth" und "Verbindung schließen" eingestellt sind. Die folgenden grünen Warnmeldungen sind möglich:

- **Das Programm wurde geändert**: Informiert Sie darüber, dass ein Programm, dem Sie zuvor den Zugriff auf das Internet gestattet hatten, verändert wurde. Sie können das Programm blockieren, wenn Sie jedoch nicht eingreifen, wird die Warnmeldung geschlossen und das Programm hat weiterhin Zugriff auf das Internet.
- **Programm kann auf das Internet zugreifen**: Informiert Sie darüber, dass einem Programm der Zugriff auf das Internet gewährt wurde. Sie können das Programm blockieren, wenn Sie jedoch nicht eingreifen, wird die Warnmeldung geschlossen und das Programm hat weiterhin Zugriff auf das Internet.

Benutzereingriff

Viele Firewall-Warnungen enthalten weiterführende Informationen, die Sie bei der Verwaltung der Sicherheit Ihres Computers unterstützen. Hierzu gehören die folgenden Meldungen:

- **Weitere Informationen über dieses Programm**: Startet die McAfee-Website zur globalen Sicherheit, auf der Sie Informationen zu einem Programm finden, das Firewall auf Ihrem Computer erkannt hat.
- **Informieren Sie McAfee über dieses Programm**: Senden Sie Informationen über eine unbekannte Datei, die Firewall auf Ihrem Computer erkannt hat, an McAfee.
- **McAfee-Empfehlung**: Empfehlungen zur Handhabung von Warnungen. Beispielsweise kann eine Warnung empfehlen, dass Sie einem Programm den Zugriff auf das Internet gewähren.

Informationswarnungen verwalten

Mit Firewall können Sie Informationswarnungen während bestimmter Ereignisse anzeigen oder ausblenden.

Warnungen während eines Spiels anzeigen

In der Standardeinstellung verhindert Firewall, dass Informationswarnungen angezeigt werden, während ein Spiel im Vollbild angezeigt wird. Sie können Firewall jedoch auch so konfigurieren, dass Informationswarnungen während eines Spiels angezeigt werden, wenn Firewall einen Intrusionsversuch oder eine verdächtige Aktivität feststellt.

So zeigen Sie Warnungen während eines Spiels an:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Aktivieren Sie im Bereich **Warnoptionen** die Option **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**.

Informationswarnungen verbergen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die Ihr unmittelbares Eingreifen nicht erforderlich machen.

So verbergen Sie Informationswarnungen:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Klicken Sie im Bereich **SecurityCenter-Konfiguration** auf die Option **Informationswarnungen**.
6. Führen Sie im Bereich **Informationswarnungen** einen der folgenden Schritte aus:
   - Wählen Sie den zu verbergenden Warnungstyp aus.
   - Wählen Sie **Informationswarnungen verbergen**, um alle Informationswarnungen zu verbergen.
7. Klicken Sie auf **OK**.

KAPITEL 19

Firewall-Schutz konfigurieren

Firewall bietet verschiedene Methoden zur Verwaltung Ihrer Sicherheit und zum Anpassen der Art und Weise, wie auf Sicherheitsereignisse und -warnungen reagiert werden soll.

Nach der Erstinstallation von Firewall wird die Schutzebene auf "Standardsicherheit" gesetzt. In der Regel erfüllt diese Einstellung alle Sicherheitsanforderungen. Dennoch bietet Ihnen Firewall auch andere Sicherheitsstufen an, die von "Verbindung schließen" (sehr restriktiv) bis "Offen" (sehr tolerant) reichen.

Darüber hinaus kann Firewall Empfehlungen bei Warnungen und dem Internetzugriff von Programmen anzeigen.

In diesem Kapitel

Firewall-Sicherheitsstufen verwalten

Sie können die Sicherheitsstufen Ihren Anforderungen entsprechend anpassen, so dass Sie beispielsweise nur dann eingreifen müssen, wenn Firewall unerwünschten Netzwerkdatenverkehr sowie eingehende und ausgehende Internetverbindungen erkannt. In der Standardeinstellung ist die Sicherheitsstufe "Standardsicherheit" aktiviert.

Wenn die Sicherheitsstufe "Standardsicherheit" eingestellt und die Option "Empfehlungen" aktiviert ist, können Sie bei roten Warnungen den Zugriff für unbekannte oder geänderte Programme gewähren oder blockieren. Bei bekannten Programmen werden grüne Informationsmeldungen angezeigt und der Zugriff wird automatisch gewährt. Durch das Gewähren des Zugriffs kann eine Anwendung ausgehende Verbindungen herstellen und auf unaufgeforderte eingehende Verbindungen hin überwachen.

Allgemein gilt, je restriktiver eine Sicherheitsstufe ("Stealth" und "Eingeschränkte Sicherheit"), desto größer ist die Anzahl an Optionen und Warnungen, die angezeigt werden und Ihr Eingreifen erforderlich machen.

Firewall bietet sechs Sicherheitsstufen. Beginnend mit der restriktiven zur tolerantesten lauten die Sicherheitsstufen wie folgt:

- **Verbindung schließen**: Blockiert alle Internetverbindungen.
- **Stealth**: Blockiert alle eingehenden Internetverbindungen.
- **Eingeschränkte Sicherheit**: Warnungen erfordern Ihr Eingreifen bei jeder eingehenden und ausgehenden Internetverbindungsanforderung.
- **Standardsicherheit**: Warnungen werden angezeigt, wenn unbekannte oder neue Programme den Internetzugriff anfordern.
- **Vertrauenswürdige Sicherheit**: Gewährt alle eingehenden und ausgehenden Netzwerkverbindungen und fügt diese automatisch dem Bereich "Programmberechtigungen" hinzu.
- **Offen**: Gewährt alle eingehenden und ausgehenden Internetverbindungen.

Im Firewall-Bereich "Standardwerte für Firewall-Schutz wiederherstellen" können Sie Ihre Sicherheitsstufe unmittelbar wieder auf "Standardsicherheit" zurücksetzen.

Die Sicherheitsstufe "Verbindung schließen"

Bei der Firewall-Sicherheitsstufe "Verbindung schließen" werden alle ein- und ausgehenden Netzwerkverbindungen blockiert. Dazu gehört auch der Zugriff auf Websites, E-Mails und Sicherheitsupdates. Diese Sicherheitsstufe hat die gleichen Auswirkungen wie das Trennen Ihrer Internetverbindung. Sie können diese Einstellung verwenden, um Ports zu blockieren, die im Bereich "Systemdienste" als geöffnet konfiguriert sind. Bei der Einstellung "Verbindung schließen" können weiterhin Warnungen angezeigt werden, in denen Sie aufgefordert werden, Programme zu sperren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Verbindung schließen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Verbindung schließen** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Stealth"

Bei der Firewall-Sicherheitsstufe "Stealth" werden alle eingehenden Netzwerkverbindungen mit Ausnahme der geöffneten Ports blockiert. Diese Einstellung verbirgt Ihren Computer vollständig gegenüber dem Internet. Bei der Firewall-Sicherheitsstufe "Stealth" werden Warnungen angezeigt, wenn neue Programme versuchen, auf das Internet zuzugreifen oder über eingehende Verbindungen Anfragen erhalten. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.

So setzen Sie die Firewall-Sicherheitsstufe auf "Stealth":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Stealth** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Eingeschränkte Sicherheit"

Bei der Firewall-Sicherheitsstufe "Eingeschränkte Sicherheit" werden Sie informiert, wenn neue Programme versuchen, auf das Internet zuzugreifen oder über eingehende Verbindungen Anfragen erhalten. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt. Bei der Firewall-Sicherheitsstufe "Eingeschränkte Sicherheit" fordert ein Programm nur den Zugriffstyp an, den es zum aktuellen Zeitpunkt benötigt. So wird beispielsweise der Zugriff auf eine ausgehende Internetverbindung angefordert, den Sie entweder gewähren oder blockieren können. Benötigt das Programm zu einem späteren Zeitpunkt sowohl eine eingehende als auch eine ausgehende Verbindung, können Sie den uneingeschränkten Zugriff für das Programm im Bereich "Programmberechtigungen" gewähren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Eingeschränkte Sicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Eingeschränkte Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Standardsicherheit"

Standardsicherheit ist die standardmäßige und empfohlene Sicherheitsstufe.

Bei der Firewall-Sicherheitsstufe "Standardsicherheit" überwacht Firewall eingehende und ausgehende Verbindungen und benachrichtigt Sie, wenn neue Programme versuchen, auf das Internet zuzugreifen. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.

So setzen Sie die Firewall-Sicherheitsstufe auf "Standardsicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Standardsicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Vertrauenswürdige Sicherheit"

Bei der Firewall-Sicherheitsstufe "Vertrauenswürdige Sicherheit" werden alle eingehenden und ausgehenden Verbindungen gestattet. In dieser Einstellung gewährt Firewall automatisch allen Programmen Zugriff und fügt sie der Liste der zugelassenen Programme im Bereich "Programmberechtigungen" hinzu.

So setzen Sie die Firewall-Sicherheitsstufe auf "Vertrauenswürdige Sicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Vertrauenswürdige Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Empfehlungen für Warnungen konfigurieren

Sie können Firewall so konfigurieren, dass Empfehlungen in die Warnungen zu Programmen, die auf das Internet zuzugreifen versuchen, aufgenommen, davon ausgeschlossen oder darin angezeigt werden.

Das Aktivieren der Option "Empfehlungen" unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen. Wenn die Option "Empfehlungen" aktiviert ist (und die Sicherheitsstufe "Standardsicherheit" lautet), gewährt oder blockiert Firewall bekannte Programme automatisch. Darüber hinaus werden Sie beim Erkennen von unbekannten und potentiell schädlichen Programmen benachrichtigt und erhalten Vorschläge zu den erforderlichen Maßnahmen.

Ist die Option "Empfehlungen" hingegen deaktiviert, wird Firewall weder automatisch Internetzugriff gewähren oder blockieren noch erforderliche Maßnahmen empfehlen.

Wurde Firewall so konfiguriert, dass Empfehlungen nur angezeigt werden, fordert Sie die Warnung zum Gewähren oder Blockieren des Zugriffs auf, zeigt aber auch eine empfohlene Maßnahme an.

Empfehlungen aktivieren

Das Aktivieren der Option "Empfehlungen" unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen. Wenn die Option "Empfehlungen" aktiviert ist, wird Firewall den Internetzugriff für Programme automatisch gewähren oder blockieren. Darüber hinaus werden Sie benachrichtigt, wenn unbekannte oder potentiell schädliche Programme erkannt werden.

So aktivieren Sie die Option "Empfehlungen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Aktivieren der Empfehlungen**.
3. Klicken Sie auf **OK**.

Empfehlungen deaktivieren

Wenn die Option "Empfehlungen" deaktiviert ist, enthalten die Warnungen keine Hinweise mehr zur Vorgehensweise bei Warnungen und zur Verwaltung des Zugriffs von Programmen. Ist die Option "Empfehlungen" deaktiviert, wird Firewall den Internetzugriff für Programme weiterhin gewähren oder blockieren. Darüber hinaus werden Warnungen angezeigt, wenn unbekannte oder potentiell schädliche Programme erkannt wurden. Erkennt Firewall dabei ein neues Programm, das verdächtig erscheint oder bei dem es sich um ein bekanntes schädliches Programm handelt, blockiert es automatisch den Zugriff dieses Programms auf das Internet.

So deaktivieren Sie die Option "Empfehlungen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Deaktivieren der Empfehlungen**.
3. Klicken Sie auf **OK**.

Nur Empfehlungen anzeigen

Das Anzeigen von Empfehlungen unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen zu unbekannten und potentiell schädlichen Programmen. Ist die Option "Empfehlungen" auf **Nur Anzeige** gesetzt, werden zwar Informationen zur Vorgehensweise bei Warnungen angezeigt, aber im Gegensatz zur Option **Aktivieren der Empfehlungen** werden die angezeigten Empfehlungen nicht automatisch angewendet, und der Internetzugriff von Programmen wird nicht automatisch gestattet oder blockiert. Stattdessen unterstützen die Warnungen mit Empfehlungen Sie bei Ihrer Entscheidung, ob der Internetzugriff für bestimmte Programme gewährt oder blockiert werden soll.

So aktivieren Sie die Option "Nur Empfehlungen anzeigen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Nur Anzeige**.
3. Klicken Sie auf **OK**.

Firewall-Sicherheit optimieren

Es gibt viele Möglichkeiten, wie die Sicherheit Ihres Computers gefährdet werden könnte. Beispielsweise können einige Programme versuchen, eine Verbindung mit dem Internet herzustellen, bevor Windows(R) hochgefahren ist. Technisch versierte Anwender können ein ICMP-Echo-Request-Paket an Ihren Computer senden (pingen), um festzustellen, ob er an ein Netzwerk angeschlossen ist. Mit Firewall können Sie sich durch das Aktivieren eines Boot-Schutzes und das Blockieren von ICMP-Echo-Request-Anforderungen gegen beide Arten des Eindringens schützen. Der erste Schutzmechanismus blockiert den Zugriff von Programmen auf das Internet beim Hochfahren von Windows. Der zweite Mechanismus blockiert ICMP-Echo-Request-Anforderungen, mit denen ein anderer Benutzer feststellen kann, ob Ihr Computer mit dem Internet verbunden ist.

Zu den standardmäßigen Installationseinstellungen gehören das automatische Erkennen der am häufigsten auftretenden Einbruchsversuche, z. B. Denial-of-Service-Attacken oder Bedrohungen. Das Verwenden der standardmäßigen Installationseinstellungen gewährleistet, dass Sie vor diesen Angriffen und Prüfungen geschützt sind. Im Fenster zur Eindringungserkennung ("Intrusion Detection") haben Sie jedoch die Möglichkeit, das automatisch Erkennen von Angriffen oder Prüfungen zu deaktivieren.

Computer während des Hochfahrens schützen

Firewall kann Ihren Computer während des Hochfahrens von Windows schützen. Der Boot-Schutz blockiert alle neuen Programme, denen der Zugriff auf das Internet noch nicht gewährt wurde und die Zugriff auf das Internet anfordern. Nach dem Start von Firewall werden die entsprechenden Warnungen für die Programme angezeigt, die während des Hochfahrens einen Internetzugriff angefordert hatten. Jetzt können Sie diesen Zugriff entweder gewähren oder blockieren. Für diese Option darf Ihre Sicherheitsstufe jedoch nicht auf "Offen" oder "Verbindung schließen" eingestellt sein.

So schützen Sie Ihren Computer während des Hochfahrens:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Aktivieren Sie im Bereich "Sicherheitsstufe" unter "Sicherheitseinstellungen" die Option **Boot-Schutz aktivieren**.
3. Klicken Sie auf **OK**.

Hinweis: So lange der Boot-Schutz ausgeführt wird, werden keine blockierten Verbindungen und Intrusionsversuche protokolliert.

Einstellungen für ICMP-Echo-Request-Anforderungen konfigurieren

Technisch versierte Computerbenutzer können ein Ping-Tool verwenden, das ICMP-Echo-Request-Anforderungen sendet und empfängt, um festzustellen, ob ein bestimmter Computer mit dem Internet verbunden ist. Sie können Firewall so konfigurieren, dass Computerbenutzern das Anpingen Ihres Computers gestattet oder verweigert wird.

So konfigurieren Sie die ICMP-Echo-Request-Anforderungen:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Führen Sie im Bereich "Sicherheitsstufe" unter **Sicherheitseinstellungen** einen der folgenden Schritte aus:
   - Aktivieren Sie **ICMP-Pinganforderungen zulassen**, um die Erkennung Ihres Computers im Netzwerk durch das Senden von ICMP-Echo-Request-Anforderungen zu gestatten.

- Deaktivieren Sie **ICMP-Pinganforderungen zulassen**, um die Erkennung Ihres Computers im Netzwerk durch das Senden von ICMP-Echo-Request-Anforderungen zu verhindern.

3 Klicken Sie auf **OK**.

Erkennung von Intrusionsversuchen konfigurieren

Die Intrusionserkennung (IDS) prüft Datenpakete auf verdächtige Datenübertragungen oder Übertragungsmethoden. IDS analysiert den Datenverkehr und die Datenpakete auf bestimmte Datenverkehrsmuster, die von Angreifern verwendet werden. Wenn Firewall beispielsweise ICMP-Pakete erkennt, prüft es sie auf verdächtige Verkehrsmuster, indem es den ICMP-Datenverkehr mit den Mustern bekannter Angriffe vergleicht. Die Pakete werden mit einer Signaturdatenbank verglichen und automatisch verworfen, wenn sie von dem verdächtigen Computer stammen. Das Ereignis kann optional protokolliert werden.

Zu den standardmäßigen Installationseinstellungen gehören das automatische Erkennen der am häufigsten auftretenden Einbruchsversuche, z. B. Denial-of-Service-Attacken oder Bedrohungen. Das Verwenden der standardmäßigen Installationseinstellungen gewährleistet, dass Sie vor diesen Angriffen und Prüfungen geschützt sind. Im Fenster zur Eindringungserkennung ("Intrusion Detection") haben Sie jedoch die Möglichkeit, das automatisch Erkennen von Angriffen oder Prüfungen zu deaktivieren.

So konfigurieren Sie die Erkennung von Intrusionsversuchen:

1 Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.

2 Klicken Sie im Bereich "Firewall" auf **Intrusionserkennung**.

3 Führen Sie unter **Intrusionsversuche erkennen** einen der folgenden Schritte aus:

- Wählen Sie einen Namen, um einen Angriff oder Scan-Versuch automatisch zu erkennen.
- Entfernen Sie einen Namen, um die automatische Erkennung eines Angriffs oder Scan-Versuchs zu deaktivieren.

4 Klicken Sie auf **OK**.

Statuseinstellungen für den Firewall-Schutz konfigurieren

SecurityCenter verfolgt Probleme, die ein Teil Ihres allgemeinen Computer-Schutzstatus darstellen. Sie können Firewall jedoch so konfigurieren, dass bestimmte Probleme auf Ihrem Computer, die den Schutzstatus beeinflussen könnten, ignoriert werden. Sie können SecurityCenter so konfigurieren, dass es eine Einstellung der Sicherheitsstufe von "Offen" ignoriert, wenn der Firewall-Dienst nicht ausgeführt wird und keine Firewall für ausgehenden Datenverkehr auf Ihrem Computer installiert ist.

So konfigurieren Sie die Statuseinstellungen für den Firewall-Schutz:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Klicken Sie im Bereich "Häufige Tasks" auf das Menü **Erweitert**.
6. Klicken Sie auf **Konfigurieren**.
7. Klicken Sie im Bereich "SecurityCenter-Konfiguration" auf die Option **Schutzstatus**.
8. Klicken Sie auf "Erweitert".
9. Wählen Sie im Bereich "Ignorierte Probleme" eine oder mehrere der folgenden Optionen:
   - **Die Firewall ist auf die Sicherheitsstufe "Offen" eingestellt.**
   - **Der Firewall-Dienst wird nicht ausgeführt.**
   - **Auf Ihrem Computer ist keine Firewall für ausgehenden Datenverkehr vorhanden.**
10. Klicken Sie auf **OK**.

Firewall sperren und wiederherstellen

Das Sperren der Firewall ist bei folgenden Situationen hilfreich: bei der Bearbeitung von computerbezogenen Notfällen; für Benutzer, die den gesamten Verkehr sperren müssen, um ein Problem auf ihrem Computer zu isolieren und zu beheben; oder für Benutzer, die unsicher sind und entscheiden müssen, wie der Zugriff eines Programms auf das Internet gehandhabt werden soll.

Firewall sofort sperren

Durch das Sperren der Firewall wird der gesamte eingehende und ausgehende Datenverkehr zwischen Ihrem Computer und dem Internet sofort blockiert. Allen Remote-Verbindungen wird der Zugriff auf Ihren Computer verweigert, und alle Programme auf Ihrem Computer können nicht mehr auf das Internet zugreifen.

So sperren Sie die Firewall sofort und blockieren den gesamten Internetdatenverkehr:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Firewall sperren**.
2. Klicken Sie im Bereich "Firewall sperren" auf **Schließen**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das sofortige Sperren des gesamten eingehenden und ausgehenden Datenverkehrs zu bestätigen.

Firewall-Sperre sofort aufheben

Durch das Sperren der Firewall wird der gesamte eingehende und ausgehende Datenverkehr zwischen Ihrem Computer und dem Internet sofort blockiert. Allen Remote-Verbindungen wird der Zugriff auf Ihren Computer verweigert, und alle Programme auf Ihrem Computer können nicht mehr auf das Internet zugreifen. Nachdem Sie den Befehl "Firewall sperren" gewählt haben, können Sie die Sperre wieder aufheben, um den Internetdatenverkehr wieder zuzulassen.

So heben Sie die Firewall-Sperre sofort auf und gestatten den gesamten Internetdatenverkehr:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Firewall sperren**.
2. Klicken Sie im Bereich "Sperrung aktiviert" auf **Sperre aufheben**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das sofortige Aufheben der Sperre des gesamten eingehenden und ausgehenden Datenverkehrs zu bestätigen.

Firewall-Standardeinstellungen wiederherstellen

Sie können die Standard-Sicherheitseinstellungen der Firewall schnell und einfach wiederherstellen. Dabei wird Ihre Sicherheitsstufe auf "Standardsicherheit" gesetzt, die Option "Empfehlungen" wird aktiviert, vertrauenswürdige und gesperrte IP-Adressen werden zurückgesetzt, und es werden alle Programme aus dem Fensterbereich "Programmberechtigungen" entfernt.

So stellen Sie die Standardeinstellungen der Firewall wieder her:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Standardwerte für Firewall wiederherstellen**.
2. Klicken Sie im Bereich "Standardwerte für Firewall-Schutz wiederherstellen" auf **Standardeinstellungen wiederherstellen**.
3. Klicken Sie im Dialogfeld "Standardwerte für Firewall-Schutz wiederherstellen" auf **Ja**, um das Wiederherstellen der Firewall-Standardeinstellungen zu bestätigen.

Die Sicherheitsstufe "Offen"

Bei der Sicherheitsstufe "Offen" gestattet die Firewall den Zugriff auf alle eingehenden und ausgehenden Verbindungen. In dem Bereich "Programmberechtigungen" können Sie den Zugriff auch für zuvor blockierte Programme gewähren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Offen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Offen** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Hinweis: Wenn die Firewall-Sicherheitsstufe auf **Offen** eingestellt ist, werden zuvor blockierte Programme auch weiterhin blockiert. Sie können dies durch Ändern der Programmregel auf **Vollzugriff** verhindern.

KAPITEL 20

Programme und Berechtigungen verwalten

Mit Firewall können Sie Zugriffsberechtigungen für bereits vorhandene und neue Programme, die Zugriff auf eingehende und ausgehende Internetverbindungen benötigen, verwalten und erstellen. Sie können Programmen den vollständigen Zugriff oder nur den Zugriff auf ausgehende Verbindungen gewähren. Alternativ können Sie Programmen den Zugriff auf Internetverbindungen dauerhaft blockieren.

In diesem Kapitel

Internetzugriff für Programme gewähren

Einige Programme, wie z. B. Internetbrowser, müssen auf das Internet zugreifen können, um ihre eigentliche Funktion ausführen zu können.

Dazu können Sie im Bereich "Programmberechtigungen" von Firewall die folgenden Einstellungen vornehmen:

- Programmen den Zugriff auf Internetverbindungen gewähren
- Programmen den Zugriff nur auf ausgehende Verbindungen gewähren
- Programmen den Zugriff auf Internetverbindungen sperren

Die Zugriffsarten "Vollständig" und "Nur ausgehender Zugriff" können Sie auch aus den Protokollen "Ausgehende Ereignisse" und "Zuletzt aufgetretene Ereignisse" gewähren.

Uneingeschränkten Zugriff für ein Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

So gewähren Sie einem Programm den uneingeschränkten Internetzugriff:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Nur ausgehender Zugriff** aus.
4. Klicken Sie unter **Aktion** auf **Vollständigen Zugriff gewähren**.
5. Klicken Sie auf **OK**.

Vollständigen Zugriff für ein neues Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Dieser Liste können Sie ein neues Programm hinzufügen und die Berechtigungen konfigurieren.

So gewähren Sie einem neuen Programm den uneingeschränkten Internetzugriff:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "**Firewall** " auf **Programmberechtigungen**.
3. Klicken Sie unter **Programmberechtigungen** auf **Erlaubtes Programm hinzufügen**.
4. Wählen Sie im Dialogfeld **Programm hinzufügen** das Programm aus, das Sie hinzufügen möchten.
5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **OK**.

   Das neu hinzugefügte Programm wird jetzt im Bereich **Programmberechtigungen** angezeigt.

Hinweis: Sie können die Berechtigungen eines neu hinzugefügten Programms auf die gleiche Weise wie die eines bereits vorhandenen Programms ändern. Dazu wählen Sie das Programm aus und klicken dann unter **Aktion** auf **Nur ausgehenden Zugriff gewähren** oder **Zugriff blockieren**.

Uneingeschränkten Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Zuletzt aufgetretene Ereignisse" auswählen und den Status "Vollständig" zuweisen.

So gewähren Sie einem Programm uneingeschränkten Zugriff über das Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus, und klicken Sie dann auf **Uneingeschränkten Zugriff gewähren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den vollständigen Internetzugriff des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

Uneingeschränkten Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Ausgehende Ereignisse" auswählen und ihm den Status "Vollständig" zuweisen.

So gewähren Sie einem Programm uneingeschränkten Zugriff über das Protokoll "Ausgehende Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus, und klicken Sie dann auf **Zugriff gewähren**.
5. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den vollständigen Internetzugriff des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

Programmen nur den Zugriff auf ausgehende Verbindungen gewähren

Viele Programme auf Ihrem Computer benötigen nur Zugriff auf ausgehende Internetverbindungen. Sie können diesen Programmen nur den Zugriff auf ausgehende Verbindungen gewähren.

Zugriff auf ausgehende Verbindungen für ein Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

So gewähren Sie einem Programm nur Zugriff auf ausgehenden Verkehr:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Vollständig** aus.
4. Klicken Sie unter **Aktion** auf **Nur ausgehenden Zugriff gewähren**.
5. Klicken Sie auf **OK**.

Nur ausgehenden Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Zuletzt aufgetretene Ereignisse" auswählen und den Status "Nur ausgehenden Zugriff" zuweisen.

So gewähren Sie einem Programm nur ausgehenden Zugriff über das Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus, und klicken Sie dann auf **Nur ausgehenden Zugriff gewähren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den Zugriff nur auf ausgehende Internetverbindungen des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

Nur ausgehenden Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Ausgehende Ereignisse" auswählen und ihm den Status "Nur ausgehenden Zugriff" zuweisen.

So gewähren Sie einem Programm nur ausgehenden Zugriff über das Protokoll "Ausgehende Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse und klicken Sie dann auf **Nur ausgehenden Zugriff gewähren**.
5. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den Zugriff nur auf ausgehende Internetverbindungen des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

Internetzugriff für Programme blockieren

Sie können bestimmten Programmen den Zugriff auf das Internet sperren. Durch das Blockieren des Internetzugriffs für ein Programm stellen Sie sicher, dass Ihre Netzwerkverbindung oder ein anderes Programm, das eine Internetverbindung für die ordnungsgemäße Funktion benötigt, nicht unterbrochen wird.

Zugriff für ein Programm sperren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können von Ihnen gesperrt werden.

So sperren Sie den Internetzugriff für ein Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Vollzugriff** oder **Nur ausgehender Zugriff** aus.
4. Klicken Sie unter **Aktion** auf **Zugriff blockieren**.
5. Klicken Sie auf **OK**.

Zugriff für ein neues Programm sperren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der Zugriff automatisch gesperrt wird. Dieser Liste können Sie ein neues Programm hinzufügen und den Zugriff auf das Internet sperren.

So sperren Sie den Internetzugriff für ein neues Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Klicken Sie unter **Programmberechtigungen** auf **Blockiertes Programm hinzufügen**.
4. Wählen Sie im Dialogfeld **Programm hinzufügen** das Programm aus, das Sie hinzufügen möchten.
5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **OK**.

   Das neu hinzugefügte Programm wird jetzt im Bereich **Programmberechtigungen** angezeigt.

Hinweis: Sie können die Berechtigungen eines neu hinzugefügten Programms auf die gleiche Weise wie die eines bereits vorhandenen Programms ändern. Dazu wählen Sie das Programm aus und klicken dann unter **Aktion** auf **Nur ausgehenden Zugriff gewähren** oder **Vollständigen Zugriff gewähren**.

Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" blockieren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Jedoch können Sie Programmen den Zugriff auf das Internet aus dem Protokoll "Zuletzt aufgetretene Ereignisse" sperren.

So sperren Sie den Internetzugriff eines Programms aus dem Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus und klicken Sie dann auf **Zugriff blockieren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um das Sperren des Internetzugriffs für ein Programm zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

Zugriffsberechtigungen für Programme entfernen

Bevor Sie eine Programmberechtigung eines Programms entfernen, müssen Sie überprüfen, ob das Sperren des Internetzugriffs für dieses Programm negative Auswirkungen auf die Funktionen des Computers oder des Netzwerks hat.

Programmberechtigung entfernen

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Sie können automatisch oder manuell hinzugefügte Programme jedoch auch wieder aus dieser Liste entfernen.

So entfernen Sie die Programmberechtigung für ein neues Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
4. Klicken Sie unter **Aktion** auf **Programmberechtigung löschen**.
5. Klicken Sie auf **OK**.

   Das Programm wird aus dem Bereich "Programmberechtigungen" Liste entfernt.

Hinweis: Durch Abblenden und Deaktivieren von Aktionen verhindert Firewall, dass Sie die Berechtigung von bestimmten Programmen ändern.

Weitere Informationen zu Programmen abrufen

Wenn Sie nicht sicher sind, welche Programmberechtigung für ein bestimmtes Programm gelten soll, können Sie entsprechende Informationen zu diesem Programm auf McAfees Hackerwatch-Website nachlesen.

Programminformationen erhalten

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

Firewall kann Ihnen bei Ihrer Entscheidung helfen, ob Sie einem Programm den Internetzugriff gewähren oder sperren sollen. Stellen Sie sicher, dass Sie eine Verbindung mit dem Internet hergestellt haben, so dass Ihr Browser die Hackerwatch-Website von McAfee aufrufen kann. Auf dieser Website finden Sie aktuelle Informationen zu Programmen, den Anforderungen an den Internetzugriff sowie bekannte Sicherheitsrisiken.

So erhalten Sie Programminformationen:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
4. Klicken Sie unter **Aktion** auf **Weitere Informationen**.

Weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" abrufen

Mit Personal Firewall können Sie weitere Informationen zu Programmen abrufen, die in dem Protokoll "Ausgehende Ereignisse" aufgeführt sind.

Bevor Sie Informationen zu einem Programm abrufen, stellen Sie sicher, dass eine Internetverbindung besteht und Sie über einen Internetbrowser verfügen.

So rufen Sie weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" ab:

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Weitere Informationen**.

   Sie können weitere Informationen zu einem gewünschten Programm auf der Hackerwatch-Website anzeigen. Hackerwatch bietet Ihnen aktuelle Informationen zu Programmen, deren Anforderungen an den Internetzugriff sowie bekannte Sicherheitsrisiken.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 181)

KAPITEL 21

Systemdienste verwalten

Einige Programme, beispielsweise Webserver oder Serverprogrammen für die Dateifreigabe, müssen für eine ordnungsgemäße Funktion nicht angeforderte Verbindungen von anderen Computern akzeptieren, die über bestimmte Systemdienstports eingehen. In der Regel schließt Firewall diese Systemdienstports, da sie eine mögliche Quelle für Sicherheitsrisiken in Ihrem System darstellen. Diese Systemdienstports müssen jedoch offen sein, damit Verbindungen von Remote-Computern akzeptiert werden können.

Die folgende Liste enthält die Standardports für allgemeine Dienste.

- File Transfer Protocol (FTP) Ports 20-21
- Mail Server (IMAP) Port 143
- Mail Server (POP3) Port 110
- Mail Server (SMTP) Port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server (MSFT SQL) Port 1433
- Remoteunterstützung / Terminalserver (RDP) Port 3389
- Remoteprozeduraufrufe (RPC) Port 135
- Secure Web Server (HTTPS) Port 443
- Universal Plug and Play (UPNP) Port 5000
- Web Server (HTTP) Port 80
- Windows-Dateifreigabe (NETBIOS) Ports 137-139

In diesem Kapitel

Systemdienstports konfigurieren

Damit ein Remotezugriff auf einen Dienst auf Ihrem Computer zustande kommen kann, müssen Sie den Dienst angeben und den zugehörigen Port als offen deklarieren. Wählen Sie einen Dienst und einen Port nur dann aus, wenn Sie sich sicher sind, dass der Port offen sein muss. Es ist nur selten notwenig, dass Sie einen Port öffnen.

Zugriff auf einen vorhandenen Systemdienstport gewähren

Im Fenster "Systemdienste" können Sie einen Anschluss öffnen oder schließen, um den Remote-Zugriff auf einen Netzwerkdienst auf Ihrem Computer zuzulassen oder abzulehnen. Ein offener Systemdienstanschluss kann für Ihren Computer ein Sicherheitsrisiko gegen Bedrohungen aus dem Internet darstellen. Öffnen Sie einen Anschluss daher nur, wenn dies erforderlich ist.

So gewähren Sie den Zugriff auf einen vorhandenen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie unter **Offener Systemdienstport** einen Systemdienst aus, um einen zugehörigen Port zu öffnen.
4. Klicken Sie auf **OK**.

Zugriff auf einen vorhandenen Systemdienstport sperren

Im Fenster "Systemdienste" können Sie einen Anschluss öffnen oder schließen, um den Remote-Zugriff auf einen Netzwerkdienst auf Ihrem Computer zuzulassen oder abzulehnen. Ein offener Systemdienstanschluss kann für Ihren Computer ein Sicherheitsrisiko gegen Bedrohungen aus dem Internet darstellen. Öffnen Sie einen Anschluss daher nur, wenn dies erforderlich ist.

So sperren Sie den Zugriff auf einen vorhandenen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie unter **Offener Systemdienstport** einen Systemdienst aus, um einen zugehörigen Port zu schließen.
4. Klicken Sie auf **OK**.

Neuen Systemdienstport konfigurieren

Im Bereich "Systemdienste" können Sie einen neuen Systemdienstport hinzufügen, den Sie dann öffnen oder schließen können, um den Remotezugriff auf einen Netzwerkdienst auf Ihrem Computer zu gestatten oder zu verweigern. Offene Systemdienstports stellen ein Sicherheitsrisiko für Ihren Computer gegenüber Bedrohungen aus dem Internet dar, daher sollten Sie einen Port nur dann öffnen, wenn es unbedingt notwendig ist.

So erstellen und konfigurieren Sie einen neuen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie unter **Portkonfiguration hinzufügen** Folgendes an:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
5. Geben Sie optional eine Beschreibung für die neue Konfiguration ein.
6. Klicken Sie auf **OK**.

   Der neu konfigurierte Systemdienstport wird unter **Offener Systemdienstport** angezeigt.

Systemdienstport bearbeiten

Ein offener bzw. geschlossener Port gestattet bzw. verweigert den Zugriff auf einen Netzwerkdienst auf Ihrem Computer. Im Bereich "Systemdienste" können Sie die Informationen für eingehende und ausgehende Verbindungen eines vorhandenen Portes bearbeiten. Wenn die Portinformationen falsch eingegeben werden, kann der Systemdienst nicht ordnungsgemäß arbeiten.

So bearbeiten Sie einen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie einen Systemdienst aus und klicken Sie dann auf **Bearbeiten**.
4. Geben Sie unter **Portkonfiguration hinzufügen** Folgendes an:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
5. Geben Sie optional eine Beschreibung für die geänderte Konfiguration ein.
6. Klicken Sie auf **OK**.

   Der geänderte Systemdienstport wird unter **Offener Systemdienstport** angezeigt.

Systemdienstport entfernen

Ein offener bzw. geschlossener Port gestattet oder verweigert den Zugriff auf einen Netzwerkdienst auf Ihrem Computer. Im Bereich "Systemdienste" können Sie einen vorhandenen Port und den dazugehörigen Systemdienst entfernen. Wenn ein Port und der dazugehörigen Systemdienst aus dem Bereich "Systemdienste" entfernt wurden, können Remote-Computer nicht mehr auf einen Netzwerkdienst auf Ihrem Computer zugreifen.

So entfernen Sie einen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie einen Systemdienst aus und klicken Sie dann auf **Entfernen**.
4. Klicken Sie im Dialogfeld **Programmberechtigungen** auf**Ja**, um das Löschen des Systemdienstes zu bestätigen.

   Der Systemdienstport wird nicht mehr im Bereich "Systemdienste" angezeigt.

KAPITEL 22

Computerverbindungen verwalten

Sie können Firewall so konfigurieren, dass bestimmte Remote-Verbindungen mit Ihrem Computer über Richtlinien verwaltet werden, die auf den IP-Adressen basieren, die diesen Remote-Computern zugeordnet sind. Computer, denen vertrauenswürdige IP-Adressen zugeordnet sind, dürfen eine Verbindung mit Ihrem Computer herstellen. Computer, deren IP-Adressen unbekannt, verdächtig oder nicht vertrauenswürdig sind, kann das Herstellen einer Verbindung mit Ihrem Computer verweigert werden.

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der Computer, den Sie als vertrauenswürdig einstufen, sicher ist. Wenn ein Computer, den Sie als vertrauenswürdig einstufen, durch einen Wurm oder auf andere Weise infiziert wird, besteht für Ihren Computer möglicherweise ebenfalls ein Risiko. McAfee empfiehlt zudem, dass der bzw. die Computer, die Sie als vertrauenswürdig einstufen, durch eine Firewall und ein aktuelles Antivirusprogramm zu schützen. Für alle IP-Adressen, die in der Liste der vertrauenswürdigen IP-Adressen enthalten sind, protokolliert Firewall weder den Datenverkehr noch generiert es Ereigniswarnungen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

In diesem Kapitel

Vertrauenswürdige Computerverbindungen

Sie können vertrauenswürdige IP-Adressen im Bereich "Vertrauenswürdige und gesperrte IPs" unter **Vertrauenswürdige IP-Adressen** hinzufügen, bearbeiten und entfernen.

In der Liste **Vertrauenswürdige IP-Adressen** im Fenster "Vertrauenswürdige und gesperrte IP-Adressen". Für IP-Adressen, die in der Liste **Vertrauenswürdige IP-Adressen** angezeigt werden, protokolliert Firewall weder Verkehr noch generiert es Ereigniswarnungen.

Firewall vertraut allen geprüften IP-Adressen in der Liste und gewährt den Datenverkehr, der von diesen IP-Adressen stammt, über jeden Port. Firewall protokolliert keine Ereignisse von vertrauenswürdigen IP-Adressen. Aktivitäten zwischen Computern, denen eine vertrauenswürdige IP Adresse zugeordnet ist und Ihrem Computer werden von Firewall weder gefiltert noch analysiert.

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der Computer, den Sie als vertrauenswürdig einstufen, sicher ist. Wenn ein Computer, den Sie als vertrauenswürdig einstufen, durch einen Wurm oder auf andere Weise infiziert wird, besteht für Ihren Computer möglicherweise ebenfalls ein Risiko. McAfee empfiehlt zudem, dass der bzw. die Computer, die Sie als vertrauenswürdig einstufen, durch eine Firewall und ein aktuelles Antivirusprogramm zu schützen.

Vertrauenswürdige Computerverbindung hinzufügen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse hinzufügen.

In der Liste **Vertrauenswürdige IP-Adressen** im Fenster "Vertrauenswürdige und gesperrte IP-Adressen". Für IP-Adressen, die in der Liste **Vertrauenswürdige IP-Adressen** angezeigt werden, protokolliert Firewall weder Verkehr noch generiert es Ereigniswarnungen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So fügen Sie eine vertrauenswürdige Computerverbindung hinzu:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Klicken Sie auf **Hinzufügen**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld "Regel für vertrauenswürdige IP-Adresse hinzufügen" auf **Ja**, um die vertrauenswürdige Computerverbindung zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzufügen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Eingehende Ereignisse" hinzufügen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So fügen Sie einen vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzu:

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse als vertrauenswürdig einstufen**.
5. Klicken Sie im Dialogfeld "Regel für vertrauenswürdige IP-Adresse hinzufügen" auf **Ja**, um die vertrauenswürdige IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 178)

Vertrauenswürdige Computerverbindung bearbeiten

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse bearbeiten.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So bearbeiten Sie eine vertrauenswürdige Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.

   Die bearbeitete IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Vertrauenswürdige Computerverbindung entfernen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse entfernen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So entfernen Sie eine vertrauenswürdige Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** auf **Ja**, um das Entfernen der vertrauenswürdigen IP-Adresse unter **Vertrauenswürdige IP-Adressen** zu bestätigen.

Sperren von Computerverbindungen

Sie können vertrauenswürdige IP-Adressen im Bereich "Vertrauenswürdige und gesperrte IPs" unter **Gesperrte IP-Adressen** hinzufügen, bearbeiten und entfernen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

Gesperrte Computerverbindung hinzufügen

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse hinzufügen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So fügen Sie eine gesperrte Computerverbindung hinzu:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Klicken Sie auf **Hinzufügen**.
5. Führen Sie unter "Regel für vertrauenswürdige IP-Adresse" einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Hinzufügen der gesperrten Computerverbindung zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Gesperrte Computerverbindung bearbeiten

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse bearbeiten.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So bearbeiten Sie eine gesperrte Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.

   Klicken Sie auf **OK**. Die bearbeitete IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Gesperrte Computerverbindung entfernen

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse entfernen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So entfernen Sie eine gesperrte Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Wählen Sie eine IP-Adresse aus und klicken Sie auf **Entfernen**.
5. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** auf **Ja**, um das Entfernen der vertrauenswürdigen IP-Adresse aus **Gesperrte IP-Adressen** zu bestätigen.

Computer aus dem Protokoll "Eingehende Ereignisse" sperren

Sie können eine Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Eingehende Ereignisse" sperren.

IP-Adressen, die in dem Protokoll "Eingehende Ereignisse" aufgeführt sind, sind gesperrt. Folglich stellt das Sperren einer Adresse keinen zusätzlichen Schutz dar, es sei denn, der Computer verfügt über absichtlich geöffnete Ports oder auf Ihrem Computer befindet sich eine Anwendung, der der Zugriff auf eingehende Internetverbindungen gewährt wurde.

Fügen Sie der Liste **Gesperrte IP-Adressen** nur dann eine IP-Adresse hinzu, wenn Sie über mindestens einen absichtlich geöffneten Port verfügen und Sie Grund zu der Annahme haben, dass der Zugriff auf offene Ports von dieser Adresse unterbunden werden muss.

Sie können die Seite "Eingehende 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 darstellt.

So sperren Sie eine vertrauenswürdige Computerverbindung aus dem Protokoll "Eingehende Ereignisse":

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Eingehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse sperren**.
5. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Sperren dieser IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 178)

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" sperren

Sie können eine Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Intrusion Detection-Ereignisse" sperren.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So sperren Sie einen Computer aus dem Protokoll "Intrusion Detection-Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Intrusion Detection-Ereignisse**.
4. Wählen Sie im Bereich "Intrusion Detection-Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse sperren**.
5. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Sperren dieser IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 178)

KAPITEL 23

Protokollierung, Überwachung und Analyse

Firewall bietet umfangreiche und leicht lesbare Protokollierung, Überwachung und Analyse für Internetereignisse und Datenverkehr. Kenntnisse des Internetdatenverkehrs und der -ereignisse helfen Ihnen bei der Verwaltung Ihrer Internetverbindungen.

In diesem Kapitel

Ereignisprotokollierung

Mit Firewall können Sie festlegen, ob die Protokollierung aktiviert oder deaktiviert werden soll und welche Ereignistypen protokolliert werden sollen. Mit der Ereignisprotokollierung können Sie vor kurzem aufgetretene eingehende und ausgehende Ereignisse anzeigen. Darüber hinaus können Sie erkannte Intrusionsversuche anzeigen.

Ereignisprotokolleinstellungen konfigurieren

Zur Verfolgung von Firewall-Ereignissen und -Aktivitäten können Sie die anzuzeigenden Ereignistypen festlegen und konfigurieren.

So konfigurieren Sie die Ereignisprotokollierung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Ereignisprotokolleinstellungen**.
3. Führen Sie im Bereich "Ereignisprotokolleinstellungen" einen der folgenden Schritte aus:
   - Wählen Sie **Ereignis protokollieren**, um die Ereignisprotokollierung zu aktivieren.
   - Wählen Sie **Ereignis nicht protokollieren**, um die Ereignisprotokollierung zu deaktivieren.
4. Geben Sie unter **Ereignisprotokolleinstellungen** die zu protokollierenden Ereignistypen an. Die folgenden Typen werden unterstützt:
   - ICMP-Ping-Signale
   - Datenverkehr von gesperrten IP-Adressen
   - Ereignisse an Systemdienstports
   - Ereignisse an unbekannten Ports
   - Ereignisse der Intrusionserkennung (IDS)
5. Wenn Sie die Protokollierung an bestimmten Ports verhindern möchten, wählen Sie **Keine Ereignisse an folgenden Ports protokollieren:** und geben dann die einzelnen Portnummern durch Kommata getrennt bzw. Portbereiche mit Bindestrichen ein. Beispiel: `137-139, 445, 400-5000`.
6. Klicken Sie auf **OK**.

Zuletzt aufgetretene Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die zuletzt aufgetretenen Ereignisse anzeigen. Der Bereich "Zuletzt aufgetretene Ereignisse" zeigt das Datum und eine Beschreibung des Ereignisses an. Der Bereich "Zuletzt aufgetretene Ereignisse" zeigt nur Aktivitäten von Programmen an, deren Zugriff auf das Internet explizit blockiert wurde.

So zeigen Sie die zuletzt aufgetretenen Ereignisse der Firewall an:

- Klicken Sie im Menü **Erweitert** im Bereich "Häufige Tasks" auf **Berichte &Protokolle** oder **Aktuelle Ereignisse anzeigen**. Alternativ können Sie auch auf **Aktuelle Ereignisse anzeigen** im Bereich "Häufige Tasks" des Menüs "Grundlagen" klicken.

Eingehende Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die eingehenden Ereignisse anzeigen und sortieren.

Das Protokoll "Eingehende Ereignisse" enthält die folgenden Protokollkategorien:

- Datum und Uhrzeit
- Quell-IP-Adresse
- Hostname
- Informationen und Ereignistyp

So zeigen Sie die eingehenden Ereignisse der Firewall an:

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.

Hinweis: Sie können eine IP-Adresse aus dem Protokoll "Eingehende Ereignisse" für vertrauenswürdig erklären, sperren und verfolgen.

Verwandte Themen

- Vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzufügen (Seite 168)
- Computer aus dem Protokoll "Eingehende Ereignisse" sperren (Seite 175)
- Computer aus dem Protokoll "Eingehende Ereignisse" verfolgen (Seite 186)

Ausgehende Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die ausgehenden Ereignisse anzeigen. Ausgehende Ereignisse enthalten den Namen des Programms, das einen Zugriff auf eine ausgehende Internetverbindung versucht hat, das Datum und die Uhrzeit des Ereignisses sowie den Speicherort des Programms auf Ihrem Computer.

So zeigen Sie die ausgehenden Ereignisse an:

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.

Hinweis: Die Zugriffsarten "Vollständig" und "Nur ausgehender Zugriff" für ein Programm können Sie auch aus dem Protokoll "Ausgehende Ereignisse" gewähren. Darüber hinaus können Sie weitere Informationen über ein Programm anzeigen.

Verwandte Themen

- Uneingeschränkten Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren (Seite 149)
- Nur ausgehenden Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren (Seite 152)
- Weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" abrufen (Seite 158)

Intrusion Detection-Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die Ereignisse der Intrusionserkennung anzeigen. Intrusion Detection-Ereignisse enthalten das Datum und die Uhrzeit des Ereignisses, die Quell-IP-Adresse und den Hostnamen des Ereignisses. Darüber hinaus beschreibt das Protokoll auch den Ereignistyp.

So zeigen Sie die Intrusion Detection-Ereignisse an:

1. Klicken Sie im Bereich "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und klicken Sie dann auf **Intrusion Detection-Ereignisse**.

Hinweis: Sie können eine IP-Adresse aus dem Protokoll "Intrusion Detection-Ereignisse" für vertrauenswürdig erklären, sperren und verfolgen.

Verwandte Themen

- Computer aus dem Protokoll "Intrusion Detection-Ereignisse" sperren (Seite 176)
- Computer aus dem Protokoll "Intrusion Detection-Ereignisse" verfolgen (Seite 187)

Mit der Statistik arbeiten

Die Firewall nutzt die Informationen auf McAfees Hackerwatch-Sicherheitswebsite, um Sie mit Statistiken zu globalen Internet Security-Ereignissen und zur Portaktivität zu versorgen.

Statistiken zu den globalen Sicherheitsereignissen anzeigen

Hackerwatch verfolgt Internet Security-Ereignisse auf der ganzen Welt, die Sie dann im SecurityCenter anzeigen können. Die Informationen umfassen verfolgte Vorfälle, die Hackerwatch während den letzten 24 Stunden, 7 Tagen und 30 Tagen gemeldet wurden.

So zeigen Sie Statistiken zu den globalen Sicherheitsereignissen an:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Zeigen Sie die Statistiken zu den Sicherheitsereignissen unter **Ereignisverfolgung** an.

Globale Portaktivität anzeigen

Hackerwatch verfolgt Internet Security-Ereignisse auf der ganzen Welt, die Sie dann im SecurityCenter anzeigen können. Die angezeigten Informationen umfassen die wichtigsten Ports, die Hackerwatch während der letzten sieben Tage gemeldet wurden. In der Regel werden hier HTTP-, TCP-, und UDP-Portinformationen angezeigt.

So zeigen Sie die weltweite Portaktivität an:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Zeigen Sie die wichtigsten Ports unter **Recent Port Activity** an.

Internetverkehr verfolgen

Die Firewall bietet Ihnen verschiedene Optionen zur Verfolgung des Internet-Datenverkehrs. Mit diesen Optionen können Sie einen Netzwerkcomputer geografisch (auf einer Weltkarte) verfolgen, Domänen- und Netzwerkinformationen erhalten und Computer aus den Protokollen "Eingehende Ereignisse" und "Intrusion Detection-Ereignisse" verfolgen.

So verfolgen Sie einen Netzwerkcomputer geografisch:

Mit Visual Tracer können Sie einen Computer, der eine Verbindung mit Ihrem Computer hergestellt hat oder herzustellen versucht, anhand seines Namens oder seiner IP-Adresse geografisch lokalisieren. Darüber hinaus können Sie mit Visual Tracer auch Informationen zum Netzwerk und den Registrierungsinformationen erhalten. Nach dem Aufrufen von Visual Tracer wird eine Weltkarte mit der wahrscheinlichsten Datenroute zwischen dem Quellcomputer und Ihrem Computer angezeigt.

So lokalisieren Sie einen Computer geografisch:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Kartenansicht**.

Hinweis: Private, ungültige oder Looped-IP-Adressen können Sie nicht verfolgen.

Registrierungsinformationen eines Computers erhalten

Mithilfe von Visual Tracer können Sie die Registrierungsinformationen eines Computers von SecurityCenter erhalten. Die Registrierungsinformationen enthalten den Namen der Domäne, den Namen des Registranten mit Adresse sowie administrative Kontaktinformationen.

So erhalten Sie Informationen zur Domäne eines Computers:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Registrant-Ansicht**.

Netzwerkinformationen eines Computers erhalten

Mithilfe von Visual Tracer können Sie die Netzwerkinformationen eines Computers von SecurityCenter erhalten. Die Netzwerkinformationen enthalten Details über das Netzwerk, in dem sich die Domäne befindet.

So erhalten Sie die Netzwerkinformationen eines Computers:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Netzwerkansicht**.

Computer aus dem Protokoll "Eingehende Ereignisse" verfolgen

In dem Bereich "Eingehende Ereignisse" können Sie eine IP-Adresse verfolgen, die im Protokoll "Eingehende Ereignisse" aufgeführt wird.

So verfolgen Sie die IP-Adresse eines Computers aus dem Protokoll "Eingehende Ereignisse":

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Eingehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse verfolgen**.
5. Wählen Sie im Bereich "Visual Tracer" eine der folgenden Optionen aus:
   - **Kartenansicht**: Lokalisieren Sie einen Computer geografisch anhand der ausgewählten IP-Adresse.
   - **Registrant-Ansicht**: Lokalisieren Sie die Domäneninformationen anhand der ausgewählten IP-Adresse.
   - **Netzwerkansicht**: Lokalisieren Sie die Netzwerkinformationen anhand der ausgewählten IP-Adresse.
6. Klicken Sie auf **Fertig**.

Verwandte Themen

- Internetverkehr verfolgen (Seite 184)
- Eingehende Ereignisse anzeigen (Seite 180)

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" verfolgen

In dem Bereich "Intrusion Detection-Ereignisse" können Sie eine IP-Adresse verfolgen, die im Protokoll "Intrusion Detection-Ereignisse" aufgeführt wird.

So verfolgen Sie die IP-Adresse eines Computers aus dem Protokoll "Intrusion Detection-Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Intrusion Detection-Ereignisse**.Wählen Sie im Bereich "Intrusion Detection-Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse verfolgen**.
4. Wählen Sie im Bereich "Visual Tracer" eine der folgenden Optionen aus:
   - **Kartenansicht**: Lokalisieren Sie einen Computer geografisch anhand der ausgewählten IP-Adresse.
   - **Registrant-Ansicht**: Lokalisieren Sie die Domäneninformationen anhand der ausgewählten IP-Adresse.
   - **Netzwerkansicht**: Lokalisieren Sie die Netzwerkinformationen anhand der ausgewählten IP-Adresse.
5. Klicken Sie auf **Fertig**.

Verwandte Themen

- Internetverkehr verfolgen (Seite 184)
- Protokollierung, Überwachung und Analyse (Seite 177)

Überwachte IP-Adresse verfolgen

Sie können eine überwachte IP-Adresse verfolgen. Dazu wird eine Weltkarte aufgerufen, die die wahrscheinlichste Datenroute zwischen dem Quellcomputer und Ihrem Computer anzeigt. Darüber hinaus können Sie die Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse in Erfahrung bringen.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Aktive Programme**.
4. Wählen Sie ein Programm und dann die IP-Adresse aus, die unterhalb des Programmnamens angezeigt wird.
5. Aktivieren Sie unter **Programmaktivität** die Option **Diese IP verfolgen**.
6. Unter **Visual Tracer** wird eine Weltkarte mit der wahrscheinlichsten Datenroute zwischen dem Quellcomputer und Ihrem Computer angezeigt. Darüber hinaus können Sie die Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse in Erfahrung bringen.

Hinweis: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Visual Tracer** auf **Aktualisieren**.

Verwandte Themen

- Internetdatenverkehr überwachen (Seite 189)

Internetdatenverkehr überwachen

Die Firewall bietet verschiedene Methoden zur Überwachung des Internetdatenverkehrs an:

- **Diagramm "Datenverkehrsanalyse"**: Zeigt die zuletzt registrierten eingehenden und ausgehenden Internetverbindungen an.
- **Diagramm "Datenverkehrsverwendung"**: Zeigt den Prozentsatz der Bandbreite an, der in den vergangenen 24 Stunden von den Anwendungen mit der höchsten Aktivität verwendet wurde.
- **Aktive Programme**: Zeigt die Anwendungen an, die momentan die meisten Netzwerkverbindungen auf dem Computer verwenden, sowie die IP-Adressen, auf die diese Anwendungen zugreifen.

Info zum Diagramm "Datenverkehrsanalyse"

Das Diagramm "Datenverkehrsanalyse" ist eine numerische und graphische Darstellung des ein- und abgehenden Internet-Datenverkehrs. Der Datenverkehrsmonitor zeigt zudem Programme an, die die höchste Anzahl an Netzwerkverbindungen auf Ihrem Computer verwenden, sowie die IP-Adressen, auf die die Programme zugreifen.

In dem Bereich "Datenverkehrsanalyse" können Sie den zuletzt registrierten eingehenden und ausgehenden Internetdatenverkehr sowie die aktuellen, mittleren und maximal Übertragungsraten anzeigen. Darüber hinaus können Sie den Datenverkehr anzeigen, einschließlich des gemessenen Datenverkehrs seit dem Start der Firewall und des gesamten Datenverkehrs für den aktuellen und die vorherigen Monate.

Im Bereich "Datenverkehrsanalyse" wird die Echtzeit-Internetaktivität auf Ihrem Computer angezeigt, einschließlich der Datenmenge und Übertragungsrate von zuletzt registriertem eingehenden und ausgehenden Internetdatenverkehr auf Ihrem Computer, der Verbindungsgeschwindigkeit und der Gesamtzahl an Bytes, die über das Internet übertragen wurden.

Die durchgezogene grüne Linie stellt die aktuelle Übertragungsrate für eingehenden Datenverkehr dar. Die gepunktete grüne Linie stellt die durchschnittliche Übertragungsrate für eingehenden Datenverkehr dar. Wenn die aktuelle und die durchschnittliche Übertragungsrate identisch sind, wird die gepunktete Linie im Diagramm nicht angezeigt. Die durchgezogene Linie stellt sowohl die durchschnittliche als auch die aktuelle Übertragungsrate dar.

Die durchgezogene rote Linie stellt die aktuelle Übertragungsrate für ausgehenden Datenverkehr dar. Die gepunktete rote Linie stellt die durchschnittliche Übertragungsrate für ausgehenden Datenverkehr dar. Wenn die aktuelle und die durchschnittliche Übertragungsrate identisch sind, wird die gepunktete Linie im Diagramm nicht angezeigt. Die durchgezogene Linie stellt sowohl die durchschnittliche als auch die aktuelle Übertragungsrate dar.

Verwandte Themen

- Eingehenden und ausgehenden Datenverkehr analysieren (Seite 191)

Eingehenden und ausgehenden Datenverkehr analysieren

Das Diagramm "Datenverkehrsanalyse" ist eine numerische und graphische Darstellung des ein- und abgehenden Internet-Datenverkehrs. Der Datenverkehrsmonitor zeigt zudem Programme an, die die höchste Anzahl an Netzwerkverbindungen auf Ihrem Computer verwenden, sowie die IP-Adressen, auf die die Programme zugreifen.

So analysieren Sie den eingehenden und ausgehenden Datenverkehr:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Datenverkehrsanalyse**.

Tipp: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Datenverkehrsanalyse** auf **Aktualisieren**.

Verwandte Themen

- Info zum Diagramm "Datenverkehrsanalyse" (Seite 190)

Programmbandbreite überwachen

Sie können ein Kreisdiagramm anzeigen, in dem der ungefähre Prozentsatz der Bandbreite dargestellt wird, der in den vergangenen 24 Stunden von den Anwendungen mit der höchsten Aktivität verwendet wurde. Das Kreisdiagramm dient der visuellen Darstellung der relativen Bandbreite, die von den Programmen genutzt wird.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Datenverkehrsverwendung**.

Tipp: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Datenverkehrsverwendung** auf **Aktualisieren**.

Programmaktivität überwachen

Sie können die eingehende und ausgehende Programmaktivität anzeigen, in der die Remote-Computerverbindungen und -ports enthalten sind.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Aktive Programme**.
4. Sie können die folgenden Informationen anzeigen:
   - Diagramm "Programmaktivität": Wählen Sie ein Programm, um dessen Aktivität in Diagrammform darzustellen.
   - Überwachungsverbindung: Wählen Sie ein Überwachungselement unter dem Programmnamen.
   - Computerverbindung: Wählen Sie eine IP-Adresse unter dem Programmnamen, Systemprozess oder Dienst.

Hinweis: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Aktive Programme** auf **Aktualisieren**.

KAPITEL 24

Weitere Informationen zu Internet Security

Die Firewall nutzt die Informationen auf McAfees Sicherheitswebsite Hackerwatch, um Ihnen aktuelle Informationen zu Programmen und der globalen Internetaktivität bereitzustellen. Außerdem bietet Hackerwatch ein HTML-Lernprogramm für die Firewall.

In diesem Kapitel

Hackerwatch-Lernprogramm starten

Wissenswertes zur Firewall finden Sie im Hackerwatch-Lernprogramm von SecurityCenter.

So starten Sie das Hackerwatch-Lernprogramm:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Klicken Sie unter **Hackerwatch-Ressourcen** auf **Lernprogramm anzeigen**.

KAPITEL 25

McAfee EasyNetwork

McAfee(R) EasyNetwork ermöglicht sichere Dateifreigabe, vereinfachte Dateiübertragungen und automatische Druckerfreigabe für die Computer in Ihrem privaten Netzwerk.

Bevor Sie mit der Verwendung von EasyNetwork beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu EasyNetwork.

In diesem Kapitel

Funktionen

EasyNetwork bietet folgende Funktionen:

Dateifreigabe

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

Dateiübertragung

Sie können Dateien an andere Computer senden, die Mitglied des verwalteten Netzwerks sind. Wenn Sie eine Datei empfangen, wird diese in Ihrem EasyNetwork-Eingangsbereich angezeigt. Der Eingangsbereich ist ein temporärer Speicherort für alle Dateien, die andere Computer im Netzwerk an Sie senden.

Automatisierte Druckerfreigabe

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

KAPITEL 26

EasyNetwork einrichten

Bevor Sie die EasyNetwork-Funktionen verwenden können, müssen Sie das Programm starten und sich beim verwalteten Netzwerk anmelden. Nach der Anmeldung können Sie das Netzwerk jederzeit wieder verlassen.

In diesem Kapitel

Starten von EasyNetwork

Standardmäßig werden Sie direkt nach der Installation von EasyNetwork gefragt, ob Sie das Programm starten möchten; Sie können EasyNetwork jedoch auch später starten.

EasyNetwork starten

Sie werden standardmäßig aufgefordert, EasyNetwork direkt nach der Installation zu starten. Sie können es jedoch auch zu einem späteren Zeitpunkt starten.

So starten Sie EasyNetwork:

- Klicken Sie im Menü **Start** auf **Programme**, **McAfee** und anschließend auf **McAfee EasyNetwork**.

Tipp: Wenn Sie während der Installation das Erstellen von Desktop- und Schnellstartsymbolen gewählt haben, können Sie EasyNetwork auch starten, indem Sie auf dem Desktop auf das McAfee EasyNetwork-Symbol doppelklicken oder indem Sie im Benachrichtigungsbereich rechts neben der Taskleiste auf das McAfee EasyNetwork-Symbol klicken.

Anmelden an einem verwalteten Netzwerk

Nach der Installation von SecurityCenter wird Ihrem Computer ein Netzwerkagent hinzugefügt, der im Hintergrund ausgeführt wird. In EasyNetwork ist der Netzwerkagent verantwortlich für das Finden einer gültigen Netzwerkverbindung, das Finden lokaler Drucker zur Freigabe und das Überwachen des Netzwerkstatus.

Wenn in dem Netzwerk, in dem Sie sich derzeit befinden, kein anderer Computer gefunden wird, der den Netzwerkagenten ausführt, werden Sie automatisch zu einem Mitglied dieses Netzwerks gemacht und müssen angeben, ob das Netzwerk vertrauenswürdig ist. Da Ihr Computer der erste ist, der dem Netzwerk beitritt, erscheint der Name Ihres Computers als Teil des Netzwerknamens; Sie können das Netzwerk jedoch jederzeit umbenennen.

Wenn ein Computer eine Verbindung mit dem Netzwerk herstellt, wird an alle anderen Computer, die sich bereits im Netzwerk verbinden, eine Beitrittsanfrage gesendet. Diese Anfrage kann von jedem Computer genehmigt werden, der über administrative Berechtigung für das Netzwerk verfügt. Der Computer, der Zugriff gewährt, kann die Berechtigungsstufe für den Computer festlegen, der gerade dem Netzwerk beitritt; beispielsweise Gast (nur Dateiübertragung) oder vollständig/administrativ (Dateiübertragung und Dateifreigabe). In EasyNetwork können Computer mit administrativem Zugriff anderen Computern Zugriff gewähren und Berechtigungen verwalten (d. h. Computer mit mehr oder weniger Rechten versehen); Computer mit vollständigem Zugriff können diese administrativen Aufgaben nicht ausführen. Bevor der Computer dem Netzwerk beitreten darf, wird außerdem eine Sicherheitsüberprüfung durchgeführt.

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder Network Manager), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Dem Netzwerk beitreten

Wenn ein Computer zum ersten Mal nach der Installation von EasyNetwork einem vertrauenswürdigen Netzwerk beitritt, wird der Benutzer gefragt, ob er dem verwalteten Netzwerk beitreten möchte. Wenn der Benutzer des Computers dem Beitritt zustimmt, wird an alle anderen Computer im Netzwerk, die über administrativen Zugriff verfügen, eine Anfrage gesendet. Diese Anfrage muss genehmigt werden, bevor der Computer Drucker oder Dateien freigeben oder Dateien im Netzwerk senden oder kopieren kann. Wenn der Computer der erste Computer im Netzwerk ist, werden ihm automatisch administrative Genehmigungen verliehen.

So treten Sie dem Netzwerk bei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Ja, diesem Netzwerk jetzt beitreten**.
   Wenn ein administrativer Computer im Netzwerk Ihre Anfrage genehmigt, wird eine Nachricht angezeigt, in der festgelegt werden muss, ob dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten dürfen.
2. Wen dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten sollen, klicken Sie auf **Ja**; klicken Sie andernfalls auf **Nein**.
3. Bestätigen Sie, dass der Computer, der den Netzwerkzugriff gewährt, die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Ihnen den Zugriff gewährt hat, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Zugriff auf das Netzwerk gewähren

Wenn ein Computer dem verwalteten Netzwerk beitreten möchte, wird den anderen Computern im Netzwerk, die über administrativen Zugriff verfügen, eine Nachricht gesendet. Der erste Computer, der auf diese Nachricht antwortet, ist der Computer, der Zugriff gewährt. Der Computer, der Zugriff gewährt, entscheidet, welche Art von Zugriff dem Computer gewährt wird: Gast, vollständig oder administrativ

So gewähren Sie Zugriff auf das Netzwerk:

1. Aktivieren Sie in der Nachricht eines der folgenden Kontrollkästchen:
   - **Zugriff als Gast gewähren**: Der Benutzer kann Dateien an andere Computer senden, aber keine Dateien freigeben.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben, anderen Computern Zugriff gewähren und die Berechtigungsstufen anderer Computer anpassen.
2. Klicken Sie auf **Zugriff gewähren**.
3. Bestätigen Sie, dass der Computer die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Gewähren des Zugriffs für diesen Computer ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Netzwerk umbenennen

Standardmäßig beinhaltet der Netzwerkname den Namen des ersten Computers, der dem Netzwerk beigetreten ist; Sie können den Netzwerknamen jedoch jederzeit ändern. Wenn Sie den Netzwerknamen ändern, können Sie die Netzwerkbeschreibung ändern, die in EasyNetwork angezeigt wird.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü **Optionen** auf **Konfiguration**.
2. Geben Sie im Dialogfeld "Konfiguration" den Namen des Netzwerks in das Feld **Netzwerkname** ein.
3. Klicken Sie auf **OK**.

Verwaltetes Netzwerk verlassen

Wenn Sie sich bei einem verwalteten Netzwerk anmelden und anschließend entscheiden, dass Sie nicht länger Mitglied dieses Netzwerks sein möchten, können Sie das Netzwerk verlassen. Wenn Sie Ihre Mitgliedschaft aufgegeben haben, können Sie sich jederzeit wieder anmelden. Ihnen muss jedoch die Berechtigung zum Anmelden gewährt und die Sicherheitsprüfung muss erneut ausgeführt werden. Weitere Informationen finden Sie unter Bei einem verwalteten Netzwerk anmelden (Seite 199).

Verwaltetes Netzwerk verlassen

Sie können ein verwaltetes Netzwerk verlassen, bei dem Sie sich zuvor angemeldet haben.

So verlassen Sie ein verwaltetes Netzwerk:

1. Klicken Sie im Menü **Tools** auf **Netzwerk verlassen**.
2. Wählen Sie im Dialogfeld "Netzwerk verlassen" den Namen des Netzwerks, das Sie verlassen möchten.
3. Klicken Sie auf **Netzwerk verlassen**.

KAPITEL 27

Dateien freigeben und senden

EasyNetwork vereinfacht das Freigeben und Senden von Dateien auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

In diesem Kapitel

Dateien freigeben

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden. Wenn Sie einen Ordner freigeben, werden alle darin und in den Unterordnern enthaltenen Dateien freigegeben. Nachträglich hinzugefügte Dateien werden jedoch nicht automatisch freigegeben. Wenn eine freigegebene Datei oder ein freigegebener Ordner gelöscht wird, wird sie bzw. er automatisch aus dem Fenster "Freigegebene Dateien" entfernt. Sie können eine Dateifreigabe jederzeit rückgängig machen.

Sie haben zwei Möglichkeiten, auf eine freigegebene Datei zuzugreifen: indem Sie die Datei direkt in EasyNetwork öffnen oder sie auf Ihren Computer kopieren und sie dann öffnen. Wenn Ihre Liste der Dateifreigaben zu lang ist, können Sie nach der freigegebenen Datei suchen, auf die Sie zugreifen möchten.

Hinweis: Auf Dateien, die über EasyNetwork freigegeben wurden, kann von anderen Computern mit Windows-Explorer nicht zugegriffen werden. Das Freigeben von Dateien über EasyNetwork erfolgt über sichere Verbindungen.

Freigabe einer Datei

Wenn Sie eine Datei freigeben, können automatisch alle anderen Mitglieder mit vollständigem oder administrativem Zugriff auf das verwaltete Netzwerk darauf zugreifen.

So geben Sie eine Datei frei:

1. Finden Sie in Windows-Explorer die Datei, die Sie freigeben möchten.
2. Ziehen Sie die Datei von ihrem Speicherort in Windows-Explorer auf das Fenster "Freigegebene Dateien" in EasyNetwork.

Tipp: Sie können eine Datei auch freigeben, indem Sie auf **Dateien freigeben** im Menü **Extras** klicken. Navigieren Sie im Dialogfeld "Freigeben" zu dem Ordner, in dem sich die Datei befindet, die freigegeben werden soll, wählen Sie die Datei aus, und klicken Sie auf **Freigeben**.

Freigabe einer Datei aufheben

Wenn Sie eine Datei im verwalteten Netzwerk freigeben, können Sie diese Freigabe jederzeit aufheben. Wenn Sie die Freigabe einer Datei aufheben, können andere Mitglieder des verwalteten Netzwerks nicht mehr darauf zugreifen.

So heben Sie die Freigabe einer Datei auf:

1. Klicken Sie im Menü **Extras** auf **Freigabe von Dateien stoppen**.
2. Wählen Sie im Dialogfeld "Freigabe von Dateien stoppen" die Datei aus, die Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Freigegebene Datei kopieren

Sie können freigegebene Dateien von einem beliebigen Computer im verwalteten Netzwerk auf Ihren Computer kopieren. Wenn der Computer die Dateifreigabe anschließend stoppt, verfügen Sie noch über eine Kopie der Datei.

So kopieren Sie eine Datei:

- Ziehen Sie die Datei aus dem Fenster "Freigegebene Dateien" in EasyNetwork an einen Speicherort in Windows-Explorer oder auf dem Windows-Desktop.

Tipp: Sie können eine freigegebene Datei auch kopieren, indem Sie die Datei in EasyNetwork auswählen und anschließend im Menü **Tools** auf **Kopie an** klicken. Navigieren Sie im Dialogfeld "Kopieren in Ordner" zu dem Ordner, in den Sie die Datei kopieren möchten, wählen Sie die Datei aus und klicken Sie anschließend auf **Speichern**.

Suchen nach einer freigegebenen Datei

Sie können nach einer Datei suchen, die von Ihnen oder einem anderen Mitglied des Netzwerks freigegeben wurde. Während der Eingabe der Suchkriterien zeigt EasyNetwork automatisch die entsprechenden Ergebnisse im Fenster "Freigegebene Dateien" an.

So suchen Sie nach einer freigegebenen Datei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Suche**.
2. Klicken Sie in der Liste **Enthält** auf eine der folgenden Optionen:
   - **Alle Begriffe**: Sucht nach Datei- oder Pfadnamen, die alle Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben, in beliebiger Reihenfolge.

- **Ein beliebiger Begriff**: Sucht nach Datei- oder Pfadnamen, die eines der Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben.
- **Exakte Zeichenfolge**: Sucht nach Datei- oder Pfadnamen, die den exakten Ausdruck enthalten, den Sie in der Liste **Datei oder Pfadnamen** angeben.

3 Geben Sie einen Teil oder den gesamten Datei- oder Pfadnamen in die Liste **Datei oder Pfadname** ein.

4 Klicken Sie in der Liste **Typ** auf einen der folgenden Dateitypen:

- **Beliebig**: Durchsucht alle freigegebenen Dateitypen.
- **Dokument**: Durchsucht alle freigegebenen Dokumente.
- **Bild**: Durchsucht alle freigegebenen Bilddateien.
- **Video**: Durchsucht alle freigegebenen Videodateien.
- **Audio**: Durchsucht alle freigegebenen Audiodateien.

5 Klicken Sie in den Listen **Von** und **Bis** auf die Daten, die den Datumsbereich festlegen, in dem die Datei erstellt wurde.

Senden von Dateien an andere Computer

Sie können Dateien an andere Computer senden, die Mitglieder des verwalteten Netzwerks sind. Vor dem Senden einer Datei überprüft EasyNetwork, ob der Computer, der die Datei enthält, über ausreichend freien Speicherplatz verfügt.

Wenn Sie eine Datei erhalten, wird diese in Ihrem EasyNetwork-Posteingang angezeigt. Der Posteingang ist ein temporärer Speicherort für alle Dateien, die Sie von anderen Computern im Netzwerk erhalten. Wenn EasyNetwork geöffnet ist, wenn Sie eine Datei erhalten, wird die Datei sofort in Ihrem Posteingang angezeigt; andernfalls wird eine Nachricht im Benachrichtigungsbereich rechts der Windows-Taskleiste angezeigt. Wenn Sie keine Benachrichtigungen erhalten möchten, können Sie diese deaktivieren. Wenn eine Datei mit demselben Namen bereits im Posteingang vorhanden ist, wird dem Namen der neuen Datei eine Zahl als Suffix hinzugefügt. Dateien bleiben in Ihrem Posteingang, bis Sie sie akzeptieren (sie also an einen Speicherort auf Ihrem Computer kopieren).

Eine Datei an einen anderen Computer senden

Sie können eine Datei direkt an einen anderen Computer im verwalteten Netzwerk senden, ohne sie freizugeben. Bevor ein Benutzer die Datei auf dem empfangenden Computer anzeigen kann, muss sie lokal gespeichert werden. Weitere Informationen hierzu finden Sie unter Dateien von einem anderen Computer akzeptieren (Seite 210).

So senden Sie eine Datei an einen anderen Computer:

1. Suchen Sie die zu sendende Datei in Windows-Explorer.
2. Ziehen Sie die Datei in Windows-Explorer von ihrem Speicherort auf ein aktives Computersymbol in EasyNetwork.

Tipp: Sie können mehrere Dateien an einen Computer senden, indem Sie beim Auswählen der Dateien die STRG-Taste gedrückt halten. Sie können die Dateien auch senden, indem Sie im Menü **Tools** auf **Senden** klicken, die Dateien auswählen und anschließend auf **Senden** klicken.

Akzeptieren einer Datei von einem anderen Computer

Wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet, müssen Sie diese akzeptieren (indem Sie sie in einem Ordner auf Ihrem Computer speichern). Wenn EasyNetwork nicht geöffnet ist oder sich nicht im Vordergrund befindet, wenn eine Datei an Ihren Computer gesendet wird, erhalten Sie eine Benachrichtigung im Benachrichtigungsbereich rechts der Taskleiste. Klicken Sie auf die Benachrichtigung, um EasyNetwork zu öffnen und auf die Datei zuzugreifen.

So erhalten Sie eine Datei von einem anderen Computer:

- Klicken Sie auf **Erhalten** und ziehen Sie eine Datei von Ihrem EasyNetwork-Posteingang in einen Ordner in Windows-Explorer.

Tipp: Sie können eine Datei von einem anderen Computer auch erhalten, indem Sie die Datei in Ihrem EasyNetwork-Posteingang auswählen und im Menü **Extras** auf **Akzeptieren** klicken. Navigieren Sie im Dialogfeld "Akzeptieren für Ordner" auf den Ordner, in dem die Dateien, die Sie erhalten, gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie auf **Speichern**.

Benachrichtigung bei gesendeter Datei erhalten

Sie können eine Benachrichtigung erhalten, wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet. Wenn EasyNetwork aktuell nicht geöffnet oder auf dem Desktop nicht im Vordergrund angezeigt wird, wird rechts neben der Windows-Taskleiste eine Benachrichtigungsmeldung angezeigt.

So erhalten Sie Benachrichtungen bei gesendeten Dateien:

1. Kllicken Sie im Menü **Optionen** auf **Konfigurieren**.
2. Aktivieren Sie im Dialogfeld "Konfigurieren" das Kontrollkästchen **Benachrichtigen, wenn Dateien von anderen Computern gesendet werden**.
3. Klicken Sie auf **OK**.

KAPITEL 28

Drucker freigeben

Wenn Sie sich bei einem verwalteten Netzwerk angemeldet haben, gibt EasyNetwork automatisch alle mit Ihrem Computer verbundenen lokalen Drucker frei. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

In diesem Kapitel

Mit freigegebenen Druckern arbeiten

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden. Wenn Sie einen Druckertreiber über einen Netzwerk-Druckerserver konfiguriert haben (z. B. ein Wireless-USB-Druckerserver), betrachtet EasyNetwork den Drucker als lokalen Drucker und gibt ihn automatisch im Netzwerk frei. Sie können eine Druckerfreigabe jederzeit rückgängig machen.

EasyNetwork erkennt auch Drucker, die von allen anderen Computern im Netzwerk freigegeben wurden. Wenn es einen Remote-Drucker erkennt, der noch nicht mit Ihrem Computer verbunden ist, wird beim erstmaligen Öffnen von EasyNetwork im Fenster "Freigegebene Dateien" der Link **Verfügbare Netzwerkdrucker** angezeigt. Dies ermöglicht Ihnen, verfügbare Drucker zu installieren oder Drucker zu deinstallieren, die mit Ihrem Computer bereits verbunden sind. Sie können zudem die Liste der im Netzwerk erkannten Drucker aktualisieren.

Wenn Sie sich beim verwalteten Netzwerk noch nicht angemeldet haben, mit diesem aber bereits verbunden sind, können Sie über die Drucker-Systemsteuerung von Windows auf die freigegebenen Drucker zugreifen.

Freigabe eines Druckers aufheben

Sie können die Freigabe eines Druckers jederzeit aufheben. Mitglieder, die den Drucker installiert haben, können ihn nicht mehr zum Drucken verwenden.

So heben Sie die Freigabe eines Druckers auf:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Netzwerkdrucker verwalten" auf den Namen des Druckers, den Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Installieren eines verfügbaren Netzwerkdruckers

Als Mitglied eines verwalteten Netzwerks können Sie auf die Drucker zugreifen, die im Netzwerk freigegeben sind. Dazu müssen Sie die Druckertreiber installieren, die der Drucker verwendet. Wenn der Eigentümer des Druckers dessen Freigabe aufhebt, nachdem Sie ihn installiert haben, können Sie mit diesem Drucker nicht mehr drucken.

So installieren Sie einen verfügbaren Netzwerkdrucker:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Verfügbare Netzwerkdrucker" auf den Namen eines Druckers.
3. Klicken Sie auf **Installieren**.

KAPITEL 29

Referenz

Das Begriffsglossar enthält und definiert die am häufigsten in McAfee-Produkten verwendete Sicherheitsterminologie.

Info zu McAfee enthält rechtliche Informationen zu McAfee Corporation.

Glossar

"

"Man-in-the-Middle"-Angriff

Der Angreifer fängt Nachrichten bei einem öffentlichen Schlüsselaustausch ab und überträgt sie neu, wobei er den angeforderten Schlüssel durch deren eigene öffentliche Schlüssel ersetzt, so dass die beiden ursprünglichen Parteien weiterhin den Eindruck haben, direkt miteinander zu kommunizieren. Dabei verwendet der Angreifer ein Programm, dass sich dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der Angriff kann dazu dienen, einfach nur Zugriff auf die Nachrichten zu erhalten. Der Angreifer hat aber auch die Möglichkeit, die Nachrichten zu ändern, bevor er sie wieder weiterleitet. Der Begriff leitet sich von einem Ballspiel ab, bei dem mehrere Personen versuchen, sich gegenseitig den Ball zuzuwerfen, während ein einzelner Mitspieler in der Mitte versucht, den Ball abzufangen.

8

802.11

Eine Reihe von IEEE-Standards für Funk-LANs. 802.11 legt eine Schnittstelle für den Funkverkehr zwischen einem drahtlosen Client und einer Basisstation oder zwischen zwei drahtlosen Clients fest. Zu den verschiedenen Spezifikationen von 802.11 gehören die Standards 802.11a (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band), 802.11b (für Netzwerke mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band), 802.11g (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 2,4 GHz-Band) sowie 802.11i (eine Reihe von Sicherheitsstandards für alle drahtlosen Ethernet-Netzwerke).

802.11a

Eine Erweiterung von 802.11 für Funk-LANs zum Senden von Daten mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

802.11b

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 11 Mbit/s im 2,4 GHz-Band bietet. 802.11b gilt derzeit als Standard für drahtlose Netzwerkverbindungen.

802.11g

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 54 Mbit/s im 2,4 GHz-Band bietet.

802.1x

Wird von Wireless Home Network Security nicht unterstützt. Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken, wird aber vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet. Dieser Standard bietet eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Außerdem bietet 802.1x dynamische, benutzer- und sitzungsspezifische WEP-Schlüssel, wodurch der bei statischen WEP-Schlüsseln übliche Verwaltungsaufwand und die Sicherheitsrisiken beseitigt werden.

A

Anschluss

Hierbei handelt es sich um einen Ort, an dem Informationen bei einem Computer ein- oder ausgehen. Ein konventionelles Analogmodem ist beispielsweise an einen seriellen Anschluss angeschlossen. Die Anschlussnummern bei der TCP/IP-Kommunikation sind virtuelle Werte, die den Datenverkehr in anwendungsspezifische Datenströme aufteilen. Anschlüsse werden Standardprotokollen wie SMTP oder HTTP zugeordnet, damit die Programme "wissen", über welchen Anschluss eine Verbindung hergestellt werden kann. Der Zielanschluss für TCP-Pakete gibt die gesuchte Anwendung oder den gesuchten Server an.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

Authentifizierung

Der Vorgang des Identifizierens eines bestimmten Benutzers, meist anhand von Benutzername und Kennwort. Mit der Authentifizierung wird sichergestellt, dass es sich bei einem Benutzer auch wirklich um denjenigen handelt, der er oder sie zu sein vorgibt. Über die Zugriffsrechte dieses Benutzers sagt die Authentifizierung jedoch nichts aus.

B

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums übertragen werden kann. Bei digitalen Geräten wird die Bandbreite meist in Bit pro Sekunde (Bit/s) oder Byte pro Sekunde angegeben. Bei analogen Geräten wird die Bandbreite als Taktzahl pro Sekunde bzw. Hertz (Hz) angegeben.

Bibliothek

Der Online-Speicherbereich für Dateien, die von Benutzern der Datensicherung veröffentlicht werden. Die Bibliothekt ist eine Website im Internet, auf die jeder mit Internetzugriff zugreifen kann.

Bilderanalyse

Verhindert die Anzeige potentiell unangemessener Bilder. Bilder werden für alle Benutzer blockiert, außer für Mitglieder der Altersgruppe "Erwachsener".

Browser

Ein Clientprogramm, das mit Hilfe von HTTP (Hypertext Transfer Protocol) Anforderungen an Webserver im Internet richtet. Ein Webbrowser zeigt dem Benutzer den Inhalt graphisch an.

Brute-Force-Angriff

Eine Vorgehensweise nach dem Fehler-Treffer-Prinzip, die auch unter dem Begriff "Brute-Force-Cracking" bekannt ist. Dabei versuchen entsprechende Programme, verschlüsselte Daten (z. B. Kennwörter) mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien zu entschlüsseln.
Brute-Force-Anwendungen probieren nacheinander alle möglichen Kombinationen von zulässigen Zeichen aus – wie bei einem Safe, bei dem alle Zahlenkombinationen ausprobiert werden, um ihn zu öffnen, was genauso eine strafbare Handlung ist.
Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großen Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt.

C

chiffrierter Text

Das sind Daten, die verschlüsselt wurden. Chiffrierter Text ist nicht lesbar, solange er nicht mithilfe eines Schlüssels wieder in Klartext umgewandelt (entschlüsselt) wurde.

Client

Eine Anwendung, die auf einem PC oder einer Workstation ausgeführt wird und zum Durchführen bestimmter Vorgänge auf einen Server angewiesen ist. Beispiel: Ein E-Mail-Client ist eine Anwendung, mit der Sie E-Mails senden und empfangen können.

Cookie

Ein Datenblock im World Wide Web, den ein Webserver auf einem Clientsystem speichert. Wenn ein Benutzer erneut dieselbe Website besucht, sendet der Browser eine Kopie des Cookies zurück an den Server. Cookies werden für die Identifizierung von Benutzern, zur Anweisung an den Server, eine benutzerdefinierte Version der angeforderten Webseite zu senden, zum Senden von Kontoinformationen an den Benutzer sowie für andere administrative Aufgaben verwendet.

Diese Datei ermöglicht es, dass die Website sich an Sie "erinnert", und der Betreiber kann feststellen, wie viele Benutzer die Website besucht haben bzw. wann welche Seiten der Website aufgerufen wurden. Unternehmen versuchen, ihre Websites mithilfe von Cookies gezielt auf die Vorlieben und Anforderungen verschiedener Benutzer abzustimmen. Zahlreiche Websites gestatten beispielsweise den Zugriff auf bestimmte Seiten der Website erst dann, wenn Sie einen Benutzernamen und ein Kennwort eingeben, und senden ein Cookie an Ihren Computer, so dass Sie sich beim nächsten Besuch dieser Seiten nicht erneut anmelden müssen. Cookies können jedoch auch missbraucht werden. Online-Werbefirmen verwenden oft Cookies, um zu analysieren, welche Websites häufig von Ihnen besucht werden, und nutzen diese Erkenntnisse zum Platzieren von Werbeanzeigen auf den meistbesuchten Websites. Bevor Sie Cookies von einer Website zulassen, sollten Sie sicher sein, dass Sie dieser Website vertrauen können.

Cookies sind nicht nur für rechtsgültige Unternehmen eine Informationsquelle, sondern können zu diesem Zweck auch von Hackern missbraucht werden. Zahlreiche Websites von Onlineshops speichern Kreditkartennummern und andere persönliche Informationen in Cookies, um den Kunden das Einkaufen zu erleichtern. Leider sind Sicherheitslücken nicht auszuschließen, die es Hackern ermöglichen, über die auf den Kundencomputern gespeicherten Cookies auf vertrauliche Daten zuzugreifen.

D

Denial of Service, DoS

Ein DoS-Angriff (Denial-of-Service, Dienstverweigerung) ist ein Störfall im Internet, durch den Benutzer oder Unternehmen nicht mehr auf bestimmte Ressourcen oder Dienste zugreifen können. Dabei handelt es sich meist um die Nichtverfügbarkeit eines einzelnen Netzwerkdienstes (z. B. E-Mail) oder den vorübergehenden Verlust aller Netzwerkverbindungen und -dienste. Im schlimmsten Fall kann beispielsweise eine Website, auf die täglich Millionen Benutzer zugreifen, zeitweise gezwungen sein, ihren Betrieb einzustellen. Bei einem DoS-Angriff können auch Programme und Dateien in einem Computersystem zerstört werden. Auch wenn DoS-Angriffe meist absichtlich und böswillig sind, können sie manchmal auch unbeabsichtigt passieren. Ein DoS-Angriff stellt eine Art von Sicherheitsverletzung dar, die meist nicht zu einem Diebstahl von Informationen oder anderen Sicherheitsverlusten führt. Trotzdem können solche Angriffe für die Zielperson bzw. das geschädigte Unternehmen mit einem beträchtlichen Zeitaufwand und erheblichen Kosten verbunden sein.

DNS

Acronym für Domain Name System. Das hierarchische System, über das Hosts im Internet sowohl Domänennamenadressen (wie bluestem.prairienet.org) und IP-Adressen (wie 192.17.3.4) erhalten. Die Domänennamenadresse wird von Personen verwendet und automatisch in die numerische IP-Adresse übersetzt, die von der Paket-Weiterleitungssoftware verwendet wird. DNS-Namen bestehen aus einer Domäne auf der obersten Ebene (wie .com, .org, und .net), einer Domäne auf der zweiten Ebene (der Site-Name eines Unternehmens, einer Organisation oder einer Einzelperson) und möglicherweise einer oder mehreren untergeordneten Domänen (Server innerhalb einer Domäne auf der zweiten Ebene). Siehe auch DNS-Server und IP-Adresse.

DNS-Server

Abkürzung für Domain Name System-Server. Ein Computer, der Domain Name System (DNS)-Abfragen beantworten kann. Der DNS-Server verwaltet eine Datenbank mit Host-Computern und ihren dazugehörigen IP-Adressen. Der DNS-Server, der durch den Namen apex.com dargestellt wird, würde beispielsweise die IP-Adresse des fiktiven Unternehmens Apex zurückgeben. Auch bezeichnet als: Namensserver Siehe auch DNS- und IP-Adresse.

Domäne

Eine Adresse einer Netzwerkverbindung, die den Inhaber dieser Adresse in einem hierarchischen Format identifiziert: server.organisation.typ. Beispielsweise bezeichnet www.whitehouse.gov den Webserver des Weißen Hauses, das Teil der US-Regierung ist.

Drahtloser Adapter

Enthält die Schaltkreise, mit denen ein Computer oder ein anderes Gerät mit einem (an einem drahtlosen Netzwerk angeschlossenen) drahtlosen Router kommunizieren kann. Drahtlose Adapter können entweder im Hauptschaltkreis eines Hardwaregeräts integriert sein oder sich auf einer separaten Zusatzkarte befinden, die in den entsprechenden Anschluss eines Geräts eingesteckt wird.

E

E-Mail

E-Mails sind "elektronische Post", also Nachrichten, die über das Internet oder innerhalb eines Unternehmens über LAN oder WAN gesendet werden. E-Mail-Anlagen in Form von EXE-Dateien (ausführbare Dateien) oder VBS-Dateien (Visual Basic-Skriptdateien) werden immer häufiger für die Übertragung von Viren und trojanischen Pferden zweckentfremdet.

E-Mail-Client

Ein E-Mail-Konto. Beispielsweise Microsoft Outlook oder Eudora.

Echtzeit-Scans

Dateien werden auf Viren und andere Aktivitäten gescannt, wenn Sie oder Ihr Computer darauf zugreifen.

Ereignis

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 Firewall die Pakete vor der TCP/IP-Validierung erhält, kann es solche Pakete möglicherweise als Ereignis melden.

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 Trojaner gesucht hat. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Ereignisse von 127.0.0.1

Manchmal wird von Ereignissen als IP-Quelladresse 127.0.0.1 angegeben. Hierbei ist zu beachten, dass es sich um eine spezielle IP-Adresse handelt, die auch Loopbackadresse genannt wird.

Unabhängig davon, welchen Computer Sie verwenden, 127.0.0.1 bezieht sich stets auf Ihren lokalen Computer. 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 seriöse Programme verwenden die Loopbackadresse zur 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.

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. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert. Das Erstellen von Berichten zu Ereignissen der IP-Adresse 127.0.0.1 ist offensichtlich nicht hilfreich und daher unnötig.

Das heißt, dass für einige Programme, vor allem Netscape ab Version 6.2 und höher gilt, jedoch dass die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** aufgenommen werden muss. Die Komponenten dieser Programme kommunizieren so miteinander, dass Firewall nicht bestimmen kann, ob es sich um einen lokalen Datenverkehr handelt oder nicht.

Bei Netscape 6.2 können Sie zum Beispiel Ihre Buddyliste nicht verwenden, wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen. Wenn Sie also Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr sicherheitshalber blockieren. Sollte jedoch ein Programm (wie Netscape) Probleme haben, nehmen Sie die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** in 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 **Vertrauenswürdige IP-Adressen** behoben, müssen Sie Ihre Entscheidungsmöglichkeiten abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, allerdings erhöht sich 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

Für die meisten LAN-Einstellungen in Unternehmen können Sie allen Computern in Ihrem LAN vertrauen.

Ereignisse von privaten IP-Adressen

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

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 **Vertrauenswürdige IP-Adressen** aufnehmen. Dadurch wird der Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie sich nicht in einem privaten Netzwerk befinden und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die IP-Quelladresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Da private IP-Adressen von IP-Adressen im Internet getrennt sind, hat das Melden dieser Ereignisse keine Auswirkungen.

ESS (Extended Service Set)

Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

Externe Festplatte

Eine Festplatte, die außerhalb des Computergehäuses aufbewahrt wird.

Firewall

Ein System, das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. Firewalls können in Form von Hardware, Software oder einer Kombination von beiden implementiert werden. Sie werden häufig verwendet, um zu verhindern, dass nicht autorisierte Internetbenutzer auf private Netzwerke (insbesondere Intranets) zugreifen, die mit dem Internet verbunden sind. Alle Nachrichten, die in das Intranet gelangen oder dieses verlassen, laufen durch eine Firewall. Von dieser werden alle Nachrichten überprüft und jene blockiert, die nicht die angegebenen Sicherheitskriterien erfüllen. Firewalls werden als erste Verteidigungslinie beim Schutz privater Informationen betrachtet. Zur höheren Sicherheit können die Daten verschlüsselt werden.

Freigeben

Ein Vorgang, der es E-Mail-Empfängern ermöglicht, für eine begrenzte Zeit auf ausgewählte gesicherte Dateien zuzugreifen. Wenn Sie eine Datei freigeben, senden Sie die gesicherte Kopie der Datei an die E-Mail-Empfänger, die Sie angeben. Die Empfänger erhalten eine E-Mail der Datensicherung, die ihnen mitteilt, dass Dateien für sie freigegeben wurden. Die E-Mail enthält außerdem einen Link zu den freigegebenen Dateien.

freigegebenes Geheimnis

Siehe auch RADIUS. Schützt den sensiblen Teil von RADIUS-Nachrichten. Der gemeinsame geheime Schlüssel ist ein Kennwort, das von dem Authentifikator und dem Authentifizierungsserver auf eine bestimmte sichere Weise gemeinsam verwendet wird.

Hotspot

Ein bestimmter örtlicher Standort, an dem ein Zugriffspunkt mobilen Besuchern den Zugriff auf öffentliche Breitband-Netzwerkdienste über ein drahtloses Netzwerk ermöglicht. Hotspots befinden sich oft in der Nähe von stark frequentierten Einrichtungen, z. B. Flughäfen, Bahnhöfen, Bibliotheken, Jachthäfen, Messe-Centern und Hotels. Sie haben meist eine geringe Reichweite.

Inhaltsklassifikationsgruppen

Altersgruppen, zu denen ein Benutzer gehört. Der Inhalt wird auf der Grundlage der Inhaltsklassifikationsgruppe bewertet (das bedeutet verfügbar gemacht oder blockiert), zu der der Benutzer gehört. Inhaltsklassifikationsgruppen umfassen Folgendes: kleines Kind, Kind, jüngerer Teenager, älterer Teenager und Erwachsener.

integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunkts, Routers und einer Firewall kombiniert sind. Einige Geräte können auch Sicherheitsoptimierungen und Überbrückungsfunktionen enthalten.

Internet

Das Internet besteht aus einer großen Menge verbundener Netzwerke, die TCP/IP-Protokolle zur Ermittlung und Übertragung von Daten verwenden. Ursprünglich ist das Internet aus miteinander verbundenen Universitätscomputern entstanden. Daraus entwickelte sich das Ende der 60er Jahre vom US-Verteidigungsministerium gegründete ARPANET, das als Wegbereiter für das Internet gilt. Heute ist das Internet ein globales Netzwerk von nahezu 100.000 unabhängigen Netzwerken.

Intranet

Ein privates Netzwerk, in der Regel innerhalb einer Organisation, das im Wesentlichen wie das Internet funktioniert. Auf ein Intranet kann auch von externen Computern aus zugegriffen werden, beispielsweise durch Studenten, die auf das Intranet einer Universität, oder externe Mitarbeiter, die auf das Internet eines Unternehmens Zugriff erhalten haben. Firewalls, Anmeldeprozeduren und Kennwörter dienen der Sicherheit eines Intranets.

IP-Adresse

Die IP-Adresse (Internet Protocol Number) ist eine eindeutige Zahlenfolge, deren vier Bestandteile durch Punkte voneinander getrennt sind (z. B. 63.227.89.66). Jeder Internetcomputer verfügt über eine eindeutige IP-Adresse - vom größten Server bis hin zum Laptop, der per Mobilanschluss kommuniziert. Nicht jeder Computer weist einen Domänennamen auf, aber jeder Computer hat eine IP-Adresse.

Im Folgenden werden einige ungewöhnliche Typen von IP-Adressen aufgeführt:

- Nicht routbare IP-Adressen: Diese stellen einen privaten IP-Adressraum dar. Hierbei handelt es sich um IP-Adressen, die im Internet nicht verwendet werden können. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x.
- Loopback-IP-Adressen**:** Diese Adressen werden zu Testzwecken verwendet. Datenpakete, die an diesen IP-Adressblock gesendet werden, kehren sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da an diese IP-Adressen gerichtete Datenpakete das Gerät überhaupt nicht verlassen, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block beginnt mit 127.x.x.x.

Null-IP-Adressen Hierbei handelt es sich um 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 wird von einer Anwendung empfangen, die den Paketinhalt (d. h. die anwendungsspezifischen Anweisungen) versteht und damit entsprechend umgehen kann. Jede Adresse, die mit 0 beginnt (0.x.x.x), ist eine Null-Adresse. Beispiel: 0.0.0.0 ist eine Null-IP-Adresse.

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Dieses Methode wird in vielen Arten von Angriffen einschließlich dem "Session-Hijacking" verwendet. Sie wird oftmals auch dazu verwendet, die Kopfzeilen von SPAM-E-Mails zu fälschen, damit diese E-Mails nicht mehr zurückverfolgt werden können.

isolieren

Wenn verdächtige Dateien erkannt werden, werden sie isoliert. Sie können dann die entsprechende Aktion ausführen.

Kennwort

Ein (in der Regel alphanumerischer) Code, über den Sie Zugriff auf Ihren Computer bzw. auf ein Programm oder eine Website erhalten.

Kennwort-Tresor

Ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht es Ihnen, Ihre Kennwörter sicher zu speichern in dem Wissen, dass kein anderer Benutzer (auch kein McAfee-Administrator oder Systemadministrator) darauf zugreifen kann.

Knoten

Hierbei handelt es sich um einen Computer, der mit einem Netzwerk verbunden ist.

Komprimierung

Ein Vorgang, bei dem Daten (Dateien) in eine Form komprimiert werden, die den zum Speichern oder Übermitteln erforderlichen Platz minimiert.

Kopfzeile

Bei einem Header handelt es sich um Informationen, die im Lauf der Übermittlung zur E-Mail hinzugefügt wurden. Die Kopfzeile bestimmt die Übermittlung der E-Mail durch die Internetsoftware und enthält außerdem die Adresse für die Rückantwort, eine eindeutige Kennung für die E-Mail und andere administrative Angaben. Beispiele für diese Kopfzeilenfelder sind: An, Von, CC, Datum, Betreff, Nachrichten-ID und Empfangen.

LAN (Local Area Network)

Ein Computernetzwerk, dass sich über ein relativ kleines Gebiet erstreckt. Die meisten LANs sind auf ein einzelnes Gebäude oder eine Gruppe von Gebäuden beschränkt. Per Telefonverbindungen oder Funkwellen kann ein LAN aber auch über eine beliebige Entfernung mit anderen LANs verbunden werden. Ein System aus LANs, die auf diese Weise miteinander verbunden sind, wird WAN (Wide-Area Network) genannt. In den meisten LANs werden Workstations und PCs über normale Hubs oder Switches miteinander verbunden. Jeder Knoten (ein einzelner Computer) in einem LAN hat seine eigene CPU, mit der er Programme ausführt, kann aber auch auf Daten und Geräte (z. B. Drucker) im LAN zugreifen. Auf diese Weise können teure Geräte (z. B. Laserdrucker) sowie Daten von vielen Benutzern gemeinsam genutzt werden. Über ein LAN können Benutzer auch miteinander kommunizieren, z. B. E-Mails senden oder an Chat-Sitzungen teilnehmen.

MAC (Media Access Control oder Message Authenticator Code)

Für das Erstgenannte von beiden siehe "MAC-Adresse". Die zweite ausgeschriebene Abkürzung (Message Authenticator Code) bezeichnet einen Code, der zum Identifizieren einer bestimmten Nachricht (z. B. einer RADIUS-Nachricht) verwendet wird. Der Code ist gewöhnlich ein kryptographisch starker Hash des Nachrichteninhalts, der einen eindeutigen Wert als Replay-Schutz enthält.

MAC-Adresse (Media Access Control Address)

Eine Adresse auf unterer Ebene, die einem physikalischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

MAPI-Konto

Acronym für Messaging Application Programming Interface. Die Microsoft-Schnittstellenspezifikation, die es verschiedenen Messaging- und Arbeitsgruppenanwendungen (einschließlich E-Mail, Voice-Mail und Fax) ermöglicht, einen einzigen Client zu verwenden, wie den Exchange-Client. MAPI wird daher häufig in Unternehmensumgebungen mit Microsoft® Exchange Server eingesetzt. Zahlreiche Benutzer verwenden allerdings Microsoft Outlook für persönliche Internet-E-Mails.

MSN-Konto

Acronym für Microsoft Network. Ein Online-Dienst und Internetportal. Dies ist ein webbasiertes Konto.

Netzwerk

Ein Netzwerk entsteht durch die Verbindung von mehreren Computern.

Netzwerk-Laufwerk

Ein Disketten- oder Band-Laufwerk, das mit einem Server in einem Netzwerk verbunden ist, das für mehrere Benutzer freigegeben ist. Netzwerk-Laufwerke werden gelegentlich auch als Remote-Laufwerke bezeichnet.

Netzwerkzuordnung

In Network Manager ist die Netzwerkzuordnung eine graphische Darstellung des Computers und der Komponenten, die Ihr privates Netzwerk ausmachen.

NIC (Network Interface Card, Netzwerkkarte)

Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

Online-Sicherungs-Repository

Der Speicherort auf dem Online-Server, an dem Ihre überwachten Dateien nach der Sicherung gespeichert werden.

Parental controls

Einstellungen, die das Konfigurieren von Inhaltsklassifikationen und Internetzugriffszeiten ermöglichen. Darin wird festgelegt, welche Inhalte und Websites ein Benutzer anzeigen kann und wann und wie lange dieser Benutzer auf das Internet zugreifen kann. Mit Kindersicherungen können Sie außerdem allgemeine Beschränkungen für den Zugriff auf bestimmte Websites festlegen oder den Zugriff auf der Grundlage von Altersgruppen und Stichwörtern gewähren oder blockieren.

PCI-Drahtlosadapter-Karte

Verbindet einen Desktopcomputer mit einem Netzwerk. Die Karte wird in einen PCI-Erweiterungssteckplatz im Computer gesteckt.

Phishing

Als "Fishing" ausgesprochen, ist ein Scam, mithilfe dessen Ihnen wertvolle Informationen, wie Ihre Kreditkarten- und Sozialversicherungsnummer, Benutzer-IDs und Kennwörter gestohlen werden sollen. Eine offiziell aussehende E-Mail wird an potentielle Opfer gesendet. Dabei wird behauptet, die Mail stamme vom ISP, der Bank oder einem Geschäft, bei dem die Benutzer einkaufen. E-Mails können an Personen auf ausgewählten oder beliebigen Listen gesendet werden, in der Erwartung, dass ein gewisser Prozentsatz der Empfänger tatsächlich über ein Konto bei dem echten Unternehmen verfügt.

POP3-Konto

Acronym für Post Office Protocol 3. Die meisten privaten Benutzer haben diesen Kontotyp. Dies ist die aktuelle Version des Post Office Protocol-Standards, der häufig in TCP/IP-Netzwerken verwendet wird. Auch bekannt als standardmäßiges E-Mail-Konto.

Popups

Kleine Fenster, die über anderen Fenstern auf dem Bildschirm angezeigt werden. Popup-Fenster werden oft in Webbrowsern verwendet, um Werbung anzuzeigen. McAfee blockiert Popup-Fenster, die automatisch geladen werden, wenn eine Webseite in Ihrem Browser geladen wird. Popup-Fenster, die geladen werden, wenn Sie auf einen Link klicken, werden von McAfee nicht blockiert.

Potentiell unerwünschtes Programm

Potentiell unerwünschte Programme umfassen Spyware, Adware und andere Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und übertragen.

PPPoE

Abkürzung für "Point-to-Point Protocol Over Ethernet". PPPoE wird von vielen DSL-Providern verwendet und unterstützt die in PPP häufig verwendeten Protokollebenen und Authentifizierung. Mit PPPoE kann eine Punkt-zu-Punkt-Verbindung in der normalen Multipoint-Ethernet-Architektur hergestellt werden.

Protokoll

Ein vorab vereinbartes Format zum Übertragen von Daten zwischen zwei Geräten. Aus Sicht des Benutzers besteht der einzige interessante Aspekt bei Protokollen darin, dass der Computer oder das Gerät die entsprechenden Protokolle unterstützen muss, um mit einem jeweils anderen Computer kommunizieren zu können. Das Protokoll kann entweder in der Hardware oder in der Software implementiert sein.

Proxy

Ein Computer (oder die auf ihm ausgeführte Software), der als Barriere zwischen einem Netzwerk und dem Internet fungiert, indem er gegenüber externen Sites nur als eine einzige Netzwerkadresse auftritt. Indem er für alle internen Computer eine Zwischenwand darstellt, schützt der Proxy Netzwerkidentitäten und ermöglicht gleichzeitig Zugriff auf das Internet. Siehe auch Proxyserver.

Proxy-Server

Eine Firewallkomponente, die den ein- und ausgehenden Internetverkehr eines LAN (Local Area Network) verwaltet. Ein Proxyserver kann durch Liefern häufig angeforderter Daten, z.B. einer beliebten Webseite, die Leistung steigern und Anforderungen filtern, die der Eigentümer als nicht geeignet einstuft, z.B. Anforderungen nach unautorisiertem Zugriff auf proprietäre Dateien.

Pufferüberlauf

Pufferüberläufe finden statt, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (Speicherbereich für temporäre Dateien) auf Ihrem Computer zu speichern als erlaubt, so dass gültige Daten in nahegelegenen Puffern beschädigt oder überschrieben würden.

RADIUS (Remote Access Dial-In User Service)

Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

Reiner Text

Nachrichten, die nicht verschlüsselt sind.

Roaming

Die Fähigkeit, aus dem Empfangsbereich eines Zugriffspunkts in den eines anderen zu wechseln, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

Router

Ein Netzwerkgerät, das Pakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden anhand interner Routingtabellen, wie das Paket weitergeleitet werden soll. Die Wahl der Schnittstelle, an die ausgehende Pakete gesendet werden, kann davon abhängen, in welcher Konstellation Quell- und Zieladresse miteinander stehen, oder sich nach den aktuellen Gegebenheiten im Netzwerkverkehr (z. B. Auslastung, Leitungskosten oder ausgefallene Leitungen) richten. Für "Router" wird manchmal auch der Begriff "Zugriffspunkt" verwendet.

Schlüssel

Eine Folge von Buchstaben und/oder Zahlen, mit der zwei Geräte ihre Kommunikation miteinander authentifizieren können. Dabei müssen beide Geräte über den Schlüssel verfügen. Siehe auch WEP, WPA, WPA2, WPA-PSK und WPA2- PSK.

Schnellarchivierung

Die Archivierung nur der überwachten Dateien, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden.

Schwarze Liste

Eine Liste der Websites, die als schädlich angesehen werden. Eine Website kann in eine schwarze Liste eingetragen werden, wenn über sie betrügerische Handlungen vorgenommen werden oder wenn sie Browser-Schwachstellen ausnutzt, um potentiell unerwünschte Programme an den Benutzer zu senden.

Server

Hierbei handelt es sich um einen Computer oder eine Software, der/die bestimmte Dienste für das Ausführen einer Software auf anderen Computern zur Verfügung stellt. Der "E-Mail-Server" bei Ihrem ISP ist eine Software, die den gesamten eingehenden und ausgehenden E-Mail-Datenverkehr für alle Benutzer des ISPs verarbeitet. Bei einem Server auf einem LAN handelt es sich um eine Hardware, die den primären Knoten im Netzwerk darstellt. Diese Hardware kann wiederum Software enthalten, die den zugehörigen Clientcomputern bestimmte Dienste, Daten oder andere Funktionen zur Verfügung stellt.

sichern

Verwenden Sie diese Option, um eine Kopie Ihrer überwachten Dateien auf einem sicheren Online-Server zu erstellen.

Skript

Skripts können Dateien erstellen, kopieren oder löschen. Sie können auch Ihre Windows-Registrierung öffnen.

SMTP-Server

Acronym für Simple Mail Transfer Protocol. Ein TCP/IP-Protokoll, das für das Senden von Nachrichten von einem Computer an einen anderen in einem Netzwerk verwendet wird. Dieses Protokoll wird im Internet verwendet, um E-Mails weiterzuleiten.

Speicherort für die oberflächliche Überwachung

Ein Ordner auf Ihrem Computer, der von der Datensicherung auf Änderungen überwacht wird. Wenn Sie einen Speicherort für die oberflächliche Überwachung einrichten, sichert die Datensicherung die überwachten Dateitypen innerhalb dieses Ordners, nicht aber innerhalb der Unterordner.

Speicherort für umfassende Überwachung

Ein Ordner (und alle Unterordner) auf Ihrem Computer, der von Data Backup auf Änderungen hin überwacht wird. Wenn Sie einen Speicherort für die umfassende Überwachung festlegen, sichert Data Backup die überwachten Dateitypen in diesem Order und seinen Unterordnern.

SSID (Service Set Identifier)

Der Netzwerkname für die Geräte in einem Funk-LAN-Subsystem. Das ist eine Zeichenfolge aus 32 Zeichen, die im Klartext steht und zum Kopf jedes WLAN-Pakets hinzugefügt wird. Die SSID unterscheidet WLANs voneinander. Daher müssen alle Benutzer eines Netzwerks dieselbe SSID angeben, um auf einen bestimmten Zugriffspunkt zuzugreifen. Mit einer SSID wird der Zugriff von Clientgeräten verhindert, die eine andere SSID besitzen. Die SSID wird jedoch von Zugriffspunkten standardmäßig zusammen mit dem Signal übertragen. Dadurch kann ein Hacker die SSID per "Sniffing" selbst dann ermitteln, wenn die SSID-Übertragung deaktiviert ist.

SSL (Secure Sockets Layer)

Ein von Netscape entwickeltes Protokoll zum Übermitteln vertraulicher Dokumente über das Internet. SSL arbeitet mit einem öffentlichen Schlüssel, mit dem die Daten verschlüsselt werden, die über die SSL-Verbindung übertragen werden. SSL wird sowohl von Netscape Navigator als auch von Internet Explorer genutzt und unterstützt. Viele Websites verwenden dieses Protokoll, wenn Benutzer vertrauliche Informationen (z. B. Kreditkartennummern) eingeben müssen. Laut Konvention beginnen URLs, die eine SSL-Verbindung erfordern, mit der Zeichenfolge "https:" anstelle von "http:".

Standard-E-Mail-Konto

Dies ist die am häufigsten vorkommende Kontoart. Siehe auch POP3-Konto.

Stichwort

Ein Wort, das Sie einer gesicherten Datei zuordnen können, um eine Beziehung oder Verbindung mit anderen Dateien aufzubauen, denen dasselbe Stichwort zugeordnet ist. Durch das Zuordnen von Stichwörtern zu Dateien ist es einfacher, nach Dateien zu suchen, die Sie im Internet veröffentlicht haben.

Synchronisieren

Zur Behebung von Inkonsistenzen zwischen gesicherten Dateien und den auf Ihrem lokalen Computer gespeicherten Dateien. Sie synchronisieren Dateien, wenn die Version der Datei im Online-Sicherungs-Repository aktueller als die Version der Datei auf den anderen Computern ist. Durch die Synchronisierung wird die Kopie der Datei auf Ihren Computern mit der Version der Datei im Online-Sicherungs-Repository aktualisiert.

SystemGuard

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus.

TKIP (Temporal Key Integrity Protocol)

Eine schnelle Methode zum Lösen der konstruktionsbedingten Sicherheitsschwächen von WEP, speziell des Problems der Wiederverwendung von Verschlüsselungsschlüsseln. Bei TKIP werden temporäre Schlüssel nach jeweils 10.000 Paketen geändert. Auf diese Weise wird eine dynamische Verteilungsmethode erzielt, die die Sicherheit des Netzwerks beträchtlich erhöht. Der TKIP-Sicherheitsprozess beginnt mit einem temporären 128-Bit-Schlüssel, der von Clients und Zugriffspunkten gemeinsam verwendet wird. TKIP kombiniert diesen temporären Schlüssel mit der MAC-Adresse (des Clientcomputers) und fügt dann einen relativ großen Initialisierungsvektor (16 Oktetts) hinzu, um den Schlüssel zu erstellen, mit dem die Daten verschlüsselt werden. Durch diese Vorgehensweise wird sichergestellt, dass jede Station ihre Daten mit einem anderen Schlüssel-Stream verschlüsselt. TKIP führt die Verschlüsselung mit RC4 durch. WEP verwendet ebenfalls RC4.

Trojaner

Trojaner sind Programme, die sich als gutartige Anwendungen "tarnen". Trojaner sind keine Viren, da sie sich nicht fortpflanzen, können Ihrem Computer jedoch einen ähnlich Schaden zufügen wie Viren.

Überwachte Dateitypen

Die Dateitypen (beispielsweise .DOC, .XLS usw.), die von der Datensicherung innerhalb der Überwachungs-Speicherorte gesichert oder archiviert werden.

Überwachungs-Speicherorte

Die Ordner auf Ihrem Computer, die von der Datensicherung überwacht werden.

Unerwünschte Zugriffspunkte

Ein Zugriffspunkt, den ein Unternehmen für den Betrieb nicht autorisiert. Das Problem dabei ist, dass nicht autorisierte Zugriffspunkte oft nicht den Sicherheitsrichtlinien für WLANs (Wireless LAN, Funk-LAN) entsprechen. Ein nicht autorisierter Zugriffspunkt bietet eine offene, unsichere Schnittstelle in das Unternehmensnetzwerk von außerhalb der physikalisch kontrollierten Einrichtung.

In einem ordnungsgemäß gesicherten WLAN richten nicht autorisierte Zugriffspunkte mehr Schäden an als nicht autorisierte Benutzer. Wenn wirksame Authentifizierungsmechanismen vorhanden sind, müssen nicht autorisierte Benutzer beim Versuch, auf ein WLAN zuzugreifen, nicht unbedingt auch an wertvolle Ressourcen des Unternehmens gelangen. Zu größeren Problemen kommt es jedoch, wenn sich ein Mitarbeiter oder Hacker über den nicht autorisierten Zugriffspunkt anmeldet. Ein nicht autorisierter Zugriffspunkt erlaubt praktisch jedem, der über ein 802.11-kompatibles Gerät verfügt, den Zutritt in das Unternehmensnetzwerk. Dadurch gelangt man schnell sehr nah an geschäftskritische Ressourcen.

URL

Uniform Resource Locator. Hierbei handelt es sich um das Standardformat für Internetadressen.

USB-Drahtlosadapter-Karten

Eine erweiterbare serielle Schnittstelle mit Plug-and-Play-Funktionalität. Diese Schnittstelle bietet eine standardisierte und preisgünstige drahtlose Anschlussmöglichkeit für Peripheriegeräte wie Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Speichergeräte und Videokameras.

Veröffentlichen

Eine gesicherte Datei öffentlich im Internet verfügbar machen.

Verschlüsselung

Ein Vorgang, bei dem Daten von Text in Code umgewandelt werden, wodurch die Informationen verschleiert werden, so dass Personen, die den Code nicht entschlüsseln können, sie nicht lesen können.

Verwaltetes Netzwerk

Ein privates Netzwerk mit zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht.

Vollständige Archivierung

Die Archivierung eines kompletten Datensatzes basierend auf den von Ihnen festgelegten überwachten Dateitypen und Speicherorten.

VPN (Virtual Private Network)

Ein Netzwerk, das entsteht, indem Knoten unter Verwendung von öffentlichen Leitungen neu miteinander verbunden werden. Es gibt zum Beispiel eine Reihe von Systemen, mit denen Sie Netzwerke erstellen können, die das Internet als Medium für den Datentransport verwenden. Diese Systeme setzen Verschlüsselung und andere Sicherheitsmechanismen ein, um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen und die Daten nicht abgefangen werden können.

Wardriver

Das sind mit Notebooks bewaffnete Eindringlinge, die mit spezieller Software und modifizierter Hardware durch die Gegend streifen, um Datenverkehr von Funk-LANs abzufangen.

Web-Bugs

Kleine Grafikdateien, die sich selbst in Ihre HTML-Seiten einbetten können und es einer nicht autorisierten Quelle erlauben, Cookies auf Ihrem Computer zu platzieren. Diese Cookies können dann Informationen an die nicht autorisierte Quelle übertragen. Web-Bugs sind auch als Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs bekannt.

Weiße Liste

Eine Liste der Websites, denen der Zugriff erlaubt wird, da sie nicht als betrügerische Websites angesehen werden.

WEP (Wired Equivalent Privacy)

Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Standard 802.11. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

Wi-Fi (Wireless Fidelity)

Dieser Begriff wird allgemein für alle Arten von 802.11-kompatiblen Netzwerken verwendet, sei es 802.11b, 802.11a, Dual-Band usw. Der Begriff wird von der Wi-Fi Alliance verwendet.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht und deren Ziel darin liegt, (1) allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren und (2) den Begriff "Wi-Fi" in allen Märkten für Produkte für 802.11-basierte Funk-LANs als globalen Markennamen zu fördern. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die die gegenseitige Kompatibilität und das Wachstum dieser Branche voranbringen möchten.

Auch wenn alle Produkte der Standards 802.11a/b/g als Wi-Fi bezeichnet werden, dürfen nur die Produkte, die den Test der Wi-Fi Alliance bestanden haben, das Prädikat "Wi-Fi Certified" (eine eingetragene Marke) tragen. Produkte, die den Test erfolgreich bestanden haben, müssen ein Identifikationssiegel auf ihrer Verpackung haben, auf dem "Wi-Fi Certified" sowie das verwendete Funkfrequenzband stehen. Die Wi-Fi Alliance war früher unter der Bezeichnung Wireless Ethernet Compatibility Alliance (WECA) bekannt, änderte jedoch im Oktober 2002 ihren Namen, um die Marke "Wi-Fi" besser darstellen zu können, deren Aufbau das Ziel der Gruppe ist.

Wi-Fi Certified

Produkte, die von der Wi-Fi Alliance getestet und als Wi-Fi Certified (eine eingetragene Marke) zugelassen wurden, sind als miteinander vollständig kompatibel zertifiziert, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden. Üblicherweise funktionieren Wi-Fi-Produkte mit allen anderen Produkten zusammen, die dieselbe Funkfrequenz verwenden (z. B. 2,4 GHz bei 802.11b oder 11g; 5 GHz bei 802.11a), auch wenn diese nicht das Prädikat "Wi-Fi Certified" haben.

Wiederherstellen

Abrufen einer Kopie einer Datei aus dem Online-Sicherungs-Repository oder einem Archiv.

WLAN (Wireless Local Area Network)

Siehe auch LAN. Ein LAN, das ein drahtloses Medium zum Verbinden verwendet. In WLANs erfolgt die Kommunikation zwischen den Knoten über hochfrequente Funkwellen anstelle von Kabeln.

Wörterbuchangriff

Bei diesen Angriffen wird versucht, ein Kennwort zu ermitteln, indem unzählige Wörter aus einer Liste durchprobiert werden. Dabei geben die Angreifer diese Wörter und alle ihre Kombinationen nicht selbst manuell ein, bis sie das Kennwort von jemandem ermittelt haben, sondern verwenden dafür Tools, die diesen Vorgang automatisieren.

WPA (Wi-Fi Protected Access)

Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen stark erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Softwareupgrade entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entworfen wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus kann der Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren, und sollte die Passphrase auf jedem drahtlosen Computer und Zugriffspunkt regelmäßig ändern. Siehe auch WPA2-PSK und TKIP.

WPA2

Siehe auch WPA. WPA2 ist eine Aktualisierung des WPA-Sicherheitsstandards und basiert auf dem 802.11i IEEE-Standard.

WPA2-PSK

Siehe auch WPA-PSK und WPA2. WPA2-PSK ist WPA-PSK ähnlich und basiert auf dem WPA2-Standard. Eine häufig verwendete Funktion von WPA2-PSK ist, dass Geräte häufig mehrere Verschlüsselungsmodi (z. B. AES, TKIP) gleichzeitig unterstützten, während ältere Geräte üblicherweise nur jeweils einen Verschlüsselungsmodus unterstützten (d. h., alle Clients müssten denselben Verschlüsselungsmodus unterstützen).

Wurm

Würmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Würmer replizieren und verbrauchen Systemressourcen, wodurch die Leistung herabgesetzt und Tasks angehalten werden.

Zugriffspunkt

Ein Netzwerkgerät, das 802.11-kompatiblen Clients die Verbindung zu einem LAN (Local Area Network) ermöglicht. Zugriffspunkte erweitern die physikalische Betriebsreichweite für drahtlose Benutzer. Sie werden auch als drahtlose Router bezeichnet.

Info zu McAfee

McAfee, Inc., mit Hauptsitz in Santa Clara, Kalifornien (USA), ist Marktführer im Bereich Intrusion Prevention und Security Risk Management und bietet weltweit präventive und bewährte Lösungen und Services zum Schutz von Systemen und Netzwerken. Dank der unübertroffenen Sicherheitsexpertise von McAfee und seiner Verpflichtung zur Innovation sind private Nutzer, Unternehmen, der öffentliche Sektor und Service Provider in der Lage, Angriffe abzuwehren, Störungen zu vermeiden und ihre Sicherheit kontinuierlich zu verfolgen und zu verbessern.

Copyright

Index

E

F

G

H

I

K

L

M

N

V

W

Z