McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

Benutzerhandbuch

Inhalt

KAPITEL 1

Einführung

McAfee VirusScan Plus bietet proaktive PC-Sicherheit zur Vermeidung von bösartigen Angriffen, damit Sie schützen, was Sie schätzen und gleichzeitig mit Sicherheit surfen, suchen und Dateien herunterladen können. Mithilfe der Sicherheitsbewertung durch den McAfee SiteAdvisor können Sie unsichere Websites meiden. Dieser Service bietet auch Sicherheit gegen vielfältige Angriffe durch die Integration von Technologien zum Schutz vor Viren, Spyware und für den Firewall-Schutz. Der McAfee-Sicherheitsservice liefert die neuesten Updates für Software, damit Ihr Schutz nie veraltet. So können Sie ganz einfach für mehrere Privat-PCs Sicherheitsabonnements hinzufügen und verwalten. Die verbesserte Leistung erlaubt zudem Schutz, ohne Sie zu stören.

In diesem Kapitel

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter ermöglicht es Ihnen, den Sicherheitsstatus Ihres PCs zu überwachen, um sofort zu erkennen, ob die McAfee-Dienste zum Schutz vor Viren und Spyware sowie für E-Mails und die Firewall auf dem neuesten Stand sind, und in Bezug auf mögliche Sicherheitsschwachstellen aktiv zu werden. Es bietet Navigationstools und Steuerelemente, die Sie für die Koordination und Verwaltung aller Bereiche Ihres PC-Schutzes benötigen.

Bevor Sie mit der Konfiguration und Verwaltung Ihres PC-Schutzes beginnen, prüfen Sie die SecurityCenter-Benutzeroberfläche und vergewissern sich, dass Sie den Unterschied zwischen dem Schutzstatus, Schutzkategorien und Schutzdiensten verstehen. Aktualisieren Sie dann SecurityCenter, um sicherzustellen, dass Sie über den neuesten verfügbaren Schutz von McAfee verfügen.

Nachdem Ihre ursprünglichen Konfigurations-Tasks abgeschlossen sind, verwenden Sie SecurityCenter, um den Schutzstatus Ihres PCs zu überwachen. Wenn SecurityCenter ein Sicherheitsproblem erkennt, warnt es Sie, damit Sie das Problem entweder beheben oder ignorieren können (je nach Schweregrad). Sie können außerdem SecurityCenter-Ereignisse in einem Ereignisprotokoll überprüfen, wie Konfigurationsänderungen an Viren-Scans.

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

SecurityCenter-Funktionen

SecurityCenter bietet folgende Funktionen:

Vereinfachter Schutzstatus

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

Automatische Updates und Upgrades

Laden Sie Updates für Ihre registrierten Programme automatisch herunter, und installieren Sie sie. Wenn eine neue Version eines registrierten McAfee-Programms verfügbar wird, erhalten Sie diese während der Laufzeit Ihres Abonnements kostenlos, sodass gewährleistet wird, dass Sie stets über den aktuellsten Schutz verfügen.

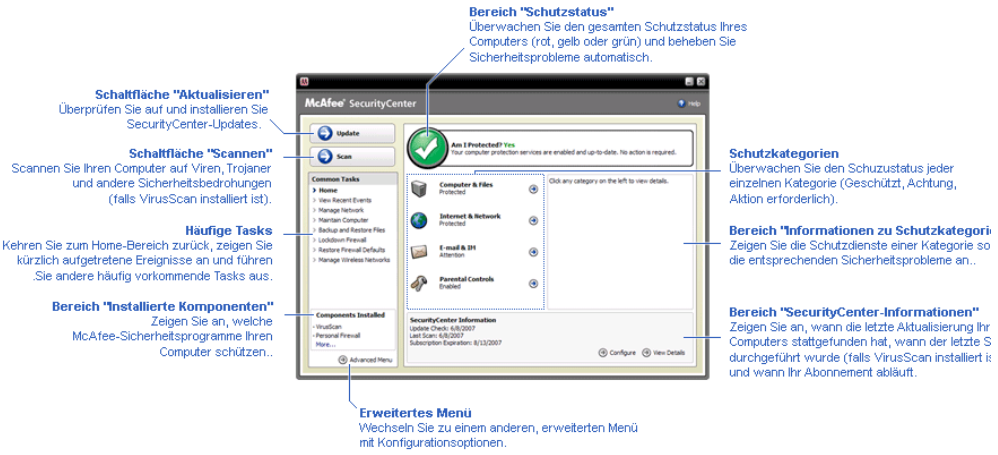
Warnungen in Echtzeit

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

KAPITEL 3

Verwenden von SecurityCenter

Bevor Sie mit der Verwendung von SecurityCenter beginnen, überprüfen Sie die Komponenten und Konfigurationsbereiche, die Sie für die Verwaltung des Schutzstatus Ihres Computers verwenden werden. Weitere Informationen zu der in diesem Bild verwendeten Terminologie finden Sie unter Erläuterungen zum Schutzstatus (Seite 8) und Erläuterungen zu den Schutzkategorien (Seite 9). Sie können dann Ihre McAfee-Kontoinformationen und die Gültigkeit Ihres Abonnements überprüfen.



In diesem Kapitel

Erläuterungen zum Schutzstatus

Der Schutzstatus Ihres Computers wird im Bereich "Schutzstatus" im Home-Bereich von SecurityCenter angezeigt. Er gibt an, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist, und kann von Dingen wie externen Sicherheitsangriffen, anderen Sicherheitsprogrammen und Programmen, die auf das Internet zugreifen, beeinflusst werden.

Der Schutzstatus Ihres Computers kann "rot", "gelb" oder "grün" sein.

Sicherheitsstatus	Beschreibung
Rot	Ihr Computer ist nicht geschützt. Der Bereich "Schutzstatus" im Home-Bereich von SecurityCenter ist rot und gibt an, dass Sie nicht geschützt sind. SecurityCenter meldet mindestens ein kritisches Sicherheitsproblem. Um umfassenden Schutz zu erhalten, müssen Sie alle kritischen Sicherheitsprobleme in jeder Schutzkategorie lösen (der Status der Problemkategorien wird auf **Aktion erforderlich** gesetzt, ist also rot). Informationen zum Beheben von Sicherheitsproblemen finden Sie unter Beheben von Sicherheitsproblemen (Seite 18).
Gelb	Ihr Computer ist teilweise geschützt. Der Bereich "Schutzstatus" im Home-Bereich von SecurityCenter ist gelb und gibt an, dass Sie nicht geschützt sind. SecurityCenter meldet mindestens ein nichtkritisches Sicherheitsproblem. Um umfassenden Schutz zu erhalten, müssen Sie nichtkritische Sicherheitsprobleme in jeder Schutzkategorie beheben oder ignorieren. Informationen zum Beheben oder Ignorieren von Sicherheitsproblemen finden Sie unter Beheben oder Ignorieren von Sicherheitsproblemen (Seite 17).
Grün	Ihr Computer ist umfassend geschützt. Der Bereich "Schutzstatus" im Home-Bereich von SecurityCenter ist grün und gibt an, dass Sie geschützt sind. SecurityCenter meldet keine kritischen oder nichtkritischen Sicherheitsprobleme. In jeder Schutzkategorie werden die Dienste aufgelistet, die Ihren Computer schützen.

Erläuterungen zu den Schutzkategorien

Die Schutzdienste von SecurityCenter sind in die folgenden vier Kategorien unterteilt: Computer & Dateien, Internet & Netzwerk, E-Mail & IM sowie Kindersicherungen. Diese Kategorien helfen Ihnen dabei, die Sicherheitsdienste, die Ihren Computer schützen, zu durchsuchen und zu konfigurieren.

Sie können auf einen Kategorienamen klicken, um seine Schutzdienste zu konfigurieren und sämtliche für diese Dienste erkannten Sicherheitsprobleme anzuzeigen. Wenn der Schutzstatus Ihres Computers "rot" oder "gelb" lautet, zeigen eine oder mehrere Kategorien eine Meldung *Aktion erforderlich* oder *Achtung* an, was darauf hinweist, dass SecurityCenter ein Problem innerhalb dieser Kategorie erkannt hat. Weitere Informationen zum Schutzstatus finden Sie unter Erläuterungen zum Schutzstatus (Seite 8).

Schutzkategorie	Beschreibung
Computer & Dateien	Die Kategorie "Computer & Dateien" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Virenschutz ▪ PUP-Schutz ▪ Systemüberwachung ▪ Windows-Schutz
Internet & Netzwerk	Die Kategorie "Internet & Netzwerk" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Firewall-Schutz ▪ Schutz der Identität
E-Mail & IM	Die Kategorie "E-Mail & IM" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ E-Mail-Schutz ▪ Spam-Schutz
Parental Controls (Kindersicherung)	Die Kategorie "Kindersicherungen" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Inhaltsblockierung

Erläuterungen zu Schutzdiensten

Schutzdienste sind Core-SecurityCenter-Komponenten, die Sie zum Schutz Ihres Computers konfigurieren können. Schutzdienste entsprechen direkt McAfee-Programmen. Wenn Sie beispielsweise VirusScan installieren, werden die folgenden Schutzdienste verfügbar: Virenschutz, PUP-Schutz, Systemüberwachung und Windows-Schutz. Detaillierte Informationen zu diesen speziellen Schutzdiensten finden Sie in der VirusScan-Hilfe.

Standardmäßig sind bei der Installation des Programms alle mit einem Programm verknüpften Schutzdienste aktiviert. Sie können einen Schutzdienst jedoch jederzeit deaktivieren. Wenn Sie beispielsweise Privacy Service installieren, werden sowohl die Inhaltsblockierung als auch der Identitätsschutz aktiviert. Wenn Sie den Schutzdienst für die Inhaltsblockierung nicht verwenden möchten, können Sie ihn vollständig deaktivieren. Sie können einen Schutzdienst auch temporär deaktivieren, während Sie Setup- oder Wartungsaufgaben ausführen.

Verwalten Ihres McAfee-Kontos

Verwalten Sie Ihr McAfee-Konto über SecurityCenter, indem Sie einfach auf Ihre Kontoinformationen zugreifen, diese überprüfen und Ihren aktuellen Abonnementstatus prüfen.

Hinweis: Wenn Sie Ihre McAfee-Programme von einer CD installiert haben, müssen Sie diese auf der McAfee-Website registrieren, um Ihr McAfee-Konto einzurichten oder zu aktualisieren. Nur dann haben Sie Anrecht auf regelmäßige automatische Programm-Updates.

Verwalten Ihres McAfee-Kontos

Sie können über SecurityCenter einfach auf Ihre McAfee-Kontoinformationen (Mein Konto) zugreifen.

1. Klicken Sie unter **Häufige Tasks** auf **Mein Konto**.
2. Melden Sie sich bei Ihrem McAfee-Konto an.

Überprüfen Ihres Abonnements

Sie können Ihr Abonnement überprüfen, um sicherzustellen, dass es noch nicht abgelaufen ist.

- Klicken Sie im Benachrichtigungsbereich rechts auf der Symbolleiste mit der rechten Maustaste auf das SecurityCenter-Symbol, und klicken Sie anschließend auf **Abonnement überprüfen**.

KAPITEL 4

SecurityCenter-Updates

Das SecurityCenter stellt sicher, dass Ihre registrierten McAfee-Programme auf aktuellem Stand sind, indem alle vier Stunden nach Online-Updates gesucht wird und diese installiert werden. Online-Updates können, in Abhängigkeit der von Ihnen installierten und registrierten Programme, Upgrades der neuesten Virusdefinitionen und Upgrades für den Schutz vor Hackern, Spam und Spyware oder für den Datenschutz enthalten. Wenn Sie innerhalb dieser vier Stunden selbst nach Updates suchen wollen, können Sie dies jederzeit tun. Während das SecurityCenter nach Updates sucht, können Sie weiterhin andere Aufgaben durchführen.

Obwohl es nicht empfohlen wird, können Sie die Einstellungen, nach denen das SecurityCenter nach Updates sucht und diese installiert, ändern. Sie können das SecurityCenter beispielsweise auch so konfigurieren, dass Updates heruntergeladen, aber nicht installiert werden oder dass Sie benachrichtigt werden, bevor Updates heruntergeladen oder installiert werden. Sie können automatische Updates auch deaktivieren.

Hinweis: Falls Sie Ihre McAfee-Programme von einer CD installiert haben, erhalten Sie regelmäßige, automatische Updates für die Programme nur, wenn Sie diese vorher auf der McAfee-Website registriert haben.

In diesem Kapitel

Suche nach Updates

Das SecurityCenter sucht standardmäßig alle vier Stunden automatisch nach Updates, wenn Ihr Computer an das Internet angeschlossen ist. Wenn Sie innerhalb dieser vier Stunden nach Updates suchen wollen, ist dies auch möglich. Wenn Sie die automatischen Updates deaktiviert haben, liegt es in Ihrer Verantwortung, regelmäßig nach Updates zu suchen.

- Klicken Sie im Fenster "Startseite" des SecurityCenter auf **Update**.

Tipp: Sie können auch nach Updates suchen, ohne das SecurityCenter zu starten, indem Sie mit der rechten Maustaste im Benachrichtigungsbereich rechts neben der Taskleiste auf das SecurityCenter-Symbol und anschließend auf **Updates** klicken.

Konfigurieren automatischer Updates

In der Standardeinstellung sucht das SecurityCenter automatisch alle vier Stunden nach neuen Updates und installiert sie, sofern Ihr Computer mit dem Internet verbunden ist. Wenn Sie diese Standardeinstellung ändern wollen, können Sie das SecurityCenter so konfigurieren, dass Updates automatisch heruntergeladen werden und Sie dann benachrichtigt werden, wenn die Updates zur Installation bereit sind oder dass Sie vor dem Herunterladen der Updates benachrichtigt werden.

Hinweis: Das SecurityCenter informiert Sie durch eine Warnung, wenn Updates zum Herunterladen oder zur Installation bereitstehen. Bei den Warnungen haben Sie die Option, die Updates herunterzuladen oder zu installieren oder die Installation auf einen späteren Zeitpunkt zu verschieben. Wenn Sie Ihre Programme von einer Warnung aus aktualisieren, werden Sie möglicherweise aufgefordert, vor dem Herunterladen und der Installation Ihr Abonnement prüfen zu lassen. Weitere Informationen erhalten Sie unter Arbeiten mit Warnungen (Seite 23).

1 Öffnen Sie den SecurityCenter-Konfigurationsbereich.

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.

2 Klicken Sie im SecurityCenter-Konfigurationsbereich unter **Automatische Updates deaktiviert** auf **Ein** und anschließend auf **Erweitert**.

3 Klicken Sie auf eine der folgenden Schaltflächen:

- **Updates automatisch installieren und benachrichtigen, wenn meine Dienste aktualisiert werden (empfohlene Einstellung)**
- **Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist**
- **Vor dem Herunterladen von Updates benachrichtigen**

4 Klicken Sie auf **OK**.

Deaktivieren von automatischen Updates

Wenn Sie die automatischen Updates deaktivieren, liegt es in Ihrer Verantwortung, regelmäßig nach Updates zu suchen. Andernfalls verfügt Ihr Computer nicht über den neuesten Sicherheitsschutz. Weitere Informationen zur manuellen Suche nach Updates erhalten Sie unter Prüfen auf Updates (Seite 14).

1 Öffnen Sie den SecurityCenter-Konfigurationsbereich.

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.

2 Klicken Sie im SecurityCenter-Konfigurationsbereich unter **Automatische Updates aktiviert** auf **Aus**.

Tipp: Sie können die automatischen Updates aktivieren, indem Sie auf **Ein** klicken oder indem Sie im Bereich "Update-Optionen" die Auswahl **Automatische Updates deaktivieren und manuelle Suche nach Updates zulassen** aufheben.

KAPITEL 5

Beheben oder Ignorieren von Sicherheitsproblemen

Das SecurityCenter meldet alle kritischen und nichtkritischen Sicherheitsprobleme, sobald sie erkannt werden. Kritische Sicherheitsprobleme erfordern unverzügliche Maßnahmen und gefährden Ihren Sicherheitsstatus (die Farbe wechselt zu rot). Nichtkritische Sicherheitsprobleme erfordern keine unverzüglichen Maßnahmen und gefährden möglicherweise Ihren Sicherheitsstatus (in Abhängigkeit von der Art des Problems). Um den Sicherheitsstatus der Kategorie "grün" zu erhalten, müssen Sie alle kritischen Probleme beheben und alle nichtkritischen Probleme beheben oder ignorieren. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician starten. Weitere Informationen zum McAfee Virtual Technician erhalten Sie im Hilfebereich des McAfee Virtual Technician.

In diesem Kapitel

Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden. Bei einigen Problemen müssen Sie jedoch selbst Maßnahmen ergreifen. Wenn z. B. der Firewall-Schutz deaktiviert ist, kann das SecurityCenter diesen automatisch aktivieren. Wenn der Firewall-Schutz jedoch nicht installiert ist, müssen Sie ihn installieren. In der folgenden Tabelle werden einige andere Maßnahmen beschrieben, die Sie unternehmen können, wenn Sie Sicherheitsprobleme manuell beheben:

Problem:	Maßnahme
Während der vergangenen 30 Tage wurde keine Überprüfung Ihres Computers durchgeführt.	Überprüfen Sie Ihren Computer manuell. Weitere Informationen finden Sie im Hilfebereich von VirusScan.
Ihre Entdeckungssignaturdateien (DATs) sind veraltet.	Aktualisieren Sie Ihren Schutz manuell. Weitere Informationen finden Sie im Hilfebereich von VirusScan.
Ein Programm ist nicht installiert.	Installieren Sie das Programm von der McAfee-Website oder der CD.
Bei einem Programm fehlen Komponenten.	Installieren Sie das Programm von der McAfee-Website oder der CD erneut.
Ein Programm ist nicht registriert und erhält keinen vollständigen Schutz.	Registrieren Sie das Programm auf der McAfee-Website.
Ein Programm ist abgelaufen.	Überprüfen Sie Ihren Kontostatus auf der McAfee-Website.

Hinweis: In vielen Fällen wirkt sich ein Sicherheitsproblem auf mehrere Schutzkategorien aus. In diesem Fall wird es bei der Behebung des Problems in einer Kategorie in allen Kategorien gelöscht.

Automatisches Beheben von Sicherheitsproblemen

Das SecurityCenter kann die meisten Sicherheitsprobleme automatisch beheben. Die Änderungen der Konfiguration, die das SecurityCenter während der automatischen Behebung von Sicherheitsproblemen vornimmt, werden nicht im Ereignisprotokoll aufgezeichnet. Weitere Informationen zu Ereignissen finden Sie unter Ereignisse anzeigen (Seite 29).

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" im Schutzstatusbereich auf **Beheben**.

Manuelles Beheben von Sicherheitsproblemen

Falls Probleme weiterhin bestehen, nachdem Sie versucht haben, sie automatisch zu beheben, können Sie die Probleme manuell beheben.

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf die Schutzkategorie, in der das SecurityCenter das Problem meldet.
3. Klicken Sie auf den Link hinter der Problembeschreibung.

Ignorieren von Sicherheitsproblemen

Wenn das SecurityCenter ein nichtkritisches Problem erkennt, haben Sie die Option, es zu beheben oder zu ignorieren. Andere nichtkritische Probleme (z. B. wenn Anti-Spam oder Privacy Service nicht installiert sind) werden automatisch ignoriert. Ignorierte Probleme werden im Informationsbereich für Schutzkategorien im Bereich "SecurityCenter Home" nicht angezeigt, es sei denn, der Schutzstatus Ihres Computers hat die Kategorie "grün". Wenn Sie ein Problem ignorieren und später entscheiden, dass es im Informationsbereich für Schutzkategorien angezeigt werden soll, auch wenn der Schutzstatus Ihres Computers nicht die Kategorie "grün" aufweist, können Sie das ignorierte Problem anzeigen lassen.

Ignorieren eines Sicherheitsproblems

Wenn das SecurityCenter ein nichtkritisches Problem erkennt, das Sie nicht beheben wollen, können Sie es ignorieren. Wenn Sie das Problem ignorieren, wird das Problem im Informationsbereich für Schutzkategorien im SecurityCenter nicht mehr angezeigt.

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf die Schutzkategorie, in der das Problem gemeldet wird.
3. Klicken Sie neben dem Sicherheitsproblem auf den Link **Ignorieren**.

Anzeigen oder Verbergen von ignorierten Problemen

In Abhängigkeit von deren Schweregrad kann man ignorierte Sicherheitsprobleme anzeigen lassen oder verbergen.

1. Öffnen Sie den Bereich "Warnoptionen".

   Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Klicken Sie im Bereich "SecurityCenter-Konfiguration" auf **Ignorierte Probleme**.

3 Führen Sie im Bereich "Ignorierte Probleme" einen der folgenden Schritte aus:

- Um ein Problem zu ignorieren, wählen Sie das entsprechende Kontrollkästchen aus.
- Um ein Problem im Informationsbereich für Schutzkategorien zu melden, deaktivieren Sie das entsprechende Kontrollkästchen.

4 Klicken Sie auf **OK**.

Tipp: Sie können ein Problem auch ignorieren, indem Sie auf den Link **Ignorieren** neben dem gemeldeten Problem im Informationsbereich für Schutzkategorien klicken.

KAPITEL 6

Arbeiten mit Warnungen

Warnungen sind kleine Popup-Dialogfelder, die am rechten unteren Rand Ihres Bildschirmes erscheinen, wenn bestimmte SecurityCenter-Ereignisse auftreten. Eine Warnung gibt detallierte Informationen zu einem Ereignis sowie Empfehlungen und Optionen zur Lösung der Probleme, die mit dem Ereignis verknüpft sein könnten. Einige Warnungen enthalten auch Links zu zusätzlichen Informationen über das Ereignis. Mit diesen Links können Sie die globale McAfee-Website öffnen oder Informationen zur Problembehebung an McAfee senden.

Es gibt drei Warntypen: rot, gelb und grün.

Warntyp:	Beschreibung
Rot	Eine rote Warnung ist eine kritische Benachrichtigung, bei der ein Eingreifen Ihrerseits erforderlich ist. Rote Warnungen erscheinen, wenn das SecurityCenter das Sicherheitsproblem nicht automatisch beheben kann.
Gelb	Eine gelbe Warnung ist eine nichtkritische Benachrichtigung, bei der in der Regel kein Eingreifen Ihrerseits erforderlich ist.
Grün	Eine grüne Warnung ist eine nichtkritische Benachrichtigung, bei der kein Eingreifen Ihrerseits erforderlich ist. Grüne Warnungen geben grundlegende Informationen zu einem Ereignis.

Da Warnungen eine wichtige Rolle bei der Überwachung und der Verwaltung Ihres Schutzstatus spielen, können sie nicht deaktiviert werden. Sie können jedoch steuern, ob bestimmte Typen von Informationswarnungen erscheinen und einige andere Warnoptionen konfigurieren (so z. B. ob das SecurityCenter bei Warnungen ein Audiosignal ausgibt oder beim Start den Splash-Bildschirm von McAfee anzeigt).

In diesem Kapitel

Anzeigen und Verbergen von Informationswarnungen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die für die Sicherheit Ihres Computers keine Bedrohung darstellen. Wenn Sie z. B. den Firewall-Schutz eingestellt haben, erscheint jedes Mal, wenn einem Programm auf Ihrem Computer der Zugang zum Internet gewährt wird, standardmäßig eine Informationswarnung. Wenn Sie nicht wollen, dass ein spezifischer Typ von Informationswarnungen angezeigt wird, können Sie diese verbergen. Wenn Sie nicht wollen, dass Informationswarnungen angezeigt werden, können Sie diese alle verbergen. Sie können auch alle Informationswarnungen verbergen, wenn Sie auf Ihrem Computer ein Spiel im Vollbildschirmmodus spielen. Wenn Sie mit dem Spiel fertig sind und den Vollbildschirmmodus verlassen, beginnt das SecurityCenter, die Informationswarnungen anzuzeigen.

Wenn Sie fälschlicherweise eine Informationswarnung verborgen haben, können Sie sie jederzeit wieder anzeigen. Im Standardmodus zeigt das SecurityCenter alle Informationswarnungen an.

Anzeigen und Verbergen von Informationswarnungen

Sie können das SecurityCenter so konfigurieren, dass einige Informationswarnungen angezeigt und andere verborgen werden, oder so, dass alle Informationswarnungen verborgen werden.

1 Öffnen Sie den Bereich "Warnoptionen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Klicken Sie im Bereich "SecurityCenter-Konfiguration" auf **Informationswarnungen**.

3 Führen Sie im Bereich "Informationswarnungen" einen der folgenden Schritte aus:

- Um eine Informationswarnung anzuzeigen, deaktivieren Sie das entsprechende Kontrollkästchen.
- Um eine Informationswarnung zu verbergen, aktivieren Sie das entsprechende Kontrollkästchen.

- Um alle Informationswarnungen zu verbergen, aktivieren Sie das Kontrollkästchen **Informationswarnungen nicht anzeigen**.

4 Klicken Sie auf **OK**.

Tipp: Sie können die Informationswarnungen auch verbergen, indem Sie das Kontrollkästchen **Diese Warnung nicht mehr anzeigen** in der Warnung selbst aktivieren. Wenn Sie dies tun, können Sie die Informationswarnung wieder anzeigen lassen, indem Sie das entsprechende Kontrollkästchen im Bereich "Informationswarnungen" deaktivieren.

Anzeigen und Verbergen von Informationswarnungen während eines Spieles

Sie können Informationswarnungen verbergen, wenn Sie auf Ihrem Computer ein Spiel im Vollbildschirmmodus spielen. Wenn Sie das Spiel beendet haben und den Vollbildschirmmodus verlassen, beginnt das SecurityCenter, die Informationswarnungen anzuzeigen.

1 Öffnen Sie den Bereich "Warnoptionen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Aktivieren oder deaktivieren Sie im Bereich "Warnoptionen" die Option **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**.

3 Klicken Sie auf **OK**.

Konfigurieren von Warnoptionen

Das Erscheinungsbild und die Häufigkeit von Warnungen wird durch das SecurityCenter konfiguriert. Sie können jedoch einige grundlegende Warnoptionen einstellen. Sie haben beispielsweise die Möglichkeit, mit Warnungen ein Audiosignal ausgeben zu lassen oder den Splash-Bildschirm beim Start von Windows zu verbergen. Sie können auch Warnungen verbergen, die Sie über Virenausbrüche und andere Sicherheitsbedrohungen in der Online-Community informieren.

Bei Warnungen ein Audiosignal ausgeben

Wenn Sie bei Warnungen ein akustisches Signal erhalten möchten, können Sie das SecurityCenter so konfigurieren, dass bei jeder Warnung ein Audiosignal ausgegeben wird.

1 Öffnen Sie den Bereich "Warnoptionen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Wählen Sie im Bereich "Warnoptionen" unter **Audiosignal** das Kontrollkästchen **Akustisches Signal bei Warnungen ausgeben** aus.

Splash-Bildschirm beim Starten verbergen

Standardmäßig erscheint beim Start von Windows kurz der Splash-Bildschirm von McAfee, wodurch Sie informiert werden, dass Ihr Computer durch das SecurityCenter geschützt wird. Sie haben jedoch die Möglichkeit, den Splash-Bildschirm zu verbergen, wenn Sie ihn nicht angezeigt haben wollen.

1 Öffnen Sie den Bereich "Warnoptionen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Deaktivieren Sie im Bereich "Warnoptionen" unter **Splash-Bildschirm** das Kontrollkästchen

Splash-Bildschirm von McAfee beim Starten von Windows anzeigen.

Tipp: Sie können den Splash-Bildschirm jederzeit wieder anzeigen lassen, indem Sie das Kontrollkästchen **Splash-Bildschirm von McAfee beim Starten von Windows anzeigen** aktivieren.

Virenausbruchswarnungen verbergen

Sie können Warnungen verbergen, die Sie über Virenausbrüche und andere Sicherheitsbedrohungen in der Online-Community informieren.

1 Öffnen Sie den Bereich "Warnoptionen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im rechten Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
3. Klicken Sie unter **Warnungen** auf **Erweitert**.

2 Deaktivieren Sie im Bereich "Warnoptionen" das Kontrollkästchen **Bei Viren oder Sicherheitsbedrohungen benachrichtigen**.

Tipp: Sie können die Warnungen für Virenausbrüche jederzeit wieder anzeigen, indem Sie das Kontrollkästchen **Bei Viren oder Sicherheitsbedrohungen benachrichtigen** aktivieren.

KAPITEL 7

Anzeigen von Ereignissen

Ein Ereignis ist eine Aktion oder eine Änderung der Konfiguration in einer Schutzkategorie und den damit verbundenen Schutzdiensten. Verschiedene Schutzdienste erfassen verschiedene Typen von Ereignissen. Das SecurityCenter erfasst beispielsweise ein Ereignis, wenn ein Schutzdienst aktiviert oder deaktiviert wird. Der Virenschutz erfasst jedes Mal ein Ereignis, wenn ein Virus erkannt und entfernt wird. Der Firewall-Schutz erfasst jedes Mal ein Ereignis, wenn der Versuch einer Internetverbindung blockiert wird. Weitere Informationen zu Schutzkategorien finden Sie unter Erläuterungen zu den Schutzkategorien (Seite 9).

Sie können Ereignisse anzeigen, wenn Sie Konfigurationsprobleme behandeln und wenn Sie von anderen Anwendern durchgeführte Vorgänge überprüfen. Viele Eltern verwenden die Ereignisprotokolle, um das Online-Verhalten Ihrer Kinder zu überwachen. Lassen Sie sich die zuletzt aufgetretenen Ereignisse anzeigen, um die letzten 30 aufgetretenen Ereignisse zu untersuchen. Lassen Sie sich alle aufgetretenen Ereignisse anzeigen, um eine umfassende Liste aller aufgetretenen Ereignisse zu untersuchen. Wenn Sie alle Ereignisse anzeigen, startet das SecurityCenter ein Ereignisprotokoll, in dem die Ereignisse nach der Schutzkategorie, in der sie aufgetreten sind, sortiert sind.

In diesem Kapitel

Zuletzt aufgetretene Ereignisse anzeigen

Lassen Sie sich die zuletzt aufgetretenen Ereignisse anzeigen, um die letzten 30 aufgetretenen Ereignisse zu untersuchen.

- Klicken Sie unter **Häufige Tasks** auf **Aktuelle Ereignisse anzeigen**.

Alle Ereignisse anzeigen

Lassen Sie sich alle aufgetretenen Ereignisse anzeigen, um eine umfassende Liste aller aufgetretenen Ereignisse zu untersuchen.

1. Klicken Sie unter **Häufige Tasks** auf **Aktuelle Ereignisse anzeigen**.
2. Klicken Sie im Fenster "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
3. Klicken Sie im linken Bereich des Ereignisprotokolls auf den Typ von Ereignis, den Sie anzeigen möchten.

KAPITEL 8

McAfee VirusScan

Die erweiterten Prüf- und Schutzdienste von VirusScan schützen Sie und Ihren Computer vor den neuesten Sicherheitsbedrohungen, wie Viren, Trojanern, Verfolgungscookies, Spyware, Adware und anderen potentiell unerwünschten Programmen. Der Schutz geht über die Dateien und Ordner auf Ihrem Desktop hinaus und ist auf Bedrohungen aus verschiedenen Eintrittspunkten gerichtet, so auch E-Mail, Instant Messaging-Nachrichten und Internet.

Durch VirusScan ist Ihr Computer unmittelbar und permanent geschützt, ohne dass mühsame Verwaltung nötig ist. Während Sie arbeiten, spielen, im Netz surfen oder Ihre E-Mail lesen, läuft es im Hintergrund und überwacht, durchsucht und erkennt potentielle Bedrohungen in Echtzeit. Umfassende Scans werden nach Zeitplan durchgeführt und untersuchen Ihren Computer regelmäßig unter Verwendung ausgefeilter Optionen. VirusScan bietet Ihnen die Möglichkeit, diese Vorgänge individuell anzupassen, wenn Sie dies wünschen. Wenn Sie das nicht wollen, ist Ihr Computer trotzdem weiterhin geschützt.

Bei der normalen Nutzung eines Computers können Viren, Würmer und andere potentielle Bedrohungen auf Ihren Computer gelangen. Wenn dies vorkommt, informiert VirusScan Sie über diese Bedrohung, normalerweise behandelt es das Problem jedoch selbst, indem die infizierten Elemente gesäubert oder in Quarantäne verschoben werden, bevor Schaden auftritt. Obwohl dies selten vorkommt, müssen gelegentlich weitere Maßnahmen ergriffen werden. In diesen Fällen gibt VirusScan Ihnen die Möglichkeit, über weitere Schritte zu entscheiden (erneuter Scan beim nächsten Start des Computers, das erkannte Element behalten oder Entfernen des erkannten Elements).

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

VirusScan-Funktionen

VirusScan bietet die folgenden Funktionen.

Umfassenden Virenschutz

Die erweiterten Prüf- und Schutzdienste von VirusScan schützen Sie und Ihren Computer vor den neuesten Sicherheitsbedrohungen, wie Viren, Trojanern, Verfolgungscookies, Spyware, Adware und anderen potentiell unerwünschten Programmen. Der Schutz geht über die Dateien und Ordner auf Ihrem Desktop hinaus und ist auf Bedrohungen aus verschiedenen Eintrittspunkten gerichtet, so auch E-Mail, Instant Messaging-Nachrichten und Internet. Mühsame Verwaltung ist nicht erforderlich.

Scan-Optionen mit Erkennung der Ressourcen

Falls es zu langsamen Scan-Geschwindigkeiten kommen sollte, können Sie diese Option deaktivieren, um minimale Ressourcen des Computers zu nutzen. Beachten Sie jedoch, dass so dem Virenschutz eine höhere Priorität gegeben wird als anderen Aufgaben. VirusScan bietet Ihnen die Möglichkeit, Optionen für Echtzeit- und manuelle Scans anzupassen, wenn Sie dies wünschen. Wenn Sie das nicht wollen, ist Ihr Computer trotzdem weiterhin geschützt.

Automatische Reparaturen

Wenn VirusScan während eines Echtzeit- oder manuellen Scans eine Sicherheitsbedrohung erkennt, versucht es, diese Bedrohung je nach Bedrohungstyp automatisch zu beheben. Auf diese Art werden die meisten Bedrohungen erkannt und neutralisiert, ohne dass Sie eingreifen müssen. Obwohl dies selten auftritt, kann es vorkommen, dass VirusScan eine Bedrohung nicht selbständig neutralisieren kann. In diesen Fällen gibt VirusScan Ihnen die Möglichkeit, über weitere Schritte zu entscheiden (erneuter Scan beim nächsten Start des Computers, das erkannte Element behalten oder Entfernen des erkannten Elements).

Anhalten von Tasks im Vollbildschirmmodus

Wenn Sie gerne Filme sehen, Spiele auf dem Computer spielen oder andere Aktivitäten ausführen, die den gesamten Bildschirm beanspruchen, hält VirusScan verschiedene Tasks an, wie z. B. automatische Updates und manuelle Scans.

Start des Echtzeit-Virenschutzes

VirusScan bietet zwei Arten des Virenschutzes: Echtzeit-Scans und manuelle Scans. Der Echtzeit-Virenschutz überwacht Ihren Computer permanent bezüglich Virenaktivität und durchsucht Dateien jedes Mal, wenn Sie oder Ihr Computer darauf zugreifen. Mit dem manuellen Virenschutz können Sie Dateien nach Bedarf auf Viren durchsuchen. Um sicherzugehen, dass Ihr Computer vor den neuesten Sicherheitsbedrohungen geschützt bleibt, lassen Sie den Echtzeit-Virenschutz eingeschaltet und richten Sie einen Zeitplan für regelmäßige, umfassendere manuelle Scans ein. Standardmäßig führt VirusScan einmal wöchentlich einen Scan durch. Weitere Informationen zu Echtzeit- und manuellen Scans finden Sie unter Überprüfen Ihres Computers (Seite 59).

Obwohl dies selten auftritt, kann es vorkommen, dass Sie die Echtzeit-Scans kurzzeitig stoppen möchten (z. B. um einige Scan-Optionen zu ändern oder um ein Leistungsproblem zu beheben). Wenn der Echtzeit-Virenschutz deaktiviert ist, ist Ihr Computer nicht geschützt, und der Schutzstatus Ihres SecurityCenter ist rot. Weitere Informationen zum Schutzstatus finden Sie unter "Erläuterungen zum Schutzstatus" im Hilfebereich des SecurityCenter.

Starten des Echtzeit-Virenschutzes

Standardmäßig ist der Echtzeit-Virenschutz eingeschaltet und schützt Ihren Computer vor Viren, Trojanern und anderen Sicherheitsbedrohungen. Wenn Sie den Echtzeit-Virenschutz ausschalten, müssen Sie ihn wieder einschalten, um geschützt zu bleiben.

1. Öffnen Sie den Konfigurationsbereich für "Computer und Dateien".

   Wie?

   1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
   2. Klicken Sie auf **Konfigurieren**.
   3. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

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

Anhalten des Echtzeit-Virenschutzes

Sie können den Echtzeit-Virenschutz vorübergehend ausschalten und dann spezifizieren, wenn er wieder eingeschaltet ist. Sie können den Schutz automatisch nach 15, 30, 45 oder 60 Minuten, bei Neustart des Computers oder gar nicht wieder einstellen.

1 Öffnen Sie den Konfigurationsbereich für "Computer und Dateien".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

2 Klicken Sie unter **Virenschutz** auf **Aus**.

3 Wählen Sie im Dialogfeld, wann der Echtzeit-Scan wieder aufgenommen werden soll.

4 Klicken Sie auf **OK**.

KAPITEL 9

Aktivieren des zusätzlichen Schutzes

Zusätzlich zum Echtzeit-Virenschutz bietet VirusScan erweiterten Schutz gegen Skripts, Spyware und potentiell gefährliche Anhänge von E-Mails und Instant Messaging-Nachrichten. Standardmäßig sind Skriptprüfungen und der Schutz vor Spyware und von E-Mail und Instant Messaging-Nachrichten eingeschaltet und schützen Ihren Computer.

Skriptprüfungen

Die Skriptprüfung erkennt potentiell gefährliche Skripts und verhindert, dass diese auf Ihrem Computer ausgeführt werden. Sie bewacht Ihren Computer bezüglich verdächtiger Skriptaktivitäten, wie z. B. ein Skript, dass Dateien erstellt, kopiert oder löscht oder Ihre Windows-Registrierung öffnet, und warnt Sie, bevor ein Schaden entsteht.

Spyware-Schutz

Spyware-Schutz erkennt Spyware, Adware und andere potentiell unerwünschte Programme. Spyware ist Software, die unbemerkt auf Ihrem Computer installiert wird, um Ihr Verhalten zu beobachten, persönliche Informationen zu sammeln oder sogar um in die Steuerung Ihres Computers einzugreifen, indem zusätzliche Software installiert wird oder Ihr Browser umgeleitet wird.

E-Mail-Schutz

Der E-Mail-Schutz erkennt verdächtige Aktivitäten in den E-Mails und Anhängen, die Sie senden und empfangen.

Instant Messaging-Schutz

Der Instant Messaging-Schutz erkennt Sicherheitsbedrohungen von Instant Messaging-Nachrichten, die Sie erhalten. Er verhindert auch die Herausgabe von persönlichen Informationen durch Instant Messaging-Programme.

In diesem Kapitel

Skriptprüfungen starten

Schalten Sie die Skriptprüfung ein, um potentiell gefährliche Skripts zu erkennen und zu verhindern, dass diese auf Ihrem Computer ausgeführt werden. Die Skriptprüfung warnt Sie, wenn ein Skript versucht, auf Ihrem Computer Dateien zu erstellen, zu kopieren oder zu löschen oder Veränderungen in Ihrer Windows-Registrierung vorzunehmen.

1 Öffnen Sie den Konfigurationsbereich für "Computer und Dateien".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

2 Klicken Sie unter **Skriptprüfung** auf **Ein**.

Hinweis: Obwohl Sie die Skriptprüfung jederzeit ausschalten können, ist Ihr Computer dadurch nicht mehr vor gefährlichen Skripts geschützt.

Spyware-Schutz starten

Stellen Sie den Spyware-Schutz ein, um Spyware, Adware und andere potentiell unerwünschte Programme, die Ihre Daten ohne Ihr Wissen und Ihre Zustimmung sammeln und weiterleiten, zu erkennen.

1 Öffnen Sie den Konfigurationsbereich für "Computer und Dateien".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

2 Klicken Sie unter **Skriptprüfung** auf **Ein**.

Hinweis: Obwohl Sie den Spyware-Schutz jederzeit ausschalten können, ist Ihr Computer dadurch nicht mehr vor potentiell unerwünschten Programmen geschützt.

E-Mail-Schutz starten

Stellen Sie den E-Mail-Schutz ein, um Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen zu erkennen.

1 Öffnen Sie den Konfigurationsbereich für "E-Mail & IM".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.

2 Klicken Sie unter **E-Mail-Schutz** auf **Ein**.

Hinweis: Obwohl Sie den E-Mail-Schutz jederzeit ausschalten können, ist Ihr Computer dadurch nicht mehr vor gefährlichen E-Mail-Bedrohungen geschützt.

Instant Messaging-Schutz starten

Schalten Sie den Instant Messaging-Schutz ein, um Sicherheitsbedrohungen, die in eingehenden Instant Messaging-Anhängen enthalten sein können, zu erkennen.

1 Öffnen Sie den Konfigurationsbereich für "E-Mail & IM".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.

2 Klicken Sie unter **Instant Messaging-Schutz** auf **Ein**.

Hinweis: Obwohl Sie den Instant Messaging-Schutz jederzeit ausschalten können, ist Ihr Computer dadurch nicht mehr vor anfälligen oder gefährlichen Instant Messaging-Anhängen geschützt.

KAPITEL 10

Einrichten des Virenschutzes

VirusScan bietet zwei Arten des Virenschutzes: Echtzeit-Scans und manuelle Scans. Beim Echtzeit-Virenschutz werden alle Dateien überprüft, auf die Sie oder Ihr Computer zugreifen. Mit dem manuellen Virenschutz können Sie Dateien nach Bedarf auf Viren durchsuchen. Sie können für die verschiedenen Schutztypen unterschiedliche Optionen einstellen. Da Ihr Computer mit dem Echtzeit-Schutz permanent überwacht wird, können Sie dafür beispielsweise bestimmte grundlegende Scan-Optionen einstellen und umfassendere Scan-Optionen für die manuellen Scans nach Bedarf reservieren.

In diesem Kapitel

Einstellung der Echtzeit-Scan-Optionen

Wenn Sie den Echtzeit-Virenschutz starten, nutzt VirusScan Standardeinstellungen für die Überprüfung von Dateien. Sie können diese Standardoptionen jedoch nach Ihren Bedürfnissen anpassen.

Um die Optionen für Echtzeit-Scans zu verändern, müssen Sie entscheiden, wonach VirusScan während eines Scans suchen soll, wo danach gesucht werden soll und welche Dateitypen durchsucht werden sollen. Sie können beispielsweise festlegen, ob VirusScan nach unbekannten Viren oder Cookies, die Websites zur Verfolgung Ihres Verhaltens nutzen können, suchen soll und ob Netzlaufwerke, die Ihrem Computer zugeordnet sind, oder nur lokale Laufwerke durchsucht werden sollen. Sie können auch festlegen, welche Dateitypen überprüft werden sollen (alle Dateien oder nur Programmdateien und Dokumente, da dort die meisten Viren erkannt werden).

Wenn Sie die Optionen für Echtzeit-Scans ändern, müssen Sie auch festlegen, ob Pufferüberlaufschutz für Ihren Computer wichtig ist. Ein Puffer ist ein Teil eines Speichers, der dazu genutzt wird, Informationen des Computers kurzzeitig zu speichern. Pufferüberläufe können auftreten, wenn die Menge an Informationen, die verdächtige Programme oder Prozesse in einem Puffer speichern, die Kapazität des Puffers übersteigt. Wenn dies auftritt, wird Ihr Computer anfälliger für Angriffe auf die Sicherheit.

Einstellen der Optionen für Echtzeit-Scans

Die Optionen für Echtzeit-Scans können eingestellt werden, um anzupassen, wonach VirusScan während eines Echtzeit-Scans suchen soll, wo danach gesucht werden soll und welche Dateitypen durchsucht werden sollen. Die Optionen umfassen die Suche nach unbekannten Viren und Verfolgungscookies und die Bereitstellung von Pufferüberlaufschutz. Sie können die Echtzeit-Scans auch so konfigurieren, dass Netzlaufwerke, die Ihrem Computer zugeordnet sind, durchsucht werden.

1 Öffnen Sie das Fenster für Echtzeit-Scans.

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der Virenschutz aktiviert ist, und klicken Sie anschließend auf **Erweitert**.

2 Geben Sie Ihre Optionen für Echtzeit-Scans ein, und klicken Sie auf **OK**.

Ziel	Aktion
Erkennen unbekannter Viren und neuer Variationen bekannter Viren	Aktivieren Sie das Kontrollkästchen **Mithilfe von Heuristik auf unbekannte Viren prüfen**.
Cookies erkennen	Aktivieren Sie das Kontrollkästchen **Nachverfolgungscookies suchen und entfernen**.
Erkennen von Viren und anderen potentiellen Bedrohungen auf Laufwerken, die mit dem Netzwerk verbunden sind	Aktivieren Sie das Kontrollkästchen **Netzlaufwerke überprüfen**.
Schutz des Computers vor Pufferüberläufen	Aktivieren Sie das Kontrollkästchen **Pufferüberlaufschutz aktivieren**.
Geben Sie an, welche Dateitypen geprüft werden sollen.	Klicken Sie auf **Alle Dateien (empfohlen)** oder auf die Option **Nur Programmdateien und Dokumente**.

Festlegen der Optionen für manuelle Scans

Mit dem manuellen Virenschutz können Sie Dateien nach Bedarf auf Viren durchsuchen. Wenn Sie einen manuellen Scan beginnen, untersucht VirusScan unter Verwendung umfassenderer Scan-Optionen Ihren Computer auf Viren und andere potentiell gefährliche Elemente. Um die Optionen für manuelle Scans zu ändern, müssen Sie entscheiden, wonach VirusScan während eines Scans suchen soll. Sie können z. B. festlegen, ob VirusScan nach unbekannten Viren, nach potentiell unerwünschten Programmen, wie Spyware oder Adware, nach Stealth-Programmen, wie z. B. Rootkits, das unerlaubten Zugriff auf Ihren Computer gewähren kann, oder nach Cookies, die Websites zur Verfolgung Ihres Verhaltens nutzen, suchen soll. Sie müssen auch entscheiden, welche Dateitypen untersucht werden sollen. Sie können z. B. festlegen, ob VirusScan alle Dateitypen oder nur Programmdateien und Dokumente (da dort die meisten Viren erkannt werden) durchsuchen soll. Sie können außerdem entscheiden, ob Archivdateien (z. B. ZIP-Dateien) in den Scan mit einbezogen werden sollen.

Standardmäßig durchsucht VirusScan alle Laufwerke und Ordner auf Ihrem Computer bei jedem manuellen Scan. Sie können die Standardeinstellungen jedoch nach Ihren Bedürfnissen verändern. Sie können beispielsweise lediglich kritische Systemdateien, Elemente auf Ihrem Desktop oder Elemente in Ihrem Ordner für Programmdateien durchsuchen lassen. Wenn Sie nicht selbst für die manuellen Scans verantwortlich sein wollen, können Sie einen Zeitplan für regelmäßige Scans einrichten. Geplante Scans durchsuchen Ihren gesamten Computer nach den Standard-Scan-Optionen. Standardmäßig führt VirusScan einmal wöchentlich einen Scan durch.

Falls es zu langsamen Scan-Geschwindigkeiten kommen sollte, können Sie diese Option deaktivieren, um minimale Ressourcen des Computers zu nutzen. Beachten Sie jedoch, dass so dem Virenschutz eine höhere Priorität gegeben wird als anderen Aufgaben.

Hinweis: Wenn Sie gerne Filme sehen, Spiele auf dem Computer spielen oder andere Aktivitäten ausführen, die den gesamten Bildschirm beanspruchen, hält VirusScan verschiedene Tasks an, wie z. B. automatische Updates und manuelle Scans.

Festlegen der Optionen für manuelle Scans

Die Optionen für manuelle Scans können eingestellt werden, um anzupassen, wonach VirusScan während eines manuellen Scans suchen soll, wo danach gesucht werden soll und welche Dateitypen durchsucht werden sollen. Die Optionen umfassen die Suche nach unbekannten Viren, Dateiarchiven, Spyware und potentiell unerwünschten Programmen, Verfolgungscookies, Rootkits und Stealth-Programmen.

1 Öffnen Sie den Bereich "manueller Scan".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der Virenschutz aktiviert ist, und klicken Sie auf **Erweitert**.
5. Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.

2 Geben Sie Ihre Optionen für manuelle Scans ein, und klicken Sie auf **OK**.

Ziel	Aktion
Erkennen unbekannter Viren und neuer Variationen bekannter Viren	Aktivieren Sie das Kontrollkästchen **Mithilfe von Heuristik auf unbekannte Viren prüfen**.
Erkennen und Entfernen von Viren in .zip- und anderen Archivdateien.	Aktivieren Sie das Kontrollkästchen **.zip-Dateien und andere Archivdateien scannen**.
Spyware, Adware und andere potentiell unerwünschte Programme erkennen	Aktivieren Sie das Kontrollkästchen **Auf Spyware und potentiell unerwünschte Programme prüfen**.
Cookies erkennen	Aktivieren Sie das Kontrollkästchen **Nachverfolgungscookies suchen und entfernen**.
Rootkits und Stealth-Programme, die existierende Windows-Systemdateien ändern und ausnutzen können, erkennen	Aktivieren Sie das Kontrollkästchen **Auf Rootkits und andere Stealth-Programme prüfen**.

Weniger Prozessorleistung für Scans nutzen und anderen Tasks (z. B. Surfen im Netz, Öffnen von Dokumenten) höhere Priorität geben	Aktivieren Sie das Kontrollkästchen **Durchsuchen unter Verwendung minimaler Ressourcen**.
Geben Sie an, welche Dateitypen geprüft werden sollen.	Klicken Sie auf **Alle Dateien (empfohlen)** oder auf die Option **Nur Programmdateien und Dokumente**.

Festlegen der Optionen für manuelle Scans

Sie stellen den Ort für den manuellen Scan ein, um festzulegen, wo VirusScan während eines manuellen Scans nach Viren und anderen gefährlichen Elementen sucht. Sie können alle Dateien, Ordner und Laufwerke auf Ihrem Computer durchsuchen oder die Suche auf bestimmte Ordner und Laufwerke begrenzen.

1 Öffnen Sie den Bereich "manueller Scan".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der Virenschutz aktiviert ist, und klicken Sie auf **Erweitert**.
5. Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.

2 Klicken Sie auf **Zu prüfender Standard-Speicherort**.

3 Geben Sie den Ort für manuelle Scans ein, und klicken Sie auf **OK**.

Ziel	Aktion
Überprüfen aller Dateien und Ordner auf Ihrem Computer	Aktivieren Sie das Kontrollkästchen **(Mein) Computer**.
Bestimmte Dateien, Ordner und Laufwerke auf Ihrem Computer durchsuchen	Deaktivieren Sie das Kontrollkästchen **(Mein) Computer**, und wählen Sie einen oder mehrere Ordner oder Laufwerke.

Kritische Systemdateien überprüfen	Deaktivieren Sie das Kontrollkästchen **(Mein) Computer**, und aktivieren Sie das Kontrollkästchen **Kritische Systemdateien**.

Einen Scan planen

Sie können für einen beliebigen Tag der Woche und eine beliebige Zeit einen Scan zur gründlichen Überprüfung Ihres Computers nach Viren und anderen Bedrohungen planen. Geplante Scans durchsuchen Ihren gesamten Computer nach den Standard-Scan-Optionen. Standardmäßig führt VirusScan einmal wöchentlich einen Scan durch. Falls es zu langsamen Scan-Geschwindigkeiten kommen sollte, können Sie diese Option deaktivieren, um minimale Ressourcen des Computers zu nutzen. Beachten Sie jedoch, dass so dem Virenschutz eine höhere Priorität gegeben wird als anderen Aufgaben.

1 Öffnen Sie den Bereich "Geplante Scans".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
   3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
   4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der Virenschutz aktiviert ist, und klicken Sie auf **Erweitert**.
   5. Klicken Sie im Fenster "Virenschutz" auf **Geplanter Scan**.

2 Wählen Sie die Option **Planmäßige Überprüfung aktivieren**.

3 Zur Reduzierung der Prozessorleistung, die normalerweise zur Überprüfung genutzt wird, wählen Sie die Option **Durchsuchen unter Verwendung minimaler Ressourcen**.

4 Wählen Sie einen oder mehrere Tage.

5 Geben Sie eine Startzeit ein.

6 Klicken Sie auf **OK**.

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

Verwenden von SystemGuards-Optionen

SystemGuards überwacht, protokolliert, berichtet über und verwaltet nicht autorisierte Veränderungen in der Window-Registrierung oder in kritischen Systemdateien auf Ihrem Computer. Nicht autorisierte Veränderungen in der Registrierung und Dateien können Ihren Computer schädigen, die Sicherheit gefährden und wichtige Systemdateien beschädigen.

Veränderungen in der Registrierung und in Dateien sind häufig und kommen regelmäßig auf Ihrem Computer vor. Da viele dieser Veränderungen harmlos sind, ist SystemGuards standardmäßig so konfiguriert, dass zuverlässiger, intelligenter und realer Schutz gegen nicht autorisierte Veränderungen, die eine signifikante potentielle Bedrohung darstellen, geboten wird. Wenn SystemGuards beispielsweise Veränderungen, die ungewöhnlich sind und eine potentiell signifikante Bedrohung darstellen, erkennt, wird diese Aktivität sofort berichtet und protokolliert. Veränderungen, die häufiger sind, aber trotzdem eine potentielle Beschädigung darstellen, werden nur protokolliert. Die Überwachung von standardmäßigen und risikoarmen Veränderungen ist jedoch im Standardmodus deaktiviert. Die SystemGuards-Technologie kann so konfiguriert werden, dass der Schutz auf eine beliebige von Ihnen gewünschte Umgebung erweitert wird.

Es gibt drei SystemGuards-Typen: SystemGuards für Programme, Windows SystemGuards und Browser SystemGuards.

SystemGuards für Programme

SystemGuards für Programme erkennt potentiell nicht autorisierte Veränderungen in der Registrierung Ihres Computers und in anderen kritischen Dateien, die von entscheidender Bedeutung für Windows sind. Zu den wichtigen Elementen der Registrierung und Dateien gehören ActiveX-Installationen, Startup-Elemente, Windows Shell Execute Hooks und Shell Service Object Delay Loads. Durch die Überwachung dieser Elemente stoppt die SystemGuards-Technologie für Programme verdächtige ActiveX-Programme (aus dem Internet) sowie Spyware und potentiell unerwünschte Programme, die automatisch beim Start von Windows gestartet werden können.

Windows SystemGuards

Windows SystemGuards erkennt potentiell nicht autorisierte Veränderungen in der Registrierung Ihres Computers und in anderen kritischen Dateien, die von entscheidender Bedeutung für Windows sind. Zu diesen wichtigen Elementen der Registrierung gehören Kontextmenü-Handler, AppInit DLLs und die Windows-Hostdatei. Durch die Überwachung dieser Elemente hilft die Windows SystemGuards-Technologie zu verhindern, dass Ihr Computer nicht autorisierte oder persönliche Informationen über das Internet sendet oder empfängt. So wird auch verhindert, dass verdächtige Programme unerwünschte Veränderungen im Erscheinungsbild und Verhalten der für Sie und Ihre Familie wichtigen Programme vornehmen.

Browser SystemGuards

Ähnlich wie SystemGuards für Programme und Windows SystemGuards erkennt Browser SystemGuards potentiell nicht autorisierte Veränderungen in der Registrierung Ihres Computers und in anderen kritischen Dateien, die von entscheidender Bedeutung für Windows sind. Browser SystemGuards überwacht jedoch Veränderungen bei wichtigen Elementen der Registrierung und Dateien, wie Internet Explorer Add-ons, Internet Explorer-URLs und Internet Explorer-Sicherheitszonen. Durch die Überwachung dieser Elemente hilft die Browser SystemGuards-Technologie dabei, nicht autorisierte Browseraktivitäten, wie die Umleitung zu verdächtigen Websites, Änderungen der Browsereinstellungen und -optionen ohne Ihr Wissen und unerwünschtes Vertrauen in verdächtige Websites, zu verhindern.

Aktivieren des SystemGuards-Schutzes

Aktivieren Sie den SystemGuards-Schutz, um potentiell nicht autorisierte Veränderungen in der Windows-Registrierung und in Dateien auf Ihrem Computer zu erkennen und davor zu warnen. Nicht autorisierte Veränderungen in der Registrierung und Dateien können Ihren Computer schädigen, die Sicherheit gefährden und wichtige Systemdateien beschädigen.

1 Öffnen Sie den Konfigurationsbereich für "Computer und Dateien".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

2 Klicken Sie unter **SystemGuard** auf **Ein**.

Hinweis: Sie können den SystemGuard-Schutz deaktivieren, indem sie auf **Aus** klicken.

Konfigurieren von SystemGuards-Optionen

Nutzen Sie das SystemGuards-Fenster, um die Optionen für den Schutz, Protokollierung und Warnungen vor nicht autorisierten Einträgen in die Registrierung und Dateien in Bezug auf Windows-Dateien, Programme und Internet Explorer zu konfigurieren. Nicht autorisierte Veränderungen in der Registrierung und Dateien können Ihren Computer schädigen, die Sicherheit gefährden und wichtige Systemdateien beschädigen.

1 Öffnen Sie das Fenster "SystemGuards".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der SystemGuard-Schutz aktiviert ist, und klicken Sie auf **Erweitert**.

2 Wählen Sie einen SystemGuards-Typ aus der Liste aus.

- **SystemGuards für Programme**
- **Windows SystemGuards**
- **Browser SystemGuards**

3 Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:

- Klicken Sie auf **Warnungen anzeigen**, um nicht autorisierte Veränderungen in der Registrierung und in Dateien in Bezug auf SystemGuards für Programme, Windows und Browser SystemGuards zu erkennen, zu protokollieren und zu berichten.
- Klicken Sie auf **Änderungen nur protokollieren**, um nicht autorisierte Veränderungen in der Registrierung und in Dateien in Bezug auf SystemGuards für Programme, Windows und Browser SystemGuards zu erkennen und zu protokollieren.

- Klicken Sie auf **SystemGuard deaktivieren**, um die Erkennung von nicht autorisierten Veränderungen in der Registrierung und in Dateien in Bezug auf SystemGuards für Programme, Windows und Browser SystemGuards zu deaktivieren.

Hinweis: Weitere Informationen zu SystemGuards-Typen finden Sie unter Info zu SystemGuards-Typen (Seite 51).

Info zu SystemGuards-Typen

SystemGuards erkennt potentiell nicht autorisierte Veränderungen in der Registrierung Ihres Computers und in anderen kritischen Dateien, die von entscheidender Bedeutung für Windows sind. Es gibt drei SystemGuards-Typen: SystemGuards für Programme, Windows SystemGuards und Browser SystemGuards

SystemGuards für Programme

Die SystemGuards-Technologie für Programme stoppt verdächtige ActiveX-Programme (aus dem Internet) sowie Spyware und potentiell unerwünschte Programme, die automatisch beim Start von Windows gestartet werden können.

SystemGuard	Erkennt...
ActiveX-Installationen	Nicht autorisierte Veränderungen der Registrierung von ActiveX-Installationen, die Ihren Computer schädigen, die Sicherheit gefährden und wichtige Systemdateien beschädigen können.
Startelemente	Spyware, Adware und andere potentiell unerwünschte Programme, die Dateiänderungen für Startup-Elemente installieren können, wodurch beim Start Ihres Computers verdächtige Programme ausgeführt werden können.
Windows Shell Execute Hooks	Spyware, Adware oder andere potentiell unerwünschte Programme, die Windows Shell Execute Hooks installieren können, um das korrekte Ausführen von Sicherheitsprogrammen zu verhindern.
Shell Service Object Delay Load	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen der Registrierung für die Shell Service Object Delay Load vornehmen können, wodurch beim Start Ihres Computers gefährliche Dateien geöffnet werden können.

Windows SystemGuards

Die Windows SystemGuards-Technologie hilft zu verhindern, dass Ihr Computer nicht autorisierte oder persönliche Informationen über das Internet sendet oder empfängt. So wird auch verhindert, dass verdächtige Programme unerwünschte Veränderungen im Erscheinungsbild und Verhalten der für Sie und Ihre Familie wichtigen Programme vornehmen.

SystemGuard	Erkennt...
Kontextmenü-Handler	Nicht autorisierte Veränderungen bei Windows Kontextmenü-Handlern, die das Erscheinungsbild und das Verhalten von Windows-Menüs beeinflussen können. Kontextmenüs ermöglichen bestimmte Aktionen auf Ihrem Computer, wie z. B. das Klicken mit der rechten Maustaste auf Dateien.
AppInit DLLs	Nicht autorisierte Veränderungen in Windows AppInit DLLs, wodurch beim Start Ihres Computers möglicherweise potentiell gefährliche Dateien geöffnet werden.
Windows-Hostdatei	Spyware, Adware und potentiell unerwünschte Programme, die nicht autorisierte Veränderungen in Ihrer Windows-Hostdatei vornehmen können, wodurch Ihr Browser auf verdächtige Websites umgeleitet werden kann und Software-Updates blockiert werden können.
Winlogon-Shell	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Winlogon-Shell vornehmen können, wodurch Windows Explorer durch andere Programme ersetzt werden kann.
Winlogon User Init	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Winlogon User Init vornehmen können, wodurch beim Einloggen bei Windows verdächtige Programme ausgeführt werden können.
Windows-Protokolle	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Windows-Protokolle vornehmen können, wodurch die Art und Weise, mit der Ihr Computer Informationen über das Internet sendet und empfängt, beinflusst wird.
Winsock Layered Service Provider	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Winsock Layered Service Providers (LSPs) installieren können, um Informationen, die über das Internet gesendet und empfangen werden, abzufangen und zu verändern.

Windows Shell Open Commands	Nicht autorisierte Änderungen bei Windows Shell Open Commands, wodurch Würmer und andere gefährliche Programme auf Ihrem Computer gestartet werden können.
Shared Task Scheduler	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Registrierung und in Dateien für den Shared Task Scheduler vornehmen können, wodurch beim Start Ihres Computers potentiell gefährliche Dateien geöffnet werden können.
Windows Messenger-Dienst	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für den Windows Messenger-Dienst vornehmen können, wodurch unerwünschte Werbung und ferngesteuerte Programme auf Ihren Computer gelangen können.
Windows-Datei "Win.ini"	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Windows-Datei "Win.ini" vornehmen können, wodurch beim Start Ihres Computers verdächtige Programme ausgeführt werden können.

Browser SystemGuards

Die Browser SystemGuards-Technologie hilft dabei, nicht autorisierte Browseraktivitäten, wie die Umleitung zu verdächtigen Websites, Änderungen der Browsereinstellungen und -optionen ohne Ihr Wissen und unerwünschtes Vertrauen in verdächtige Websites, zu verhindern.

SystemGuard	Erkennt...
Browserhilfsobjekte	Spyware, Adware und andere potentiell unerwünschte Programme, die Browserhilfsobjekte verwenden können, um Browseraktivitäten zu verfolgen und unerwünschte Werbung anzuzeigen.
Internet Explorer-Leisten	Nicht autorisierte Änderungen in der Registrierung für Internet Explorer-Leisten-Programme, wie Suchen und Favoriten, die das Erscheinungsbild und das Verhalten von Internet Explorer beeinflussen können.
Internet Explorer Add-ons	Spyware, Adware und andere potentiell unerwünschte Programme, die Internet Explorer Add-ons installieren können, um Browseraktivitäten zu verfolgen und unerwünschte Werbung anzuzeigen.
Internet Explorer ShellBrowser	Nicht autorisierte Veränderungen bei Internet Explorer ShellBrowser, die das Erscheinungsbild und das Verhalten von Webbrowsern beeinflussen können.

Internet Explorer WebBrowser	Nicht autorisierte Veränderungen bei Internet Explorer WebBrowser, die das Erscheinungsbild und das Verhalten Ihres Browsers beeinflussen können.
Internet Explorer – URL-Suchhooks	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Registrierung von Internet Explorer – URL-Suchhooks vornehmen können, wodurch Ihr Browser beim Surfen auf verdächtige Websites umgeleitet werden kann.
Internet Explorer-URLs	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Internet Explorer-URLs vornehmen können, wodurch Browsereinstellungen beeinflusst werden.
Internet Explorer-Einschränkungen	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Internet Explorer-Einschränkungen vornehmen können, wodurch Browsereinstellungen und -optionen beeinflusst werden.
Internet Explorer-Sicherheitszonen	Spyware, Adware und andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für die Internet Explorer-Sicherheitszonen vornehmen können, wodurch beim Start Ihres Computers potentiell gefährliche Dateien geöffnet werden können.
Internet Explorer – Vertrauenswürdige Sites	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Internet Explorer – Vertrauenswürdige Sites vornehmen können, wodurch Ihr Browser verdächtigen Websites vertrauen könnte.
Internet Explorer-Richtlinie	Spyware, Adware oder andere potentiell unerwünschte Programme, die Änderungen in der Registrierung für Internet Explorer-Richtlinien vornehmen können, die das Erscheinungsbild und das Verhalten Ihres Browsers beeinflussen können.

Verwenden von Listen mit vertrauenswürdigen Elementen

Wenn VirusScan eine Veränderung in Dateien oder in der Registrierung (SystemGuard), einem Programm oder Pufferüberlauf erkennt, werden Sie aufgefordert, diesem zu vertrauen oder es zu entfernen. Wenn Sie dem Element vertrauen und angeben, dass Sie zukünftig keine Benachrichtigungen über dessen Aktivität erhalten möchten, wird das Element der Liste mit vertrauenswürdigen Elementen hinzugefügt, und VirusScan erkennt es nicht mehr und informiert Sie nicht über dessen Aktivität. Wenn Sie ein Element der Liste mit vertrauenswürdigen Elementen hinzugefügt haben, aber entscheiden, dass Sie dessen Aktivität blockieren wollen, können Sie dies tun. Durch das Blockieren wird verhindert, dass das Element aktiv wird oder Änderungen an Ihrem Computer vornimmt, ohne dass Sie jedes Mal informiert werden, wenn der Versuch unternommen wird. Sie können ein Element auch von der Liste vertrauenswürdiger Elemente entfernen. Durch das Entfernen erkennt VirusScan wieder Aktivitäten des Elements.

Verwalten von Listen mit vertrauenswürdigen Elementen

Verwenden Sie das Fenster "Liste mit vertrauenswürdigen Elementen", um Elementen, die zuvor erkannt und der Liste hinzugefügt wurden, zu vertrauen oder sie zu blockieren. Sie können ein Element auch von der Liste vertrauenswürdiger Elemente entfernen, damit VirusScan dieses wieder erkennt.

1 Öffnen Sie das Fenster "Liste mit vertrauenswürdigen Elementen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Computer & Dateien**.
3. Klicken Sie im Bereich für die Informationen zu "Computer & Dateien" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Computer & Dateikonfiguration", dass der Virenschutz aktiviert ist, und klicken Sie auf **Erweitert**.
5. Klicken Sie im Fenster "Virenschutz" auf **Liste mit vertrauenswürdigen Elementen**.

2 Wählen Sie einen der folgenden Listentypen:

- **SystemGuards für Programme**
- **Windows SystemGuards**

- **Browser SystemGuards**
- **Vertrauenswürdige Programme**
- **Vertrauenswürdige Pufferüberläufe**

3 Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:

- Um dem erkannten Element Eingriffe in die Windows-Registrierung oder in kritische Systemdateien auf Ihrem Computer zu erlauben, ohne Sie zu benachrichtigen, klicken Sie auf **Vertrauen**.
- Um zu verhindern, dass das erkannte Element Eingriffe in die Windows-Registrierung oder in kritische Systemdateien auf Ihrem Computer vornimmt, ohne Sie zu benachrichtigen, klicken Sie auf **Blockieren**.
- Um Elemente aus den Listen mit vertrauenswürdigen Elementen zu entfernen, klicken Sie auf **Entfernen**.

4 Klicken Sie auf **OK**.

Hinweis: Weitere Informationen zu den Listentypen finden Sie unter Info zu Typen von Listen mit vertrauenswürdigen Elementen (Seite 57).

Info zu Typen von Listen mit vertrauenswürdigen Elementen

SystemGuards im Bereich der Listen mit vertrauenswürdigen Elementen zeigt zuvor nicht autorisierte Veränderungen in der Registrierung und in Dateien an, die durch VirusScan erkannt wurden, die Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" erlaubt haben. Es gibt fünf Typen von Listen mit vertrauenswürdigen Elementen, die Sie über den Bereich der Listen mit vertrauenswürdigen Elementen verwalten können: SystemGuards für Programme, Windows SystemGuards, Browser SystemGuards, vertrauenswürdige Programme und vertrauenswürdige Pufferüberläufe.

Option	Beschreibung
SystemGuards für Programme	SystemGuards für Programme im Bereich der Liste mit vertrauenswürdigen Elemente repräsentiert zuvor nicht autorisierte Veränderungen in der Registrierung und in Dateien, die durch VirusScan erkannt wurden, die Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" erlaubt haben. SystemGuards für Programme erkennt nicht autorisierte Änderungen in Bezug auf ActiveX-Installationen, Startup-Elemente, Windows Shell Execute Hooks und Shell Service Object Delay Loads. Diese Arten der nicht autorisierten Veränderung in der Registrierung und in Dateien können Ihren Computer schädigen, die Sicherheit gefährden und wichtige Systemdateien beschädigen.
Windows SystemGuards	Windows SystemGuards im Bereich der Liste mit vertrauenswürdigen Elementen repräsentiert zuvor nicht autorisierte Veränderungen in der Registrierung und in Dateien, die durch VirusScan erkannt wurden, die Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" erlaubt haben. Windows SystemGuards erkennt nicht autorisierte Änderungen in der Registrierung und in Dateien in Bezug auf Kontextmenü-Handler, AppInit DLLs, die Windows-Hostdatei, Winlogon Shell, Winsock Layered Service Providers (LSPs) usw. Diese Arten der nicht autorisierten Veränderung in der Registrierung und in Dateien können die Art und Weise, mit der Ihr Computer Informationen über das Internet sendet und empfängt, und das Erscheinungsbild und das Verhalten von Programmen verändern sowie verdächtige Programme auf Ihrem Computer zulassen.

Browser SystemGuards	Browser SystemGuards im Bereich der Liste mit vertrauenswürdigen Elemente repräsentiert zuvor nicht autorisierte Veränderungen in der Registrierung und in Dateien, die durch VirusScan erkannt wurden, die Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" erlaubt haben. Browser SystemGuards erkennt nicht autorisierte Änderungen in der Registrierung und anderes unerwünschtes Verhalten in Bezug auf Browserhilfsobjekte, Internet Explorer Add-ons, Internet Explorer-URLs, Internet Explorer-Sicherheitszonen usw. Diese Arten der nicht autorisierten Änderungen in der Registrierung können zu unerwünschten Browseraktivitäten, wie der Umleitung zu verdächtigen Websites, Änderungen der Browsereinstellungen und -optionen und unerwünschtem Vertrauen verdächtiger Websites führen.
Vertrauenswürdige Programme	Vertrauenswürdige Programme sind potentiell unerwünschte Programme, die durch VirusScan erkannt wurden, denen Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" vertraut haben.
Vertrauenswürdige Pufferüberläufe	Vertrauenswürdige Pufferüberläufe sind potentiell unerwünschte Aktivitäten, die durch VirusScan erkannt wurden, denen Sie jedoch nach einer Warnung oder im Bereich "Prüfergebnisse" vertraut haben. Pufferüberläufe können Ihren Computer und Dateien beschädigen. Pufferüberläufe treten auf, wenn die Menge an Informationen, die verdächtige Programme oder Prozesse in einem Puffer speichern, die Kapazität des Puffers übersteigt.

KAPITEL 11

Überprüfen des Computers

Wenn Sie das SecurityCenter zum ersten Mal starten, beginnt der Echtzeit-Virenschutz von VirusScan, Ihren Computer vor potentiell gefährlichen Viren, Trojanern und anderen Sicherheitsbedrohungen zu schützen. Wenn Sie den Echtzeit-Virenschutz nicht deaktivieren, überwacht VirusScan nach den von Ihnen eingestellten Optionen für die Echtzeit-Scans Ihren Computer permanent bezüglich Virenaktivität und durchsucht Dateien jedes Mal, wenn Sie oder Ihr Computer darauf zugreifen. Um sicherzugehen, dass Ihr Computer vor den neuesten Sicherheitsbedrohungen geschützt bleibt, lassen Sie den Echtzeit-Virenschutz eingeschaltet und richten Sie einen Zeitplan für regelmäßige, umfassendere manuelle Scans ein. Weitere Informationen zu Optionen für Echtzeit- und manuelle Scans finden Sie unter Einstellen des Virenschutzes (Seite 41).

VirusScan bietet eine Reihe detaillierterer Scan-Optionen für den manuellen Virenschutz, wodurch Sie regelmäßig ausführlichere Scans durchführen können. Sie können manuelle Scans vom SecurityCenter aus starten und so nach einem Zeitplan bestimmte Orte durchsuchen. Sie können manuelle Scans aber auch während Sie arbeiten direkt im Windows Explorer ausführen. Scans im SecurityCenter haben den Vorteil, dass Sie die Scan-Optionen sofort ändern können. Scans im Windows Explorer bieten dafür einen bequemen Zugang zur Computersicherheit.

Sie können die Ergebnisse der Überprüfung am Ende einsehen, egal ob Sie die manuellen Scans vom SecurityCenter oder vom Windows Explorer ausführen. Anhand der Ergebnisse können Sie feststellen, ob VirusScan Viren, Trojaner, Spyware, Adware, Cookies und andere potentiell unerwünschte Programme erkennt, repariert oder in Quarantäne verschoben hat. Die Ergebnisse eines Scans können auf verschiedene Art und Weise dargestellt werden. Sie können z. B. eine einfache Zusammenfassung der Ergebnisse oder detaillierte Informationen, wie Infektionsstatus und-typ, betrachten. Außerdem haben Sie die Möglichkeit, allgemeine Scan-Statistiken anzuzeigen.

In diesem Kapitel

Überprüfen Ihres Computers

Sie können einen manuellen Scan entweder vom Menü "Erweitert" oder "Grundlagen" im SecurityCenter aus durchführen. Wenn Sie einen Scan vom Menü "Erweitert" aus durchführen, haben Sie die Möglichkeit, zuvor die Optionen für manuelle Scans zu bestätigen. Wenn Sie einen Scan vom Menü "Grundlagen" aus durchführen, beginnt VirusScan sofort unter Verwendung der eingestellten Scan-Optionen. Sie können einen Scan unter Verwendung der eingestellten Scan-Optionen auch vom Windows Explorer aus durchführen.

- Führen Sie einen der folgenden Vorgänge aus:

  Scannen im SecurityCenter

Ziel	Aktion
Scannen mit vorhandenen Einstellungen	Klicken Sie im Menü "Grundlagen" auf **Scannen**.
Scannen mit veränderten Einstellungen	Klicken Sie im Menü "Erweitert" auf **Scannen**, wählen Sie die zu prüfenden Orte und die Scan-Optionen und klicken Sie anschließend auf **Jetzt Überprüfen**.

  Scannen in Windows Explorer

  1. Öffnen Sie Windows Explorer.
  2. Klicken Sie mit der rechten Maustaste auf ein Laufwerk, einen Ordner oder eine Datei, und klicken Sie dann auf **Scannen**.

Hinweis: Die Ergebnisse der Überprüfung erscheinen in der Warnung "Scan abgeschlossen". Die Ergebnisse beinhalten die Anzahl der geprüften, erkannten, reparierten, in Quarantäne verschobenen und entfernten Elemente. Klicken Sie auf **Scan-Details anzeigen**, um Genaueres über die Scan-Ergebnisse zu erfahren oder um mit den infizierten Elementen zu arbeiten.

Prüfergebnisse anzeigen

Wenn ein manueller Scan beendet ist, können Sie die Ergebnisse betrachten, um festzustellen, was durch die Überprüfung gefunden wurde, und um den gegenwärtigen Schutzstatus Ihres Computers zu analysieren. Anhand der Ergebnisse können Sie feststellen, ob VirusScan Viren, Trojaner, Spyware, Adware, Cookies und andere potentiell unerwünschte Programme erkennt, repariert oder in Quarantäne verschoben hat.

- Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Scannen**, und führen Sie anschließend einen der folgenden Schritte aus...

Ziel	Aktion
Ergebnisse der Überprüfung in der Warnung betrachten	Ergebnisse der Überprüfung in der Warnung "Scan abgeschlossen" betrachten.
Weitere Informationen über die Ergebnisse betrachten	Klicken Sie in der Warnung "Scan abgeschlossen" auf **Scan-Details anzeigen**.
Anzeigen der Kurzzusammenfassung der Ergebnisse eines Scans	Richten Sie den Mauszeiger auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich Ihrer Taskleiste.
Scan-Statistik betrachten	Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich Ihrer Taskleiste.
Details zu erkannten Elementen, Infektionsstatus und -typ betrachten.	Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich Ihrer Taskleiste, und klicken Sie anschließend auf **Ergebnisse anzeigen** im Bereich "Prüfungsfortschritt: manueller Scan".

KAPITEL 12

Arbeiten mit Prüfergebnissen

Wenn VirusScan während der Ausführung eines Echtzeit- oder manuellen Scans eine Sicherheitsbedrohung feststellt, versucht es, die Bedrohung automatisch entsprechend dem Bedrohungstyp zu behandeln. Findet VirusScan beispielsweise Viren, Trojaner oder Verfolgungscookies auf Ihrem Computer, versucht es, die infizierte Datei zu säubern. Ist die Säuberung der Datei nicht möglich, isoliert VirusScan sie.

Bei einigen Sicherheitsbedrohungen ist VirusScan unter Umständen nicht in der Lage, eine Datei erfolgreich zu säubern oder zu isolieren. In diesem Falle fordert VirusScan Sie auf, die Bedrohung zu behandeln. Sie können, je nach Bedrohungstyp, verschiedene Aktionen durchführen. Wenn beispielsweise ein Virus in einer Datei gefunden wird, VirusScan die Datei aber nicht erfolgreich säubern oder isolieren kann, verweigert es den weiteren Zugang. Wenn Verfolgungscookies gefunden werden, VirusScan die Cookies aber nicht erfolgreich entfernen oder isolieren kann, können Sie auswählen, ob Sie sie löschen oder ihnen vertrauen möchten. Wenn potentiell unerwünschte Programme erkannt werden, ergreift VirusScan keine automatischen Maßnahmen, sondern überlässt Ihnen die Entscheidung, ob Sie das Programm isolieren oder ihm vertrauen möchten.

Wenn VirusScan Elemente in Quarantäne verschiebt, verschlüsselt und isoliert es sie in einem Ordner, um zu verhindern, dass die Dateien, Programme oder Cookies Ihren Computer schädigen. Sie können die isolierten Elemente wiederherstellen oder entfernen. In den meisten Fällen können Sie ein isoliertes Cookie löschen, ohne Ihr System zu beeinträchtigen; falls VirusScan jedoch ein Programm isoliert hat, das Sie kennen und benutzen, sollten Sie es wiederherstellen.

In diesem Kapitel

Work with viruses and Trojans

Wenn VirusScan während eines Echtzeit- oder manuellen Scans einen Virus oder Trojaner in einer Datei auf Ihrem Computer erkennt, versucht es, die Datei zu säubern. Ist die Säuberung der Datei nicht möglich, versucht VirusScan, sie zu isolieren. Falls dies ebenfalls nicht gelingt, wird der Zugriff auf die Datei verweigert (nur bei Echtzeit-Scans).

1 Öffnen Sie den Bereich "Scan-Ergebnisse".

Wie?

1. Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich ganz rechts auf Ihrer Taskleiste.
2. Über den Scan-Fortschritt: Bereich "Manueller Scan", klicken Sie auf **Ergebnisse anzeigen**.

2 Klicken sie in der Liste der Scan-Ergebnisse auf **Viren und Trojaner**.

Hinweis: Um mit den Dateien, die VirusScan isoliert hat, zu arbeiten, gehen Sie auf Arbeiten mit isolierten Dateien (Seite 65).

Arbeiten mit potentiell unerwünschten Programmen

Wenn VirusScan während eines Echtzeit- oder manuellen Scans ein potentiell unerwünschtes Programm auf Ihrem Computer erkennt, können sie das Programm entweder entfernen oder ihm vertrauen. Wenn Sie das potentiell unerwünschte Programm entfernen, wird es nicht vollständig aus Ihrem System gelöscht. Stattdessen wird das Programm durch das Entfernen isoliert, damit es Ihren Computer und Ihre Dateien nicht schädigen kann.

1 Öffnen Sie den Bereich "Scan-Ergebnisse".

Wie?

1. Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich ganz rechts auf Ihrer Taskleiste.
2. Über den Scan-Fortschritt: Bereich "Manueller Scan", klicken Sie auf **Ergebnisse anzeigen**.

2 Klicken Sie in der Liste der Scan-Ergebnisse auf **Potentiell unerwünschte Programme.**

3 Wählen Sie ein möglicherweise unerwünschtes Programm aus.

4 Klicken Sie unter **Ich möchte** entweder auf **Entfernen** oder auf **Vertrauen**.

5 Bestätigen Sie die ausgewählte Option.

Arbeiten mit isolierten Dateien

Wenn VirusScan infizierte Dateien isoliert, verschlüsselt und verschiebt es sie anschließend in einen Ordner, um zu verhindern, dass die Dateien Ihren Computer schädigen. Sie können die isolierten Dateien wiederherstellen oder entfernen.

1 Öffnen des Bereichs "Isolierte Dateien".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf **Dateien**.

2 Wählen Sie eine isolierte Datei aus.

3 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Wiederherstellen**, um die infizierte Datei zu reparieren und sie an Ihren ursprünglichen Speicherort auf Ihrem Computer zurückzuverschieben.
- Um die infizierte Datei von Ihrem Computer zu entfernen, klicken Sie auf **Remove**.

4 Klicken Sie zur Bestätigung der ausgewählten Option auf **Ja**.

Tipp: Sie können mehrere Dateien gleichzeitig wiederherstellen oder entfernen.

Arbeiten mit isolierten Programmen und Cookies

Wenn VirusScan potentiell unerwünschte Programme oder Verfolgungscookies isoliert, verschlüsselt und verschiebt es sie anschließend in einen geschützten Ordner, um zu verhindern, dass die Programme oder Cookies Ihren Computer schädigen. Sie können die isolierten Elemente dann wiederherstellen oder entfernen. In den meisten Fällen können Sie ein isoliertes Element löschen, ohne Ihr System zu beeinträchtigen.

1 Öffnen des Bereichs "Isolierte Programme und Verfolgungscookies".

Wie?

1. Klicken Sie im linken Bereich auf das Menü **Erweitert**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf **Programme und Cookies**.

2 Wählen Sie ein isoliertes Programm oder Cookie aus.

3 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Wiederherstellen**, um die infizierte Datei zu reparieren und sie an ihren ursprünglichen Speicherort auf Ihrem Computer zurückzuverschieben.
- Um die infizierte Datei von Ihrem Computer zu entfernen, klicken Sie auf **Entfernen**.

4 Bestätigen Sie den Vorgang, indem Sie auf **Ja** klicken.

Tipp: Sie können mehrere Dateien gleichzeitig wiederherstellen oder entfernen.

KAPITEL 13

McAfee Personal Firewall

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

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

Personal Firewall-Funktionen

Personal Firewall bietet folgende Funktionen:

Standard- und angepasste Sicherheitsstufen

Schützen Sie sich mithilfe der standardmäßigen oder angepassten Einstellungen von Firewall vor Eindringungsversuchen und verdächtigen Aktivitäten.

Echtzeit-Empfehlungen

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

Intelligente Zugriffsverwaltung für Programme

Verwalten Sie den Internetzugriff für Programme über Warnungen und Ereignisprotokolle, und konfigurieren Sie Zugriffsberechtigungen für bestimmte Programme.

Gaming-Schutz

Verhindern Sie, dass Warnungen zu Eindringungsversuchen und verdächtigen Aktivitäten während des Spielens im Vollbildmodus angezeigt werden.

Schutz beim Hochfahren des Computers

Sobald Windows® gestartet wird, schützt Firewall Ihren Computer vor Eindringungsversuchen, unerwünschten Programmen und unerwünschtem Netzwerkverkehr.

Systemdienstanschlüsse steuern

Verwalten Sie offene und geschlossene Systemdienstanschlüsse, die für einige Programme erforderlich sind.

Computerverbindungen verwalten

Lassen Sie Verbindungen zwischen Ihrem und anderen Computern zu, oder blockieren Sie diese.

Integration von HackerWatch-Informationen

Verfolgen Sie weltweite Hacking- und Eindringungsmuster über die HackerWatch-Website, auf der außerdem aktuelle Sicherheitsinformationen zu den Programmen auf Ihrem Computer sowie globale Sicherheitsereignisse und Statistiken zu Internetanschlüssen zur Verfügung gestellt werden.

Firewall sperren

Sperren Sie umgehend den gesamten ein- und ausgehenden Netzwerkverkehr zwischen Ihrem Computer und dem Internet.

Firewall wiederherstellen

Stellen Sie umgehend die ursprünglichen Sicherheitseinstellungen für Firewall wieder her.

Erweiterte Erkennung von Trojanern

Erkennen und blockieren Sie potentiell schädliche Anwendungen wie Trojaner, damit Ihre persönlichen Daten nicht in das Internet gelangen.

Ereignisprotokollierung

Verfolgen Sie den zuletzt registrierten eingehenden und ausgehenden Datenverkehr sowie die zuletzt registrierten Eindringungsversuche.

Internetverkehr überwachen

Zeigen Sie geografische Karten an, mit deren Hilfe Sie weltweit die Quelle von feindlichen Angriffen und feindlichen Datenverkehrs ausfindig machen können. Zudem werden detaillierte Eigentümerinformationen und geografische Daten für Ursprungs-IP-Adressen bereitgestellt. Des Weiteren können Sie ein- und ausgehenden Datenverkehr analysieren sowie die Programmbandbreite und die Programmaktivität überwachen.

Eindringschutz

Schützen Sie Ihre persönlichen Daten vor möglichen Bedrohungen aus dem Internet. Durch die Verwendung Heuristik-ähnlicher Funktionen bietet McAfee eine dritte Sicherheitsstufe, mit deren Hilfe alle Objekte blockiert werden, die Angriffssymptome oder Eigenschaften von Hacker-Angriffen aufweisen.

Detaillierte Datenverkehrsanalyse

Überprüfen Sie 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 ergreifen.

KAPITEL 14

Starten von Firewall

Ihr Computer ist direkt nach der Installation von Firewall vor versuchtem Eindringen und unerwünschtem Internetdatenverkehr geschützt. Darüber hinaus können Sie von Firewall Warnungen erhalten sowie den Zugriff auf eingehende und ausgehende Internetverbindungen bekannter und unbekannter Programme verwalten. Empfehlungen und die Sicherheitsstufe "Vertrauenswürdige Sicherheit" (wobei Programmen nur ausgehender Internetzugriff erlaubt wird) werden automatisch aktiviert.

Sie können Firewall zwar im Bereich "Internet & Netzwerkkonfiguration" deaktivieren, jedoch ist Ihr Computer dann nicht mehr gegen versuchtes Eindringen 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 Standard-Firewall ein.

Hinweis: Öffnen Sie zum Konfigurieren von Firewall den Bereich "Netzwerk- & Internetkonfiguration".

In diesem Kapitel

Aktivieren des Firewall-Schutzes

Das Aktivieren der Firewall schützt Ihren Computer vor versuchtem Eindringen und unerwünschtem Internetdatenverkehr und ermöglicht die Verwaltung eingehender und ausgehender Internetverbindungen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz** auf **Ein**.

Deaktivieren des Firewall-Schutzes

Sie können Firewall deaktivieren, wenn Sie Ihren Computer nicht vor versuchtem Eindringen und unerwünschtem Internetdatenverkehr schützen möchten. Wenn Firewall deaktiviert ist, können Sie die eingehenden und ausgehenden Internetverbindungen nicht verwalten.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Aus**.

KAPITEL 15

Arbeiten mit Warnungen

Firewall unterstützt Sie mit verschiedenen Warnungen bei der Verwaltung Ihrer Sicherheit. Diese Warnungen können in drei grundlegende Typen unterteilt werden:

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Warnungen können auch Empfehlungen dazu enthalten, wie Sie bei angezeigten Warnungen vorgehen sollten oder weitere Informationen zu den auf Ihrem Computer ausgeführten Programmen abrufen können.

In diesem Kapitel

Informationen zu Warnungen

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

Rote Warnungen

Die rote Warnung wird angezeigt, wenn Firewall einen Trojaner auf Ihrem Computer erkennt und dann blockiert. Sie sollten Ihr System in jedem Fall nach weiteren Bedrohungen scannen. 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. Diese Warnung wird bei jeder Sicherheitsstufe angezeigt, außer bei der Sicherheitsstufe "Offen".

Gelbe Warnungen

Der häufigste Warnungstyp ist die gelbe Warnung, in der Sie über von Firewall erkannte Programmaktivitäten oder Netzwerkereignisse informiert werden. Wenn dies auftritt, enthält die Warnung eine Beschreibung der Programmaktivität oder des Netzwerkereignisses und bietet eine oder mehrere Optionen, die Ihr Eingreifen erfordern. Beispielsweise wird die Warnung **Neues Netzwerk gefunden** angezeigt, 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. Wenn die Option "Empfehlungen" aktiviert ist, werden Programme zum Bereich "Programmberechtigungen" hinzugefügt.

Grüne Warnungen

In den meisten Fällen enthalten grüne Warnungen allgemeine Angaben zu einem Ereignis, und es ist kein Eingreifen Ihrerseits erforderlich. Grüne Warnungen sind standardmäßig deaktiviert und treten in der Regel nur dann auf, wenn die Sicherheitsstufen "Standardsicherheit", "Vertrauenswürdige Sicherheit", "Eingeschränkte Sicherheit" und "Stealth" festgelegt sind.

Hilfe für Benutzer

Viele Firewall-Warnungen enthalten zusätzliche 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 den Zugriff für ein Programm zulassen.

KAPITEL 16

Informationswarnungen verwalten

Firewall ermöglicht Ihnen das Anzeigen oder Ausblenden von Informationswarnungen, wenn Eindringungsversuche oder verdächtige Aktivitäten während bestimmter Ereignisse erkannt werden, beispielsweise während ein Spiel im Vollbildmodus angezeigt wird.

In diesem Kapitel

Warnungen während eines Spiels anzeigen

Sie können zulassen, dass Informationswarnungen von Firewall auch während eines Spiels im Vollbildmodus angezeigt werden, wenn Firewall einen Eindringungsversuch oder verdächtige Aktivitäten feststellt.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Warnungen** auf die Option **Erweitert**.
4. Wählen Sie im Bereich "Warnoptionen" die Option **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird** aus.
5. Klicken Sie auf **OK**.

Informationswarnungen verbergen

Sie können verhindern, dass Informationswarnungen von Firewall angezeigt werden, wenn Firewall einen Eindringungsversuch oder verdächtige Aktivitäten feststellt.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Warnungen** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "SecurityCenter-Konfiguration" auf die Option **Informationswarnungen**.
5. Führen Sie im Bereich "Informationswarnungen" einen der folgenden Schritte aus:
   - Wählen Sie **Informationswarnungen nicht anzeigen**, um alle Informationswarnungen auszublenden.
   - Wählen Sie die auszublendende Warnung aus.
6. Klicken Sie auf **OK**.

KAPITEL 17

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 Sicherheitsstufe "Vertrauenswürdige Sicherheit" für Ihren Computer festgelegt, und für Ihre Programme wird der ausgehende Zugriff auf das Internet zugelassen. 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

Mithilfe der Sicherheitsstufen von Firewall können Sie steuern, inwieweit Sie Warnungen verwalten und wie Sie diese behandeln möchten. Diese Warnungen werden angezeigt, wenn unerwünschter Netzwerkverkehr sowie ein- und ausgehende Internetverbindungen erkannt werden. Standardmäßig ist in Firewall die Sicherheitsstufe "Vertrauenswürdige Sicherheit" festgelegt, bei der nur ausgehender Zugriff zulässig ist.

Wenn die Sicherheitsstufe "Vertrauenswürdige Sicherheit" festgelegt und die Option "Empfehlungen" aktiviert ist, können Sie bei gelben Warnungen den eingehenden Zugriff für unbekannte Programme gewähren oder blockieren. Bei bekannten Programmen werden grüne Informationsmeldungen angezeigt, und der Zugriff wird automatisch gewährt. Durch Gewähren des Zugriffs kann ein Programm ausgehende Verbindungen herstellen und unaufgefordert eingehende Verbindungen 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.

In der folgenden Tabelle werden die sechs Sicherheitsstufen von Firewall beschrieben, beginnend mit der restriktivsten:

Stufe	Beschreibung
Verbindung schließen	Alle ein- und ausgehenden Netzwerkverbindungen einschließlich des Zugriffs auf Websites, E-Mails und Sicherheitsupdates werden blockiert. 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.
Stealth	Alle eingehenden Netzwerkverbindungen (mit Ausnahme offener Ports) werden blockiert, und Ihr Computer ist im Internet nicht sichtbar. Wenn ein neues Programm versucht, eine ausgehende Internetverbindung herzustellen, oder Internetverbindungsanforderungen erhält, werden Sie von der Firewall benachrichtigt. Blockierte und hinzugefügte Programme werden im Bereich "Programmberechtigungen" angezeigt.

Eingeschränkte Sicherheit	Wenn ein neues Programm versucht, eine ausgehende Internetverbindung herzustellen, oder Internetverbindungsanforderungen erhält, werden Sie benachrichtigt. Blockierte und hinzugefügte Programme werden im Bereich "Programmberechtigungen" angezeigt. Bei der Sicherheitsstufe "Eingeschränkte Sicherheit" fordert ein Programm nur den Zugriffstyp an, den es zum aktuellen Zeitpunkt benötigt. So wird beispielsweise ausgehender Zugriff 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 im Bereich "Programmberechtigungen" den Vollzugriff für das Programm gewähren.
Standardsicherheit	Eingehende und ausgehende Verbindungen werden überwacht. Wenn ein neues Programm versucht, auf das Internet zuzugreifen, werden Sie benachrichtigt. Blockierte und hinzugefügte Programme werden im Bereich "Programmberechtigungen" angezeigt.
Vertrauenswürdige Sicherheit	Gewährt Programmen entweder eingehenden und ausgehenden Zugriff (Vollzugriff) oder nur ausgehenden Zugriff auf das Internet. Standardmäßig ist die Sicherheitsstufe "Vertrauenswürdige Sicherheit" festgelegt und die Option ausgewählt, bei der nur ausgehender Zugriff für Programme zulässig ist. Wenn einem Programm Vollzugriff gewährt wird, stuft Firewall dieses automatisch als vertrauenswürdig ein und fügt es im Bereich "Programmberechtigungen" der Liste der zulässigen Programme hinzu. Wenn einem Programm nur ausgehender Zugriff gewährt wird, stuft Firewall dieses nur dann als vertrauenswürdig ein, wenn eine ausgehende Internetverbindung hergestellt wird. Eingehende Verbindungen werden nicht automatisch als vertrauenswürdig eingestuft.
Öffnen	Gewährt Zugriff für alle eingehenden und ausgehenden Internetverbindungen.

Im Bereich "Standardwerte für Firewall-Schutz wiederherstellen" können Sie die Sicherheitsstufe umgehend wieder auf "Vertrauenswürdige Sicherheit" zurücksetzen (und so ausschließlich ausgehenden Zugriff gewähren).

Festlegen der Sicherheitsstufe "Verbindung schließen"

Wenn Sie die Firewall-Sicherheitsstufe auf "Verbindung schließen" festlegen, werden sämtliche eingehenden und ausgehenden Internetverbindungen blockiert.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Verbindung schließen** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Stealth"

Sie können die Firewall-Sicherheitsstufe auf "Stealth" festlegen, um alle eingehenden Netzwerkverbindungen (mit Ausnahme offener Ports) zu blockieren, damit Ihr Computer im Internet nicht sichtbar ist.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Stealth** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

Hinweis: Im Stealth-Modus werden Sie von Firewall benachrichtigt, wenn ein neues Programm versucht, eine ausgehende Internetverbindung herzustellen oder eingehende Internetverbindungsanforderungen erhält.

Festlegen der Sicherheitsstufe "Eingeschränkte Sicherheit"

Wenn Sie die Sicherheitsstufe "Eingeschränkte Sicherheit" festlegen, werden Sie informiert, wenn neue Programme versuchen, auf das Internet zuzugreifen oder über eingehende Verbindungen Anfragen erhalten.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Eingeschränkte Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

Hinweis: Im Modus "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" zulassen.

Festlegen der Sicherheitsstufe "Standardsicherheit"

Wenn Sie die Sicherheitsstufe "Standardsicherheit" festlegen, werden eingehende und ausgehende Verbindungen überwacht, und Sie werden benachrichtigt, wenn neue Programme versuchen, auf das Internet zuzugreifen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Standardsicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Vertrauenswürdige Sicherheit"

Sie können die Firewall-Sicherheitsstufe "Vertrauenswürdige Sicherheit" festlegen, um entweder Vollzugriff oder nur ausgehenden Netzwerkzugriff zu gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Vertrauenswürdige Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie uneingeschränkten eingehenden und ausgehenden Netzwerkzugriff gewähren möchten, wählen Sie **Vollzugriff zulassen** aus.
   - Wenn Sie nur ausgehenden Netzwerkzugriff gewähren möchten, wählen Sie **Nur ausgehenden Zugriff zulassen** aus.
5. Klicken Sie auf **OK**.

Hinweis: Bei **Nur ausgehenden Zugriff zulassen** handelt es sich um die Standardoption.

Festlegen der Sicherheitsstufe "Offen"

Wenn Sie die Firewall-Sicherheitsstufe auf "Offen" festlegen, werden sämtliche eingehenden und ausgehenden Internetverbindungen zugelassen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Offen** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

Empfehlungen für Warnungen konfigurieren

Sie können Firewall so konfigurieren, dass bei einer Warnung bezüglich eines Programms, das auf das Internet zuzugreifen versucht, Empfehlungen eingeschlossen, ausgeschlossen oder in der Warnung angezeigt werden. Das Aktivieren der Option "Empfehlungen" unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen.

Wenn die Option "Empfehlungen" aktiviert ist (die Sicherheitsstufe "Vertrauenswürdige Sicherheit" lautet und die Option für ausgehenden Zugriff aktiviert ist), wird der Zugriff für bekannte Programme automatisch von Firewall gewährt oder blockiert. Darüber hinaus wird in der Warnung eine Empfehlung angezeigt, wenn ein potentiell schädliches Programm erkannt wird.

Ist die Option "Empfehlungen" hingegen deaktiviert, wird der Internetzugriff von Firewall nicht automatisch gewährt oder blockiert, und es werden keine erforderlichen Maßnahmen empfohlen.

Wenn für Empfehlungen die Option "Nur Anzeige" festgelegt ist, werden Sie in einer Warnung dazu aufgefordert, den Zugriff zu gewähren oder zu blockieren, erhalten aber eine Empfehlung bezüglich der erforderlichen Maßnahmen.

Empfehlungen aktivieren

Sie können die Option "Empfehlungen" aktivieren, damit Programme von Firewall automatisch zugelassen oder blockiert werden. Darüber hinaus werden Sie benachrichtigt, wenn unbekannte oder potentiell schädliche Programme erkannt werden.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Empfehlungen aktivieren** aus.
4. Klicken Sie auf **OK**.

Empfehlungen deaktivieren

Sie können die Option "Empfehlungen" deaktivieren, damit Programme von Firewall zugelassen oder blockiert werden. Darüber hinaus werden Sie benachrichtigt, wenn unbekannte oder potentiell schädliche Programme erkannt werden. Diese Warnungen schließen jedoch keine Empfehlungen für den Programmzugriff ein. Wenn Firewall ein neues Programm erkennt, das verdächtig erscheint oder bei dem es sich um ein bekanntes schädliches Programm handelt, blockiert Firewall automatisch den Zugriff dieses Programms auf das Internet.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Empfehlungen deaktivieren** aus.
4. Klicken Sie auf **OK**.

Nur Empfehlungen anzeigen

Sie können Empfehlungen anzeigen, damit in Warnungen nur eine Empfehlung für die zu ergreifenden Maßnahmen angezeigt wird und Sie entscheiden können, ob Sie unbekannte oder potentiell schädliche Programme zulassen oder blockieren möchten.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Nur Anzeige** aus.
4. Klicken Sie auf **OK**.

Firewall-Sicherheit optimieren

Die Sicherheit Ihres Computers kann auf viele Arten gefährdet werden. Beispielsweise können einige Programme versuchen, eine Verbindung mit dem Internet herzustellen, bevor Windows® hochgefahren ist. Technisch versierte Anwender können einen trace- oder ping-Befehl an Ihren Computer senden, um festzustellen, ob er an ein Netzwerk angeschlossen ist. Mit Firewall können Sie sich gegen beide Arten des Eindringens schützen, indem Sie einen Schutz beim Hochfahren des Computers aktivieren und ping-Anforderungen blockieren. Der erste Schutzmechanismus blockiert den Zugriff von Programmen auf das Internet beim Hochfahren von Windows. Der zweite Mechanismus blockiert ping-Anforderungen, mit denen andere Benutzer feststellen können, 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 Exploits (Programme oder Scripts, die Sicherheitslücken von Programmen ausnutzen). 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

Sie können Ihren Computer bereits beim Starten von Windows schützen, um neue Programme zu blockieren, die zuvor nicht über Internetzugriff verfügt haben und diesen während des Hochfahrens anfordern. Firewall zeigt die entsprechenden Warnungen für die Programme an, die Internetzugriff angefordert haben, den Sie nun gewähren oder blockieren können. Für diese Option darf Ihre Sicherheitsstufe jedoch nicht auf "Offen" oder "Verbindung schließen" eingestellt sein.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Wählen Sie im Bereich "Sicherheitsstufe" unter **Sicherheitseinstellungen** die Option **Schutz beim Hochfahren aktivieren** aus.
4. Klicken Sie auf **OK**.

Hinweis: Wenn der Schutz beim Hochfahren aktiviert ist, werden keine blockierten Verbindungen und Eindringungsversuche protokolliert.

Einstellungen für Pinganforderungen konfigurieren

Sie können die Erkennung Ihres Computers im Netzwerk durch andere Computerbenutzer erlauben oder verhindern.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. 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 Pinganforderungen zu gestatten.
   - Deaktivieren Sie **ICMP-Pinganforderungen zulassen**, um die Erkennung Ihres Computers im Netzwerk durch das Senden von Pinganforderungen zu verhindern.
4. Klicken Sie auf **OK**.

Erkennung von Eindringungsversuchen konfigurieren

Sie können die Erkennung von Eindringungsversuchen aktivieren, um Ihren Computer vor Angriffen und nicht autorisierten Scans zu schützen. Zu den standardmäßigen Firewall-Einstellungen gehören das automatische Erkennen der am häufigsten auftretenden Eindringungsversuche, wie beispielsweise DoS-Angriffe (Denial of Service) oder Exploits. Sie können die automatische Erkennung jedoch für eine oder mehrere Angriffe oder Scans deaktivieren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Intrusionserkennung**.
4. 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.
5. Klicken Sie auf **OK**.

Statuseinstellungen für den Firewall-Schutz konfigurieren

Sie können Firewall so konfigurieren, dass ignoriert wird, wenn bestimmte Probleme auf Ihrem Computer nicht an das SecurityCenter gemeldet werden.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.
2. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Schutzstatus** auf die Option **Erweitert**.
3. Wählen Sie im Bereich "Ignorierte Probleme" eine oder mehrere der folgenden Optionen aus:
   - **Der Firewall-Schutz ist deaktiviert.**
   - **Die Firewall ist auf die Sicherheitsstufe "Offen" eingestellt.**
   - **Der Firewall-Dienst wird nicht ausgeführt.**
   - **Auf Ihrem Computer ist kein Firewall-Schutz vorhanden.**
   - **Ihre Windows-Firewall ist deaktiviert.**
   - **Auf Ihrem Computer ist keine Firewall für ausgehenden Datenverkehr vorhanden.**
4. Klicken Sie auf **OK**.

Firewall sperren und wiederherstellen

Durch das Sperren wird sämtlicher eingehender und ausgehender Netzwerkdatenverkehr blockiert, um Ihnen das Isolieren und Beheben von Problemen auf Ihrem Computer zu erleichtern.

Firewall sofort sperren

Sie können Firewall sperren, um den gesamten Netzwerkverkehr zwischen Ihrem Computer und dem Internet umgehend zu blockieren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf die Option **Firewall sperren**.
2. Klicken Sie im Bereich "Firewall sperren" auf **Sperren**.
3. Klicken Sie zur Bestätigung auf **Ja**.

Tipp: Sie können Firewall auch sperren, indem Sie mit der rechten Maustaste im Benachrichtigungsbereich ganz rechts auf der Taskleiste auf das Symbol "SecurityCenter" klicken. Klicken Sie anschließend auf **Direkte Links** und dann auf **Firewall sperren**.

Firewall-Sperre sofort aufheben

Sie können die Firewall-Sperre aufheben, um sämtlichen Netzwerkverkehr zwischen Ihrem Computer und dem Internet direkt freizugeben.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Firewall sperren**.
2. Klicken Sie im Bereich "Sperrung aktiviert" auf **Sperre aufheben**.
3. Klicken Sie zur Bestätigung auf **Ja**.

Firewall-Standardeinstellungen wiederherstellen

Sie können die Standard-Sicherheitseinstellungen der Firewall schnell und einfach wiederherstellen. Diese Wiederherstellung bewirkt Folgendes: Festlegung Ihrer Sicherheitsstufe auf "Vertrauenswürdig" und Gewährung nur ausgehenden Netzwerkzugriffs, Aktivierung der Empfehlungen, Wiederherstellung der Liste der Standardprogramme und ihrer Berechtigungen im Bereich "Programmberechtigungen", Entfernung der vertrauenswürdigen und der gesperrten IP-Adressen sowie die Wiederherstellung der Systemdienste, der Ereignisprotokolleinstellungen und der Intrusionserkennung.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Standardwerte für Firewall wiederherstellen**.
2. Klicken Sie im Bereich "Standardwerte für Firewall-Schutz wiederherstellen" auf **Standardeinstellungen wiederherstellen**.
3. Klicken Sie zur Bestätigung auf **Ja**.

Tipp: Sie können die Standardeinstellungen der Firewall auch wiederherstellen, indem Sie mit der rechten Maustaste rechts neben der Taskleiste im Benachrichtigungsbereich auf das Symbol "SecurityCenter" klicken. Klicken Sie auf **Direkte Links** und dann auf **Standardwerte für Firewall wiederherstellen**.

KAPITEL 18

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

Die können Programmen vollständigen oder nur ausgehenden Zugriff auch über die Protokolle "Ausgehende Ereignisse" und "Zuletzt aufgetretene Ereignisse" gewähren.

Vollständigen Zugriff für ein Programm gewähren

Sie können einem bestehenden, blockierten Programm auf Ihrem Computer vollständigen eingehenden und ausgehenden Internetzugriff gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Nur ausgehender Zugriff** aus.
5. Klicken Sie unter **Aktion** auf **Zugriff gewähren**.
6. Klicken Sie auf **OK**.

Vollständigen Zugriff für ein neues Programm gewähren

Sie können einem neuen Programm auf Ihrem Computer vollständigen eingehenden und ausgehenden Internetzugriff gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Klicken Sie unter **Programmberechtigungen** auf **Erlaubtes Programm hinzufügen**.
5. Wählen Sie im Dialogfeld **Programm hinzufügen** das Programm aus, das Sie hinzufügen möchten, und klicken Sie dann auf **Öffnen**.

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**.

Vollständigen Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" gewähren

Sie können einem gesperrten Programm, das im Protokoll "Zuletzt aufgetretene Ereignisse" angezeigt wird, vollständigen Zugriff auf eingehende und ausgehende Internetverbindungen gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** die Ereignisbeschreibung aus, und klicken Sie dann auf **Zugriff gewähren**.
4. Klicken Sie im Dialogfeld "Programmberechtigungen" zur Bestätigung auf **Ja**.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 124)

Vollständigen Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Sie können einem gesperrten Programm, das im Protokoll "Ausgehende Ereignisse" angezeigt wird, vollständigen Zugriff auf eingehende und ausgehende Internetverbindungen gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
4. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Ausgehende Ereignisse**.
5. Wählen Sie ein Programm aus, und klicken Sie unter **Ich möchte** auf **Zugriff gewähren**.
6. Klicken Sie im Dialogfeld "Programmberechtigungen" zur Bestätigung auf **Ja**.

Gewähren von nur ausgehendem Zugriff für Programme

Einige Programme auf Ihrem Computer benötigen Zugriff auf ausgehende Internetverbindungen. Sie können die Programmberechtigungen in der Firewall so konfigurieren, dass der Zugriff nur auf ausgehende Internetverbindungen gewährt wird.

Ausgehenden Zugriff für ein Programm zulassen

Sie können für ein Programm ausgehenden Internetzugriff zulassen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Vollständig** aus.
5. Klicken Sie unter **Aktion** auf **Nur ausgehenden Zugriff gewähren**.
6. Klicken Sie auf **OK**.

Nur ausgehenden Zugriff über das Protokoll "Zuletzt aufgetretene Ereignisse" zulassen

Sie können für ein vorhandenes, blockiertes Programm, das im Protokoll "Zuletzt aufgetretene Ereignisse" aufgeführt ist, nur ausgehenden Internetzugriff zulassen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** eine Ereignisbeschreibung aus, und klicken Sie dann auf **Nur ausgehenden Zugriff gewähren**.
4. Klicken Sie im Dialogfeld "Programmberechtigungen" zur Bestätigung auf **Ja**.

Nur ausgehenden Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Sie können einem gesperrten Programm, das im Protokoll "Ausgehende Ereignisse" angezeigt wird, Zugriff nur auf ausgehende Internetverbindungen gewähren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
4. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Ausgehende Ereignisse**.
5. Wählen Sie ein Programm aus, und klicken Sie unter **Ich möchte** auf **Nur ausgehenden Zugriff gewähren**.
6. Klicken Sie im Dialogfeld "Programmberechtigungen" zur Bestätigung auf **Ja**.

Internetzugriff für Programme blockieren

Sie können für bestimmte Programme den Zugriff auf das Internet sperren. Das Blockieren des Internetzugriffs für ein Programm beeinträchtigt weder Ihre Netzwerkverbindung noch andere Programme, die eine Internetverbindung für die ordnungsgemäße Funktion benötigen.

Zugriff für ein Programm sperren

Sie können die Berechtigung für eingehenden und ausgehenden Internetzugriff für ein Programm sperren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Vollzugriff** oder **Nur ausgehender Zugriff** aus.
5. Klicken Sie unter **Aktion** auf **Zugriff blockieren**.
6. Klicken Sie auf **OK**.

Zugriff für ein neues Programm sperren

Sie können für ein neues Programm den Zugriff auf eingehende und ausgehende Internetverbindungen sperren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Klicken Sie unter **Programmberechtigungen** auf **Blockiertes Programm hinzufügen**.
5. Suchen Sie im Dialogfeld "Programm hinzufügen" das gewünschte Programm, wählen Sie es aus, und klicken Sie dann auf **Öffnen**.

Hinweis: Sie können die Berechtigungen eines neu hinzugefügten Programms ändern. Wählen Sie hierzu das Programm aus, und klicken Sie dann unter **Aktion** auf **Nur ausgehenden Zugriff gewähren** oder **Zugriff gewähren**.

Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" blockieren

Sie können den eingehenden und ausgehenden Internetzugriff für ein Programm sperren, dass im Protokoll "Zuletzt aufgetretene Ereignisse" aufgeführt ist.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** eine Ereignisbeschreibung aus, und klicken Sie dann auf **Zugriff blockieren**.
4. Klicken Sie im Dialogfeld "Programmberechtigungen" zur Bestätigung auf **Ja**.

Zugriffsberechtigungen für Programme entfernen

Bevor Sie eine Berechtigung 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

Sie können die Berechtigung für eingehenden und ausgehenden Internetzugriff für ein Programm entfernen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
5. Klicken Sie unter **Aktion** auf **Programmberechtigung entfernen**.
6. Klicken Sie auf **OK**.

Hinweis: Firewall verhindert durch Abblenden und Deaktivieren einiger Aktionen, 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 abrufen

Um zu entscheiden, ob der Zugriff auf eingehende und ausgehende Internetverbindungen gewährt oder gesperrt werden soll, können Sie auf der Hackerwatch-Website von McAfee Programminformationen abrufen.

Hinweis: Stellen Sie sicher, dass eine Internetverbindung besteht, sodass Ihr Browser die Hackerwatch-Website von McAfee aufrufen kann. Auf dieser Website finden Sie aktuelle Informationen zu Programmen, Internetzugriffanforderungen und Sicherheitsrisiken.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
4. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
5. Klicken Sie unter **Aktion** auf **Weitere Informationen**.

Weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" abrufen

Um zu entscheiden, ob der Zugriff auf eingehende und ausgehende Internetverbindungen gewährt oder gesperrt werden soll, können Sie vom Protokoll "Ausgehende Ereignisse" aus auf der Hackerwatch-Website von McAfee Programminformationen abrufen.

Hinweis: Stellen Sie sicher, dass eine Internetverbindung besteht, sodass Ihr Browser die Hackerwatch-Website von McAfee aufrufen kann. Auf dieser Website finden Sie aktuelle Informationen zu Programmen, Internetzugriffanforderungen und Sicherheitsrisiken.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" ein Ereignis aus, und klicken Sie dann auf **Protokoll anzeigen**.
4. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Ausgehende Ereignisse**.
5. Wählen Sie eine IP-Adresse aus, und klicken Sie dann auf **Weitere Informationen**.

KAPITEL 19

Systemdienste verwalten

Einige Programme, beispielsweise Webserver oder Serverprogramme 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.

In diesem Kapitel

Systemdienstports konfigurieren

Sie können die Systemdienstports so konfigurieren, dass der Remote-Netzwerkzugriff auf einen Dienst auf Ihrem Computer gewährt oder gesperrt wird.

In der folgenden Liste werden die allgemeinen Systemdienste und die dazugehörigen Ports angezeigt:

- 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
- Netzwerkzeitprotokoll Port 123
- Remotedesktop / 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

Sie können die Systemdienstports auch so konfigurieren, dass ein Computer seine Internetverbindungen für andere Computer, die mit ihm über dasselbe Netzwerk verbunden sind, freigibt. Durch diese Verbindung, die als "Gemeinsame Nutzung der Internetverbindung (ICS)" bezeichnet wird, kann der freigebende Computer für die anderen Netzwerkcomputer als Schnittstelle zum Internet fungieren.

Hinweis: Wenn Ihr Computer über eine Anwendung verfügt, die entweder Web- oder FTP-Serververbindungen akzeptiert, muss auf dem freigebenden Computer möglicherweise der dazugehörige Systemdienstport geöffnet und die Weiterleitung eingehender Verbindungen für diese Ports erlaubt werden.

Zugriff auf einen vorhandenen Systemdienstport gewähren

Sie können einen vorhandenen Port öffnen, um Remote-Zugriff auf einen Netzwerkdienst auf Ihrem Computer zu erlauben.

Hinweis: Ein offener Systemdienstport kann für Ihren Computer ein Sicherheitsrisiko gegen Bedrohungen aus dem Internet darstellen. Öffnen Sie einen Port daher nur, wenn dies erforderlich ist.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
4. Wählen Sie unter **Offener Systemdienstport** einen Systemdienst aus, um den zugehörigen Port zu öffnen.
5. Klicken Sie auf **OK**.

Zugriff auf einen vorhandenen Systemdienstport sperren

Sie können einen vorhandenen Port schließen, um Remote-Netzwerkzugriff auf einen Dienst auf Ihrem Computer zu blockieren.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
4. Deaktivieren Sie unter **Offener Systemdienstport** einen Systemdienst, um einen zugehörigen Port zu schließen.
5. Klicken Sie auf **OK**.

Neuen Systemdienstport konfigurieren

Sie können auf Ihrem Computer einen neuen Netzwerkdienstport konfigurieren, mit dem Sie durch Öffnen oder Schließen des Ports Remote-Zugriff auf Ihren Computer gewähren oder sperren können.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie im Bereich "Systemdienste" unter **Ports und Systemdienste** Folgendes ein:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
6. Wenn Sie die Aktivitätsdaten für diesen Port an einen anderen Windows-Computer im Netzwerk senden möchten, der dieselbe Internetverbindung nutzt, wählen Sie **Netzwerkaktivitäten an diesem Port an Netzwerkbenutzer weiterleiten, die die "Gemeinsame Nutzung der Internetverbindung (ICS)" nutzen**.
7. Geben Sie optional eine Beschreibung für die neue Konfiguration ein.
8. Klicken Sie auf **OK**.

Hinweis: Wenn Ihr Computer über eine Anwendung verfügt, die entweder Web- oder FTP-Serververbindungen akzeptiert, muss auf dem freigebenden Computer möglicherweise der dazugehörige Systemdienstport geöffnet und die Weiterleitung eingehender Verbindungen für diese Ports erlaubt werden. Wenn Sie "Gemeinsame Nutzung der Internetverbindung (ICS)" verwenden, müssen Sie außerdem zur Liste der vertrauenswürdigen IP-Adressen eine vertrauenswürdige Computerverbindung hinzufügen. Weitere Informationen finden Sie unter "Vertrauenswürdige Computerverbindung hinzufügen".

Systemdienstport bearbeiten

Sie können die Informationen über eingehenden und ausgehenden Netzwerkzugriff für vorhandene Systemdienstports ändern.

Hinweis: Wenn die Portinformationen falsch eingegeben werden, funktioniert der Systemdienst nicht ordnungsgemäß.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
4. Wählen Sie einen Systemdienst aus, und klicken Sie dann auf **Bearbeiten**.
5. Geben Sie im Bereich "Systemdienste" unter **Ports und Systemdienste** Folgendes ein:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
6. Wenn Sie die Aktivitätsdaten für diesen Port an einen anderen Windows-Computer im Netzwerk senden möchten, der dieselbe Internetverbindung nutzt, wählen Sie **Netzwerkaktivitäten an diesem Port an Netzwerkbenutzer weiterleiten, die die "Gemeinsame Nutzung der Internetverbindung (ICS)" nutzen**.
7. Geben Sie optional eine Beschreibung für die geänderte Konfiguration ein.
8. Klicken Sie auf **OK**.

Systemdienstport entfernen

Sie können einen vorhandenen Systemdienstport von Ihrem Computer entfernen. Nach dem Entfernen können Remote-Computer nicht mehr auf den Netzwerkdienst auf Ihrem Computer zugreifen.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
4. Wählen Sie einen Systemdienst aus, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie zur Bestätigung auf **Ja**.

KAPITEL 20

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 als vertrauenswürdig eingestufte Computer 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 werden Ereigniswarnungen generiert.

Sie können verhindern, dass Verbindungen von Computern, denen unbekannte, verdächtige oder nicht vertrauenswürdige IP-Adressen zugeordnet sind, zu Ihrem Computer hergestellt werden.

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 ein von einem gesperrten Computer stammendes Ereignis erkannt wird.

In diesem Kapitel

Vertrauenswürdige Computerverbindungen

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

Mithilfe der Liste **Vertrauenswürdige IP-Adressen** im Bereich "Vertrauenswürdige und gesperrte IP-Adressen" können Sie den Datenverkehr von einem bestimmten Computer zu Ihrem Computer zulassen. Für IP-Adressen, die in der Liste **Vertrauenswürdige IP-Adressen** angezeigt werden, wird von Firewall weder Datenverkehr protokolliert noch werden Ereigniswarnungen generiert.

Firewall vertraut allen geprüften IP-Adressen in der Liste und lässt Datenverkehr, der von diesen IP-Adressen stammt, über alle Ports zu. Aktivitäten zwischen Computern, denen eine vertrauenswürdige IP Adresse zugeordnet ist, und Ihrem Computer werden von Firewall weder gefiltert noch analysiert. In "Vertrauenswürdige IP-Adressen" wird standardmäßig das erste private Netzwerk aufgeführt, das Firewall findet.

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der als vertrauenswürdig eingestufte Computer 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.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
4. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen** aus, und klicken Sie dann auf **Hinzufügen**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie **Einzelne IP-Adresse** aus, und geben Sie dann die IP-Adresse ein.

- Wählen Sie **IP-Adressbereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein.

6 Wenn ein Systemdienst "Gemeinsame Nutzung der Internetverbindung (ICS)" verwendet, können Sie den folgenden IP-Adressbereich hinzufügen: 192.168.0.1 bis 192.168.0.255.

7 Aktivieren Sie bei Bedarf die Option **Regel läuft ab in**, und geben Sie die Anzahl von Tagen ein, für die diese Regel gelten soll.

8 Auf Wunsch können Sie eine Beschreibung der Regel eingeben.

9 Klicken Sie auf **OK**.

10 Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** zur Bestätigung auf **Ja**.

Hinweis: Weitere Informationen zu "Gemeinsame Nutzung der Internetverbindung (ICS)" finden Sie unter "Neuen Systemdienst konfigurieren".

Vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzufügen

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

1 Klicken Sie in "McAfee SecurityCenter" im Bereich "Häufige Tasks" auf das Menü **Erweitert**.

2 Klicken Sie auf **Berichte & Protokolle**.

3 Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.

4 Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Eingehende Ereignisse**.

5 Wählen Sie eine Quell-IP-Adresse aus, und klicken Sie unter **Ich möchte** auf **Diese Adresse als vertrauenswürdig einstufen**.

6 Klicken Sie zur Bestätigung auf **Ja**.

Vertrauenswürdige Computerverbindung bearbeiten

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

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
4. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
5. Wählen Sie eine IP-Adresse aus, und klicken Sie dann auf **Bearbeiten**.
6. Führen Sie unter **Vertrauenswürdige IP-Adresse bearbeiten** einen der folgenden Schritte aus:
   - Wählen Sie **Einzelne IP-Adresse** aus, und geben Sie dann die IP-Adresse ein.
   - Wählen Sie **IP-Adressbereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein.
7. Sie können bei Bedarf die Option **Regel läuft ab in** aktivieren und die Anzahl von Tagen eingeben, für die diese Regel gelten soll.
8. Auf Wunsch können Sie eine Beschreibung der Regel eingeben.
9. Klicken Sie auf **OK**.

Hinweis: Die Standard-Computerverbindungen, die von Firewall automatisch von einem vertrauenswürdigen privaten Netzwerk hinzugefügt wurden, können Sie nicht bearbeiten.

Vertrauenswürdige Computerverbindung entfernen

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

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
4. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
5. Wählen Sie eine IP-Adresse aus, und klicken Sie dann auf **Entfernen**.
6. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** zur Bestätigung auf **Ja**.

Sperren von Computerverbindungen

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

Sie können verhindern, dass Verbindungen von Computern, denen unbekannte, verdächtige oder nicht vertrauenswürdige IP-Adressen zugeordnet sind, zu Ihrem Computer hergestellt werden.

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 ein von einem gesperrten Computer stammendes Ereignis erkannt wird.

Gesperrte Computerverbindung hinzufügen

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

Hinweis: Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. den DNS- bzw. DHCP-Server oder andere Server Ihres ISP.

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
4. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus, und klicken Sie dann auf **Hinzufügen**.
5. Führen Sie unter **Regel für gesperrte IP-Adresse hinzufügen** einen der folgenden Schritte aus:
   - Wählen Sie **Einzelne IP-Adresse** aus, und geben Sie dann die IP-Adresse ein.
   - Wählen Sie **IP-Adressbereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein.

6 Aktivieren Sie bei Bedarf die Option **Regel läuft ab in**, und geben Sie die Anzahl von Tagen ein, für die diese Regel gelten soll.

7 Auf Wunsch können Sie eine Beschreibung der Regel eingeben.

8 Klicken Sie auf **OK**.

9 Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** zur Bestätigung auf **Ja**.

Gesperrte Computerverbindung bearbeiten

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

1 Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.

2 Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.

3 Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.

4 Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus, und klicken Sie dann auf **Bearbeiten**.

5 Führen Sie unter **Gesperrte IP-Adresse bearbeiten** einen der folgenden Schritte aus:

- Wählen Sie **Einzelne IP-Adresse** aus, und geben Sie dann die IP-Adresse ein.
- Wählen Sie **IP-Adressbereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein.

6 Aktivieren Sie bei Bedarf die Option **Regel läuft ab in**, und geben Sie die Anzahl von Tagen ein, für die diese Regel gelten soll.

7 Auf Wunsch können Sie eine Beschreibung der Regel eingeben.

8 Klicken Sie auf **OK**.

Gesperrte Computerverbindung entfernen

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

1. Klicken Sie im Bereich "McAfee SecurityCenter" auf **Internet & Netzwerk** und dann auf **Konfigurieren**.
2. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
3. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
4. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
5. Wählen Sie eine IP-Adresse aus, und klicken Sie dann auf **Entfernen**.
6. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** zur Bestätigung auf **Ja**.

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 im Protokoll "Eingehende Ereignisse" angezeigt werden, 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 das Internet 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.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
4. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Eingehende Ereignisse**.
5. Wählen Sie eine Quell-IP-Adresse aus, und klicken Sie unter **Ich möchte** auf **Diese Adresse sperren**.
6. Klicken Sie im Dialogfeld **Regel für gesperrte IP-Adresse hinzufügen** zur Bestätigung auf **Ja**.

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" sperren

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

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf das Menü **Erweitert**.
2. Klicken Sie auf **Berichte & Protokolle**.
3. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
4. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Intrusion Detection-Ereignisse**.
5. Wählen Sie eine Quell-IP-Adresse aus, und klicken Sie unter **Ich möchte** auf **Diese Adresse sperren**.
6. Klicken Sie im Dialogfeld **Regel für gesperrte IP-Adresse hinzufügen** zur Bestätigung auf **Ja**.

KAPITEL 21

Protokollierung, Überwachung und Analyse

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

In diesem Kapitel

Ereignisprotokollierung

Sie können in Firewall die Ereignisprotokollierung aktivieren oder deaktivieren und, bei aktivierter Ereignisprotokollierung, die erfassten Ereignistypen festlegen. Mit der Ereignisprotokollierung können Sie zuletzt aufgetretene ein- und ausgehende Ereignisse sowie versuchtes Eindringen anzeigen.

Ereignisprotokolleinstellungen konfigurieren

Sie können angeben, welche Firewall-Ereignistypen protokolliert werden sollen, und Sie können sie konfigurieren. Standardmäßig ist die Ereignisprotokollierung für alle Ereignisse und Aktivitäten aktiviert.

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Firewall-Schutz aktiviert** auf **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Ereignisprotokolleinstellungen**.
3. Wählen Sie ggf. die Option **Ereignisprotokollierung aktivieren**.
4. Markieren Sie unter **Ereignisprotokollierung aktivieren** die Ereignistypen, die Sie protokollieren möchten, und heben Sie die Markierung bei den Ereignistypen auf, die Sie nicht protokollieren möchten. Die folgenden Typen werden unterstützt:
   - Gesperrte Programme
   - 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. Im Bereich "Zuletzt aufgetretene Ereignisse" werden das Datum und eine Beschreibung des Ereignisses angezeigt. Es werden Aktivitäten der Programme angezeigt, für die der Internetzugriff ausdrücklich gesperrt wurde.

- 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 eingehende Ereignisse anzeigen. Für eingehende Ereignisse werden Datum und Uhrzeit, Quell-IP-Adresse, Hostname und -informationen sowie der Ereignistyp erfasst.

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

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

Ausgehende Ereignisse anzeigen

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

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

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

Intrusion Detection-Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie versuchtes Eindringen anzeigen. Intrusion Detection-Ereignisse enthalten das Datum und die Uhrzeit des Ereignisses, die Quell-IP-Adresse sowie den Hostnamen und den Typ des Ereignisses.

1. Klicken Sie im Bereich "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**.

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

Arbeit mit Statistiken

Firewall nutzt die Informationen auf der HackerWatch-Sicherheitswebsite von McAfee, um Sie mit Statistiken zu globalen Internet Security-Ereignissen und Portaktivitäten 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.

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. Unter "Event Tracking" werden Statistiken zu Sicherheitsereignissen angezeigt.

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.

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 Port-Ereignisse unter **Recent Port Activity** an.

Verfolgen von Internetverkehr

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 abrufen 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 abrufen. Nach dem Aufrufen von Visual Tracer wird eine Weltkarte mit der wahrscheinlichsten Datenroute zwischen dem Quellcomputer und Ihrem Computer angezeigt.

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 abrufen

Mithilfe von Visual Tracer können Sie die Registrierungsinformationen eines Computers von SecurityCenter abrufen. Die Registrierungsinformationen enthalten den Namen der Domäne, den Namen und die Adresse des Registranten sowie Informationen zum administrativen Kontakt.

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 abrufen

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

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

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

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

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" verfolgen

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

1. Klicken Sie im Bereich "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**.

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.

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

Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse abrufen.

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

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 grafische Darstellung des ein- und ausgehenden Internetdatenverkehrs. 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.

Im Bereich "Datenverkehrsanalyse" können Sie den zuletzt registrierten eingehenden und ausgehenden Internetdatenverkehr sowie die aktuelle, mittlere und maximale Übertragungsrate anzeigen. Darüber hinaus können Sie den Datenverkehr anzeigen, einschließlich des gemessenen Datenverkehrs seit dem Start von 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.

Eingehenden und ausgehenden Datenverkehr analysieren

Das Diagramm "Datenverkehrsanalyse" ist eine numerische und grafische Darstellung des ein- und ausgehenden Internetdatenverkehrs. 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.

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**.

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.

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 eingehende und ausgehende Programmaktivitäten anzeigen, in denen Remote-Computerverbindungen und -ports angezeigt werden.

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 22

Weitere Informationen zu Internet Security

Firewall nutzt die Informationen auf der HackerWatch-Sicherheitswebsite von McAfee, um Ihnen aktuelle Informationen zu Programmen und globalen Internetaktivitäten bereitzustellen. Außerdem bietet Hackerwatch ein HTML-Lernprogramm für Firewall.

In diesem Kapitel

Hackerwatch-Lernprogramm starten

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

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 23

McAfee QuickClean

QuickClean verbessert die Leistung Ihres Computers, indem nicht mehr benötigte Dateien gelöscht werden. Das Programm löscht den Inhalt Ihres Papierkorbs und temporäre Dateien, Verknüpfungen, Fragmente verloren gegangener Dateien, Registrierungsdateien, im Cache gespeicherte Dateien, Cookies, Browser-Verlaufsdateien, versendete und gelöschte E-Mails, kürzlich verwendete Dateien, ActiveX-Dateien und Systemwiederherstellungspunkt-Dateien. QuickClean schützt auch Ihre privaten Dateien mithilfe der McAfee Shredder-Komponente, um Objekte sicher und dauerhaft zu löschen, die vertrauliche, persönliche Informationen wie Ihren Namen und Ihre Adresse enthalten. Informationen zum Vernichten von Dateien finden Sie unter McAfee Shredder.

Das Defragmentierungsprogramm ordnet Dateien und Ordner auf Ihrem Computer, um sicherzustellen, dass sie beim Speichern auf der Festplatte Ihres Computers nicht fragmentiert (in verschiedene Teile aufgeteilt) werden. Durch die regelmäßige Defragmentierung Ihrer Festplatte stellen Sie sicher, dass diese fragmentierten Dateien und Ordner geordnet werden und somit später schneller abgerufen werden können.

Wenn Sie Ihren Computer nicht manuell warten möchten, können Sie QuickClean und das Defragmentierungsprogramm so einrichten, dass sie in gewünschten Abständen automatisch als unabhängige Tasks ausgeführt werden.

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

QuickClean-Funktionen

QuickClean bietet verschiedene Cleaner, die überflüssige Dateien sicher und effizient löschen. Durch das Löschen dieser Dateien erhöhen Sie den freien Platz auf der Festplatte Ihres Computers und verbessern so seine Leistung.

Bereinigen Ihres Computers

QuickClean löscht Dateien, die zu Datenmüll auf Ihrem Computer führen können. Das Programm löscht den Inhalt Ihres Papierkorbs und temporäre Dateien, Verknüpfungen, Fragmente verloren gegangener Dateien, Registrierungsdateien, im Cache gespeicherte Dateien, Cookies, Browser-Verlaufsdateien, versendete und gelöschte E-Mails, kürzlich verwendete Dateien, ActiveX-Dateien und Systemwiederherstellungspunkt-Dateien. QuickClean löscht diese Objekte ohne Auswirkungen auf andere grundlegende Informationen.

Sie können sämtliche QuickClean-Cleaner verwenden, um überflüssige Dateien von Ihrem Computer zu löschen. Die folgende Tabelle beschreibt die QuickClean-Cleaner:

Name	Funktion
Papierkorb-Cleaner	Löscht Dateien aus dem Papierkorb.
Cleaner für temporäre Dateien	Löscht Dateien, die in temporären Ordnern gespeichert sind.
Verknüpfungs-Cleaner	Löscht beschädigte Verknüpfungen und solche, mit denen kein Programm verknüpft ist.
Cleaner für verlorene Dateifragmente	Löscht verlorene Dateifragmente von Ihrem Computer.
Registrierungs-Cleaner	Löscht Windows®-Registrierungsinformationen für Programme, die von Ihrem Computer gelöscht wurden. Die Registrierung ist eine Datenbank, in der Windows die Konfigurationsinformationen speichert. Die Registrierung enthält Profile für jeden PC-Benutzer sowie Informationen zu System-Hardware, installierten Programmen und Eigenschafteneinstellungen. Windows verwendet diese Informationen im laufenden Betrieb ständig.

Cache Cleaner	Entfernt Dateien aus dem Cache, die beim Surfen im Internet gespeichert werden. Diese Dateien werden normalerweise als temporäre Dateien in einem Cache-Ordner gespeichert. Ein Cache-Ordner ist ein temporärer Speicherbereich auf Ihrem Computer. Um die Geschwindigkeit und die Effizienz des Surfens im Internet zu erhöhen, kann Ihr Browser eine Webseite aus seinem Cache abrufen (anstatt von einem Remote-Server), wenn Sie sie das nächste Mal anzeigen möchten.
Cookie Cleaner	Löscht Cookies. Diese Dateien werden normalerweise als temporäre Dateien gespeichert. Ein Cookie ist eine kleine Datei mit Informationen, die normalerweise einen Benutzernamen und das aktuelle Datum und die Uhrzeit umfassen, die auf dem Computer einer Person gespeichert wird, die im Internet surft. Cookies werden hauptsächlich von Websites dazu verwendet, Benutzer zu identifizieren, die sich zuvor auf der Website registriert oder sie besucht haben. Cookies können jedoch auch eine Informationsquelle für Hacker darstellen.
Browser-Verlaufs-Cleaner	Löscht Ihren Browser-Verlauf.
Outlook Express und Outlook E-Mail Cleaner (für gelöschte und gesendete Elemente)	Löscht gesendete und gelöschte E-Mails aus Outlook® und Outlook Express.
Cleaner für zuletzt verwendete Dateien	Löscht kürzlich verwendete Dateien, die mit einem der folgenden Programme erstellt wurden: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

ActiveX-Cleaner	Löscht ActiveX-Steuerelemente. ActiveX ist eine Software-Komponente, mit der Programmen oder Webseiten Funktionen hinzufügen, die integriert und als Bestandteil des Programms oder der Webseite angezeigt werden. Die meisten ActiveX-Steuerelemente sind harmlos, einige können jedoch Informationen von Ihrem Computer sammeln.
Cleaner für Systemwiederherstellungspunkte	Löscht alte Systemwiederherstellungspunkte (außer dem neuesten) von Ihrem Computer. Systemwiederherstellungspunkte werden von Windows erstellt, um sämtliche Änderungen zu markieren, die an Ihrem Computer vorgenommen werden, sodass Sie ihn auf einen vorhergehenden Status zurücksetzen können, falls Probleme auftreten.

Säubern Ihres Computers

Sie können sämtliche QuickClean-Cleaner verwenden, um überflüssige Dateien von Ihrem Computer zu löschen. Nach Abschluss können Sie unter **Zusammenfassung von QuickClean** den Festplattenspeicher anzeigen, der nach dem Säubern erforderlich ist, die gelöschten Dateien und das Datum sowie die Uhrzeit, wann der letzte QuickClean-Vorgang auf Ihrem Computer ausgeführt wurde.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie 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.** Wenn Sie den Cleaner für zuletzt verwendete Dateien auswählen, können Sie auf **Eigenschaften** klicken, um die Dateien auszuwählen oder zu löschen, die kürzlich mit einem der Programme aus der Liste erstellt wurden, und anschließend auf **OK** klicken.
   - 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**.

5 Klicken Sie auf **Weiter**, um den Löschvorgang zu bestätigen.

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 (bis zu 10) an. Klicken Sie anschließend auf **Weiter**. Das Vernichten von Dateien kann ein langwieriger Prozess sein, wenn eine große Menge an Informationen gelöscht werden muss.

7 Wenn einige Dateien oder Elemente während des Säuberns gesperrt wurden, werden Sie möglicherweise dazu aufgefordert, den Computer neu zu starten. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

8 Klicken Sie auf **Fertig stellen**.

Hinweis: Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden. Informationen zum Vernichten von Dateien finden Sie unter McAfee Shredder.

Defragmentieren Ihres Computers

Das Defragmentierungsprogramm ordnet Dateien und Ordner auf Ihrem Computer, um sicherzustellen, dass sie beim Speichern auf der Festplatte Ihres Computers nicht fragmentiert werden. Durch die regelmäßige Defragmentierung Ihrer Festplatte stellen Sie sicher, dass diese fragmentierten Dateien und Ordner für das spätere schnelle Abrufen geordnet werden.

Defragmentieren Ihres Computers

Sie können Ihren Computer defragmentieren, um den Zugriff auf und das Abrufen von Dateien und Ordnern zu verbessern.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie unter **Defragmentierungsprogramm** auf **Analysieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Hinweis: Weitere Informationen zum Defragmentierungsprogramm finden Sie in der Windows-Hilfe.

Planen eines Tasks

Der Taskplaner automatisiert die Häufigkeit, mit der QuickClean oder das Defragmentierungsprogramm auf Ihrem Computer ausgeführt werden. Sie können einen QuickClean-Task beispielsweise so planen, dass Ihr Papierkorb jeden Sonntag um 21.00 Uhr geleert wird. Oder Sie können einen Task für das Defragmentierungsprogramm so planen, dass die Festplatte Ihres Computers jeweils am letzten Tag des Monats defragmentiert wird. Sie können einen Task jederzeit erstellen, bearbeiten oder löschen. Sie müssen an Ihrem Computer angemeldet sein, damit ein geplanter Task ausgeführt wird. Wenn ein Task aus einem beliebigen Grund nicht ausgeführt wird, wird er neu geplant für fünf Minuten, nachdem Sie sich erneut anmelden.

Planen eines QuickClean-Tasks

Sie können einen QuickClean-Task so planen, dass Ihr Computer automatisch mithilfe eines oder mehrerer Cleaner gesäubert wird. Nach Abschluss des Tasks können Sie unter **Zusammenfassung von QuickClean** das Datum und die Uhrzeit anzeigen, für die die nächste Ausführung Ihres Tasks geplant ist.

1. Öffnen Sie den Taskplaner-Bereich.

   Wie?

   1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
   2. Klicken Sie unter **Taskplaner** auf **Start**.

2. Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **McAfee QuickClean**.
3. Geben Sie einen Namen für Ihren Task in das Feld **Aufgabenname** ein und klicken Sie dann auf **Erstellen**.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um die in der Liste ausgewählten Cleaner zu übernehmen.
   - Wählen Sie die gewünschten Cleaner aus und klicken Sie anschließend auf **Weiter**. Wenn Sie den Cleaner für zuletzt verwendete Dateien auswählen, können Sie auf **Eigenschaften** klicken, um die Dateien auszuwählen oder zu löschen, die kürzlich mit einem der Programme aus der Liste erstellt wurden, und anschließend auf **OK** klicken.
   - Klicken Sie auf **Standardwerte wiederherstellen**, um die Standard-Cleaner wiederherzustellen, und klicken Sie anschließend auf **Weiter**.

5 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Zeitplanung**, 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 (bis zu 10) an. Klicken Sie anschließend auf **Zeitplanung**.

6 Wählen Sie im Dialogfeld **Zeitplanung** die Häufigkeit aus, mit der der Task ausgeführt werden soll, und klicken Sie dann auf **OK**.

7 Wenn Sie Änderungen an den Eigenschaften des Cleaners für zuletzt verwendete Dateien vorgenommen haben, werden Sie möglicherweise aufgefordert, Ihren Computer neu zu starten. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

8 Klicken Sie auf **Fertig stellen**.

Hinweis: Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden. Informationen zum Vernichten von Dateien finden Sie unter McAfee Shredder.

Bearbeiten eines QuickClean-Tasks

Sie können einen geplanten QuickClean-Task so bearbeiten, dass andere Cleaner verwendet werden oder dass sich die Häufigkeit ändert, mit der der Task automatisch auf Ihrem Computer ausgeführt wird. Nach Abschluss des Tasks können Sie unter **Zusammenfassung von QuickClean** das Datum und die Uhrzeit anzeigen, für die die nächste Ausführung Ihres Tasks geplant ist.

1 Öffnen Sie den Taskplaner-Bereich.

Wie?

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie unter **Taskplaner** auf **Start**.

2 Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **McAfee QuickClean**.

3 Wählen Sie den Task in der Liste **Vorhandene Aufgabe auswählen** aus und klicken Sie dann auf **Ändern**.

4 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Weiter**, um die für den Task ausgewählten Cleaner zu übernehmen.

- Wählen Sie die gewünschten Cleaner aus und klicken Sie anschließend auf **Weiter**. Wenn Sie den Cleaner für zuletzt verwendete Dateien auswählen, können Sie auf **Eigenschaften** klicken, um die Dateien auszuwählen oder zu löschen, die kürzlich mit einem der Programme aus der Liste erstellt wurden, und anschließend auf **OK** klicken.
- Klicken Sie auf **Standardwerte wiederherstellen**, um die Standard-Cleaner wiederherzustellen, und klicken Sie anschließend auf **Weiter**.

5 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Zeitplanung**, 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 (bis zu 10) an. Klicken Sie anschließend auf **Zeitplanung**.

6 Wählen Sie im Dialogfeld **Zeitplanung** die Häufigkeit aus, mit der der Task ausgeführt werden soll, und klicken Sie dann auf **OK**.

7 Wenn Sie Änderungen an den Eigenschaften des Cleaners für zuletzt verwendete Dateien vorgenommen haben, werden Sie möglicherweise aufgefordert, Ihren Computer neu zu starten. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

8 Klicken Sie auf **Fertig stellen**.

Hinweis: Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden. Informationen zum Vernichten von Dateien finden Sie unter McAfee Shredder.

Löschen eines QuickClean-Tasks

Sie können einen geplanten QuickClean-Task löschen, wenn Sie nicht mehr möchten, dass dieser automatisch ausgeführt wird.

1 Öffnen Sie den Taskplaner-Bereich.

Wie?

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie unter **Taskplaner** auf **Start**.

2 Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **McAfee QuickClean**.

3 Wählen Sie den Task in der Liste **Vorhandene Aufgabe auswählen** aus.

4 Klicken Sie auf **Löschen** und anschließend auf **Ja**, um das Löschen zu bestätigen.

5 Klicken Sie auf **Fertig stellen**.

Planen eines Defragmentierungs-Tasks

Sie können bei einem Defragmentierungs-Task die Häufigkeit planen, mit der die Festplatte Ihres Computers automatisch defragmentiert wird. Nach Abschluss des Tasks können Sie unter **Defragmentierungsprogramm** das Datum und die Uhrzeit anzeigen, für die die nächste Ausführung Ihres Tasks geplant ist.

1 Öffnen Sie den Taskplaner-Bereich.

Wie?

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie unter **Taskplaner** auf **Start**.

2 Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **Defragmentierungsprogramm**.

3 Geben Sie einen Namen für Ihren Task in das Feld **Aufgabenname** ein und klicken Sie dann auf **Erstellen**.

4 Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie auf **Zeitplanung**, um die Standardoption **Defragmentierung auch bei geringem freien Speicherplatz durchführen** zu übernehmen.
- Deaktivieren Sie die Option **Defragmentierung auch bei geringem freien Speicherplatz durchführen** und klicken Sie anschließend auf **Zeitplanung**.

5 Wählen Sie im Dialogfeld **Zeitplanung** die Häufigkeit aus, mit der der Task ausgeführt werden soll, und klicken Sie dann auf **OK**.

6 Klicken Sie auf **Fertig stellen**.

Ändern eines Defragmentierungs-Tasks

Sie können die Häufigkeit ändern, mit der ein geplanter Task für das Defragmentierungsprogramm auf Ihrem Computer ausgeführt wird. Nach Abschluss des Tasks können Sie unter **Defragmentierungsprogramm** das Datum und die Uhrzeit anzeigen, für die die nächste Ausführung Ihres Tasks geplant ist.

1 Öffnen Sie den Taskplaner-Bereich.

   Wie?

   1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
   2. Klicken Sie unter **Taskplaner** auf **Start**.

2 Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **Defragmentierungsprogramm**.

3 Wählen Sie den Task in der Liste **Vorhandene Aufgabe auswählen** aus, und klicken Sie dann auf **Ändern**.

4 Führen Sie einen der folgenden Vorgänge aus:

   - Klicken Sie auf **Zeitplanung**, um die Standardoption **Defragmentierung auch bei geringem freien Speicherplatz durchführen** zu übernehmen.
   - Deaktivieren Sie die Option **Defragmentierung auch bei geringem freien Speicherplatz durchführen** und klicken Sie anschließend auf **Zeitplanung**.

5 Wählen Sie im Dialogfeld **Zeitplanung** die Häufigkeit aus, mit der der Task ausgeführt werden soll, und klicken Sie dann auf **OK**.

6 Klicken Sie auf **Fertig stellen**.

Löschen eines Defragmentierungs-Tasks

Sie können einen geplanten Defragmentierungs-Task löschen, wenn Sie nicht mehr möchten, dass dieser automatisch ausgeführt wird.

1 Öffnen Sie den Taskplaner-Bereich.

   Wie?

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Computer warten**.
2. Klicken Sie unter **Taskplaner** auf **Start**.

2 Klicken Sie in der Liste **Zu planenden Vorgang auswählen** auf **Defragmentierungsprogramm**.

3 Wählen Sie den Task in der Liste **Vorhandene Aufgabe auswählen** aus.

4 Klicken Sie auf **Löschen** und anschließend auf **Ja**, um das Löschen zu bestätigen.

5 Klicken Sie auf **Fertig stellen**.

KAPITEL 24

McAfee Shredder

McAfee Shredder löscht (oder vernichtet) Objekte dauerhaft von der Festplatte Ihres Computers. Sogar wenn Sie Dateien und Ordner manuell löschen, Ihren Papierkorb leeren oder Ihren Ordner mit temporären Internetdateien leeren, können Sie diese Informationen dennoch über die forensischen Tools Ihres Computers wiederherstellen. Auch eine gelöschte Datei kann wiederhergestellt werden, da einige Programme temporäre, verborgene Kopien offener Dateien anlegen. Shredder schützt Ihre Privatsphäre, indem es diese unerwünschten Dateien permanent löscht. Beachten Sie, dass mit Shredder vernichtete Dateien nicht wiederhergestellt werden können.

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

Shredder-Funktionen

Shredder löscht Objekte von der Festplatte Ihres Computers, sodass die damit verknüpften Informationen nicht wiederhergestellt werden können. Das Programm schützt Ihre Privatsphäre, indem es Dateien und Ordner, Objekte in Ihrem Papierkorb und im Ordner für temporäre Internetdateien sowie den gesamten Inhalt Ihrer Computer-Laufwerke, wie wiederbeschreibbare CDs, externe Festplatten und Diskettenlaufwerke, dauerhaft löscht.

Vernichten von Dateien, Ordnern und Datenträgern

Shredder stellt sicher, dass die in den gelöschten Dateien und Ordnern in Ihrem Papierkorb und in Ihrem Ordner für temporäre Internetdateien enthaltenen Informationen nicht wiederhergestellt werden können, nicht einmal mit speziellen Tools. Mit Shredder können Sie angeben, wie viele Male ein Objekt vernichtet werden soll (bis zu 10 Mal). Eine hohe Anzahl an Vernichtungsdurchläufen erhöht Ihre Stufe für die sichere Dateientfernung.

Dateien und Ordner vernichten

Sie können Dateien und Ordner von der Festplatte Ihres Computers löschen, einschließlich Objekte in Ihrem Papierkorb und in Ihrem Ordner mit temporären Internetdateien.

1. Öffnen Sie **Shredder**.

   Wie?

   1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf das Menü **Erweitert**.
   2. Klicken Sie im linken Bereich auf **Extras**.
   3. Klicken Sie auf **Shredder**.

2. Klicken Sie im Bereich "Dateien und Ordner vernichten" unter **Ich möchte** auf **Dateien und Ordner löschen**.
3. Klicken Sie unter **Vernichtungsstufe** auf eine der folgenden Vernichtungsstufen:
   - **Schnell**: Vernichtet das/die ausgewählte(n) Element(e) einmal.
   - **Umfassend**: Vernichtet das/die ausgewählte(n) Element(e) in sieben Durchläufen.
   - **Benutzerdefiniert**: Vernichtet das/die ausgewählte(n) Element(e) in bis zu zehn Durchläufen.
4. Klicken Sie auf **Weiter**.
5. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Liste **Zu vernichtende Datei(en) auswählen** entweder auf **Papierkorbinhalte** oder auf **Temporäre Internetdateien**.
   - Klicken Sie auf **Durchsuchen**, navigieren Sie zu der zu vernichtenden Datei, wählen Sie sie aus, und klicken Sie dann auf **Öffnen**.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie auf **Start**.

8 Wenn Shredder das Vernichten abgeschlossen hat, klicken Sie auf **Fertig**.

Hinweis: Arbeiten Sie nicht an Dateien, bis Shredder diese Aufgabe abgeschlossen hat.

Vernichten gesamter Datenträger

Sie können die gesamten Inhalte eines Laufwerks auf einmal vernichten. Es können auch nur die Inhalte von entfernbaren Laufwerken, wie externen Festplatten, beschreibbaren CDs und Diskettenlaufwerken, vernichtet werden.

1 Öffnen Sie **Shredder**.

   Wie?

   1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf das Menü **Erweitert**.
   2. Klicken Sie im linken Bereich auf **Extras**.
   3. Klicken Sie auf **Shredder**.

2 Klicken Sie im Bereich "Dateien und Ordner vernichten" unter **Ich möchte** auf **Die Daten eines ganzen Datenträgers löschen**.

3 Klicken Sie unter **Vernichtungsstufe** auf eine der folgenden Vernichtungsstufen:

   - **Schnell**: Vernichtet das ausgewählte Laufwerk in einem Durchgang.
   - **Umfassend**: Vernichtet das ausgewählte Laufwerk in sieben Durchläufen.
   - **Benutzerdefiniert**: Vernichtet das ausgewählte Laufwerk in bis zu zehn Durchläufen.

4 Klicken Sie auf **Weiter**.

5 Klicken Sie in der Liste **Datenträger auswählen** auf das Laufwerk, dessen Inhalt Sie vernichten möchten.

6 Klicken Sie auf **Weiter** und dann zur Bestätigung auf **Ja**.

7 Klicken Sie auf **Start**.

8 Wenn Shredder das Vernichten abgeschlossen hat, klicken Sie auf **Fertig**.

Hinweis: Arbeiten Sie nicht an Dateien, bis Shredder diese Aufgabe abgeschlossen hat.

KAPITEL 25

McAfee Network Manager

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

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

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

Network Manager-Funktionen

Der Network Manager bietet die folgenden Funktionen.

Grafische Netzwerkzuordnung

Die Netzwerkzuordnung des Network Managers bietet eine grafische Übersicht über den Schutzstatus der Computer und der Komponenten, aus denen Ihr privates Netzwerk besteht. Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (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 für die Komponenten anzeigen, die in der Netzwerkzuordnung angezeigt werden.

Remote-Verwaltung

Verwenden Sie die Netzwerkübersicht des Network Managers zur Verwaltung des Schutzstatus 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.

Erläuterungen zu den Network Manager-Symbolen

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 SecurityCenter installiert ist
	Steht für einen unverwalteten Computer, der offline ist.
	Steht für einen Computer, der online ist und auf dem SecurityCenter nicht installiert ist, oder für ein unbekanntes Netzwerkgerät.
	Steht für einen Computer, der SecurityCenter ist und auf dem SecurityCenter nicht installiert ist, oder für ein unbekanntes Netzwerkgerät.
	Bedeutet, dass das entsprechende Element geschützt und verbunden ist.
	Bedeutet, dass das entsprechende Element möglicherweise Ihrer Aufmerksamkeit bedarf.
	Bedeutet, dass das entsprechende Element Ihrer sofortigen Aufmerksamkeit bedarf.
	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 26

Einrichten eines verwalteten Netzwerks

Um ein verwaltetes Netzwerk einzurichten, arbeiten Sie mit den Elementen in Ihrer Netzwerkzuordnung und fügen Mitglieder (Computer) zum Netzwerk hinzu. 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 administrativen Berechtigungen gewährt.

Sie können die Details für jede der Komponenten anzeigen, die in der Netzwerkzuordnung angezeigt werden, selbst nachdem Sie Änderungen an Ihrem Netzwerk vorgenommen haben (wenn Sie z. B. einen Computer hinzugefügt haben).

In diesem Kapitel

Arbeiten mit der Netzwerkzuordnung

Jedes Mal, wenn Sie auf einem Computer eine Verbindung zum Netzwerk herstellen, analysiert Network Manager den Status des Netzwerks, um zu ermitteln, ob verwaltete oder unverwaltete Mitglieder vorhanden sind, welche Router-Attribute vorliegen 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 administrativen Berechtigungen. Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, der eine Verbindung zum Netzwerk herstellt und auf dem SecurityCenter installiert ist. Sie können das Netzwerk aber jederzeit umbenennen.

Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (z. B. einen Computer hinzufügen), können Sie die Netzwerkzuordnung an Ihre Bedürfnisse anpassen. So können Sie beispielsweise die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen. Sie können auch Details anzeigen, die den in der Netzwerkzuordnung angezeigten Komponenten zugeordnet sind.

Zugreifen auf die Netzwerkzuordnung

Die Netzwerkzuordnung bietet eine grafische Darstellung des Computers und der Komponenten, die Ihr Home-Netzwerk bilden.

- Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**.

Hinweis: Wenn Sie das erste Mal auf die Netzwerkübersicht zugreifen, werden Sie gefragt, ob Sie die anderen Computer im Netzwerk als vertrauenswürdig einstufen möchten.

Netzwerkzuordnung aktualisieren

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

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**.
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, der eine Verbindung zum Netzwerk herstellt und auf dem SecurityCenter installiert ist. Sie können den Namen bei Bedarf ändern.

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**.
2. Klicken Sie unter **Ich möchte** auf **Netzwerk umbenennen**.
3. Geben Sie im Feld **Netzwerkname** 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 eines Elements in der Netzwerkzuordnung

Standardmäßig werden alle Computer und Komponenten in Ihrem Home-Netzwerk in der Netzwerkzuordnung angezeigt. Wenn Sie 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 in der Netzwerkzuordnung	Klicken Sie in der Netzwerkzuordnung auf ein Element, und klicken Sie anschließend unter **Ich möchte** auf **Dieses Element verbergen**. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
Anzeigen verborgener Elemente in der Netzwerkzuordnung	Klicken Sie unter **Ich möchte** auf **Verborgene Elemente anzeigen**.

Anzeigen von Details zu einem Element

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

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 administrativen Berechtigungen gewährt. Um sicherzustellen, dass sich nur vertrauenswürdige Computer am Netzwerk anmelden, müssen Benutzer des gewährenden und des beitretenden 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 seinen Schutzstatus nicht sichtbar macht, wird er ein unverwaltetes Mitglied des Netzwerks. Unverwaltete Mitglieder im Netzwerk sind normalerweise Gastcomputer, die auf andere Netzwerkfunktionen zugreifen möchten, z. B. Dateien senden oder einen freigegebenen Drucker nutzen.

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. EasyNetwork), wird der Computer nach dem Beitritt auch von diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer in Network Manager zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen zur Bedeutung von vollständigen, administrativen und Gastberechtigungen in anderen McAfee-Netzwerkprogrammen finden Sie in der Dokumentation zu dem jeweiligen Programm.

Anmelden an einem verwalteten Netzwerk

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

1. Stellen Sie sicher, dass im Dialogfeld "Verwaltetes Netzwerk" das Kontrollkästchen **Zulassen, dass jeder Computer im Netzwerk die Sicherheitseinstellungen überwachen kann** aktiviert ist.
2. Klicken Sie auf **Anmelden**.
   Wenn Sie die Einladung annehmen, werden zwei Spielkarten angezeigt.
3. Bestätigen Sie, dass die Spielkarten mit denen auf dem Computer übereinstimmen, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden.
4. Klicken Sie auf **OK**.

Hinweis: Wenn der Computer, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden, nicht die gleichen Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Der Beitritt zum Netzwerk kann für Ihren Computer ein Risiko darstellen. Klicken Sie daher im Dialogfeld "Verwaltetes Netzwerk" auf **Abbrechen**.

Einladen eines Computers, sich am verwalteten Netzwerk anzumelden

Wenn ein Computer dem verwalteten Netzwerk hinzugefügt wird oder ein anderer unverwalteter Computer im Netzwerk vorhanden ist, können Sie diesen Computer einladen, sich am verwalteten Netzwerk anzumelden. Nur Computer mit administrativen Berechtigungen für das Netzwerk können andere Computer zur Anmeldung einladen. Wenn Sie die Einladung senden, können Sie auch die Berechtigungsstufe angeben, die Sie dem anzumeldenden Computer zuweisen möchten.

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.
3. Führen Sie im Dialogfeld "Einladen eines Computers, sich am verwalteten Netzwerk anzumelden" einen der folgenden Schritte aus:
   - Klicken Sie auf **Gastzugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer Zugriff auf das Netzwerk zu gewähren. (Diese Option eignet sich z. B. für Benutzer, die sich vorübergehend bei Ihnen zu Hause aufhalten.)
   - Klicken Sie auf **Vollständigen Zugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer den Zugriff auf das Netzwerk zu erlauben.
   - Klicken Sie auf **Administrativen Zugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer den Zugriff mit administrativen Berechtigungen auf das Netzwerk zu erlauben. Dieser Zugriff erlaubt es dem Computer außerdem, anderen Computern Zugriff zu gewähren, die sich am verwalteten Netzwerk anmelden möchten.

4 Klicken Sie auf **OK**.
Es wird eine Einladung an den Computer gesendet, sich beim verwalteten Netzwerk anzumelden. Wenn der Computer die Einladung annimmt, werden zwei Spielkarten angezeigt.

5 Bestätigen Sie, dass die Spielkarten mit denen auf dem Computer übereinstimmen, den Sie zur Anmeldung am verwalteten Netzwerk eingeladen haben.

6 Klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer, den Sie zur Anmeldung am verwalteten Netzwerk eingeladen haben, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Wenn Sie die Anmeldung des Computers am Netzwerk zulassen, werden andere Computer dadurch möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Sicherheitsbestätigung auf **Zugriff verweigern**.

Vertrauenswürdigkeit von Computern im Netzwerk aufheben

Wenn Sie andere Computer im Netzwerk fälschlicherweise als vertrauenswürdig eingestuft haben, können Sie dies rückgängig machen.

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

Hinweis: Der Link **Computern in diesem Netzwerk nicht mehr vertrauen** ist nicht verfügbar, wenn Sie über administrative Berechtigungen verfügen und sich andere verwaltete Computer im Netzwerk befinden.

KAPITEL 27

Remote-Verwaltung des Netzwerks

Nachdem Sie Ihr verwaltetes Netzwerk eingerichtet haben, können Sie die enthaltenen Computer und Komponenten remote verwalten. Sie können den Status und die Berechtigungsstufen der Computer und Komponenten überwachen und die meisten Sicherheitslücken remote beheben.

In diesem Kapitel

Überwachen von Status und Berechtigungen

Ein verwaltetes Netzwerk umfasst verwaltete und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, bei unverwalteten Mitgliedern ist dies nicht der Fall. Unverwaltete Mitglieder sind normalerweise Gastcomputer, die auf andere Netzwerkfunktionen zugreifen möchten, z. B. Dateien senden oder einen freigegebenen Drucker nutzen. 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 zu einem unverwalteten Computer werden.

Verwaltete Computer können administrative, vollständige oder Gast-Berechtigungen besitzen. 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 Geräte enthalten kann (z. B. Router), können Sie Network Manager auch für die Verwaltung dieser Geräte verwenden. Sie können auch die Anzeigeeigenschaften eines Geräts in der Netzwerkzuordnung konfigurieren und ändern.

Überwachen des Schutzstatus eines Computers

Wenn der Schutzstatus eines Computers nicht im Netzwerk überwacht wird (der Computer ist kein Mitglied oder ein unverwaltetes Mitglied), können Sie eine Überwachung für diesen anfordern.

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 für einen verwalteten Computer in Ihrem Netzwerk stoppen. Der Computer wird dann jedoch unverwaltet, und Sie können dessen Schutzstatus nicht remote überwachen.

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 Bestätigungsdialogfeld auf **Ja**.

Ändern der Berechtigungen eines verwalteten Computers

Sie können die Berechtigungen eines verwalteten Computers jederzeit ändern. Damit ändern Sie, welche Computer den Schutzstatus anderer Computer im Netzwerk überwachen können.

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 entsprechende Kontrollkästchen, um anzugeben, ob dieser Computer und andere Computer im verwalteten Netzwerk gegenseitig 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 auf die zugehörige Verwaltungs-Website zugreifen.

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 im 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 des Geräts zu konfigurieren.

Ändern der Anzeigeeigenschaften eines Geräts

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

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Geräteeigenschaften ändern**.
3. Zum Angeben des Anzeigenamens für das Gerät geben Sie im Feld **Name** einen Namen ein.
4. Zum Angeben des Gerätetyps klicken Sie auf **Standardrouter**, wenn es sich nicht um einen drahtlosen Router handelt, oder auf **Drahtloser Router**, wenn das Gerät drahtlos ist.
5. Klicken Sie auf **OK**.

Beheben von Sicherheitslücken

Verwaltete Computer mit administrativen Berechtigungen können den McAfee-Schutzstatus anderer verwalteter Computer im Netzwerk überwachen und gemeldete Sicherheitslücken remote beheben. Wenn beispielsweise der McAfee-Schutzstatus eines verwalteten Computers angibt, dass VirusScan deaktiviert ist, kann ein anderer verwalteter Computer mit administrativen Berechtigungen VirusScan remote aktivieren.

Wenn Sie Sicherheitslücken remote beheben, repariert Network Manager die meisten gemeldeten Probleme. Einige Sicherheitslücken erfordern jedoch möglicherweise ein manuelles Eingreifen auf dem lokalen Computer. In diesem Fall behebt Network Manager die 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 die empfohlene Lösung, auf dem Remote-Computer bzw. den Remote-Computern im Netzwerk die neueste Version von SecurityCenter zu installieren.

Sicherheitslücken schließen

Mit Network Manager können Sie die meisten Sicherheitslücken auf verwalteten Remote-Computern beheben. Wenn beispielsweise VirusScan auf einem Remote-Computer deaktiviert ist, können Sie es aktivieren.

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: Network Manager schließt die meisten Sicherheitslücken zwar automatisch, dennoch kann es zum Beheben einiger Probleme erforderlich sein, SecurityCenter auf dem betroffenen Computer zu öffnen und die angegebenen Empfehlungen zu befolgen.

Installieren der McAfee-Sicherheits-Software auf Remote-Computern

Wenn auf einem oder mehreren Computern in Ihrem Netzwerk nicht die neueste Version des SecurityCenter ausgeführt wird, kann deren Schutzstatus nicht remote überwacht werden. Wenn Sie diese Computer remote überwachen möchten, müssen Sie auf allen Computern die neueste Version des SecurityCenter installieren.

1. Öffnen Sie SecurityCenter auf dem Computer, auf dem Sie Ihre Sicherheitssoftware installieren möchten.
2. Klicken Sie unter **Häufige Tasks** auf **Mein Konto**.
3. Melden Sie sich mit der E-Mail-Adresse und dem Kennwort an, das Sie bei der ersten Installation der Sicherheitssoftware zur Registrierung verwendet haben.
4. Wählen Sie das entsprechende Produkt aus, klicken Sie auf **Installation/Download**, und befolgen Sie die Anweisungen auf dem Bildschirm.

KAPITEL 28

McAfee EasyNetwork

EasyNetwork ermöglicht die sichere Dateifreigabe, vereinfacht Dateiübertragungen und erleichtert die automatische Druckerfreigabe für die Computer in Ihrem privaten Netzwerk. Für die Nutzung dieser Funktionen muss auf den Computern in Ihrem Netzwerk jedoch EasyNetwork installiert sein.

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

Hinweis: SecurityCenter meldet kritische und nichtkritische Sicherheitsprobleme, sobald diese erkannt wurden. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician ausführen.

In diesem Kapitel

EasyNetwork-Funktionen

EasyNetwork bietet folgende Funktionen:

Dateifreigabe

EasyNetwork vereinfacht die Dateifreigabe für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die über vollen oder administrativen Zugriff auf Ihr verwaltetes Netzwerk verfügen (Mitglieder), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

Dateiübertragung

Sie können Dateien an andere Computer senden, die über vollen oder administrativen Zugriff auf Ihr verwaltetes Netzwerk verfügen (Mitglieder). Wenn Sie eine Datei erhalten, wird diese in Ihrem EasyNetwork-Posteingang angezeigt. Der Posteingang ist ein temporärer Speicherort für alle Dateien, die von anderen Computern im Netzwerk an Sie gesendet werden.

Automatisierte Druckerfreigabe

Wenn Sie Mitglied eines verwalteten Netzwerks werden, können Sie lokale Drucker, die an Ihren Computer angeschlossen sind, für andere Mitglieder freigeben, wobei der aktuelle Name des Druckers als Name der Druckerfreigabe verwendet wird. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht es Ihnen, diese Drucker zu konfigurieren und zu verwenden.

KAPITEL 29

EasyNetwork einrichten

Bevor Sie EasyNetwork verwenden können, müssen Sie das Programm öffnen und sich bei einem verwalteten Netzwerk anmelden. Wenn Sie sich bei einem verwalteten Netzwerk angemeldet haben, können Sie Dateien für andere Computer im Netzwerk freigeben, Dateien auf anderen Computern suchen und Dateien an andere Computer senden. Sie können auch Drucker freigeben. Sie können das Netzwerk jederzeit wieder verlassen.

In diesem Kapitel

EasyNetwork öffnen

Nach der Installation werden Sie standardmäßig aufgefordert, EasyNetwork zu öffnen. Sie können EasyNetwork jedoch auch zu einem späteren Zeitpunkt öffnen.

- Zeigen Sie im Menü **Start** auf **Programme** und dann auf **McAfee**, und klicken Sie anschließend auf **McAfee EasyNetwork**.

Tipp: Wenn Sie während der Installation Desktop- und Schnellstartsymbole erstellt haben, können Sie EasyNetwork auch öffnen, indem Sie auf das McAfee EasyNetwork-Symbol auf dem Desktop oder im Benachrichtigungsbereich ganz rechts in der Taskleiste doppelklicken.

Anmelden an einem verwalteten Netzwerk

Wenn in dem Netzwerk, mit dem Sie verbunden sind, kein anderer Computer über SecurityCenter verfügt, werden Sie zu einem Mitglied dieses Netzwerks und müssen angeben, ob das Netzwerk vertrauenswürdig ist. Da Ihr Computer der erste ist, der sich am Netzwerk anmeldet, wird der Name Ihres Computers als Teil des Netzwerknamens verwendet. Sie können das Netzwerk jedoch jederzeit umbenennen.

Wenn ein Computer eine Verbindung mit dem Netzwerk herstellt, wird an alle anderen Computer im Netzwerk eine Anmeldungsanfrage gesendet. Diese Anfrage kann von jedem Computer genehmigt werden, der über administrative Berechtigungen für das Netzwerk verfügt. Der Computer, der Zugriff gewährt, kann die Berechtigungsstufe für den Computer festlegen, der sich am Netzwerk anmeldet. Die Anmeldung kann beispielsweise als Gast (nur Dateiübertragung) erfolgen oder vollständig/administrativ (Dateiübertragung und Dateifreigabe). In EasyNetwork können Computer mit Administratorzugriff anderen Computern Zugriff gewähren und Berechtigungen verwalten (d. h. Computer mit mehr oder weniger Rechten versehen). Computer mit Vollzugriff können diese administrativen Aufgaben nicht ausführen.

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (beispielsweise Network Manager), wird der Computer nach der Anmeldung auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer in EasyNetwork zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen zur Bedeutung von vollständigen, administrativen und Gastberechtigungen in anderen McAfee-Netzwerkprogrammen finden Sie in der Dokumentation zu dem jeweiligen Programm.

Beitritt zum Netzwerk

Wenn ein Computer zum ersten Mal nach der Installation von EasyNetwork einem vertrauenswürdigen Netzwerk beitritt, wird der Benutzer in einer Meldung 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. Dem ersten Computer im Netzwerk werden automatisch administrative Berechtigungen gewährt.

1 Klicken Sie im Fenster "Freigegebene Dateien" auf **Diesem Netzwerk beitreten**.
Wenn ein administrativer Computer im Netzwerk Ihre Anfrage genehmigt, wird eine Nachricht angezeigt, in der festgelegt werden muss, ob dieser und andere Computer im

Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten dürfen.

2 Wenn dieser und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten sollen, klicken Sie auf **OK**; klicken Sie andernfalls auf **Abbrechen**.

3 Bestätigen Sie, dass der gewährende Computer die Spielkarten anzeigt, die im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, und klicken Sie dann auf **OK**.

Hinweis: Wenn der Computer, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden, nicht die gleichen Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Der Beitritt zum Netzwerk kann für Ihren Computer ein Risiko darstellen. Klicken Sie daher im Dialogfeld für die Sicherheitsbestätigung auf **Abbrechen**.

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 Computer, der als Erster antwortet, wird der Zugriff gewährende Computer. Der Zugriff gewährende Computer entscheidet, welche Art von Zugriff dem Computer gewährt wird: vollständiger, administrativer oder Gast-Zugriff.

1 Klicken Sie in der Meldung auf die gewünschte Zugriffsstufe.

2 Führen Sie im Dialogfeld "Einladen eines Computers, sich am verwalteten Netzwerk anzumelden" einen der folgenden Schritte aus:

- Klicken Sie auf **Gastzugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer Zugriff auf das Netzwerk zu gewähren. (Diese Option eignet sich z. B. für Benutzer, die sich vorübergehend bei Ihnen zu Hause aufhalten.)
- Klicken Sie auf **Vollständigen Zugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer den Zugriff auf das Netzwerk zu erlauben.
- Klicken Sie auf **Administrativen Zugriff auf verwaltete Netzwerkprogramme zulassen**, um dem Computer den Zugriff mit administrativen Berechtigungen auf das Netzwerk zu erlauben. Dieser Zugriff erlaubt es dem Computer außerdem, anderen Computern Zugriff zu gewähren, die sich am verwalteten Netzwerk anmelden möchten.

3 Klicken Sie auf **OK**.

4 Bestätigen Sie, dass der Computer die Spielkarten anzeigt, die im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, und klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer nicht die gleichen Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Das Gewähren des Zugriffs für diesen Computer kann für Ihren Computer ein Risiko darstellen. Klicken Sie daher im Dialogfeld für die Sicherheitsbestätigung auf **Zugriff verweigern**.

Netzwerk umbenennen

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

1. Klicken Sie im Menü **Optionen** auf **Konfigurieren**.
2. Geben Sie im Dialogfeld "Konfigurieren" 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 kein Mitglied dieses Netzwerks sein möchten, können Sie das Netzwerk verlassen. Sie können sich nach dem Verlassen des verwalteten Netzwerks jederzeit wieder anmelden, dazu müssen Ihnen jedoch wieder Berechtigungen gewährt werden. Weitere Informationen zur Anmeldung finden Sie unter Anmelden an einem verwalteten Netzwerk (Seite 178).

Verwaltetes Netzwerk verlassen

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

1. Klicken Sie im Menü **Extras** 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 30

Dateien freigeben und senden

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

Hinweis: Wenn Sie eine hohe Anzahl von Dateien freigeben, kann dies Ihre Computerressourcen beeinträchtigen.

In diesem Kapitel

Freigeben von Dateien

Nur Computer, die Mitglied des verwalteten Netzwerks sind (voller oder Administratorzugriff), 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 diese bzw. dieser aus dem Fenster "Freigegebene Dateien" entfernt. Sie können eine Dateifreigabe jederzeit rückgängig machen.

Zum Zugreifen auf eine freigegebene Datei öffnen Sie die Datei direkt in EasyNetwork, oder kopieren Sie die Datei auf Ihren Computer, und öffnen Sie sie dort. Wenn die Liste der freigegebenen Dateien sehr groß ist und es Schwierigkeiten bereitet, die Datei zu finden, können Sie danach suchen.

Hinweis: Auf Dateien, die über EasyNetwork freigegeben wurden, kann nicht mit Windows-Explorer von anderen Computern aus zugegriffen werden, da die Dateifreigabe von EasyNetwork über sichere Verbindungen ausgeführt werden muss.

Freigabe einer Datei

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

1. Navigieren Sie in Windows-Explorer zu der 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 im Menü **Extras** auf **Dateien freigeben** 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 auf diese Datei zugreifen.

1. Klicken Sie im Menü **Extras** auf **Freigabe von Dateien stoppen**.
2. Wählen Sie im Dialogfeld "Freigabe von Dateien stoppen" die Datei aus, deren Freigabe Sie aufheben möchten.
3. Klicken Sie auf **OK**.

Freigegebene Datei kopieren

Kopieren Sie eine freigegebene Datei, um weiterhin über diese zu verfügen, wenn die Freigabe aufgehoben wird. Sie können eine freigegebene Datei von einem beliebigen Computer im verwalteten Netzwerk kopieren.

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

Tipp: Sie können eine freigegebene Datei auch kopieren, indem Sie die Datei in EasyNetwork auswählen und anschließend im Menü **Extras** 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 die entsprechenden Ergebnisse im Fenster "Freigegebene Dateien" an.

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Suche**.
2. Klicken Sie in der Liste **Enthält** auf die gewünschte Option (Seite 186).
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 den gewünschten Dateityp (Seite 186).
5. Klicken Sie in den Listen **Von** und **Bis** auf die Datumsangaben, die den Datumsbereich festlegen, in dem die Datei erstellt wurde.

Suchkriterien

In den folgenden Tabellen werden die Suchkriterien beschrieben, die Sie beim Suchen nach freigegebenen Dateien angeben können.

Dateiname oder -pfad

Enthält	Beschreibung
Alle Begriffe	Sucht nach einem Datei- oder Pfadnamen, der in beliebiger Reihenfolge alle Wörter enthält, die Sie in der Liste **Datei oder Pfadname** angegeben haben.
Einen beliebigen Begriff	Sucht nach einem Datei- oder Pfadnamen, die eines der Wörter enthält, die Sie in der Liste **Datei oder Pfadname** angegeben haben.
Exakte Zeichenfolge	Sucht nach einem Datei- oder Pfadnamen, der den exakten Ausdruck enthält, den Sie in der Liste **Datei oder Pfadname** angegeben haben.

Dateityp

Typ	Beschreibung
Beliebig	Sucht nach allen freigegebenen Dateitypen.
Dokument	Sucht nach allen freigegebenen Dokumenten.
Bild	Sucht nach allen freigegebenen Bilddateien.
Video	Sucht nach allen freigegebenen Videodateien.
Audio	Sucht nach allen freigegebenen Audiodateien.
Komprimiert	Sucht nach allen komprimierten Dateien (beispielsweise ZIP-Dateien).

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 erhält, über ausreichend freien Speicherplatz verfügt.

Wenn Sie eine Datei erhalten, wird diese in Ihrem EasyNetwork-Posteingang angezeigt. Der Posteingang ist ein temporärer Speicherort für Dateien, die Sie von anderen Computern im Netzwerk erhalten. Wenn EasyNetwork beim Empfang einer Datei geöffnet ist, wird die Datei sofort in Ihrem Posteingang angezeigt. Andernfalls wird eine Nachricht im Benachrichtigungsbereich ganz rechts auf der Taskleiste angezeigt. Wenn Sie keine Benachrichtigungen erhalten möchten (weil Sie diese beispielsweise bei der Arbeit stören), können Sie diese Funktion deaktivieren. Wenn eine Datei mit demselben Namen bereits im Posteingang vorhanden ist, wird dem Namen der neuen Datei eine Zahl als Suffix hinzugefügt. Die Dateien bleiben in Ihrem Posteingang, bis Sie diese akzeptieren (sie also an einen Speicherort auf Ihrem Computer kopieren).

Eine Datei an einen anderen Computer senden

Sie können eine Datei 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 Akzeptieren einer Datei von einem anderen Computer (Seite 188).

1. Navigieren Sie in Windows-Explorer zu der Datei, die Sie senden möchten.
2. Ziehen Sie die Datei in Windows-Explorer von ihrem Speicherort auf ein aktives Computersymbol in EasyNetwork.

Tipp: Um mehrere Dateien an einen Computer zu senden, halten Sie beim Auswählen der Dateien die STRG-Taste gedrückt. Sie können die Dateien auch senden, indem Sie im Menü **Extras** 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 eine Datei an Sie sendet, müssen Sie diese akzeptieren, indem Sie sie in einem Ordner auf Ihrem Computer speichern. Wenn EasyNetwork nicht geöffnet ist, wenn eine Datei an Ihren Computer gesendet wird, erhalten Sie eine Benachrichtigung im Benachrichtigungsbereich ganz rechts auf der Taskleiste. Klicken Sie auf die Benachrichtigung, um EasyNetwork zu öffnen und auf die Datei zuzugreifen.

- Klicken Sie auf **Erhalten**, und ziehen Sie die 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" zu dem Ordner, in dem die erhaltenen Dateien gespeichert werden sollen, wählen Sie diesen aus, und klicken Sie dann auf **Speichern**.

Benachrichtigung bei gesendeter Datei erhalten

Sie können eine Benachrichtigungsmeldung erhalten, wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet. Wenn EasyNetwork nicht ausgeführt wird, wird die Benachrichtigungsmeldung im Benachrichtigungsbereich ganz rechts in der Taskleiste angezeigt.

1. Klicken 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 31

Drucker freigeben

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Als Name der Druckerfreigabe wird dabei der Name des Druckers verwendet. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese zu konfigurieren und zu verwenden.

Wenn Sie einen Druckertreiber über einen Netzwerk-Druckserver konfiguriert haben (z. B. einen drahtlosen USB-Druckserver), behandelt EasyNetwork den Drucker als lokalen Drucker und gibt ihn im Netzwerk frei. Sie können eine Druckerfreigabe jederzeit rückgängig machen.

In diesem Kapitel

Arbeiten mit freigegebenen Druckern

EasyNetwork erkennt Drucker, die von den Computern im Netzwerk freigegeben wurden. Wenn EasyNetwork einen Remote-Drucker erkennt, der nicht mit Ihrem Computer verbunden ist, wird beim erstmaligen Öffnen von EasyNetwork im Fenster "Freigegebene Dateien" der Link **Verfügbare Netzwerkdrucker** angezeigt. Auf diese Weise können Sie verfügbare Drucker installieren oder Drucker deinstallieren, die bereits mit Ihrem Computer verbunden sind. Sie können die Liste der Drucker auch aktualisieren, um sicherzustellen, dass Sie aktuelle Informationen anzeigen.

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

Freigabe eines Druckers aufheben

Wenn Sie die Freigabe eines Druckers aufheben, können die Mitglieder ihn nicht verwenden.

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

Installieren eines verfügbaren Netzwerkdruckers

Wenn Sie Mitglied eines verwalteten Netzwerks sind, können Sie auf die freigegebenen Drucker zugreifen. Sie müssen jedoch den vom Drucker verwendeten Druckertreiber installieren. Wenn der Eigentümer des Druckers die Druckerfreigabe aufhebt, können Sie den Drucker nicht verwenden.

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**.

Referenz

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

Glossar

"

"Man-in-the-Middle"-Angriff

Eine Methode des Abhörens und möglicherweise Bearbeitens von Nachrichten, die zwischen zwei Benutzern versendet werden, ohne dass diese wissen, dass Ihre Kommunikation abgehört wird.

8

802.11

Eine Reihe von IEEE-Standards für die Datenübertragung über ein drahtloses Netzwerk. 802.11 ist allgemein als Wi-Fi bekannt.

802.11a

Eine Erweiterung von 802.11 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 zum Senden von Daten mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar geringer als bei 802.11a, die Reichweite ist jedoch größer.

802.1x

Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken. 802.1x wird vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet.

A

ActiveX-Steuerelement

Eine Software-Komponente, die von Programmen oder Webseiten verwendet wird, um Funktionen hinzuzufügen, die als normaler Teil des Programms oder der Webseite angezeigt werden. Die meisten ActiveX-Steuerelemente sind harmlos, einige können jedoch Informationen von Ihrem Computer sammeln.

Anforderungsscan

Ein Scan, der auf Anforderung gestartet wird (d. h., wenn Sie den Vorgang starten). Im Gegensatz zu Echtzeit-Scans werden Anforderungsscans nicht automatisch gestartet.

Anschluss

Ein Ort, an dem Informationen auf einen Computer gelangen und/oder diesen verlassen. Wenn beispielsweise ein konventionelles analoges Modem mit einem seriellen Anschluss verbunden ist.

archivieren

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

Authentifizierung

Der Vorgang der Indentifizierung eines bestimmten Benutzers, meist anhand eines eindeutigen Namens und eines Kennwortes.

B

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraumes übertragen werden kann.

Bibliothek

Ein Online-Speicherbereich für Dateien, die Sie gesichert und veröffentlicht haben. Die Datensicherungs-Bibliothek ist eine Website im Internet, auf die jeder mit Internetzugriff zugreifen kann.

Bildfilterung

Eine Option für Kindersicherungen, die potentiell unangemessene Webbilder blockiert, sodass sie nicht angezeigt werden können.

Browser

Ein Programm zum Anzeigen von Websites im Internet. Zu den gängisten Webbrowsern zählen Microsoft Internet Explorer und Mozilla Firefox.

Brute-Force-Angriff

Eine Methode zur Decodierung verschlüsselter Daten, wie beispielsweise Kennwörtern, mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien. Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großem Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt. Brute-Force-Angriffe sind auch unter dem Begriff "Brute-Force-Cracking" bekannt.

C

Cache

Ein temporärer Speicherbereich auf Ihrem Computer. Um beispielsweise die Geschwindigkeit und die Effizienz des Surfens im Internet zu erhöhen, kann Ihr Browser eine Webseite aus seinem Cache abrufen (anstatt von einem Remote-Server), wenn Sie sie das nächste Mal anzeigen möchten.

Chiffrierter Text

Verschlüsselter Text. Chiffrierter Text ist nicht lesbar, solange er nicht 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

Eine kleine Datei mit Informationen, die normalerweise einen Benutzernamen und das aktuelle Datum und die Uhrzeit umfassen, die auf dem Computer einer Person, die im Internet surft, gespeichert werden. Cookies werden hauptsächlich von Websites dazu verwendet, Benutzer zu identifizieren, die sich zuvor auf der Website registriert oder sie besucht haben. Cookies können auch eine Informationsquelle für Hacker darstellen.

D

DAT

(Datensignaturdateien) Dateien, die Definitionen enthalten, die für die Erkennung von Viren, Trojanern, Spyware, Adware und anderen potentiell unerwünschten Programmen auf Ihrem Computer oder USB-Laufwerk verwendet werden.

Dateifragmente

Überbleibsel einer Datei, deren Teile auf einer Festplatte verteilt sind. Dateifragmentierung findet dann statt, wenn Dateien hinzugefügt oder gelöscht werden, und kann die Leistung Ihres Computers herabsetzen.

Denial of Service

Ein Angriffstyp, bei dem der Datenverkehr in einem Netzwerk verlangsamt oder angehalten wird. Ein Denial of Service-Angriff (DoS-Angriff) findet statt, wenn ein Netzwerk mit so vielen zusätzlichen Anfragen überflutet wird, dass der reguläre Datenverkehr verlangsamt oder ganz unterbrochen wird. Dies führt normalerweise zu Diebstahl von Informationen oder anderen Sicherheitslücken.

Dialer

Software, die Ihnen dabei hilft, eine Internetverbindung herzustellen. Wenn sie mit bösem Vorsatz verwendet werden, können Dialer Ihre Internetverbindungen an jemand anderen als Ihren standardmäßigen Internet Service Provider (ISP) umleiten, ohne dass Sie über die zusätzlichen Kosten informiert werden.

DNS

(Domain Name System) Ein System, das Hostnamen oder Domänennamen in IP-Adressen konvertiert. Im Internet wird DNS verwendet, um leicht lesbare Webadressen (z. B. www.myhostname.com) in IP-Adressen zu konvertieren (z. B. 111.2.3.44), damit die Website abgerufen werden kann. Ohne DNS müssten Sie die IP-Adresse selbst in den Webbrowser eingeben.

DNS-Server

(Domain Name System-Server) Ein Computer, der die mit einem Host oder einem Domänennamen verknüpfte IP-Adresse zurückgibt. Siehe auch DNS.

Domäne

Ein lokales Subnetzwerk oder eine Beschreibung für Websites im Internet.

In einem Local Area Network (LAN) ist eine Domäne ein Subnetzwerk, das aus Client- und Servercomputern besteht, die durch eine Sicherheitsdatenbank gesteuert werden. In diesem Kontext können Domänen die Leistung verbessern. Im Internet ist eine Domäne ein Teil jeder Webadresse (in www.abc.com z. B. ist abc die Domäne).

Drahtloser Adapter

Ein Gerät, mit dessen Hilfe Drahtlosfunktionen für einen Computer oder einen PDA bereitgestellt werden. Es wird über einen USB-Anschluss, einen PC-Kartensteckplatz (CardBus), einen Speicherkartensteckplatz oder intern über den PCI-Bus angeschlossen.

E

E-Mail

(Elektronische Mail) Nachrichten, die elektronisch in einem Computer-Netzwerk versendet und empfangen werden. Siehe auch Webmail.

E-Mail-Client

Ein Programm, das Sie auf Ihrem Computer ausführen, um E-Mails zu senden und zu empfangen (z. B. Microsoft Outlook).

Echtzeit-Scans

Zum Scannen von Dateien und Ordnern auf Viren und andere Aktivitäten, wenn Sie oder Ihr Computer darauf zugreifen.

Ereignis

Eine entweder durch den Benutzer, ein Gerät oder den Computer selbst initiierte Aktion, die eine Reaktion auslöst. McAfee zeichnet Ereignisse im Ereignisprotokoll auf.

ESS

(Extended Service Set) Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

Externe Festplatte

Eine Festplatte, die außerhalb des Computers aufbewahrt wird.

F

Firewall

Ein System (Hardware, Software oder beides), das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. 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, passieren die Firewall, die alle Nachrichten prüft und diejenigen blockiert, die die festgelegten Sicherheitskriterien nicht erfüllen.

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

Eine Zeichenfolge oder ein Schlüssel (üblicherweise ein Kennwort), das zwischen zwei miteinander kommunizierenden Benutzern vor Beginn der Kommunikation freigegeben wurde. Ein freigegebenes Geheimnis wird verwendet, um wichtige Teile von RADIUS-Nachrichten zu schützen.

H

Hotspot

Eine geografische Grenze, die durch einen Wi-Fi (802.11)-Zugriffspunkt (AP) abgedeckt ist. Benutzer, die mit einem Notebook einen Hotspot betreten, können eine Internetverbindung herstellen, vorausgesetzt, dass der Hotspot seine Anwesenheit preisgibt und keine Authentifizierung erforderlich ist. Hotspots befinden sich häufig in stark besiedelten Gebieten, wie Flughäfen.

I

Inhaltsklassifikationsgruppe

Innerhalb der Kindersicherungen eine Altersgruppe, der ein Benutzer angehört. Der Inhalt wird auf der Grundlage der Inhaltsklassifikationsgruppe, zu der der Benutzer gehört, verfügbar gemacht oder blockiert. Inhaltsklassifikationsgruppen umfassen Folgendes: kleines Kind, Kind, jüngerer Teenager, älterer Teenager und Erwachsener.

integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunktes, 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 Computer-Netzwerk, üblicherweise innerhalb eines Unternehmens, auf das nur autorisierte Benutzer zugreifen können.

IP-Adresse

Ein Bezeichner für einen Computer oder ein Gerät in einem TCP/IP-Netzwerk. Netzwerke, die das TCP/IP-Protokoll verwenden, leiten Nachrichten anhand der IP-Adresse des Zieles weiter. Das Format einer IP-Adresse besteht aus einer numerischen 32-Bit-Adresse, die in Form von vier, durch Punkte getrennte Zahlen geschrieben wird. Jede Nummer kann zwischen 0 und 255 liegen (z. B. 192.168.100).

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Diese Methode wird in vielen Arten von Angriffen einschließlich "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.

K

Kennwort

Ein Code (normalerweise aus Buchstaben und Ziffern bestehend), den Sie verwenden, um Zugriff auf Ihren Computer, ein Programm oder eine Website zu erlangen.

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 Administrator) darauf zugreifen kann.

Kindersicherungen

Einstellungen, die dabei helfen zu kontrollieren, was Ihre Kinder anzeigen und tun, während sie im Internet surfen. Um die Kindersicherung einzurichten, können Sie die Bildfilterung aktivieren oder deaktivieren, eine Inhaltsklassifikationsgruppe auswählen und zeitliche Beschränkungen für das Surfen im Internet festlegen.

Knoten

Hierbei handelt es sich um einen Computer, der mit einem Netzwerk verbunden ist.

Komprimierung

Ein Vorgang, bei dem Dateien in eine Form komprimiert werden, die den zum Speichern oder Übermitteln erforderlichen Platz minimiert.

L

LAN

(Local Area Network) Ein Computer-Netzwerk, das einen relativ kleinen Bereich abdeckt (z. B. ein einzelnes Gebäude). Computer in einem LAN können miteinander kommunizieren und Ressourcen wie Drucker und Dateien freigeben.

Launchpad

Eine U3-Schnittstellenkomponente, die als Ausgangspunkt für das Starten und Verwalten von U3 USB-Programmen fungiert.

Liste der vertrauenswürdigen IP-Adressen

Enthält Einträge, die Sie als vertrauenswürdig eingestuft haben und die deshalb nicht erkannt werden. Wenn Sie ein Element versehentlich als vertrauenswürdig eingestuft haben (beispielsweise ein potentiell unerwünschtes Programm oder eine Änderung der Registrierung) oder ein Element wieder erkannt werden soll, entfernen Sie diesen aus der Liste.

M

MAC-Adresse

(Media Access Control address) Eine eindeutige Seriennummer, die einem phyischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

MAPI

(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.

Message Authentication Code (MAC)

Ein Sicherheitscode zur Verschlüsselung von Nachrichten, die zwischen Computern übertragen werden. Die Nachricht wird akzeptiert, wenn der Computer den entschlüsselten Code als gültig ansieht.

MSN

(Microsoft Network) Eine Gruppe webbasierter Dienste der Microsoft Corporation, einschließlich einer Suchmaschine, E-Mail, Instant Messaging und eines Portals.

N

Netzwerk

Eine Sammlung von Zugriffspunkten und den damit verbundenen Benutzern, entsprechend einem ESS.

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

Eine grafische 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.

O

Online-Sicherungs-Repository

Der Speicherort auf dem Online-Server, an dem Ihre Dateien nach der Sicherung gespeichert werden.

P

Papierkorb

Ein simulierter Papierkorb für gelöschte Dateien und Ordner in Windows.

PCI-Drahtlosadapter-Karte

(Peripheral Component Interconnect) Eine drahtlose Adapterkarte, die an einen PCI-Erweiterungssteckplatz im Computer angeschlossen werden kann.

Phishing

Ein Internet-Scam im Rahmen eines Internet-Betrugs für die Beschaffung wertvoller Informationen (wie Kreditkarten- und Sozialversicherungsnummern, Benutzer-IDs und Kennwörter) von unwissenden Benutzern.

Plugin

Ein kleines Software-Programm, das mit einem größeren Programm verbunden wird, sodass zusätzliche Funktionen zur Verfügung gestellt werden können. Plugins ermöglichen dem Webbrowser beispielweise den Zugriff und die Ausführung von Dateien, die in HTML-Dokumente eingebettet sind und Formate aufweisen, die der Browser normalerweise nicht erkennen würde (z. B. Animationen, Videos und Audiodateien).

POP3

(Post Office Protocol 3) Eine Schnittstelle zwischen einem E-Mail-Client-Programm und dem E-Mail-Server. Die meisten privaten Benutzer haben ein POP3-E-Mail-Konto, auch bekannt als Standard-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.

Potentiell unerwünschtes Programm (PUP)

Ein Programm, das ohne Ihre Erlaubnis persönliche Informationen sammelt und überträgt (z. B. Spyware und Adware).

PPPoE

(Point-to-Point Protocol Over Ethernet) Eine Methode der Verwendung des Point-to-Point Protocol (PPP)-Einwahlprotokolls mit Ethernet zur Übertragung.

Privates Netzwerk

Zwei oder mehr Computer, die in einer privaten Umgebung mit dem Internet verbunden sind, sodass sie Dateien freigeben und auf das Internet zugreifen können. Siehe auch LAN.

Protokoll

Ein Format (Hardware oder Software) für die Übertragung von Dateien zwischen zwei Geräten. Ihr Computer oder Gerät muss das richtige Protokoll unterstützen, wenn Sie mit anderen Computern kommunizieren möchten.

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 alle internen Computer repräsentiert, schützt der Proxy Netzwerkidentitäten und ermöglicht gleichzeitig Zugriff auf das Internet. Siehe auch Proxyserver.

Proxyserver

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

Ein Fehler, der auftritt, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (temporärer Speicherbereich) auf Ihrem Computer zu speichern, als dieser aufnehmen kann. Pufferüberläufe schädigen oder überschreiben Daten in benachbarten Puffern.

Q

Quarantäne

Der Vorgang des Isolierens. Wenn beispielsweise in VirusScan verdächtige Dateien erkannt und isoliert werden, sodass sie Ihrem Computer oder Ihren Dateien keinen Schaden zufügen können.

R

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 RADIUS-Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

Registrierung

Eine Datenbank, in der Windows seine Konfigurationsinformationen speichert. Die Registrierung enthält Profile für jeden PC-Benutzer sowie Informationen zur System-Hardware, zu installierten Programmen und Eigenschafteneinstellungen. Windows verwendet diese Informationen ständig während der Durchführung seiner Aktivitäten.

reiner Text

Text, der nicht verschlüsselt ist. Siehe auch Verschlüsselung.

Roaming

Die Fähigkeit, aus dem Empfangsbereich eines Zugriffspunktes in den eines anderen zu wechseln, ohne dabei den Betrieb zu unterbrechen oder die Verbindung zu verlieren.

Rogue-Zugriffspunkt

Ein nicht autorisierter Zugriffspunkt. Rogue-Zugriffspunkte können in einem sicheren Unternehmensnetzwerk installiert werden, um nicht autorisierten Personen Netzwerkzurgiff zu gewähren. Sie können auch erstellt werden, um es einem Angreifer zu erlauben, einen Man-in-the-Middle-Angriff durchzuführen.

Rootkit

Eine Sammlung von Tools (Programmen), die einem Benutzer Zugriffsrechte auf Administratorebene für einen Computer oder ein Computer-Netzwerk gewähren. Rootkits können Spyware und andere potentiell unerwünschte Programme umfassen, die ein zusätzliches Risiko für die Sicherheit der Daten auf Ihrem Computer und Ihre persönlichen Informationen darstellen können.

Router

Ein Netzwerkgerät, das Datenpakete von einem Netzwerk in ein anderes weiterleitet. Basierend auf internen Routingtabellen lesen Router jedes eingehende Paket und entscheiden, wie es auf der Grundlage einer beliebigen Kombination von Quell- und Zieladresse sowie der aktuellen Datenverkehrsbedingungen (z. B. Ladung, Verbindungskosten, nicht funktionierende Verbindungen) weitergeleitet werden soll. Ein Router wird gelegentlich auch als Zugriffspunkt (Access Point, AP) bezeichnet.

S

Schlüssel

Eine Folge von Buchstaben und 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 Dateien, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden. Siehe auch "Vollständige Archivierung"

Schwarze Liste

Beim Anti-Phishing eine Liste von Websites, die als betrügerisch eingestuft werden.

Server

Ein Computer oder Programm, das Verbindungen von anderen Computern oder Programmen akzeptiert und entsprechende Reaktionen ausgibt. Beispielsweise stellt Ihr E-Mail-Programm jedes Mal eine Verbindung zu einem E-Mail-Server her, wenn Sie eine E-Mail-Nachricht empfangen oder versenden.

sichern

Verwenden Sie diese Option, um eine Kopie wichtiger Dateien auf einem sicheren Online-Server zu erstellen.

Skript

Eine Liste mit Befehlen, die automatisch ausgeführt werden können (also ohne Eingreifen des Benutzers). Anders als andere Programme werden Skripts typischerweise als reine Textdateien gespeichert und jedes Mal komprimiert, wenn sie ausgeführt werden. Makros und Batch-Dateien werden auch Skripts genannt.

Smart-Laufwerk

Siehe USB-Laufwerk.

SMTP

(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 auf Ihrem Computer, der von der Datensicherung auf Änderungen überwacht wird. Bei einem Speicherort mit umfassender Überwachung sichert die Datensicherung die überwachten Dateitypen in diesem Ordner und in allen Unterordnern.

SSID

(Service Set Identifier) Ein Token (geheimer Schlüssel), der ein Wi-Fi-Netzwerk (802.11) identifiziert. Der SSID wird durch den Netzwerkadministrator festgelegt und muss Benutzern mitgeteilt werden, die Zugriff auf das Netzwerk erlangen möchten.

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. URLs, die eine SSL-Verbindung erfordern, beginnen mit https anstatt mit http.

Standard-E-Mail-Konto

Siehe POP3.

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.

SystemGuard

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

Systemwiederherstellungspunkt

Ein Abbild der Inhalte im Speicher oder in einer Datenbank des Computers. Windows erstellt in regelmäßigen Abständen und wenn wichtige Systemereignisse stattfinden (z. B. wenn ein Programm oder Treiber installiert wird) Systemwiederherstellungspunkte. Sie können jdeoch auch jederzeit Ihre eigenen Wiederherstellungspunkte erstellen und diese benennen.

T

Temporäre Datei

Eine vom Betriebssystem oder einem anderen Programm im Speicher oder auf einem Datenträger erstellte Datei, die während einer Sitzung verwendet und anschließend gelöscht wird.

TKIP

(Temporal Key Integrity Protocol) Ein Protokoll, das die Schwächen der WEP-Sicherheit behandelt, insbesondere die 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 Clients und fügt dann einen großen Initialisierungsvektor (16 Oktette) 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.

Trojaner

Ein Programm, das legitim scheint, jedoch wichtige Dateien beschädigen, die Leistung Ihres PCs herabsetzen und unbefugten Personen den Zugriff auf Ihren Computer erlauben kann.

U

U3

(Für Sie: Mehr Benutzerfreundlichkeit, Effizienz und Mobilität) Eine Plattform, durch die Windows 2000- oder Windows XP-Programme direkt von einem USB-Laufwerk aus ausgeführt werden können. Die U3-Initiative wurde 2004 von M-Systems und SanDisk gegründet und ermöglicht es Benutzern, U3-Programme auf einem Windows-Computer auszuführen, ohne dass Dateien oder Einstellungen auf dem Computer installiert oder gespeichert werden müssen.

Ü

Überwachte Dateitypen

Die Dateitypen (beispielsweise .doc, .xls usw.), die von Data Backup innerhalb der Überwachungs-Speicherorte gesichert oder archiviert werden.

Überwachungs-Speicherorte

Die Ordner auf Ihrem Computer, die von Data Backup überwacht werden.

U

URL

(Uniform Resource Locator) Das Standardformat für Internetadressen.

USB

(Universal Serial Bus) Eine standardisierte serielle Computer-Schnittstelle, die es Ihnen ermöglicht, Peripheriegeräte, wie Tastaturen, Joysticks und Drucker, an Ihren Computer anzuschließen.

USB-Drahtlosadapter-Karte

Eine Drahtlosadapter-Karte, die in einen USB-Anschluss am Computer eingesteckt wird.

USB-Laufwerk

Ein kleines Speicherlaufwerk, das an den USB-Port eines Computers angeschlossen werden kann. Ein USB-Laufwerk funktioniert wie ein kleines Festplattenlaufwerk, das es leicht macht, Dateien von einem Computer auf einen anderen zu übertragen.

V

Verknüpfung

Eine Datei, die nur den Speicherort einer anderen Datei auf Ihrem Computer enthält.

Veröffentlichen

Eine gesicherte Datei öffentlich im Internet verfügbar machen. Sie können auf veröffentlichte Dateien zugreifen, indem Sie die Datensicherungs-Bibliothek durchsuchen.

Verschlüsselung

Ein Vorgang, bei dem Daten von Text in Code umgewandelt werden, wodurch die Informationen verschleiert werden, sodass Personen, die den Code nicht entschlüsseln können, sie nicht lesen können. Verschlüsselte Daten sind auch als chiffrierter Text bekannt.

Verwaltetes Netzwerk

Ein privates Netzwerk mit zwei Arten von Mitgliedern: verwalteten Mitgliedern und unverwalteten Mitgliedern. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht.

Virus

Computerviren sind sich selbst replizierende Programme, die Ihre Dateien oder Daten ändern können. Oft scheinen diese von einer vertrauenswürdigen Quelle zu stammen oder nützliche Inhalte zu bieten.

Vollständige Archivierung

Die Archivierung eines kompletten Datensatzes basierend auf den von Ihnen festgelegten Dateitypen und Speicherorten. Siehe auch Schnellarchivierung.

VPN

(Virtual Private Network) Ein privates Netzwerk, das innerhalb eines öffentlichen Netzwerks konfiguriert wurde, um die Verwaltungsfunktionen des öffentlichen Netzwerks nutzen zu können. Unternehmen verwenden VPNs zum Erstellen von WANs (Wide Area Networks), die große geografische Gebiete umfassen, um Site-to-Site-Verbindungen mit ihren Filialen herzustellen oder mobilen Benutzern die Einwahl in die LANs (Local Area Networks) des Unternehmens zu ermöglichen.

W

Wardriver

Eine Person, die nach Wi-Fi-Netzwerken (802.11) sucht, indem sie ausgerüstet mit einem Wi-Fi-Computer und spezieller Hard- oder Software durch eine Stadt fährt.

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 werden auch als Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs bezeichnet.

Web-Mail

Nachrichten, die auf elektronischem Wege über das Internet gesendet und empfangen werden. Siehe auch E-Mail.

Weiße Liste

Eine Liste der Websites, auf die die Benutzer zugreifen dürfen, da sie nicht als betrügerische Websites angesehen werden.

WEP

(Wired Equivalent Privacy) Ein Verschlüsselungs- und Authentifizierungsprotokoll, das im Rahmen des Wi-Fi-Standards (802.11) definiert ist. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und weisen beträchtliche Schwächen auf. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit diese bei der Übertragung zwischen zwei Endpunkten geschützt sind. Es hat sich jedoch herausgestellt, dass WEP weniger sicher als ursprünglich angenommen ist.

Wi-Fi

(Wireless Fidelity) Ein von der Wi-Fi Alliance verwendeter Begriff zur Bezeichnung eines Netzwerks vom Typ 802.11.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht. Das Ziel der Wi-Fi Alliance liegt darin, allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren und den Begriff "Wi-Fi" in allen Märkten für 802.11-basierte Funk-LAN-Produkte als globalen Markennamen zu fördern. Die Organisation dient als Verband, Testlabor und Informationszentrale für Anbieter, die zum Wachstum dieser Branche beitragen möchten.

Wi-Fi Certified

Von der Wi-Fi Alliance getestet und zugelassen. Produkte mit dem Prädikat "Wi-Fi Certified" werden als miteinander kompatibel deklariert, auch wenn diese möglicherweise von unterschiedlichen Herstellern stammen. Der Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken verwenden, die ebenfalls zertifiziert sind.

Wiederherstellen

Abrufen einer Kopie einer Datei aus dem Online-Sicherungs-Repository oder einem Archiv.

WLAN

(Wireless Local Area Network) Ein LAN (Local Area Network), das eine drahtlose Verbindung verwendet. In WLANs erfolgt die Kommunikation zwischen den einzelnen Computern über hochfrequente Funkwellen anstelle von Kabeln.

Wörterbuchangriff

Eine Art gewaltsamen Angriffs, der häufig verwendete Wörter benutzt, um ein Kennwort herauszufinden.

WPA

(Wi-Fi Protected Access) Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen erheblich erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und mit diesem kompatibel und kann auf vorhandener Hardware in Form eines Softwareupgrades ausgeführt werden. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt sind und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entwickelt wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus können Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren. Die Passphrase sollte auf allen drahtlosen Computern und Zugriffspunkten regelmäßig geändert werden. Siehe auch WPA2-PSK und TKIP.

WPA2

Eine Verbesserung des Sicherheitsstandards WPA, der auf dem Standard 802.11i IEEE beruht.

WPA2-PSK

Ein auf dem WPA2-Standard basierender spezieller WPA-Modus, der WPA-PSK ähnelt. Eine typische Funktion von WPA2-PSK besteht darin, dass Geräte häufig mehrere Verschlüsselungsmodi (z. B. AES, TKIP) gleichzeitig unterstützen, während ältere Geräte üblicherweise nur jeweils einen Verschlüsselungsmodus unterstützen (d. h. alle Clients müssten denselben Verschlüsselungsmodus verwenden).

Wurm

Ein sich selbst replizierender Virus, der sich im Arbeitsspeicher eines Computers befindet und Kopien von sich selbst per E-Mail verbreitet. Würmer replizieren sich und verbrauchen Systemressourcen, wodurch die Leistung reduziert bzw. Tasks verlangsamt werden.

Z

Zugriffspunkt

Ein Netzwerkgerät (auch "drahtloser Router" genannt), das an einen Ethernet-Hub oder -Switch angeschlossen wird, um die physikalische Betriebsreichweite für drahtlose Benutzer zu erweitern. Wenn drahtlose Benutzer Roaming für Ihre mobilen Geräte nutzen, geht die Übertragung von einem Zugriffspunkt auf den anderen über, damit die Konnektivität erhalten bleibt.

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

Lizenz

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DER BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI VON DER WEBSITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE NICHT ALLEN BEDINGUNGEN DIESER VEREINBARUNG ZUSTIMMEN, INSTALLIEREN SIE DIE SOFTWARE NICHT. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE, INC., ODER AN DIE STELLE ZURÜCKGEBEN, AN DER SIE DAS PRODUKT ERWORBEN HABEN.

KAPITEL 32

Kundendienst und technischer Support

Das SecurityCenter meldet alle kritischen und nichtkritischen Sicherheitsprobleme, sobald sie erkannt werden. Kritische Sicherheitsprobleme erfordern unverzügliche Maßnahmen und gefährden Ihren Sicherheitsstatus (die Farbe wechselt zu rot). Nichtkritische Sicherheitsprobleme erfordern keine unverzüglichen Maßnahmen und gefährden möglicherweise Ihren Sicherheitsstatus (in Abhängigkeit von der Art des Problems). Um den Sicherheitsstatus der Kategorie "grün" zu erhalten, müssen Sie alle kritischen Probleme beheben und alle nichtkritischen Probleme beheben oder ignorieren. Wenn Sie Hilfe bei der Diagnose Ihrer Sicherheitsprobleme benötigen, können Sie den McAfee Virtual Technician starten. Weitere Informationen zum McAfee Virtual Technician erhalten Sie im Hilfebereich des McAfee Virtual Technician.

Wenn Sie Ihre Sicherheitssoftware bei einem Partner oder einem anderen Anbieter als McAfee erworben haben, öffnen Sie einen Webbrowser, und gehen Sie auf www.mcafeehilfe.com. Wählen Sie anschließend unter den Partner-Links Ihren Partner oder Anbieter aus, um Zugriff auf McAfee Virtual Technician zu erhalten.

Hinweis: Um McAfee Virtual Technician zu installieren und auszuführen, müssen Sie sich in Ihrem Computer bei Windows als Administrator anmelden. Andernfalls könnte MVT nicht in der Lage sein, Ihre Probleme zu lösen. Informationen über die Anmeldung als Administrator bei Windows finden Sie in der Windows-Hilfe. Bei Windows Vista™ erhalten Sie Anweisungen, wenn Sie MVT ausführen. Sollte dies der Fall sein, klicken sie auf **Akzeptieren**. Der Virtual Technician ist nicht mit Mozilla® Firefox kompatibel.

In diesem Kapitel

Verwenden des McAfee Virtual Technician

Wie ein persönlicher Kontakt beim technischen Support sammelt der Virtual Technician Informationen zu Ihren SecurityCenter-Programmen, sodass er dabei helfen kann, Probleme beim Schutz Ihres Computers zu lösen. Wenn Sie den Virtual Technician ausführen, prüft er, ob Ihre SecurityCenter-Programme ordnungsgemäß ausgeführt werden können. Wenn er Probleme erkennt, bietet der Virtual Technician an, diese für Sie zu lösen, oder er stellt Ihnen detailliertere Informationen dazu zur Verfügung. Wenn er fertig ist, zeigt der Virtual Technician die Ergebnisse seiner Analysen an, und ermöglicht es Ihnen, weiteren technischen Support von McAfee zu erhalten, falls erforderlich.

Um die Sicherheit und Integrität Ihres Computers und Ihrer Dateien zu wahren, sammelt der Virtual Technician keine persönlichen Informationen zu Ihrer Person.

Hinweis: Für weitere Informationen zum Virtual Technician klicken Sie auf das Symbol **Hilfe** in Virtual Technician.

Starten des Virtual Technician

Virtual Technician sammelt Informationen zu Ihren SecurityCenter-Programmen, sodass er Ihnen dabei helfen kann, Ihre Sicherheitsprobleme zu lösen. Um Ihre persönlichen Daten zu schützen, umfassen diese Informationen keine Daten, anhand derer Sie als Person identifiziert werden könnten.

1. Klicken Sie unter **Häufige Tasks** auf **McAfee Virtual Technician**.
2. Befolgen Sie die Bildschirmanweisungen für das Herunterladen und Ausführen des Virtual Technician.

Support und Downloads

Schauen Sie in den folgenden Tabellen nach McAfee-Kundendienst- und Download-Seiten einschließlich Benutzerhandbüchern in Ihrem Land.

Kundendienst und Downloads

Land	Technischer Kundendienst von McAfee	McAfee-Downloads
Australien	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilien	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Kanada (Englisch)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (Französisch)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
China (CHN)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (TW)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tschechien	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Dänemark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finnland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankreich	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Deutschland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Großbritannien	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italien	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexiko	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norwegen	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp

Polen	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spanien	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Schweden	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Türkei	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection-Benutzerhandbücher

Land	McAfee-Benutzerhandbücher
Australien	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (Englisch)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (Französisch)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (CHN)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (TW)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tschechien	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finnland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankreich	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf

Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norwegen	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee-Benutzerhandbücher für Sicherheit im Internet

Land	McAfee-Benutzerhandbücher
Australien	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (Englisch)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (Französisch)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (CHN)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (TW)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tschechien	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finnland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf

Frankreich	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norwegen	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus-Benutzerhandbücher

Land	McAfee-Benutzerhandbücher
Australien	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (Englisch)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (Französisch)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (CHN)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf

China (TW)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tschechien	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finnland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Frankreich	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norwegen	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan-Benutzerhandbücher

Land	McAfee-Benutzerhandbücher
Australien	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf

Brasilien	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (Englisch)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Kanada (Französisch)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
China (CHN)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (TW)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tschechien	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finnland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankreich	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norwegen	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Schauen Sie in der folgenden Tabelle nach dem McAfee Threat Center sowie Virusinformationsseiten in Ihrem Land.

Land	Security Headquarters	Virusinformationen
Australien	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilien	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (Englisch)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (Französisch)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (CHN)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (TW)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tschechien	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dänemark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finnland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankreich	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Deutschland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Großbritannien	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Niederlande	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italien	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexiko	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norwegen	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo

Polen	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Spanien	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Schweden	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Türkei	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Schauen Sie in der folgende Tabelle nach HackerWatch-Seiten in Ihrem Land.

Land	HackerWatch
Australien	www.hackerwatch.org
Brasilien	www.hackerwatch.org/?lang=pt-br
Kanada (Englisch)	www.hackerwatch.org
Kanada (Französisch)	www.hackerwatch.org/?lang=fr-ca
China (CHN)	www.hackerwatch.org/?lang=zh-cn
China (TW)	www.hackerwatch.org/?lang=zh-tw
Tschechien	www.hackerwatch.org/?lang=cs
Dänemark	www.hackerwatch.org/?lang=da
Finnland	www.hackerwatch.org/?lang=fi
Frankreich	www.hackerwatch.org/?lang=fr
Deutschland	www.hackerwatch.org/?lang=de
Großbritannien	www.hackerwatch.org
Niederlande	www.hackerwatch.org/?lang=nl
Italien	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexiko	www.hackerwatch.org/?lang=es-mx
Norwegen	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl

Portugal	www.hackerwatch.org/?lang=pt-pt
Spanien	www.hackerwatch.org/?lang=es
Schweden	www.hackerwatch.org/?lang=sv
Türkei	www.hackerwatch.org/?lang=tr
USA	www.hackerwatch.org

Index

E

F

G

H

I

W

Z