McAfee®

Internet Security

Benutzerhandbuch

Inhalt

KAPITEL 1

McAfee Internet Security

Wie ein Sicherheitssystem für Zuhause schützt Internet Security Sie und Ihre Familie vor den neuesten Bedrohungen, während es gleichzeitig Ihre Online-Erfahrungen sicherer macht. Sie können Internet Security zum Schutz Ihres PCs vor Viren, Hackern und Spyware verwenden. Sie können außerdem den Internet-Datenverkehr auf verdächtige Aktivitäten überwachen, die persönlichen Daten Ihrer Familie schützen, risikoreiche Websites bewerten und mehr.

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

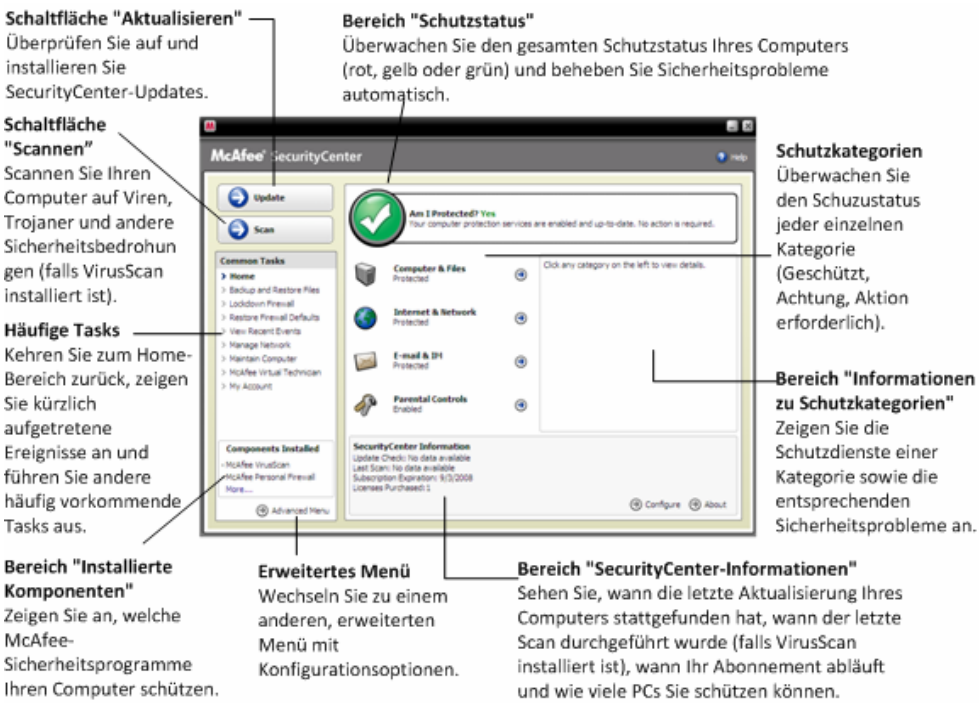
SecurityCenter-Funktionen

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 ist, 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.

Klicken Sie auf einen Kategorienamen, 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 ▪ Spyware-Schutz ▪ SystemGuards ▪ Windows-Schutz ▪ PC-Gesundheit
Internet & Netzwerk	Die Kategorie "Internet & Netzwerk" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Firewall-Schutz ▪ Phishing-Schutz ▪ Identitätsschutz
E-Mail & IM	Die Kategorie "E-Mail & IM" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Virenschutz für E-Mails ▪ IM-Virenschutz ▪ Spyware-Schutz für E-Mails ▪ IM-Spyware-Schutz ▪ Spam-Schutz
Kindersicherungen	Die Kategorie "Kindersicherungen" ermöglicht die Konfiguration der folgenden Schutzdienste: ▪ Inhaltsblockierung

Erläuterungen zu Schutzdiensten

Schutzdienste sind verschiedene Sicherheitskomponenten, die Sie zum Schutz Ihres Computers und Ihrer Dateien konfigurieren können. Schutzdienste entsprechen direkt McAfee-Programmen. Wenn Sie beispielsweise VirusScan installieren, werden die folgenden Schutzdienste verfügbar: Virenschutz, Spyware-Schutz, SystemGuards und Skriptscans. 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 die Kindersicherungen 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 Ihrer Abonnements

Jedes McAfee-Sicherheitsprodukt, das Sie kaufen, umfasst ein Abonnement, mit dem Sie das Produkt für einen bestimmten Zeitraum auf einer bestimmten Anzahl an Computern verwenden können. Die Abonnementdauer fällt je nach Kauf unterschiedlich aus, beginnt aber üblicherweise mit der Produktaktivierung. Die Aktivierung ist einfach und kostenlos – Sie benötigen dafür lediglich eine Internetverbindung. Mit diesem wichtigen Schritt wird Ihnen Zugang zu den automatischen Produkt-Updates gewährt, die Ihren Computer vor den neuesten Bedrohungen schützen.

Die Aktivierung findet normalerweise bei der Installation des Produkts statt. Wenn Sie jedoch damit warten möchten (z. B. weil Sie keinen Internetanschluss haben), können Sie das Produkt auch innerhalb von 15 Tagen aktivieren. Wenn Sie die Aktivierung nicht innerhalb von 15 Tagen durchführen, erhalten Sie für Ihre Produkte keine wichtigen Updates mehr, und es werden keine Scans durchgeführt. Wir benachrichtigen Sie auch regelmäßig (mit Bildschirmmeldungen), dass Ihr Abonnement bald abläuft. Auf diese Weise können Sie Unterbrechungen bei Ihrem Schutz vermeiden, indem Sie ihn frühzeitig erneuern oder auf unserer Website die automatische Erneuerung einrichten.

Wenn Sie in SecurityCenter einen Link sehen, der Sie zur Aktivierung auffordert, wurde Ihr Abonnement noch nicht aktiviert. Das Ablaufdatum Ihres Abonnements können Sie auf Ihrer Kontoseite überprüfen.

Zugreifen auf Ihr McAfee-Konto

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

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

Aktivieren Ihres Produkts

Die Aktivierung erfolgt normalerweise bei der Installation Ihres Produkts. Wenn dies jedoch nicht der Fall ist, sehen Sie im SecurityCenter einen Link, der Sie zur Aktivierung auffordert. Wir werden Sie auch regelmäßig benachrichtigen.

- Klicken Sie auf der SecurityCenter-Startseite unter **SecurityCenter-Informationen** auf **Aktivieren Sie Ihr Abonnement**.

Tipp: Sie können die Aktivierung auch über die Warnung durchführen, die regelmäßig angezeigt wird.

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**.

Erneuern Ihres Abonnements

Kurz bevor Ihr Abonnement abläuft, sehen Sie im SecurityCenter einen Link, der Sie zur Erneuerung auffordert. Wir weisen Sie auch regelmäßig mit Warnmeldungen darauf hin, dass Ihr Abonnement in Kürze abläuft.

- Klicken Sie auf der SecurityCenter-Startseite unter **SecurityCenter-Informationen** auf die Option **Erneuern**.

Tipp: Sie können Ihr Produkt auch über die Benachrichtigungsmeldung erneuern, die regelmäßig angezeigt wird. Oder gehen Sie zu Ihrer Kontoseite, auf der Sie die Erneuerung durchführen oder die automatische Erneuerung einrichten können.

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, je nach den von Ihnen installierten und aktivierten Programmen, 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: Wenn Sie Ihr McAfee-Produkt von einer CD installiert haben, müssen Sie es innerhalb von 15 Tagen aktivieren. Andernfalls erhalten Sie für Ihre Produkte keine wichtigen Updates und können keine Scans durchführen.

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 21).

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 13).

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**.
3. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

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 ergreifen 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 Erkennungssignaturdateien (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 aktiviert und erhält keinen vollständigen Schutz.	Aktivieren Sie das Programm auf der McAfee-Website.
Ihr Abonnement ist abgelaufen.	Überprüfen Sie Ihren Kontostatus auf der McAfee-Website. Weitere Informationen finden Sie unter Verwalten Ihrer Abonnements (Seite 10).

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 27).

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 nicht kritisches Problem erkennt, haben Sie die Option, es zu beheben oder zu ignorieren. Andere nicht kritische Probleme (z. B. wenn Anti-Spam oder die Kindersicherungen 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.

Sicherheitsmeldungen ausblenden

Sie können Sicherheitsbenachrichtigungen zum Schutz mehrerer Computer in Ihrem privaten Netzwerk ausblenden. Die Nachrichten bieten Informationen zu Ihrem Abonnement, der Anzahl an Computern, die Sie mit Ihrem Abonnement schützen können, und dazu, wie Sie Ihr Abonnement erweitern können, um noch mehr Computer zu schützen.

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 **Zeigt Virenwarnungen oder andere Sicherheitsmeldungen an**.

Tipp: Sie können diese Sicherheitsbenachrichtigungen jederzeit wieder anzeigen, indem Sie das Kontrollkästchen **Zeigt Virenwarnungen oder andere Sicherheitsmeldungen an** 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

Umfassender Virenschutz

Verteidigen Sie sich und Ihren Computer gegen die neuesten Sicherheitsbedrohungen, einschließlich Viren, Trojanern, Nachverfolgungs-Cookies, Spyware, Adware und anderer potentiell unerwünschter Programme. Der Schutz geht über die Dateien und Ordner auf Ihrem Desktop hinaus und erstreckt sich auf Bedrohungen an verschiedenen Eintrittspunkten, einschließlich E-Mail, Instant Messages und Internet. Es ist keine aufwändige Verwaltung erforderlich.

Scan-Optionen auf Grundlage der Ressourcen

VirusScan bietet Ihnen die Flexibilität, Echtzeit- und manuelle Scan-Optionen anzupassen, wenn Sie dies möchten. Anderenfalls bleibt Ihr Computer ebenfalls geschützt. Wenn Sie merken, dass sich die Scan-Geschwindigkeit reduziert, können Sie diese Option deaktivieren, um nur minimale Computerressourcen zu nutzen. Bedenken Sie aber, dass dem Virenschutz eine höhere Priorität eingeräumt wird als anderen Aufgaben.

Automatische Reparaturen

Wenn VirusScan während der Ausführung eines Echtzeit- oder manuellen Scans Sicherheitsbedrohungen erkennt, versucht es, die Bedrohung automatisch entsprechend dem Bedrohungstyp zu behandeln. Dadurch können die meisten Bedrohungen erkannt und neutralisiert werden, ohne dass Sie eingreifen müssen. Ganz selten kann es vorkommen, dass VirusScan nicht in der Lage ist, eine Bedrohung alleine zu neutralisieren. In diesen Fällen lässt VirusScan Sie entscheiden, was Sie tun möchten (einen erneuten Scan durchführen, wenn der PC das nächste Mal hochgefahren wird, das erkannte Element behalten oder es löschen).

Pausieren von Tasks im Vollbildschirmmodus

Wenn Sie auf Ihrem PC einen Film ansehen, Spiele spielen oder irgendeiner anderen Aktivität nachgehen, die den ganzen Bildschirm benötigt, pausiert VirusScan eine gewisse Anzahl an Tasks, wie manuelle Scans.

KAPITEL 9

Scannen des Computers

Noch bevor 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 Scan-Optionen finden Sie unter Einstellen des Virenschutzes (Seite 47).

VirusScan bietet eine Reihe detaillierterer Scan-Optionen für den Virenschutz, wodurch Sie regelmäßig ausführlichere Scans durchführen können. Sie können umfassende, schnelle, benutzerdefinierte oder geplante Scans über das SecurityCenter ausführen. Sie können manuelle Scans aber auch während Sie arbeiten 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 eines Scans am Ende einsehen, egal ob Sie die 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

Scannen Ihres PCs

VirusScan bietet einen umfassenden Satz an Scan-Optionen für den Virenschutz, einschließlich Echtzeit-Scans (wodurch Ihr PC dauerhaft auf Bedrohungsaktivitäten überwacht wird), manuelle Scans von Windows Explorer aus sowie umfassende, schnelle, benutzerdefinierte oder geplante Scans über das SecurityCenter.

Ziel	Aktion
Starten Sie Echtzeit-Scans, um Ihren Computer permanent bezüglich Virenaktivität zu überwachen und Dateien jedes Mal zu scannen, wenn Sie oder Ihr Computer darauf zugreifen.	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**. **Hinweis**: Echtzeit-Scans sind standardmäßig aktiviert.
Starten Sie einen QuickScan, um Ihren Computer schnell auf Bedrohungen zu prüfen.	1. Klicken Sie im Menü "Grundlagen" auf **Scannen**. 2. Klicken Sie im Bereich "Scan-Optionen" unter "Schnellprüfung" auf **Start**.
Starten Sie einen umfassenden Scan, um Ihren Computer gründlich auf Bedrohungen zu prüfen.	1. Klicken Sie im Menü "Grundlagen" auf **Scannen**. 2. Klicken Sie im Bereich "Scan-Optionen" unter "Umfassender Scan" auf **Start**.

Ziel	Aktion
Starten Sie einen benutzerdefinierten Scan auf der Grundlage Ihrer eigenen Einstellungen.	1. Klicken Sie im Menü "Grundlagen" auf **Scannen**. 2. Klicken Sie im Bereich "Scan-Optionen" unter "Auswählen" auf **Start**. 3. Passen Sie einen Scan an, indem Sie Folgendes deaktivieren oder auswählen: **Alle Bedrohungen in allen Dateien** **Unbekannte Viren** **Archivdateien** **Spyware und potentielle Bedrohungen** **Nachverfolgungs-Cookies** **Diebstahlprogramme** 4. Klicken Sie auf **Start**.
Starten Sie einen manuellen Scan, um in Dateien, Ordnern oder Laufwerken nach Bedrohungen zu suchen.	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**.

Ziel	Aktion
Starten Sie einen geplanten Scan, der Ihren Computer in regelmäßigen Abständen auf Bedrohungen scannt.	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**.

Die Scan-Ergebnisse 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.

Hinweis: Um mehr über Scan-Optionen zu erfahren, lesen Sie nach unter Scan-Typen (Seite 40).

Prüfergebnisse anzeigen

Wenn ein 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.	1. Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereich Ihrer Taskleiste. 2. Klicken Sie bei einem umfassenden, schnellen, benutzerdefinierten oder manuellen Scan im jeweiligen Bereich auf **Details**.
Zeigen Sie Details zu Ihrem letzten Scan an.	Doppelklicken Sie auf das Symbol **Scan abgeschlossen** im Benachrichtigungsbereicht Ihrer Symbolleiste, und zeigen Sie Details zu Ihrem letzten Scan unter "Ihr Scan" im Bereich für einen umfassenden, schnellen, benutzerdefinierten oder manuellen Scan an.

KAPITEL 10

Arbeiten mit Prüfergebnissen

Wenn VirusScan während der Ausführung eines Scans Sicherheitsbedrohungen erkennt, 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. VirusScan isoliert Dateien stets, bevor es versucht, sie zu säubern. Wenn die Datei nicht sauber ist, wird sie isoliert.

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

Arbeiten mit Viren und Trojanern

Findet VirusScan Viren oder Trojaner auf Ihrem Computer, 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 39).

Arbeiten mit potentiell unerwünschten Programmen

Wenn VirusScan ein potentiell unerwünschtes Programm auf Ihrem Computer erkennt, können Sie das Programm entfernen oder es als vertrauenswürdig markieren. Wenn Sie das Programm nicht kennen, empfehlen wir, es eher zu entfernen. 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.

Scan-Typen

VirusScan bietet einen umfassenden Satz an Scan-Optionen für den Virenschutz, einschließlich Echtzeit-Scans (wodurch Ihr PC dauerhaft auf Bedrohungsaktivitäten überwacht wird), manuelle Scans von Windows Explorer aus sowie die Möglichkeit, umfassende, schnelle oder benutzerdefinierte Scans über das SecurityCenter auszuführen oder einzustellen, wann geplante Scans stattfinden sollen. Scans im SecurityCenter haben den Vorteil, dass Sie die Scan-Optionen sofort ändern können.

Echtzeit-Scans:

Der Echtzeit-Virenschutz überwacht 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.

Sie können Standardoptionen für Echtzeit-Scans festlegen, die das Scannen auf unbekannte Viren und das Prüfen auf Bedrohungen in Nachverfolgungs-Cookies und Netzwerk-Laufwerken umfassen. Sie können auch den Pufferüberlaufschutz nutzen, der standardmäßig aktiviert ist (außer, wenn Sie ein Windows Vista-64-Bit-Betriebssystem verwenden). Für weitere Informationen lesen Sie nach unter Festlegen der Echtzeit-Scan-Optionen (Seite 48).

Schnellprüfung

Schnellprüfungen erlauben es Ihnen, Prozesse, wichtige Windows-Dateien und andere anfällige Bereiche Ihres Computers auf Bedrohungsaktivitäten zu prüfen.

Umfassender Scan

Mit einem umfassenden Scan können Sie Ihren gesamten Computer gründlich auf Viren, Spyware und andere Sicherheitsbedrohungen prüfen, die irgendwo auf Ihrem PC vorliegen.

Benutzerdefinierter Scan

Mit einem benutzerdefinierten Scan können Sie Ihre eigenen Scan-Einstellungen auswählen, um auf Bedrohungsaktivitäten auf Ihrem PC zu prüfen. Benutzerdefinierte Scan-Optionen umfassen das Prüfen auf Bedrohungen in allen Dateien, in Archivdateien und in Cookies sowie das Scannen auf unbekannte Viren, Spyware und Diebstahlprogramme.

Sie können einen Standardsatz an Optionen für benutzerdefinierte Scans festlegen, der das Scannen auf unbekannte Viren, Archivdateien, Spyware und potentielle Bedrohungen, Nachverfolgungs-Cookies und Diebstahlprogramme umfasst. Sie können auch unter Nutzung minimaler Computerressourcen einen Scan ausführen. Für weitere Informationen lesen Sie nach unter Festlegen der benutzerdefinierten Scan-Optionen (Seite 51).

Manueller Scan

Mit einem manuellen Scan können Sie über den Windows Explorer auf Bedrohungen in Dateien, Ordnern und Laufwerken prüfen, während Sie arbeiten.

Geplanter Scan

Mit einem geplanten Scan können Sie für einen beliebigen Tag der Woche und eine beliebige Zeit einen Scan zur gründlichen Überprüfung Ihres Computers auf Viren und andere 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. Weitere Informationen finden Sie unter Planen eines Scans (Seite 54).

Hinweis: Um zu erfahren, wie Sie die beste Scan-Option für sich starten, lesen Sie nach unter Scannen Ihres PCs (Seite 32).

KAPITEL 11

Verwenden 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

Skriptscans erkennen potentiell gefährliche Skripts und verhindern, dass diese auf Ihrem Computer oder in Ihrem Webbrowser ausgeführt werden. Sie bewachen Ihren Computer bezüglich verdächtiger Skriptaktivitäten, wie z. B. ein Skript, dass Dateien erstellt, kopiert oder löscht oder Ihre Windows-Registrierung öffnet, und warnen 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.

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 12

Einrichten des Virenschutzes

Sie können verschiedene Optionen für geplante, benutzerdefinierte und Echtzeit-Scans festlegen. 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.

Sie können auch entscheiden, wie VirusScan möglicherweise nicht autorisierte oder unerwünschte Änderungen an Ihrem PC mit SystemGuards und Listen vertrauenswürdiger Websites überwacht und verwaltet. SystemGuards überwacht, protokolliert, berichtet über und verwaltet nicht autorisierte Veränderungen in der Windows-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. Sie können Listen vertrauenswürdiger Websites verwenden, wenn Sie entscheiden müssen, ob Sie Regeln, die Datei- oder Registrierungsänderungen (SystemGuard), Programme oder Pufferüberläufe erkennen, vertrauen oder diese entfernen möchten. 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.

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	Wählen Sie **Auf unbekannte Viren prüfen**.
Cookies erkennen	Wählen Sie **Nachverfolgungs-Cookies suchen und entfernen**.
Erkennen von Viren und anderen potentiellen Bedrohungen auf Laufwerken, die mit dem Netzwerk verbunden sind	Wählen Sie **Netzlaufwerke überprüfen**.
Schutz des Computers vor Pufferüberläufen	Wählen Sie **Pufferüberlaufschutz aktivieren**.
Geben Sie an, welche Dateitypen geprüft werden sollen.	Klicken Sie auf **Alle Dateien (empfohlen)** oder auf die Option **Nur Programmdateien und Dokumente**.

Anhalten des Echtzeit-Virenschutzes

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.

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**.

Festlegen der benutzerdefinierten Scan-Optionen

Mit dem benutzerdefinierten Virenschutz können Sie Anforderungsscans für Ihre Dateien durchführen. Wenn Sie einen benutzerdefinierten Scan beginnen, untersucht VirusScan unter Verwendung umfassenderer Scan-Optionen Ihren Computer auf Viren und andere potentiell gefährliche Elemente. Um die Optionen für benutzerdefinierte 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 Diebstahlprogrammen und Rootkits (die unerlaubten Zugriff auf Ihren Computer gewähren können) 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 sowie alle Netzwerk-Laufwerke bei jedem manuellen Scan. Sie können die Standardeinstellungen jedoch nach Ihren Bedürfnissen verändern. Sie können beispielsweise lediglich kritische PC-Dateien, Elemente auf Ihrem Desktop oder Elemente in Ihrem Ordner für Programmdateien durchsuchen lassen. Wenn Sie nicht selbst für die Initiierung jedes benutzerdefinierten 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 benutzerdefinierte Scans.

Festlegen der benutzerdefinierten Scan-Optionen

Die Optionen für benutzerdefinierte Scans können eingestellt werden, um anzupassen, wonach VirusScan während eines benutzerdefinierten 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 Diebstahlprogrammen. Sie stellen den Ort für den benutzerdefinierten Scan ein, um festzulegen, wo VirusScan während eines benutzerdefinierten 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 "Benutzerdefinierter 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 benutzerdefinierte Scans ein, und klicken Sie auf **OK**.

Ziel	Aktion
Erkennen unbekannter Viren und neuer Variationen bekannter Viren	Wählen Sie **Auf unbekannte Viren prüfen**.
Erkennen und Entfernen von Viren in .zip- und anderen Archivdateien.	Wählen Sie **Archivdateien prüfen**.
Spyware, Adware und andere potentiell unerwünschte Programme erkennen	Wählen Sie **Auf Spyware und potentielle Bedrohungen prüfen**.
Cookies erkennen	Wählen Sie **Nachverfolgungs-Cookies suchen und entfernen**.

Ziel	Aktion
Rootkits und Diebstahlprogramme, die existierende Windows-Systemdateien ändern und ausnutzen können, erkennen	Wählen Sie **Auf Diebstahlprogramme prüfen**.
Weniger Prozessorleistung für Scans nutzen und anderen Tasks (z. B. Surfen im Netz, Öffnen von Dokumenten) höhere Priorität geben	Wählen Sie **Unter Verwendung minimaler Computerressourcen scannen**.
Geben Sie an, welche Dateitypen geprüft werden sollen.	Klicken Sie auf **Alle Dateien (empfohlen)** oder auf die Option **Nur Programmdateien und Dokumente**.

3 Klicken Sie auf **Zu scannendes Standardverzeichnis**, und wählen oder deaktivieren Sie dann diejenigen Orte, die gescannt oder übersprungen werden sollen. Klicken Sie dann auf **OK**:

Ziel	Aktion
Überprüfen aller Dateien und Ordner auf Ihrem Computer	Wählen Sie **(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**.

Einplanen eines Scans

Sie können für einen beliebigen Tag der Woche und eine beliebige Zeit einen Scan zur gründlichen Überprüfung Ihres Computers nach Viren und andere 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.

Planen Sie Scans, die mithilfe Ihrer standardmäßigen Scan-Optionen Ihren gesamten Computer gründlich auf Viren und andere Bedrohungen prüfen. Standardmäßig führt VirusScan einmal wöchentlich einen Scan durch.

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 58).

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.

SystemGuard	Erkennt...
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.

SystemGuard	Erkennt...
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.

SystemGuard	Erkennt...
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 64).

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.

Option	Beschreibung
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 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

Standardmäßige und benutzerdefinierte Sicherheitsstufen	Schützt Sie vor Eindringversuchen und verdächtigen Aktivitäten mithilfe der standardmäßigen oder anpassbaren Schutzeinstellungen von Firewall.
Empfehlungen in Echtzeit	Lassen Sie sich dynamisch Empfehlungen zukommen, um zu ermitteln, ob Programmen Internetzugriff gewährt 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 spezifische Programme.
Gaming-Schutz	Verhindern Sie, dass Warnungen zu Eindringversuchen und verdächtigen Aktivitäten während des Spielens im Vollbildmodus angezeigt werden.
Schutz beim Computer-Start	Schützt Ihren Computer vor Eindringversuchen sowie vor unerwünschten Programmen und unerwünschtem Netzwerkverkehr, sobald Windows® gestartet wird.
Kontrolle des Systemdienstanschlusses	Verwaltet offene und geschlossene Systemdienstanschlüsse, die für einige Programme erforderlich sind.
Verwalten von Computer-Verbindungen	Erlaubt und blockiert Remote-Verbindungen zwischen anderen Computern und Ihrem Computer.
Integration von HackerWatch-Informationen	Verfolgt globale Hacking- und Eindringmuster über die HackerWatch-Website, auf der Sie auch aktuelle Sicherheitsinformationen zu Programmen auf Ihrem Computer sowie Statistiken zu globalen Sicherheitsereignissen und Internetanschlüssen finden.
Firewall sperren	Blockiert unverzüglich den gesamten ein- und ausgehenden Netzwerkverkehr zwischen Ihrem Computer und dem Internet.
Sicherheitseinstellungen für Firewall wiederherstellen	Stellt sofort die ursprünglichen Schutzeinstellungen der 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	Verfolgt kürzlich aufgetretene eingehende, ausgehende und Eindringereignisse.
Überwachen des Internetverkehrs	Prüft weltweite Zuordnungen, die die Quellen feindlicher Angriffe und feindlichen Verkehrs zeigen. 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	Schützt Ihre Privatsphäre vor möglichen Internetbedrohungen. Durch die Verwendung Heuristik-ähnlicher Funktionen bietet McAfee eine dritte Schutzstufe, da alle Objekte blockiert werden, die Angriffssymptome oder Eigenschaften von Hacker-Angriffen aufweisen.

Intelligente Datenverkehrsanalyse

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

KAPITEL 14

Firewall starten

Schon direkt nach der Installation von Firewall ist Ihr Computer vor Eindringversuchen und unerwünschtem Internetdatenverkehr geschützt. Darüber hinaus können Sie mit Firewall Warnungen erhalten sowie den Zugriff auf eingehende und ausgehende Internetverbindungen bekannter und unbekannter Programme verwalten. Empfehlungen und die Sicherheitsstufe "Automatisch" (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 Eindringversuche und unerwünschten Internetdatenverkehr geschützt. Außerdem sind Sie dann nicht mehr in der Lage, eingehende und ausgehende Internetverbindungen effektiv zu verwalten. Daher sollten Sie den Firewall-Schutz nur vorübergehend und nur wenn absolut notwendig deaktivieren. Sie können Firewall auch im Bereich "Internet & Netzwerkkonfiguration" aktivieren.

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

Hinweis: Öffnen Sie zum Konfigurieren von Firewall 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.

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 **Neue Netzwerkverbindung** angezeigt, wenn ein Computer, auf dem Firewall installiert ist, mit einem neuen Netzwerk verbunden wird. Sie können die Vertrauensebene angeben, die Sie diesem neuen Netzwerk zuweisen möchten und die dann in Ihrer Netzwerkliste angezeigt wird. Wenn die Option "Empfehlungen" aktiviert ist, werden Programme automatisch 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.

Benutzereingriff

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

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

Wenn die Sicherheitsstufe "Automatisch" festgelegt und die Option "Empfehlungen" aktiviert ist, können Sie bei gelben Warnungen den eingehenden Zugriff für unbekannte Programme gewähren oder blockieren. Obwohl grüne Warnungen standardmäßig deaktiviert sind, werden sie angezeigt, wenn bekannte Programme erkannt werden, und der Zugriff wird ihnen automatisch erlaubt. Durch Gewähren des Zugriffs kann ein Programm ausgehende Verbindungen herstellen und unaufgefordert eingehende Verbindungen überwachen.

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

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

Stufe	Beschreibung
Tarnung	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 Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.
Standard	Eingehende und ausgehende Verbindungen werden überwacht. Wenn ein neues Programm versucht, auf das Internet zuzugreifen, werden Sie benachrichtigt. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.

Stufe	Beschreibung
Automatisch	Gewährt Programmen entweder eingehenden und ausgehenden Zugriff (Vollzugriff) oder nur ausgehenden Zugriff auf das Internet. Standardmäßig ist die Sicherheitsstufe "Automatisch" 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.

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

Die Sicherheitsstufe "Tarnung"

Sie können die Firewall-Sicherheitsstufe auf "Tarnung" 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 **Tarnung** als aktuelle Sicherheitsstufe angezeigt wird.
4. Klicken Sie auf **OK**.

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

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 "Automatisch"

Sie können die Firewall-Sicherheitsstufe "Automatisch" 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 **Automatisch** als aktuelle Sicherheitsstufe angezeigt wird.
4. Führen Sie einen der folgenden Vorgänge 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.

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 Empfehlungen aktiviert sind (und die Sicherheitsstufe auf "Automatisch" gesetzt ist, sodass nur der ausgehende Zugriff aktiviert ist), lässt Firewall bekannte Programme automatisch zu und blockiert potentiell gefährliche Programme.

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, Firewall gibt aber eine Empfehlung in der Warnung.

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 verwenden**.
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 nicht verwenden**.
4. Klicken Sie auf **OK**.

Empfehlungen anzeigen

Sie können Empfehlungen verwenden, um nur eine Empfehlung in den Warnungen anzuzeigen, sodass Sie entscheiden, ob Sie nicht erkannte und potentiell gefährliche 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 **Empfehlungen anzeigen**.
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, wenn Windows® hochgefahren wird. Technisch versierte Anwender können einen trace- oder ping-Befehl an Ihren Computer senden, um festzustellen, ob er an ein Netzwerk angeschlossen ist. Sie können auch mithilfe des UDP-Protokolls Informationen in Form von Nachrichteneinheiten (Datengrammen) an Ihren Computer senden. Firewall schützt Ihren Computer vor diesen Typen von Eindringversuchen, indem es Ihnen ermöglicht, Programme beim Windows-Start zu blockieren, sodass sie nicht auf das Internet zugreifen können und Sie Ping-Anfragen blockieren können, die anderen Benutzern dabei helfen, Ihren Computer in einem Netzwerk zu erkennen. Dadurch können Sie verhindern, dass andere Benutzer Informationen in Form von Nachrichteneinheiten (Datengrammen) an Ihren Computer senden.

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.

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 **Aktivieren Sie den Schutz beim Starten von Windows** aus.
4. Klicken Sie auf **OK**.

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

Konfigurieren der UDP-Einstellungen

Sie können es anderen Netzwerkcomputern erlauben, Nachrichteneinheiten (Datengramme) mithilfe des UDP-Protokolls an Ihren Computer zu senden. Sie können dies jedoch nur tun, wenn Sie einen Systemdienstport geschlossen haben, sodass er dieses Protokoll 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. Führen Sie im Bereich "Sicherheitsstufe" unter **Sicherheitseinstellungen** einen der folgenden Schritte aus:
   - Wählen Sie **UDP-Nachverfolgung aktivieren**, um es anderen Computerbenutzern zu erlauben, Nachrichteneinheiten (Datengramme) an Ihren Computer zu senden.
   - Heben Sie die Auswahl von **UDP-Nachverfolgung aktivieren** auf, um zu verhindern, dass andere Computerbenutzer Nachrichteneinheiten (Datengramme) an Ihren Computer senden.
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.**
   - **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

Die Sperrung blockiert unverzüglich die gesamten ein- und ausgehenden Netzwerkverbindungen einschließlich des Zugriffs auf Websites, E-Mails und Sicherheitsupdates. Die Sperrung hat dieselbe Wirkung wie das Trennen der Netzwerkkabel von Ihrem Computer. Sie können diese Einstellung verwenden, um offene Ports im Bereich "Systemdienste" zu blockieren und Ihnen dabei zu helfen, ein Problem auf Ihrem Computer zu isolieren und Fehler zu beheben.

Firewall unverzüglich sperren

Sie können Firewall sperren, um den gesamten Netzwerkverkehr zwischen Ihrem Computer und einem Netzwerk umgehend zu blockieren, einschließlich des Internets.

1. Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Firewall sperren**.
2. Klicken Sie im Bereich "Firewall sperren" auf **Firewall-Sperrung aktivieren**.

3 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

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-Sperrung sofort aufheben

Sie können die Firewall entsperren, um den gesamten Netzwerkverkehr zwischen Ihrem Computer und dem Internet umgehend zuzulassen, einschließlich des Internets.

1 Klicken Sie im Bereich "McAfee SecurityCenter" unter **Häufige Tasks** auf **Firewall sperren**.

2 Klicken Sie im Bereich "Sperrung aktiviert" auf **Firewall-Sperrung deaktivieren**.

3 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Firewall-Standardeinstellungen wiederherstellen

Sie können die Standard-Sicherheitseinstellungen der Firewall schnell und einfach wiederherstellen. Diese Wiederherstellung bewirkt Folgendes: Festlegung Ihrer Sicherheitsstufe auf "Automatisch" 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 auf **Ja**, um den Vorgang zu bestätigen.

4 Klicken Sie auf **OK**.

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 120)

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

Computerverbindungen verwalten

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

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der Computer, den Sie als vertrauenswürdig einstufen, sicher ist. Wenn ein Computer, den Sie als vertrauenswürdig einstufen, durch einen Wurm oder auf andere Weise infiziert wird, besteht für Ihren Computer möglicherweise ebenfalls ein Infektionsrisiko. McAfee empfiehlt zudem, den 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 **Netzwerke** enthalten sind, protokolliert Firewall weder den Datenverkehr noch generiert es Ereigniswarnungen.

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

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten IP-Adressen nur dann blockieren, wenn Sie sicher sind, dass eine Internetverbindung eine Bedrohung darstellen würde. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP.

In diesem Kapitel

Info zu Computerverbindungen

Computerverbindungen sind Verbindungen, die Sie zwischen anderen Computern in einem beliebigen Netzwerk und Ihrem Computer herstellen. Sie können IP-Adressen zur Liste **Netzwerke** hinzufügen, diese bearbeiten oder wieder aus der Liste entfernen. Diese IP-Adressen sind mit Netzwerken verknüpft, denen Sie eine Vertrauensebene für Verbindungen mit Ihrem Computer zuweisen können: Vertrauenswürdig, Standard und Öffentlich.

Stufe	Beschreibung
Vertrauenswürdig	Firewall lässt zu, dass Verkehr von einer IP-Adresse Ihren Computer über einen beliebigen Port erreicht. Aktivitäten zwischen Computern, denen eine vertrauenswürdige IP-Adresse zugeordnet ist, und Ihrem Computer werden von Firewall weder gefiltert noch analysiert. Standardmäßig ist das erste private Netzwerk, das Firewall findet, in der Liste **Netzwerke** als "Vertrauenswürdig" aufgeführt. Ein Beispiel für ein vertrauenswürdiges Netzwerk ist ein oder mehrere Computer in Ihrem lokalen oder privaten Netzwerk.
Standard	Firewall steuert Verkehr von einer IP-Adresse (aber nicht von anderen Computern in diesem Netzwerk), wenn eine Verbindung zu Ihrem Computer hergestellt wird, und lässt diesen zu oder blockiert ihn, je nach den Regeln in der Liste **Systemdienste**. Firewall protokolliert Verkehr und erzeugt Ereigniswarnungen von Standard-IP-Adressen. Ein Beispiel für ein Standardnetzwerk ist ein oder mehrere Computer in einem Unternehmensnetzwerk.
Öffentlich	Firewall steuert Verkehr von einem öffentlichen Netzwerk entsprechend den Regeln in der Liste **Systemdienste**. Ein Beispiel für "Öffentlich" ist ein Internet-Netzwerk in einem Café, Hotel oder an einem Flughafen.

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

Hinzufügen einer Computerverbindung

Sie können eine vertrauenswürdige, standardmäßige oder öffentliche 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 **Netzwerke**.
4. Klicken Sie im Bereich "Netzwerke" auf **Hinzufügen**.
5. Wenn sich die Computerverbindung in einem IPv6-Netzwerk befindet, wählen Sie das Kontrollkästchen **IPv6** aus.
6. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie **Einzeln** aus, und geben Sie dann die IP-Adresse in das Feld **IP-Adresse** ein.
   - Wählen Sie **Bereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein. Wenn Ihre Computerverbindung sich in einem IPv6-Netzwerk befindet, geben Sie die Von IP-Adresse und die Präfixlänge in den Feldern **Von IP-Adresse** und **Präfixlänge** ein.
7. Führen Sie dann unter **Typ** einen der folgenden Schritte aus:
   - Wählen Sie **Vertrauenswürdig** aus, um anzugeben, dass diese Computerverbindung vertrauenswürdig ist (z. B. ein Computer in einem privaten Netzwerk).
   - Wählen Sie **Standard** aus, um anzugeben, dass diese Computerverbindung (und nicht die anderen Computer im Netzwerk) vertrauenswürdig ist (z. B. ein Computer in einem Unternehmensnetzwerk).
   - Wählen Sie **Öffentlich**, um anzugeben, dass diese Computerverbindung öffentlich ist (z. B. ein Computer in einem Internetcafé, Hotel oder an einem Flughafen).

8 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.

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

10 Optional geben Sie eine Beschreibung der Regel ein.

11 Klicken Sie auf **OK**.

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

Hinzufügen eines Computers aus dem Protokoll "Eingehende Ereignisse"

Sie können eine vertrauenswürdige oder standardmäßige Computerverbindung und die dazugehörige 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 führen Sie unter **Ich möchte** eine der folgenden Aktionen durch:

- Klicken Sie auf **Diese IP-Adresse als vertrauenswürdig hinzufügen**, um diesen Computer als vertrauenswürdig zu Ihrer Liste **Netzwerke** hinzuzufügen.
- Klicken Sie auf **Diese IP-Adresse als Standard hinzufügen**, um diese Computerverbindung als Standard zu Ihrer Liste **Netzwerke** hinzuzufügen.

6 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Bearbeiten einer Computerverbindung

Sie können eine vertrauenswürdige, standardmäßige oder öffentliche Computerverbindung und die dazugehörige 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 **Netzwerke**.
4. Wählen Sie im Bereich "Netzwerk" eine IP-Adresse aus, und klicken Sie dann auf **Bearbeiten**.
5. Wenn sich die Computerverbindung in einem IPv6-Netzwerk befindet, wählen Sie das Kontrollkästchen **IPv6** aus.
6. Führen Sie dann unter **Regel bearbeiten** einen der folgenden Schritte aus:
   - Wählen Sie **Einzeln** aus, und geben Sie dann die IP-Adresse in das Feld **IP-Adresse** ein.
   - Wählen Sie **Bereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein. Wenn Ihre Computerverbindung sich in einem IPv6-Netzwerk befindet, geben Sie die Von IP-Adresse und die Präfixlänge in den Feldern **Von IP-Adresse** und **Präfixlänge** ein.
7. Führen Sie dann unter **Typ** einen der folgenden Schritte aus:
   - Wählen Sie **Vertrauenswürdig** aus, um anzugeben, dass diese Computerverbindung vertrauenswürdig ist (z. B. ein Computer in einem privaten Netzwerk).
   - Wählen Sie **Standard** aus, um anzugeben, dass diese Computerverbindung (und nicht die anderen Computer im Netzwerk) vertrauenswürdig ist (z. B. ein Computer in einem Unternehmensnetzwerk).
   - Wählen Sie **Öffentlich**, um anzugeben, dass diese Computerverbindung öffentlich ist (z. B. ein Computer in einem Internetcafé, Hotel oder an einem Flughafen).
8. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
9. Optional geben Sie eine Beschreibung der Regel ein.
10. Klicken Sie auf **OK**.

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

Entfernen einer Computerverbindung

Sie können eine vertrauenswürdige, standardmäßige oder öffentliche Computerverbindung und die dazugehörige 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 **Netzwerke**.
4. Wählen Sie im Bereich "Netzwerk" eine IP-Adresse aus, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Sperren von Computerverbindungen

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

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

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten IP-Adressen nur dann blockieren, wenn Sie sicher sind, dass eine Internetverbindung eine Bedrohung darstellen würde. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP.

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 **Gesperrte IP-Adressen**.
4. Klicken Sie im Bereich "Gesperrte IP-Adressen" auf **Hinzufügen**.

5 Wenn sich die Computerverbindung in einem IPv6-Netzwerk befindet, wählen Sie das Kontrollkästchen **IPv6** aus.

6 Führen Sie dann unter **Regel hinzufügen** einen der folgenden Schritte aus:

- Wählen Sie **Einzeln** aus, und geben Sie dann die IP-Adresse in das Feld **IP-Adresse** ein.
- Wählen Sie **Bereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein. Wenn Ihre Computerverbindung sich in einem IPv6-Netzwerk befindet, geben Sie die Von IP-Adresse und die Präfixlänge in den Feldern **Von IP-Adresse** und **Präfixlänge** ein.

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 Optional geben Sie eine Beschreibung der Regel ein.

9 Klicken Sie auf **OK**.

10 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

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 **Gesperrte IP-Adressen**.

4 Klicken Sie im Bereich "Gesperrte IP-Adressen" auf **Bearbeiten**.

5 Wenn sich die Computerverbindung in einem IPv6-Netzwerk befindet, wählen Sie das Kontrollkästchen **IPv6** aus.

6 Führen Sie dann unter **Regel bearbeiten** einen der folgenden Schritte aus:

- Wählen Sie **Einzeln** aus, und geben Sie dann die IP-Adresse in das Feld **IP-Adresse** ein.
- Wählen Sie **Bereich**, und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse** und **Bis IP-Adresse** ein. Wenn Ihre Computerverbindung sich in einem IPv6-Netzwerk befindet, geben Sie die Von IP-Adresse und die Präfixlänge in den Feldern **Von IP-Adresse** und **Präfixlänge** ein.

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 Optional geben Sie eine Beschreibung der Regel ein.

9 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 **Gesperrte IP-Adressen**.

4 Wählen Sie im Bereich "Gesperrte IP-Adressen" eine IP-Adresse aus, und klicken Sie dann auf **Entfernen**.

5 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Computer aus dem Protokoll "Eingehende Ereignisse" sperren

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

Fügen Sie eine IP-Adresse zu Ihrer Liste **Gesperrte IP-Adressen** hinzu, wenn Sie den gesamten eingehenen Internetverkehr von dieser IP-Adresse sperren möchten, unabhängig davon, ob Ihre Systemdienstports geöffnet oder geschlossen sind.

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 IP-Adresse sperren**.

6 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Computer aus dem Protokoll "Intrusionserkennungs-Ereignisse" sperren

Sie können eine Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Intrusionserkennungs-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 **Intrusionserkennungs-Ereignisse**.
5. Wählen Sie eine Quell-IP-Adresse aus, und klicken Sie unter **Ich möchte** auf **Diese IP-Adresse sperren**.
6. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

KAPITEL 20

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. Diese Systemdienstports können für Computer, die als vertrauenswürdig, Standard oder öffentlich in Ihrer Liste **Netzwerke** aufgeführt sind, geöffnet oder geschlossen werden.

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

- Häufig verwendeter Betriebssystem-Port 5357
- 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-Netzwerkzugriff auf einen Systemdienst 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 **Bearbeiten**.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Um den Port auf einem beliebigen Computer in einem vertrauenswürdigen, standardmäßigen oder öffentlichen Netzwerk zu öffnen (z. B. in einem privaten Netzwerk, einem Unternehmensnetzwerk oder einem Internet-Netzwerk), wählen Sie **Vertrauenswürdig, Standard oder Öffentlich**.
   - Um den Port auf einem beliebigen Computer in einem Standardnetzwerk zu öffnen (z. B. in einem Unternehmensnetzwerk), wählen Sie **Standard (umfasst "Vetrauenswürdig")**.
7. Klicken Sie auf **OK**.

Zugriff auf einen vorhandenen Systemdienstport sperren

Sie können einen vorhandenen Port schließen, um Remote-Netzwerkzugriff auf einen Systemdienst 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. Heben Sie unter **Offener Systemdienstport** die Auswahl des Kontrollkästchens neben dem Systemdienstport auf, den Sie schließen möchten.
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 **Systemdienstregel hinzufügen** Folgendes ein:
   - Systemdienstname
   - Systemdienstkategorie
   - Lokale TCP/IP-Ports
   - Lokale UDP-Ports
6. Führen Sie einen der folgenden Vorgänge aus:
   - Um den Port auf einem beliebigen Computer in einem vertrauenswürdigen, standardmäßigen oder öffentlichen Netzwerk zu öffnen (z. B. in einem privaten Netzwerk, einem Unternehmensnetzwerk oder einem Internet-Netzwerk), wählen Sie **Vertrauenswürdig, Standard oder Öffentlich**.
   - Um den Port auf einem beliebigen Computer in einem Standardnetzwerk zu öffnen (z. B. in einem Unternehmensnetzwerk), wählen Sie **Standard (umfasst "Vetrauenswürdig")**.

7 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 Netzwerkcomputer weiterleiten, die die "Gemeinsame Nutzung der Internetverbindung (ICS)" nutzen**.

8 Geben Sie optional eine Beschreibung für die neue Konfiguration ein.

9 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 **Netzwerke** eine vertrauenswürdige Computerverbindung hinzufügen. Weitere Informationen finden Sie unter "Hinzufügen einer Computerverbindung".

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 Klicken Sie auf das Kontrollkästchen neben einem Systemdienst, und klicken Sie dann auf **Bearbeiten**.

5 Bearbeiten Sie im Bereich "Systemdienste" unter **Systemdienstregel hinzufügen** Folgendes:

- Systemdienstname
- Lokale TCP/IP-Ports
- Lokale UDP-Ports

6 Führen Sie einen der folgenden Vorgänge aus:

- Um den Port auf einem beliebigen Computer in einem vertrauenswürdigen, standardmäßigen oder öffentlichen Netzwerk zu öffnen (z. B. in einem privaten Netzwerk, einem Unternehmensnetzwerk oder einem Internet-Netzwerk), wählen Sie **Vertrauenswürdig, Standard oder Öffentlich**.
- Um den Port auf einem beliebigen Computer in einem Standardnetzwerk zu öffnen (z. B. in einem Unternehmensnetzwerk), wählen Sie **Standard (umfasst "Vetrauenswürdig")**.

7 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 Netzwerkcomputer weiterleiten, die die "Gemeinsame Nutzung der Internetverbindung (ICS)" nutzen**.

8 Geben Sie optional eine Beschreibung für die geänderte Konfiguration ein.

9 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 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.

Mit der Statistik arbeiten

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

Statistiken zu den globalen Sicherheitsereignissen anzeigen

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

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

In dem 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 IP-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 "Intrusionserkennungs-Ereignisse" verfolgen

In dem Bereich "Intrusionserkennungs-Ereignisse" können Sie eine IP-Adresse verfolgen, die im Protokoll "Intrusionserkennungs-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 "Intrusionserkennungs-Ereignisse" eine Quell-IP-Adresse aus, und klicken Sie dann auf **Diese IP-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 die Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse in Erfahrung bringen.

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 graphische Darstellung des ein- und abgehenden Internetdatenverkehrs. Der Datenverkehrsmonitor zeigt die Programme an, die momentan die meisten Netzwerkverbindungen auf dem Computer verwenden, sowie die IP-Adressen, auf die diese Anwendungen 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 graphische Darstellung des ein- und abgehenden Internetdatenverkehrs. Der Datenverkehrsmonitor zeigt die Programme an, die momentan die meisten Netzwerkverbindungen auf dem Computer verwenden, sowie die IP-Adressen, auf die diese Anwendungen 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

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

In diesem Kapitel

Hackerwatch-Lernprogramm starten

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

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 Anti-Spam

Anti-Spam (früher als SpamKiller bekannt) hindert unerwünschte E-Mails daran, in Ihren Posteingang zu gelangen. Dazu werden Ihre eingehenden E-Mails überprüft und dann als Spam (E-Mails, die Sie zum Kauf auffordern) oder Phishing (E-Mails, mit denen Sie veranlasst werden, persönliche Daten auf einer Website preiszugeben, bei der es sich um Betrug handeln könnte) gekennzeichnet. Anti-Spam filtert dann die Spam-E-Mail und verschiebt sie in den McAfee Anti-Spam-Ordner.

Wenn Sie manchmal seriöse E-Mails bekommen, die fälschlicherweise als Spam erkannt werden könnten, können Sie das Herausfiltern dieser E-Mails verhindern, indem Sie die betreffenden E-Mail-Adressen zur Freunde-Liste von Anti-Spam hinzufügen. Sie können Sie Spam-Erkennung auch anpassen. Sie können z. B. Nachrichten stärker filtern, angeben, wonach in der Nachricht gesucht werden soll, und Ihre eigenen Filter erstellen.

Anti-Spam schützt Sie auch, wenn Sie versuchen, über eine Verknüpfung in einer E-Mail-Nachricht auf eine potentiell betrügerische Website zuzugreifen. Wenn Sie auf eine Verknüpfung zu einer potentiell betrügerischen Website klicken, werden Sie zurück auf die sichere Phishing-Filterseite geleitet. Wenn es Websites gibt, die Sie nicht filtern möchten, können Sie diese zur Weißen Liste hinzufügen (die Websites in dieser Liste werden nicht gefiltert).

Anti-Spam kann mit verschiedenen E-Mail-Programmen verwendet werden, wie etwa Yahoo®, MSN®/Hotmail®, Windows® Mail und Live™ Mail, Microsoft® Outlook® und Outlook Express sowie Mozilla Thunderbird™, sowie auch in Verbindung mit verschiedenen E-Mail-Konten, wie etwa POP3, POP3 Webmail und MAPI (Microsoft Exchange Server). Wenn Sie Ihre E-Mails über einen Browser abrufen, müssen Sie Ihr Webmail-Konto zu Anti-Spam hinzufügen. Alle anderen Konten werden automatisch konfiguriert und müssen nicht zu Anti-Spam hinzugefügt werden.

Sie müssen Anti-Spam nicht nach der Installation konfigurieren; wenn Sie jedoch ein erfahrener Benutzer sind, möchten Sie vielleicht die erweiterten Spam- und Phishing-Schutzfunktionen entsprechend Ihrer Bedürfnisse anpassen.

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

Anti-Spam-Funktionen

Spam-Filter	Verhindert, dass unerwünschte E-Mails in Ihren Posteingang gelangen. Die erweiterten Anti-Spam-Filter werden automatisch für alle Ihre E-Mail-Konten aktualisiert. Sie können auch benutzerdefinierte Filter erstellen, um zu gewährleisten, dass Spam vollständig gefiltert wird, und Spam zu Analysezwecken an McAfee senden.
Phishing-Filter	Identifizieren Sie potentielle (betrügerische) Phishing-Websites, die persönliche Informationen abfragen.
Angepasste Spam-Verarbeitung	Lässt Sie unerwünschte E-Mails als Spam markieren und in Ihren McAfee Anti-Spam-Ordner verschieben oder legitime E-Mails als Nicht-Spam markieren und in Ihren Posteingang verschieben.
Freunde	Importieren Sie die E-Mail-Adressen Ihrer Freunde in die Freunde-Liste, damit deren E-Mail-Adressen nicht gefiltert werden.

KAPITEL 24

Konfigurieren der Spam-Erkennung

Mit Anti-Spam können Sie die Spam-Erkennung anpassen. Sie können Nachrichten stärker filtern, angeben, wonach in der Nachricht gesucht werden soll, und bei der Spam-Analyse nach bestimmten Zeichensätzen suchen. Sie können auch persönliche Filter erstellen, um die Spamerkennung zu optimieren. Wenn z. B. unerwünschte E-Mails, die das Wort "Hypothek" enthalten, nicht gefiltert werden, können Sie einen Filter für das Wort "Hypothek" hinzufügen.

Wenn es zu Problemen mit dem E-Mail-Programm kommt, können Sie den Spam-Schutz im Rahmen der Problembehebung deaktivieren.

In diesem Kapitel

Einstellen von Filteroptionen

Passen Sie die Filteroptionen von Anti-Spam an, wenn Sie Nachrichten stärker filtern möchten, angeben möchten, wie Spam verarbeitet werden soll, und bei der Spam-Analyse nach bestimmten Zeichensätzen suchen möchten.

Filterstufe

Die Filterstufe bestimmt, wie stark Ihre E-Mail gefiltert wird. Wenn z. B. die Spam-E-Mails, die Sie erhalten, nicht gefiltert werden und Ihre Filterstufe auf den Grad "Mittel" eingestellt ist, können Sie sie in "Mittel-Hoch" oder "Hoch" ändern. Wenn die Filterstufe jedoch auf "Hoch" eingestellt ist, werden nur E-Mail-Nachrichten von den Sendern in Ihrer Freunde-Liste akzeptiert, alle anderen werden gefiltert.

Verarbeiten von Spam

Mit Anti-Spam können Sie verschiedene Optionen zur Spam-Verarbeitung anpassen. Beispielsweise können Sie Spam- und Phishing-E-Mails in bestimmte Ordner platzieren, den Namen des Tags ändern, das in der Betreffzeile der Spam- und Phishing-Mails angezeigt wird, eine maximale Filtergröße angeben oder angeben, wie häufig Ihre Spam-Regeln aktualisiert werden sollen.

Zeichensätze

Anti-Spam kann bei der Spam-Analyse nach bestimmten Zeichensätzen suchen. Zeichensätze werden zur Darstellung einer Sprache verwendet, z. B. das entsprechende Alphabet, die Ziffern und andere Symbole. Wenn Sie Spam auf Griechisch empfangen, können Sie alle Nachrichten filtern, die den griechischen Zeichensatz enthalten.

Achten Sie darauf, keine Zeichensätze für die Sprachen zu filtern, in denen Sie seriöse E-Mails empfangen. Wenn Sie z. B. nur Nachrichten auf Italienisch filtern möchten, könnten Sie "Westeuropa" auswählen, da Italien in Westeuropa liegt. Wenn Sie jedoch seriöse E-Mails auf Englisch erhalten, werden durch die Einstellung "Westeuropa" auch die Nachrichten auf Englisch und allen anderen Sprachen mit dem westeuropäischen Zeichensatz gefiltert. In einem solchen Fall gibt es keine Möglichkeit, die Nachrichten nur nach Italienisch zu filtern.

Hinweis: Das Angeben eines Zeichensatzfilters gilt nur für erfahrene Benutzer.

Filterstufe ändern

Sie können festlegen, wie stark Ihre E-Mails gefiltert werden sollen. Wenn beispielsweise seriöse Nachrichten gefiltert werden, können Sie die Filterstufe herabsetzen.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Filteroptionen**.

3 Wählen Sie in der Liste **Spam-Filterebene angeben** die entsprechende Stufe aus, und klicken Sie dann auf **OK**.

Stufe	Beschreibung
Niedrig	Die meisten E-Mails werden akzeptiert.
Mittel – Niedrig	Es werden nur Nachrichten blockiert, die offensichtlich Spam-Nachrichten sind.
Mittel (empfohlen)	Dies ist die empfohlene Filterstufe.
Mittel – Hoch	Alle E-Mail-Nachrichten, die wie Spam aussehen, werden gefiltert.
Hoch	Nur Nachrichten von Absendern in der Freunde-Liste werden akzeptiert.

Ändern der Spam-Verarbeitungs- und -markierungsart

Sie können einen Ordner angeben, in dem Spam- und Phishing-E-Mails abgelegt werden sollen, das Tag [SPAM] oder [PHISH] ändern, das in der Betreffzeile der E-Mail angezeigt wird, eine maximale Filtergröße angeben und angeben, wie häufig Ihre Spam-Regeln aktualisiert werden sollen.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Filteroptionen**.

3 Wählen Sie die gewünschte Option aus, oder bearbeiten Sie sie, und klicken Sie anschließend auf **OK**.

Ziel	Aktion
Angeben des Ortes, an dem Spam- und Phishing-E-Mails abgelegt werden sollen	Wählen Sie in der Liste **Spam-E-Mails in diesem Ordner speichern** einen Ordner aus. Der Standardordner ist McAfee Anti-Spam.
Ändern der Betreffzeile in der Spam-E-Mail	Geben Sie unter **Betreff der Spam-E-Mail markieren mit** ein Tag an, das der Betreffzeile der Spam-E-Mail hinzugefügt werden soll. Das Standard-Tag ist [SPAM].
Ändern der Betreffzeile in der Phishing-E-Mail	Geben Sie unter **Betreff der Phishing-E-Mail markieren mit** ein Tag an, das der Betreffzeile der Phishing-E-Mail hinzugefügt werden soll. Das Standard-Tag ist [PHISH].
Angeben der größten zu filternden E-Mail	Geben Sie unter **Größte zu filternde E-Mail (Größe in KB) angeben** die Maximalgröße von zu filternden E-Mails ein.
Aktualisieren der Spam-Regeln	Wählen Sie **Spam-Regeln aktualisieren (in Minuten)**, und geben Sie dann die Häufigkeit ein, mit der Ihre Spam-Regeln aktualisiert werden sollen. Die empfohlene Häufigkeit lautet 30 Minuten. Wenn Sie über eine schnelle Netzwerkverbindung verfügen, können Sie eine höhere Häufigkeit eingeben, wie alle 5 Minuten, um bessere Ergebnisse zu erzielen.

Ziel	Aktion
Keine Aktualisierung der Spam-Regeln	Wählen Sie **Spam-Regeln nicht aktualisieren**.

Zeichensatzfilter anwenden

Hinweis: Das Filtern von Nachrichten, die Zeichen aus einem bestimmten Zeichensatz enthalten, ist nur für fortgeschrittene Benutzer geeignet.

Sie können den Zeichensatz einer bestimmten Sprache filtern. Achten Sie jedoch darauf, keine Zeichensätze für die Sprachen zu filtern, in denen Sie seriöse E-Mails empfangen.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Zeichensätze**.

3 Aktivieren Sie das Kontrollkästchen für die zu filternden Zeichensätze.

4 Klicken Sie auf **OK**.

Verwenden von persönlichen Filtern

Ein persönlicher Filter gibt an, ob E-Mails auf der Grundlage bestimmter Wörter oder Ausdrücke zugelassen oder blockiert werden sollen. Wenn eine E-Mail ein Wort oder einen Ausdruck enthält, den der Filter blockiert, wird die Nachricht als Spam markiert und in Ihrem Posteingang belassen oder in den McAfee Anti-Spam-Ordner verschoben. Weitere Informationen zum Umgang mit Spam finden Sie unter Nachrichtenverarbeitungs- und -markierungsart ändern (Seite 138).

Anti-Spam bietet einen erweiterten Filter, der verhindert, dass unerwünschte E-Mails in Ihren Posteingang gelangen. Wenn Sie jedoch die Feineinstellungen vornehmen möchten, welche Nachrichten Anti-Spam als Spam erkennt, können Sie einen persönlichen Filter erstellen. Wenn Sie z. B. einen Filter für das Wort "Hypothek" hinzufügen, filtert Anti-Spam alle Nachrichten mit dem Wort "Hypothek". Erstellen Sie keine Filter für Wörter, die häufig in seriösen E-Mail-Nachrichten auftreten, da sonst auch diese Nachrichten gefiltert werden. Nachdem Sie einen Filter erstellt haben, können Sie ihn bearbeiten, wenn er immer noch nicht alle Spam-E-Mails erkennt. Wenn Sie z. B. einen Filter für das Wort "Viagra" in der Betreffzeile einer Nachricht erstellt haben und Sie immer noch Nachrichten mit dem Wort "Viagra" empfangen, da es im Textkörper der Nachricht vorkommt, ändern Sie den Filter so, dass nun nach dem Wort "Viagra" im Nachrichtentext gesucht wird.

Reguläre Ausdrücke (RegEx) sind spezielle Zeichen und Zeichenfolgen, die auch in persönlichen Filtern verwendet werden können. McAfee empfiehlt jedoch nur fortgeschrittenen Benutzern die Verwendung regulärer Ausdrücke. Wenn Sie mit regulären Ausdrücken nicht vertraut sind oder mehr über deren Verwendung erfahren möchten, können Sie im Internet das Stichwort "Reguläre Ausdrücke" recherchieren (z. B. unter http://de.wikipedia.org/wiki/Regul%C3%A4rer_Ausdruck).

Persönlichen Filter hinzufügen

Sie können Filter hinzufügen, um die Klassifizierung von Nachrichten durch Anti-Spam genauer einzustellen.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Persönliche Filter**.

3 Klicken Sie auf **Hinzufügen**.

4 Geben Sie die Elemente an, nach denen der Filter in einer E-Mail suchen soll (Seite 142).

5 Klicken Sie auf **OK**.

Persönlichen Filter bearbeiten

Sie können vorhandene Filter bearbeiten, um die Spam-Erkennung von Nachrichten genauer einzustellen.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Persönliche Filter**.

3 Wählen Sie den zu bearbeitenden Filter aus, und klicken Sie dann auf **Bearbeiten**.

4 Geben Sie die Elemente an, nach denen der Filter in einer E-Mail suchen soll (Seite 142).

5 Klicken Sie auf **OK**.

Persönlichen Filter entfernen

Nicht mehr benötigte Filter können dauerhaft entfernt werden.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Persönliche Filter**.

3 Wählen Sie den zu entfernenden Filter aus, und klicken Sie dann auf **Entfernen**.

4 Klicken Sie auf **OK**.

Angeben eines persönlichen Filters

In der folgenden Tabelle wird beschrieben, wonach ein persönlicher Filter in einer E-Mail-Nachricht sucht.

Ziel	Aktion
Angeben der zu filternden Teile einer E-Mail	Klicken Sie in der Liste **E-Mail-Teil** auf einen Eintrag, um festzulegen, ob der Filter die Wörter oder Begriffe in der Betreffzeile, im Nachrichtentext, im Header, im Absender oder im Empfänger der Nachricht sucht. Klicken Sie in der Liste **E-Mail-Teil** auf einen Eintrag, um festzulegen, ob der Filter nach E-Mails sucht, die die festgelegten Wörter oder Begriffe enthalten oder nicht enthalten.
Angeben der Wörter oder Ausdrücke in Ihrem Filter	Geben Sie unter **Wörter oder Begriffe** ein, wonach in einer E-Mail gesucht werden soll. Wenn Sie beispielsweise *hypothek* eingeben, werden alle E-Mails, die dieses Wort enthalten, gefiltert.
Angeben, dass der Filter reguläre Ausdrücke verwendet	Wählen Sie **Dieser Filter verwendet reguläre Ausdrücke**.
Auswählen, ob E-Mails entsprechend der Wörter oder Begriffe in Ihrem Filter blockiert oder zugelassen werden sollen	Wählen Sie unter **Diese Aktion ausführen** entweder **Blockieren** oder **Zulassen** aus, um E-Mails zuzulassen oder zu blockieren, die die Wörter oder Begriffe in Ihrem Filter enthalten.

Verwalten des Spam-Schutzes

Sie können den Spam-Schutz deaktivieren, um zu verhindern, dass Anti-Spam E-Mails filtert.

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

Tipp: Denken Sie daran, unter **Spam-Schutz ist aktiviert** auf **An** zu klicken, damit Sie gegen Spam geschützt sind.

KAPITEL 25

Filtern von E-Mail-Nachrichten

Anti-Spam überprüft alle eingehenden E-Mails und stuft sie als Spam (E-Mails, die Sie zum Kauf auffordern) oder als Phishing (E-Mails, mit denen Sie veranlasst werden, persönliche Daten auf einer Website preiszugeben, bei der es sich um Betrug handeln könnte) ein. Anti-Spam markiert dann standardmäßig jede unerwünschte E-Mail als Spam oder Phishing (das Tag [SPAM] oder [PHISH] wird in der Betreffzeile der Nachricht angezeigt) und verschiebt die Nachricht dann in den Ordner "McAfee Anti-Spam".

Sie können in der Anti-Spam-Symbolleiste eine E-Mail als Spam oder keine Spam markieren, den Ort ändern, an den Spam-Nachrichten verschoben werden, oder das Tag ändern, das in der Betreffzeile angezeigt wird.

Wenn Probleme mit Ihrem E-Mail-Programm auftreten, können Sie die Symbolleiste von Anti-Spam im Rahmen der Problembehebung deaktivieren.

In diesem Kapitel

Nachricht über die Anti-Spam-Symbolleiste markieren

Wenn Sie eine Nachricht als Spam markieren, wird die Nachricht in der Betreffzeile mit dem Tag [SPAM] oder einem von Ihnen festgelegten Tag versehen und verbleibt in Ihrem Posteingang, Ihrem Ordner "McAfee Anti-Spam" (Outlook, Outlook Express, Windows Mail, Thunderbird) oder Ihrem Ordner für Junk-E-Mails (Eudora®). Wenn Sie eine Nachricht als Nicht-Spam markieren, wird der Nachrichten-Tag entfernt, und die Nachricht wird in Ihren Posteingang verschoben.

So markieren Sie eine Nachricht in...	Wählen Sie eine Nachricht aus, und...
Outlook, Outlook Express, Windows Mail	Klicken Sie auf **Als Spam markieren** oder **Nicht als Spam markieren**.
Eudora	Klicken Sie im Menü **Anti-Spam** auf **Als Spam markieren** oder auf **Nicht als Spam markieren**.

So markieren Sie eine Nachricht in...	Wählen Sie eine Nachricht aus, und...
Thunderbird	Zeigen Sie in der **Anti-Spam**-Symbolleiste auf **M**, zeigen Sie auf **Markieren als**, und klicken Sie dann auf **Spam** oder **Keine Spam**.

Anti-Spam-Symbolleiste deaktivieren

Wenn Sie Outlook, Outlook Express, Windows Mail, Eudora oder Thunderbird verwenden, können Sie die Anti-Spam-Symbolleiste deaktivieren.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **E-Mail-Symbolleisten**.

3 Deaktivieren Sie das Kontrollkästchen neben der Symbolleiste, die deaktiviert werden soll.

4 Klicken Sie auf **OK**.

Tipp: Sie können die Anti-Spam-Symbolleisten jederzeit wieder aktivieren, indem Sie die entsprechenden Kontrollkästchen aktivieren.

KAPITEL 26

Einrichten von Freunden

Da der verbesserte Filter in Anti-Spam legitime E-Mails erkennt und zulässt, kommt es selten vor, dass Sie die E-Mail-Adressen Ihrer Freunde zu Ihrer Freunde-Liste hinzufügen müssen, egal, ob Sie sie manuell hinzufügen oder Ihre Adressbücher importieren. Wenn Sie dennoch die E-Mail-Adresse eines Freundes hinzufügen möchten und jemand sie fälscht, lässt Anti-Spam Nachrichten von dieser E-Mail-Adresse zu, und sie gelangen in Ihren Posteingang.

Wenn Sie dennoch Ihre Adressbücher importieren möchten und diese sich verändern, müssen Sie sie erneut importieren, da Anti-Spam Ihre Freunde-Listen nicht automatisch aktualisiert.

Sie können Ihre Anti-Spam Freunde-Liste auch manuell aktualisieren oder eine gesamte Domäne hinzufügen, wenn alle Benutzer dieser Domäne zu Ihrer Freunde-Liste hinzugefügt werden sollen. Wenn Sie z. B. die Domäne firma.com hinzufügen, dann wird keine E-Mail aus dieser Organisation gefiltert.

In diesem Kapitel

Importieren von Adressbüchern

Importieren Sie Ihre Adressbücher, wenn Sie möchten, dass Anti-Spam die darin enthaltenen E-Mail-Adressen zu Ihrer Freunde-Liste hinzufügt.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.

3 Klicken Sie im Fenster "Freunde" auf **Importieren**.

4 Wählen Sie den Typ des zu importierenden Adressbuchs in der Liste **Adressbuch für Import auswählen** aus.

5 Klicken Sie auf **Jetzt importieren**.

Manuelles Einrichten von Freunden

Sie aktualisieren Ihre Freunde-Liste manuell, indem Sie die Einträge einzeln bearbeiten. Sie können z. B. die E-Mail-Adresse eines Freundes, die sich nicht in Ihrem Adressbuch befindet, direkt nach Erhalt einer E-Mail dieses Freundes manuell hinzufügen. Am einfachsten geschieht dies unter Verwendung der Anti-Spam-Symbolleiste. Wenn Sie die Anti-Spam-Symbolleiste nicht verwenden, müssen Sie die Informationen Ihres Freundes angeben.

Einen Freund über die Anti-Spam-Symbolleiste hinzufügen

Wenn Sie eines der E-Mail-Programme Outlook, Outlook Express, Windows Mail, Eudora™ oder Thunderbird verwenden, können Sie Freunde direkt über die Anti-Spam-Symbolleiste hinzufügen.

So fügen Sie einen Freund hinzu in...	Wählen Sie eine Nachricht aus, und...
Outlook, Outlook Express, Windows Mail	klicken Sie auf **Freund hinzufügen**.
Eudora	Klicken Sie im Menü **Anti-Spam** auf **Freund hinzufügen**.
Thunderbird	Zeigen Sie in der **Anti-Spam**-Symbolleiste auf **M**, zeigen Sie auf **Markieren als**, und klicken Sie dann auf **Freund**.

Freund manuell hinzufügen

Wenn Sie einen Freund nicht direkt aus der Symbolleiste hinzufügen möchten, oder wenn Sie dies nach dem Erhalt einer E-Mail vergessen, können Sie dennoch einen Freund zu Ihrer Freunde-Liste hinzufügen.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.

3 Klicken Sie im Fenster "Freunde" auf **Hinzufügen**.

4 Geben Sie in das Feld **Name** den Namen des Freundes ein.

5 Wählen Sie in der Liste **Typ** das Element **Einzelne E-Mail-Adresse** aus.

6 Geben Sie im Feld **E-Mail-Adresse** die E-Mail-Adresse Ihres Freundes ein.

7 Klicken Sie auf **OK**.

Domäne hinzufügen

Fügen Sie eine gesamte Domäne hinzu, wenn Sie jeden Benutzer in dieser Domäne zu Ihrer Freunde-Liste hinzufügen möchten. Wenn Sie z. B. die Domäne firma.com hinzufügen, dann wird keine E-Mail aus dieser Organisation gefiltert.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.

3 Klicken Sie im Fenster "Freunde" auf **Hinzufügen**.

4 Geben Sie im Feld **Name** den Namen der Organisation oder Gruppe ein.

5 Wählen Sie in der Liste **Typ** das Element **Gesamte Domäne** aus.

6 Geben Sie im Feld **E-Mail-Adresse** den Domänennamen ein.

7 Klicken Sie auf **OK**.

Daten für diesen Freund bearbeiten

Wenn sich die Informationen zu einem Freund ändern, können Sie die Liste Ihrer Freunde aktualisieren, damit Anti-Spam Nachrichten Ihrer Freunde nicht als Spam kennzeichnet.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.

3 Wählen Sie den zu bearbeitenden Freund aus, und klicken Sie anschließend auf **Bearbeiten**.

4 Ändern Sie im Feld **Name** den Namen des Freundes.

5 Ändern Sie im Feld **E-Mail-Adresse** die E-Mail-Adresse Ihres Freundes.

6 Klicken Sie auf **OK**.

Domäne bearbeiten

Wenn sich die Informationen für eine Domäne ändern, können Sie Ihre Freunde-Liste aktualisieren, um sicherzustellen, dass Anti-Spam Nachrichten von dieser Domäne nicht als Spam kennzeichnet.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.

3 Klicken Sie im Fenster "Freunde" auf **Hinzufügen**.

4 Ändern Sie den Namen der Organisation oder Gruppe im Feld **Name**.

5 Wählen Sie in der Liste **Typ** das Element **Gesamte Domäne** aus.

6 Ändern Sie im Feld **E-Mail-Adresse** den Domänennamen.

7 Klicken Sie auf **OK**.

Freund entfernen

Wenn eine Person oder eine Domäne in Ihrer Freunde-Liste Ihnen Spam-E-Mails sendet, entfernen Sie sie von Ihrer Anti-Spam Freunde-Liste, damit die entsprechenden E-Mail-Nachrichten wieder gefiltert werden.

1 Öffnen Sie den Bereich "Spam-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
   2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Freunde**.

3 Wählen Sie den zu entfernenden Freund aus, und klicken Sie dann auf **Entfernen**.

KAPITEL 27

Einrichten Ihrer Webmail-Konten

Wenn Sie zum Abrufen Ihrer E-Mail-Nachrichten einen Browser verwenden, müssen Sie Anti-Spam so konfigurieren, dass es eine Verbindung zu Ihrem Konto herstellt und Ihre Nachrichten filtert. Um Ihr Webmail-Konto zu Anti-Spam hinzuzufügen, fügen Sie einfach die Kontoinformationen hinzu, die Sie von Ihrem E-Mail-Anbieter erhalten haben.

Nach dem Hinzufügen eines Webmail-Kontos können Sie Ihre Kontoinformationen bearbeiten und weitere Informationen über die gefilterte Webmail abrufen. Wenn Sie das Webmail-Konto nicht mehr verwenden oder es nicht mehr gefiltert werden soll, können Sie es entfernen.

Anti-Spam kann mit verschiedenen E-Mail-Programmen verwendet werden, wie etwa Yahoo!®, MSN®/Hotmail®, Windows® Mail und Live™ Mail, Microsoft® Outlook® und Outlook Express sowie Mozilla Thunderbird™, sowie auch in Verbindung mit verschiedenen E-Mail-Konten, wie etwa POP3, POP3 Webmail und MAPI (Microsoft Exchange Server). POP3 ist der häufigste Kontotyp und gleichzeitig der Standardtyp für Internet-E-Mail. Bei einem POP3-Konto stellt Anti-Spam eine direkte Verbindung zum E-Mail-Server her und filtert dort die Nachrichten, bevor sie durch das Webmail-Konto abgerufen werden. POP3 Webmail-, Yahoo!-, MSN/Hotmail- und Windows Mail-Konten sind webbasiert. POP3-Webmail-Konten werden auf ähnliche Weise wie POP3-Konten gefiltert.

In diesem Kapitel

Webmail-Konto hinzufügen

Fügen Sie ein POP3- (z. B. Yahoo), MSN/Hotmail- oder Windows Mail- (nur bezahlte Versionen werden voll unterstützt) Webmail-Konto hinzu, wenn Sie die Nachrichten in diesem Konto nach Spam filtern möchten.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Webmail-Konten**.

3 Klicken Sie im Bereich "Webmail-Konten" auf **Hinzufügen**.

4 Geben Sie die Kontoinformationen (Seite 153) an, und klicken Sie dann auf **Weiter**.

5 Geben Sie unter **Überprüfungsoptionen** an, wann Anti-Spam Ihr Konto auf Spam überprüfen soll (Seite 153).

6 Wenn Sie eine Einwahlverbindung verwenden, geben Sie an, wie Anti-Spam eine Verbindung zum Internet herstellt (Seite 153).

7 Klicken Sie auf **Fertig stellen**.

Webmail-Konto bearbeiten

Bei Änderungen an Ihrem Webmail-Konto müssen Sie Ihre Kontoinformationen bearbeiten. Bearbeiten Sie Ihr Webmail-Konto z. B., wenn Sie Ihr Kennwort ändern oder wenn Anti-Spam die Nachrichten häufiger auf Spam überprüfen soll.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Webmail-Konten**.

3 Wählen Sie das Konto aus, das bearbeitet werden soll, und klicken Sie dann auf **Bearbeiten**.

4 Geben Sie die Kontoinformationen (Seite 153) an, und klicken Sie dann auf **Weiter**.

5 Geben Sie unter **Überprüfungsoptionen** an, wann Anti-Spam Ihr Konto auf Spam überprüfen soll (Seite 153).

6 Wenn Sie eine Einwahlverbindung verwenden, geben Sie an, wie Anti-Spam eine Verbindung zum Internet herstellt (Seite 153).

7 Klicken Sie auf **Fertig stellen**.

Webmail-Konto entfernen

Wenn ein Webmail-Konto nicht mehr nach Spam gefiltert werden soll, entfernen Sie dieses Konto. Wenn Ihr Konto z. B. nicht mehr aktiv ist oder Probleme damit auftreten, können Sie das Konto während der Problembehebung entfernen.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **Webmail-Konten**.

3 Wählen Sie das zu entfernende Konto aus, und klicken Sie dann auf **Entfernen**.

Erläuterungen zu den Webmail-Kontoinformationen

In den folgenden Tabellen werden die Informationen beschrieben, die Sie angeben müssen, wenn Sie ein Webmail-Konto hinzufügen oder bearbeiten.

Kontoinformationen

Informationen	Beschreibung
Beschreibung	Beschreiben Sie das Konto für Ihre eigenen Referenzzwecke. Sie können beliebige Informationen in dieses Feld eingeben.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse an, die zu diesem E-Mail-Konto gehört.
Kontotyp	Geben Sie den E-Mail-Kontotyp an, den Sie hinzufügen möchten, z. B. POP3 Webmail oder MSN/Hotmail.
Server	Geben Sie den Namen des Mailservers an, der dieses Konto hostet. Den Namen des Servers finden Sie in den Informationen, die Sie von Ihrem Internetdienstanbieter (Internet Service Provider, ISP) erhalten haben.

Informationen	Beschreibung
Benutzername	Geben Sie den Benutzernamen für dieses E-Mail-Konto an. Wenn z. B. Ihre E-Mail-Adresse *Benutzername*@hotmail.com lautet, dann lautet der Benutzername wahrscheinlich *Benutzername*.
Kennwort	Geben Sie das Kennwort für dieses E-Mail-Konto an.
Kennwort bestätigen	Bestätigen Sie das Kennwort für dieses E-Mail-Konto.

Überprüfungsoptionen

Option	Beschreibung
Überprüfen alle	Anti-Spam überprüft dieses Konto auf Spam im angegebenen Intervall (Anzahl Minuten). Das Intervall muss zwischen 5 und 3600 Minuten liegen.
Beim Starten prüfen	Anti-Spam überprüft dieses Konto jedes Mal, wenn Sie den Computer neu starten.

Verbindungsoptionen

Option	Beschreibung
Nie eine Einwahlverbindung herstellen	Anti-Spam stellt nicht automatisch eine Einwahlverbindung her. Sie müssen Ihre Einwahlverbindung manuell starten.
Einwählen, wenn keine Verbindung verfügbar ist	Wenn keine Internetverbindung vorhanden ist, versucht Anti-Spam automatisch, unter Verwendung der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.
Immer mit der angegebenen Verbindung einwählen	Anti-Spam versucht unter Verwendung der angegebenen Einwahlverbindung eine Verbindung herzustellen. Wenn die aktuelle Verbindung nicht über die angegebene Einwahlverbindung hergestellt wurde, wird die Verbindung getrennt.
Mit dieser Verbindung einwählen	Geben Sie die Einwahlverbindung an, mit der Anti-Spam eine Verbindung zum Internet herstellt.
Verbindung beibehalten, nachdem die Filterung abgeschlossen wurde	Ihr Computer bleibt mit dem Internet verbunden, nachdem der Filtervorgang abgeschlossen wurde.

KAPITEL 28

Arbeiten mit gefilterten E-Mails

Manchmal werden Spam-Nachrichten nicht als solche erkannt. Wenn dies passiert, können Sie die Spam-Nachrichten an McAfee senden, wo diese analysiert werden, um entsprechende Filteraktualisierungen zu erstellen.

Wenn Sie ein Webmail-Konto verwenden, können Sie die gefilterten E-Mail-Nachrichten anzeigen, exportieren oder löschen. Dies ist dann hilfreich, wenn Sie nicht sicher sind, ob eine seriöse Nachricht gefiltert wurde, oder wenn Sie wissen möchten, wann die Nachricht gefiltert wurde.

In diesem Kapitel

Melden von E-Mail-Nachrichten an McAfee

Sie können E-Mail-Nachrichten an McAfee melden, wenn Sie diese als Spam oder als kein Spam markieren, damit wir sie analysieren können, um Filter-Updates zu erstellen.

1 Öffnen Sie den Bereich "Spam-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **E-Mail & IM**.
2. Klicken Sie im E-Mail- & IM-Informationsbereich auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereich von "E-Mail & IM" unter **Spam-Schutz** auf **Erweitert**.

2 Klicken Sie im Bereich "Spam-Schutz" auf **E-Mail-Symbolleisten**.

3 Wählen Sie unter **Helfen Sie uns, Anti-Spam zu verbessern** die entsprechenden Kontrollkästchen, und klicken Sie dann auf **OK**.

Ziel	Aktion
Melden E-Mails an McAfee jedes Mal, wenn Sie eine als Spam markieren	Wählen Sie **Sie markieren E-Mails als Spam**.

Ziel	Aktion
Melden von E-Mails an McAfee jedes Mal, wenn Sie eine als keine Spam markieren	Wählen Sie **Sie markieren E-Mails als keine Spam**.
Senden der gesamten E-Mail, nicht nur des Headers an McAfee, wenn Sie eine E-Mail als keine Spam melden.	Wählen Sie **Gesamte E-Mail senden (nicht nur Header)**.

Hinweis: Wenn Sie eine E-Mail als keine Spam melden und die gesamte E-Mail an McAfee senden, wird die E-Mail nicht verschlüsselt.

Anzeigen, exportieren oder löschen gefilterter Webmail

Sie können Nachrichten, die in Ihrem Webmail-Konto gefiltert wurden, anzeigen, exportieren oder löschen.

1. Klicken Sie unter **Häufige Tasks** auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Gefilterte Webmail**.
3. Wählen Sie eine Nachricht aus.
4. Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:
   - Klicken Sie auf **Anzeigen**, um die Nachricht in Ihrem standardmäßigen E-Mail-Programm anzuzeigen.
   - Klicken Sie auf **Exportieren**, um die Nachricht auf Ihren Computer zu kopieren.
   - Klicken Sie auf **Löschen**, um die Nachricht zu löschen.

Ereignis für gefilterte Webmail anzeigen

Sie können anzeigen, an welchem Datum und zu welcher Uhrzeit eine E-Mail-Nachricht gefiltert und auf welchem Konto sie empfangen wurde.

1. Klicken Sie unter **Häufige Tasks** auf **Zuletzt aufgetretene Ereignisse anzeigen**.
2. Klicken Sie im Bereich "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
3. Erweitern Sie im linken Bereich die Liste **E-Mail & IM**, und klicken Sie anschließend auf **Webmail-Filterereignisse**.
4. Wählen Sie das Protokoll aus, das Sie anzeigen möchten.

KAPITEL 29

Konfigurieren des Phishing-Schutzes

Anti-Spam stuft unerwünschte E-Mail-Nachrichten als Spam (E-Mails, die Sie zum Kauf auffordern) oder als Phishing (E-Mails, mit denen Sie veranlasst werden, persönliche Daten auf einer Website preiszugeben, bei der es sich um Betrug handelt oder handeln könnte) ein. Der Phishing-Schutz schützt Sie vor dem Zugriff auf betrügerische Websites. Wenn Sie in einer E-Mail auf eine Verknüpfung zu einer Website klicken, bei der es sich um Betrug handelt oder handeln könnte, werden Sie zurück auf die sichere Phishing-Filterseite geleitet.

Wenn es Websites gibt, die Sie nicht filtern möchten, fügen Sie sie der Weißen Phishing-Liste hinzu. Sie können die Websites auch bearbeiten oder aus der Weißen Liste entfernen. Zu dieser Liste müssen Sie Sites wie Google®, Yahoo oder McAfee nicht hinzufügen, da diese Websites nicht als betrügerisch angesehen werden.

Hinweis: Wenn Sie SiteAdvisor installiert haben, erhalten Sie nicht den Phishing-Schutz von Anti-Spam, da SiteAdvisor bereits über einen ähnlichen Phishing-Schutz verfügt.

In diesem Kapitel

Website zur Weißen Liste hinzufügen

Sie können Websites, die nicht gefiltert werden sollen, der Weißen Liste hinzufügen.

1. Öffnen Sie den Bereich "Phishing-Schutz".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
   2. Klicken Sie im Informationsbereich zu "Internet & Netzwerk" auf **Konfigurieren**.

2. Klicken Sie im Bereich "Phishing-Schutz" auf **Erweitert**.
3. Klicken Sie unter **Weiße Liste** auf **Hinzufügen**.
4. Geben Sie die Adresse der Website ein, und klicken Sie dann auf **OK**.

Websites in Ihrer Weißen Liste bearbeiten

Wenn Sie eine Website zur Weißen Liste hinzugefügt haben und sich die Adresse dieser Website ändert, können Sie die Liste jederzeit aktualisieren.

1 Öffnen Sie den Bereich "Phishing-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
2. Klicken Sie im Informationsbereich zu "Internet & Netzwerk" auf **Konfigurieren**.

2 Klicken Sie im Bereich "Phishing-Schutz" auf **Erweitert**.

3 Wählen Sie unter **Weiße Liste** die Website aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Bearbeiten**.

4 Bearbeiten Sie die Adresse der Website, und klicken Sie dann auf **OK**.

Website aus der Weißen Liste entfernen

Wenn Sie eine Website zur Weißen Liste hinzugefügt haben, weil Sie darauf zugreifen wollten, diese jetzt aber filtern lassen möchten, entfernen Sie sie aus der Weißen Liste.

1 Öffnen Sie den Bereich "Phishing-Schutz".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
2. Klicken Sie im Informationsbereich zu "Internet & Netzwerk" auf **Konfigurieren**.

2 Klicken Sie im Bereich "Phishing-Schutz" auf **Erweitert**.

3 Wählen Sie unter **Weiße Liste** die Website aus, die Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.

Deaktivieren des Phishing-Schutzes

Wenn Sie bereits über Phishing-Software verfügen, die nicht von McAfee stammt, und es zu Konflikten kommt, können Sie den Phishing-Schutz von Anti-Spam deaktivieren.

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
2. Klicken Sie im Informationsbereich zu "Internet & Netzwerk" auf **Konfigurieren**.
3. Klicken Sie unter **Phishing-Schutz ist aktiviert** auf **Aus**.

Tipp: Denken Sie daran, nach der ausgeführten Aktion unter **Phishing-Schutz ist deaktiviert** wieder auf **An** zu klicken, damit Sie vor betrügerischen Websites geschützt sind.

KAPITEL 30

McAfee Parental Controls

Die Kindersicherungen bieten umfassenden Schutz für Sie, Ihre Familie, Ihre persönlichen Dateien und Ihren PC. Sie helfen dabei, Sie vor Online-Identitätsdiebstahl zu schützen, die Übertragung persönlicher Informationen zu verhindern und potentiell anstößige Online-Inhalte (einschließlich Bilder) zu filtern. Sie erlauben es Ihnen auch, nicht autorisierte Webbrowsing-Gewohnheiten zu überwachen, zu kontrollieren und aufzuzeichnen, und bieten einen sicheren Speicherbereich für persönliche Kennwörter.

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

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

Funktionen der Kindersicherungen

Kindersicherungen	Sie filtern für SecurityCenter-Benutzer potentiell unangemessene Bilder, aktivieren das altersgerechte Suchen, konfigurieren Inhaltsklassifikationsgruppen (Altersgruppen, die für die Beschränkung der Websites und der Inhalte verwendet werden, die ein Benutzer anzeigen kann) und setzen zeitliche Beschränkungen für das Surfen im Internet (der Zeitraum, während dessen ein Benutzer auf das Internet zugreifen kann). Mit den Kindersicherungen können Sie außerdem allgemeine Beschränkungen für den Zugriff auf bestimmte Websites festlegen oder den Zugriff auf der Grundlage verknüpfter Stichwörter gewähren oder blockieren.
Schutz für persönliche Informationen	Sie können die Übertragung sensibler oder vertraulicher Informationen (z. B. Kreditkartennummern, Bankkontonummern, Adressen usw.) über das Internet blockieren.
Kennwortdepot	Speichern Sie Ihre persönlichen Kennwörter an einem sicheren Ort, sodass kein anderer Benutzer (nicht einmal ein Administrator) darauf zugreifen kann.

KAPITEL 31

Ihre Kinder schützen

Wenn Ihre Kinder Ihren Computer verwenden, können Sie die Kindersicherungen verwenden, um einzuschränken, was jedes Kind anzeigen und tun darf, wenn es im Internet surft. Sie können beispielsweise das altersgerechte Suchen und die Bildfilterung aktivieren oder deaktivieren, eine Inhaltsklassifikationsgruppe wählen und zeitliche Beschränkungen für das Surfen im Internet festlegen.

Durch das altersgerechte Suchen können Sie gewährleisten, dass die Sicherheitsfilter einiger bekannter Suchmaschinen aktiviert sind und dass dadurch potentiell unangemessene Seiten automatisch von den Suchergebnissen Ihres Kindes ausgeschlossen werden. Die Bildfilterung blockiert potentiell unangemessene Bilder, sodass diese für Kinder nicht angezeigt werden. Die Inhaltsklassifikationsgruppe bestimmt die Art von Webinhalt, die für ein Kind zugänglich sein soll, basierend auf der Altersgruppe des Kindes. Mit den zeitlichen Beschränkungen für das Surfen im Internet definieren Sie die Tage und Uhrzeiten, wann ein Kind auf das Internet zugreifen darf. Die Kindersicherung ermöglicht Ihnen ebenfalls, bestimmte Websites für alle Kinder zu filtern (zu blockieren oder zuzulassen).

Hinweis: Um die Kindersicherungen zum Schutz Ihrer Kinder zu konfigurieren, müssen Sie sich an Ihrem Computer als Windows-Administrator anmelden. Wenn Sie ein Upgrade von einer älteren Version dieses McAfee-Produkts durchgeführt haben und noch immer McAfee-Benutzer verwenden, müssen Sie sicherstellen, dass Sie als McAfee-Administrator angemeldet sind.

In diesem Kapitel

Filtern von Websites mithilfe von Stichwörtern

Mit der Stichwort-Filterung können Sie verhindern, dass Benutzer, die nicht zur Gruppe der Erwachsenen gehören, Websites mit potentiell anstößigen Stichwörtern anzeigen. Wenn die Stichwort-Filterung aktiviert ist, werden die Inhalte für Benutzer entsprechend ihrer Inhaltsqualifikationsgruppe mithilfe der Standardliste der Stichwörter und der entsprechenden Regeln bewertet. Die Benutzer müssen einer bestimmten Gruppe angehören, um auf Websites zugreifen zu können, die bestimmte Stichwörter enthalten. Beispielsweise können nur Mitglieder der Gruppe der Erwachsenen Websites besuchen, die das Wort *Porno* enthalten, und nur Mitglieder der Gruppe der Kinder (und älter) können Websites mit dem Wort *Drogen* besuchen.

Sie können auch Ihre eigenen Stichwörter zur Standardliste hinzufügen und diese mit bestimmten Inhaltsklassifikationsgruppen verknüpfen. Von Ihnen hinzugefügte Stichwortregeln überschreiben Regeln, die möglicherweise bereits mit einem identischen Stichwort in der Standardliste verknüpft sind.

Blockieren von Websites auf der Grundlage von Stichwörtern

Wenn Sie Websites aufgrund von anstößigen Inhalten blockieren möchten, aber die genauen Website-Adressen nicht kennen, können Sie die Sites auf der Grundlage ihrer Stichwörter blockieren. Geben Sie einfach ein Stichwort ein, und legen Sie fest, welche Inhaltsklassifikationsgruppen Websites mit diesem Stichwort anzeigen können.

1 Öffnen Sie den Bereich "Parental Controls".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Parental Controls" auf **Stichwörter**, und stellen Sie sicher, dass die Stichwort-Filterung aktiviert ist.

3 Geben Sie unter **Stichwörter** im Feld **Suchen nach** das gewünschte Stichwort ein.

4 Bewegen Sie den Schieberegler **Mindestalter**, um eine Mindestaltersgruppe anzugeben.
Benutzer dieser und höherer Altersgruppen können Websites anzeigen, die das Stichwort enthalten.

5 Klicken Sie auf **OK**.

Deaktivieren der Stichwort-Filterung

Standardmäßig ist die Stichwort-Filterung aktiviert. Das bedeutet, dass die die Inhalte für Benutzer entsprechend ihrer Inhaltsqualifikationsgruppe mithilfe der Standardliste der Stichwörter und der entsprechenden Regeln bewertet werden. Sie können die Stichwort-Filterung jederzeit deaktivieren, McAfee empfiehlt dies jedoch nicht.

1 Öffnen Sie den Bereich "Parental Controls".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Parental Controls" auf **Stichwörter**.

3 Klicken Sie im Bereich "Stichwörter" auf **Aus**.

4 Klicken Sie auf **OK**.

Filtern von Websites

Sie können Websites für alle Benutzer filtern (blockieren oder zulassen), die nicht zur Gruppe der Erwachsenen gehören. Sie können eine Website blockieren, um zu verhindern, dass Ihre Kinder beim Surfen im Internet darauf zugreifen. Wenn ein Kind versucht, auf eine blockierte Website zuzugreifen, wird eine Nachricht angezeigt, dass auf die Site nicht zugegriffen werden kann, da sie von McAfee blockiert wird.

Sie können eine Website zulassen, wenn diese von McAfee standardmäßig blockiert wurde, sie jedoch für Ihre Kinder zugänglich sein soll. Weitere Informationen zu Websites, die von McAfee standardmäßig blockiert werden, finden Sie unter Filtern von Websites mithilfe von Stichwörtern (Seite 166). Sie können eine gefilterte Website auch jederzeit aktualisieren oder entfernen.

Hinweis: Benutzer (einschließlich Administratoren), die der Gruppe der Erwachsenen angehören, können auf alle Websites zugreifen, selbst wenn diese blockiert wurden. Um die gesperrten Websites zu testen, müssen Sie sich als minderjähriger Benutzer anmelden – denken Sie jedoch daran, das Surfprotokoll in Ihrem Webbrowser zu löschen, wenn Sie den Test beendet haben.

Entfernen einer gefilterten Website

Wenn Sie eine gefilterte Website nicht mehr blockieren oder zulassen möchten, können Sie diese entfernen.

1. Öffnen Sie den Bereich "Parental Controls".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2. Klicken Sie im Bereich "Parental Controls" auf **Gefilterte Websites**.
3. Klicken Sie im Bereich "Gefilterte Websites" auf einen Eintrag in der Liste **Gefilterte Websites**, und klicken Sie dann auf **Entfernen**.
4. Klicken Sie auf **OK**.

Aktualisieren einer gefilterten Website

Wenn sich eine Website-Adresse ändert oder Sie diese beim Blockieren oder Zulassen falsch eingeben, können Sie sie aktualisieren.

1 Öffnen Sie den Bereich "Parental Controls".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Parental Controls" auf **Gefilterte Websites**.

3 Klicken Sie im Bereich "Gefilterte Websites" auf einen Eintrag in der Liste **Gefilterte Websites**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.

4 Klicken Sie auf **OK**.

Zulassen einer Website

Sie können eine Website zulassen, um sicherzustellen, dass diese für keinen Benutzer blockiert wird. Wenn Sie eine Website zulassen, die von McAfee standardmäßig blockiert wurde, wird die Standardeinstellung überschrieben.

1 Öffnen Sie den Bereich "Parental Controls".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Parental Controls" auf **Gefilterte Websites**.

3 Geben Sie im Bereich "Gefilterte Websites" im Feld **http://** eine Website-Adresse ein, und klicken Sie dann auf **Zulassen**.

4 Klicken Sie auf **OK**.

Tipp: Sie können eine zuvor blockierte Website zulassen, indem Sie in der Liste **Gefilterte Websites** auf die Adresse der Website und anschließend auf **Zulassen** klicken.

Blockieren einer Website

Sie können eine Website blockieren, um zu verhindern, dass Ihre Kinder beim Surfen im Internet darauf zugreifen. Wenn ein Kind versucht, auf eine blockierte Website zuzugreifen, wird eine Nachricht angezeigt, dass auf die Site nicht zugegriffen werden kann, da sie von McAfee blockiert wird.

1 Öffnen Sie den Bereich "Parental Controls".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Vergewissern Sie sich im Bereich für die Konfiguration der Kindersicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Parental Controls" auf **Gefilterte Websites**.

3 Geben Sie im Bereich "Gefilterte Websites" im Feld **http://** eine Website-Adresse ein, und klicken Sie dann auf **Blockieren**.

4 Klicken Sie auf **OK**.

Tipp: Sie können eine zuvor zugelassene Website blockieren, indem Sie in der Liste **Gefilterte Websites** auf die Adresse der Website und anschließend auf **Blockieren** klicken.

Festlegen von Zeitbeschränkungen beim Surfen im Internet

Wenn Sie sich Sorgen um den verantwortungsvollen Umgang mit dem Internet oder dessen übermäßige Nutzung machen, können Sie für Ihre Kinder angemessene Zeitbeschränkungen für das Surfen im Internet festlegen. Wenn Sie das Surfen im Internet für Ihre Kinder auf bestimmte Zeiten beschränken, können Sie sich darauf verlassen, dass das SecurityCenter diese Beschränkungen durchsetzt – auch dann, wenn Sie nicht zu Hause sind.

Standardmäßig darf ein Kind sieben Tage pro Woche den ganzen Tag und die ganze Nacht im Internet surfen. Sie können das Surfen im Internet jedoch auf bestimmte Zeiten oder Tage beschränken oder ganz unterbinden. Wenn ein Kind versucht, zu einer Zeit im Internet zu surfen, zu der dies nicht zulässig ist, wird es von McAfee benachrichtigt, dass das Surfen im Internet zu diesem Zeitpunkt nicht möglich ist. Wenn Sie das Surfen im Internet ganz unterbinden möchten, kann sich das Kind anmelden und den Computer einschließlich anderer Internetprogramme wie E-Mail, Sofortnachrichtenprogramme, FTP, Spiele usw. verwenden, jedoch nicht im Internet surfen.

Festlegen von Zeitbeschränkungen beim Surfen im Internet

Mit dem Zeitraster zum Beschränken des Surfens im Internet können Sie das Surfen im Internet für ein Kind auf bestimmte Tage und Zeiten beschränken.

1. Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereichs für die Kindersicherung auf die Option **Erweitert**.
   4. Klicken Sie im Bereich für die Kindersicherung auf **Benutzereinstellungen**.

2. Klicken Sie im Bereich "Benutzereinstellungen" auf einen Benutzernamen, und klicken Sie anschließend auf **Bearbeiten**.
3. Im Fenster "Benutzerkonto bearbeiten" unter **Zeitlichen Beschränkungen für das Surfen im Internet** können Sie durch Ziehen der Maus die Tage und Zeiten festlegen, zu denen dieser Benutzer nicht im Internet surfen darf.
4. Klicken Sie auf **OK**.

Einrichten der Inhaltsklassifikationsgruppe

Ein Benutzer kann zu einer der folgenden Inhaltsklassifikationsgruppen gehören:

- Kleines Kind
- Kind
- Junger Teenager
- Älterer Teenager
- Erwachsener

Die Kindersicherungen bewerten Webinhalte (blockiert diese oder lässt diese zu) auf der Grundlage der Gruppe, zu der ein Benutzer gehört. Auf diese Weise können Sie bestimmte Websites für bestimmte Benutzer in Ihrem Haushalt blockieren oder zulassen. Beispielsweise können Sie bestimmte Webinhalte für Benutzer blockieren, die zur Gruppe der kleinen Kinder gehören, diese jedoch für Benutzer der Gruppe der jungen Teenager zulassen. Wenn Sie Inhalte für einen Benutzer stärker begrenzen möchten, können Sie auch festlegen, dass der Benutzer nur Websites anzeigen kann, die in der Liste **Gefilterte Websites** enthalten sind. Weitere Informationen finden Sie unter Filtern von Websites (Seite 168).

Erstellen der Inhaltsklassifikationsgruppe eines Benutzers

Standardmäßig wird ein neuer Benutzer der Gruppe der Erwachsenen hinzugefügt, sodass alle Webinhalte für den Benutzer zugänglich sind. Anschließend können Sie die Inhaltsklassifikationsgruppe für einen Benutzer in Abhängigkeit von dessen Alter und Entwicklungsstufe anpassen.

1 Öffnen Sie den Bereich "Benutzereinstellungen".

Wie?

1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
3. Klicken Sie im Konfigurationsbereichs für die Kindersicherung auf die Option **Erweitert**.
4. Klicken Sie im Bereich für die Kindersicherung auf **Benutzereinstellungen**.

2 Klicken Sie im Bereich "Benutzereinstellungen" auf einen Benutzernamen, und klicken Sie anschließend auf **Bearbeiten**.

3 Klicken Sie im Fenster "Benutzerkonto bearbeiten" unter **Inhaltsfilter** auf die Altersgruppe, die Sie dem Benutzer zuweisen möchten.

   Wenn Sie verhindern möchten, dass der Benutzer Websites besucht, die in der Liste **Gefilterte Websites** blockiert sind, aktivieren Sie das Kontrollkästchen **Dieser Benutzer verfügt nur über Zugriff auf die Websites in der Liste "Zulässige Websites"**.

4 Klicken Sie auf **OK**.

Filtern potentiell anstößiger Web-Bilder

In Abhängigkeit vom Alter oder der Entwicklungsstufe eines Benutzers können Sie potentiell anstößige Bilder beim Surfen im Internet filtern (blockieren oder zulassen). Beispielsweise können Sie die Anzeige potentiell anstößiger Bilder blockieren, wenn Ihre kleinen Kinder im Internet surfen, diese jedoch für ältere Teenager und Erwachsene in Ihrem Haushalt zulassen. Standardmäßig ist die Bild-Filterung für alle Mitglieder der Gruppe der Erwachsenen deaktiviert. Dies bedeutet, dass potentiell anstößige Bilder angezeigt werden, wenn diese Benutzer im Internet surfen. Weitere Informationen zum Festlegen der Altersgruppe für einen Benutzer finden Sie unter Einrichten der Inhaltsklassifikationsgruppe (Seite 172).

Filtern potentiell anstößiger Web-Bilder

Standardmäßig werden neue Benutzer zur Gruppe der Erwachsenen hinzugefügt, und die Bild-Filterung ist deaktiviert. Wenn Sie die Anzeige potentiell anstößiger Bilder blockieren möchten, wenn ein bestimmter Benutzer im Internet surft, können Sie die Bild-Filterung aktivieren. Jedes potentiell anstößige Web-Bild wird automatisch durch ein statisches McAfee-Bild ersetzt.

1 Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereichs für die Kindersicherung auf die Option **Erweitert**.
   4. Klicken Sie im Bereich für die Kindersicherung auf **Benutzereinstellungen**.

2 Klicken Sie im Bereich "Benutzereinstellungen" auf einen Benutzernamen, und klicken Sie anschließend auf **Bearbeiten**.

3 Klicken Sie im Fenster "Benutzerkonto bearbeiten" unter **Bild-Filterung** auf **Ein**.

4 Klicken Sie auf **OK**.

Aktivieren der altersgerechten Suche

Einige bekannte Suchmaschinen (wie Yahoo! oder Google) bieten "sicheres Suchen" – eine Sucheinstellung, die verhindert, dass potentiell unangemessene Suchergebnisse in ihren Ergebnislisten angezeigt werden. Diese Suchmaschinen lassen Sie normalerweise wählen, wie stark Sie den Filter für sicheres Suchen einschränken möchten, Sie oder ein anderer Benutzer können diesen Filter jedoch auch jederzeit wieder deaktivieren.

Das altersgerechte Suchen in den Kindersicherungen ist ein einfacher Weg, um sicherzustellen, dass "sicheres Suchen" stets aktiviert ist, wenn ein Benutzer eine der folgenden Suchmaschinen verwendet:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Wenn Sie das altersgerechte Suchen aktivieren, gewährleisten wir, dass der Filter für "sicheres Suchen" der Suchmaschine stets für diesen Benutzer aktiviert und auf die strengste Beschränkung eingestellt ist. Wenn ein Benutzer versucht, den Filter zu deaktivieren (in den Voreinstellungen oder den erweiterten Einstellungen der Suchmaschine), aktivieren wir ihn automatisch wieder.

Standardmäßig ist das altersgerechte Suchen für alle Benutzer außer Administratoren und Benutzer in der Altersgruppe der Erwachsenen aktiviert. Weitere Informationen zum Festlegen der Altersgruppe für einen Benutzer finden Sie unter Einrichten der Inhaltsklassifikationsgruppe (Seite 172).

Aktivieren des altersgerechten Suchens

Standardmäßig werden neue Benutzer zur Gruppe der Erwachsenen hinzugefügt, und das altersgerechte Suchen ist deaktiviert. Wenn Sie sicherstellen möchten, dass die Filterung für sicheres Suchen, die einige Suchmaschinen anbieten, für einen erwachsenen Benutzer aktiviert ist, können Sie das altersgerechte Suchen aktivieren.

1 Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   2. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   3. Klicken Sie im Konfigurationsbereichs für die Kindersicherung auf die Option **Erweitert**.
   4. Klicken Sie im Bereich für die Kindersicherung auf **Benutzereinstellungen**.

2 Klicken Sie im Bereich "Benutzereinstellungen" auf einen Benutzernamen, und klicken Sie anschließend auf **Bearbeiten**.

3 Klicken Sie im Fenster "Benutzerkonto bearbeiten" unter **Altersgerechtes Suchen** auf **Ein**.

4 Klicken Sie auf **OK**.

KAPITEL 32

Konfigurieren von Benutzerkonten

Um die Kindersicherungen zum Schutz Ihrer Kinder zu konfigurieren, weisen Sie ihnen im SecurityCenter bestimmte Berechtigungen zu. Diese Berechtigungen bestimmen, was jedes Kind im Internet anzeigen und tun kann.

Standardmäßig entsprechen die SecurityCenter-Benutzerkonten den Windows-Benutzerkonten, die Sie auf Ihrem Computer eingerichtet haben. Wenn Sie jedoch ein Upgrade von einer früheren Version des SecurityCenter durchgeführt haben, die McAfee-Benutzerkonten verwendet, bleiben die McAfee-Benutzerkonten und deren Berechtigungen erhalten.

Hinweis: Um Benutzer zu konfigurieren, müssen Sie sich an Ihrem Computer als Windows-Administrator anmelden. Wenn Sie ein Upgrade von einer älteren Version dieses McAfee-Produkts durchgeführt haben und noch immer McAfee-Benutzer verwenden, müssen Sie sicherstellen, dass Sie als McAfee-Administrator angemeldet sind.

In diesem Kapitel

Arbeiten mit McAfee-Benutzerkonten

Wenn Sie ein Upgrade von einer früheren Version von SecurityCenter durchgeführt haben, die McAfee-Benutzerkonten verwendet, bleiben die McAfee-Benutzerkonten und deren Berechtigungen erhalten. Sie können weiterhin McAfee-Benutzerkonten konfigurieren und verwalten. McAfee empfiehlt jedoch den Wechsel zu Windows-Benutzerkonten. Nach dem Übergang zu Windows-Benutzerkonten können Sie nicht mehr zu McAfee-Benutzerkonten zurückwechseln.

Wenn Sie weiterhin McAfee-Benutzerkonten verwenden, können Sie Benutzer hinzufügen, bearbeiten oder entfernen und das McAfee-Administratorkennwort ändern oder abrufen.

McAfee-Administratorkennwort abrufen

Falls Sie das Administratorkennwort vergessen haben, können Sie es abrufen.

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Klicken Sie in der Liste **Benutzername** auf **Administrator**, und klicken Sie anschließend auf **Kennwort vergessen?**.
3. Geben Sie in das Feld **Antwort** die Antwort auf Ihre geheime Frage ein.
4. Klicken Sie auf **Senden**.

Ändern des McAfee-Administratorkennworts

Wenn Sie sich nicht an Ihr McAfee-Administratorkennwort erinnern oder vermuten, dass es bekannt geworden ist, können Sie es ändern.

1. Melden Sie sich im SecurityCenter als Administrator an.
2. Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   4. Klicken Sie im Konfigurationsbereichs für "Parental Controls" auf die Option **Erweitert**.

3 Wählen Sie im Bereich "Benutzereinstellungen" unter **McAfee-Benutzerkonten** die Option **Administrator** aus, und klicken Sie anschließend auf **Bearbeiten**.

4 Geben Sie im Dialogfeld "Benutzerkonto bearbeiten" ein neues Kennwort im Feld **Neues Kennwort** und anschließend noch einmal im Feld **Kennwort bestätigen** ein.

5 Klicken Sie auf **OK**.

Entfernen eines McAfee-Benutzerkontos

Sie können ein McAfee-Benutzerkonto jederzeit entfernen.

So entfernen Sie ein McAfee-Benutzerkonto:

1 Melden Sie sich im SecurityCenter als Administrator an.

2 Öffnen Sie den Bereich "Benutzereinstellungen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Konfigurationsbereichs für "Parental Controls" auf die Option **Erweitert**.

3 Wählen Sie im Bereich "Benutzereinstellungen" unter **McAfee-Benutzerkonten** einen Benutzernamen aus, und klicken Sie anschließend auf **Entfernen**.

Bearbeiten der Informationen für ein McAfee-Benutzerkonto

Sie können das Kennwort, den Kontotyp oder die automatische Anmeldefunktion für einen McAfee-Benutzer ändern.

1 Melden Sie sich im SecurityCenter als Administrator an.

2 Öffnen Sie den Bereich "Benutzereinstellungen".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Konfigurationsbereichs für "Parental Controls" auf die Option **Erweitert**.

3 Klicken Sie im Bereich "Benutzereinstellungen" auf einen Benutzernamen, und klicken Sie anschließend auf **Bearbeiten**.

4 Befolgen Sie die Anweisungen auf dem Bildschirm, um das Kennwort, den Kontotyp oder die Kindersicherung des Benutzers zu bearbeiten.

5 Klicken Sie auf **OK**.

Hinzufügen eines McAfee-Benutzerkontos

Wenn Sie ein McAfee-Benutzerkonto erstellt haben, können Sie die Kindersicherung für den Benutzer konfigurieren. Weitere Informationen finden Sie im Hilfebereich der Kindersicherungen.

1 Melden Sie sich im SecurityCenter als Administrator an.

2 Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   4. Klicken Sie im Konfigurationsbereichs für "Parental Controls" auf die Option **Erweitert**.

3 Klicken Sie im Bereich "Benutzereinstellungen" auf **Hinzufügen**.

4 Befolgen Sie die Anweisungen auf dem Bildschirm, um einen Benutzernamen, ein Kennwort und einen Kontotyp anzugeben und die Kindersicherung einzurichten.

5 Klicken Sie auf **Erstellen**.

Übergehen zur Verwendung von Windows-Benutzerkonten

Um die Verwaltung zu vereinfachen, empfiehlt McAfee, dass Sie auf Windows-Benutzerkonten umsteigen. Sie können danach jedoch nicht mehr zurück zu McAfee-Benutzerkonten wechseln.

1 Öffnen Sie den Bereich "Benutzereinstellungen".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Parental Controls**.
   3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
   4. Klicken Sie im Konfigurationsbereichs für "Parental Controls" auf die Option **Erweitert**.

2 Klicken Sie im Bereich "Benutzereinstellungen" auf **Wechseln**.

3 Bestätigen Sie den Vorgang.

Arbeiten mit Windows-Benutzerkonten

Standardmäßig entsprechen die SecurityCenter-Benutzerkonten den Windows-Benutzerkonten, die Sie auf Ihrem Computer eingerichtet haben. Sie können einen Benutzer hinzufügen, die Kontoinformationen für einen Benutzer bearbeiten oder einen Benutzer unter Windows in der Computerverwaltung entfernen. Für diese Benutzer können Sie dann im SecurityCenter die Kindersicherung einrichten.

Wenn Sie ein Upgrade von einer früheren Version des SecurityCenter durchgeführt haben, die McAfee-Benutzerkonten verwendet, finden Sie weitere Informationen unter Arbeiten mit McAfee-Benutzerkonten (Seite 178).

KAPITEL 33

Datenschutz im Internet

Sie können auch verhindern, dass Ihre persönlichen Informationen (wie Ihr Name, die Adresse, Kreditkartennummern und Kontonummern) über das Internet übertragen werden, indem Sie diese zum Bereich der geschützten Informationen hinzufügen.

Hinweis: Die Kindersicherungen blockieren nicht die Übertragung persönlicher Daten durch sichere Websites (d. h. Websites, die das HTTPS-Protokoll verwenden), wie beispielsweise die Websites von Banken.

In diesem Kapitel

Schutz von persönlichen Daten

Verhindern Sie, dass Ihre persönlichen Daten (wie Ihr Name, die Adresse, Kreditkartennummer und Kontonummern) über das Internet übertragen werden, indem Sie diese blockieren. Wenn McAfee persönliche Daten im ausgehenden Datenverkehr (beispielsweise ein Formularfeld oder eine Datei) erkennt, geschieht Folgendes:

- Wenn Sie Administrator sind, werden Sie aufgefordert, das Senden der Informationen zu bestätigen.
- Wenn Sie kein Administrator sind, werden die blockierten Informationen durch Sternchen (*) ersetzt. Wenn beispielsweise eine schädliche Website versucht, Ihre Kreditkartennummer an einen anderen Computer zu senden, wird die Nummer durch Sternchen ersetzt.

Schützen von persönlichen Daten

Sie können die folgenden Typen von persönlichen Informationen blockieren: Name, Adresse, Postleitzahl, Sozialversicherungsnummer, Telefonnummer, Kreditkartennummern, Kontonummern, Broker-Konten und Telefonkarten. Wenn Sie persönliche Informationen eines anderen Typs blockieren möchten, können Sie den Typ auf **Andere** setzen.

1 Öffnen Sie den Bereich "Geschützte Informationen".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
   3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
   4. Vergewissern Sie sich im Bereich "Internet & Netzwerkkonfiguration", dass der Schutz für persönliche Informationen aktiviert ist, und klicken Sie anschließend auf **Erweitert**.

2 Klicken Sie im Bereich "Geschützte Informationen" auf **Hinzufügen**.

3 Wählen Sie den Typ der zu blockierenden Informationen aus der Liste aus.

4 Geben Sie Ihre persönlichen Informationen ein, und klicken Sie auf **OK**.

KAPITEL 34

Schützen von Kennwörtern

Der Kennwort-Tresor ist ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht Ihnen die sichere Speicherung Ihrer Kennwörter, sodass kein anderer Benutzer (auch kein Administrator) auf diese zugreifen kann.

In diesem Kapitel

Einrichten des Kennwortdepots

Bevor Sie mit der Verwendung des Kennwortdepots beginnen, müssen Sie ein Kennwort für das Depot festlegen. Nur Benutzer, denen dieses Kennwort bekannt ist, können auf Ihr Kennwortdepot zugreifen. Wenn Sie das Kennwort für Ihr Kennwortdepot vergessen, können Sie es zurücksetzen. Alle Kennwörter, die zuvor in Ihrem Kennwortdepot gespeichert waren, werden daraufhin gelöscht.

Nachdem Sie ein Kennwort für das Kennwortdepot festgelegt haben, können Sie Kennwörter zu Ihrem Depot hinzufügen, sie bearbeiten oder daraus löschen. Sie haben jederzeit die Möglichkeit, das Kennwort für Ihr Kennwortdepot zu ändern.

Zurücksetzen Ihres Kennworts für das Kennwortdepot

Wenn Sie das Kennwort für Ihr Kennwortdepot vergessen, können Sie es zurücksetzen. Alle Kennwörter, die Sie zuvor in Ihr Kennwortdepot eingegeben haben, werden jedoch daraufhin gelöscht.

1. Öffnen Sie den Bereich "Kennwortdepot".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
   3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
   4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Kennwort-Tresor** auf die Option **Erweitert**.

2. Klicken Sie auf **Kennwort vergessen?**
3. Geben Sie im Dialogfeld "Kennwortdepot zurücksetzen" ein neues Kennwort im Feld **Kennwort** und anschließend noch einmal im Feld **Kennwort bestätigen** ein.
4. Klicken Sie auf **Zurücksetzen**.
5. Klicken Sie im Dialogfeld für die Bestätigung der Zurücksetzung des Kennworts auf **Ja**.

Ändern des Kennworts für den Kennwort-Tresor

Sie haben jederzeit die Möglichkeit, das Kennwort für Ihren Kennwort-Tresor zu ändern.

1 Öffnen Sie den Bereich "Kennwort-Tresor".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
   3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
   4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Kennwort-Tresor** auf die Option **Erweitert**.

2 Geben Sie im Bereich "Kennwort-Tresor" im Feld **Kennwort** das aktuelle Kennwort ein, und klicken Sie dann auf **Öffnen**.

3 Klicken Sie im Bereich "Kennwort-Tresor verwalten" auf **Kennwort ändern**.

4 Geben Sie das neue Kennwort im Feld **Geben Sie ein Kennwort ein** und anschließend noch einmal im Feld **Kennwort bestätigen** ein.

5 Klicken Sie auf **OK**.

6 Klicken Sie im Dialogfeld "Kennwort für Kennwort-Tresor geändert" auf **OK**.

Entfernen eines Kennworts

Sie können ein Kennwort jederzeit aus dem Kennwort-Tresor entfernen. Ein Kennwort, das Sie aus dem Tresor entfernt haben, können Sie nicht wiederbeschaffen.

1 Öffnen Sie den Bereich "Kennwort-Tresor".

   Wie?

   1. Klicken Sie unter **Häufige Tasks** auf **Home**.
   2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
   3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
   4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Kennwort-Tresor** auf die Option **Erweitert**.

2 Geben Sie das Kennwort für Ihren Kennwort-Tresor in das Feld **Kennwort** ein.

3 Klicken Sie auf **Öffnen**.

4 Klicken Sie im Bereich "Kennwort-Tresor verwalten" auf einen Kennworteintrag, und klicken Sie anschließend auf **Entfernen**.

5 Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.

Ändern eines Kennworts

Um stets über korrekt und verlässliche Einträge in Ihrem Kennwort-Tresor zu verfügen, müssen Sie sie aktualisieren, wenn sich Kennwörter ändern.

1 Öffnen Sie den Bereich "Kennwort-Tresor".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Kennwort-Tresor** auf die Option **Erweitert**.

2 Geben Sie das Kennwort für Ihren Kennwort-Tresor in das Feld **Kennwort** ein.

3 Klicken Sie auf **Öffnen**.

4 Klicken Sie im Bereich "Kennwort-Tresor verwalten" auf einen Kennworteintrag, und klicken Sie anschließend auf **Bearbeiten**.

5 Ändern Sie die Beschreibung des Kennworts (z. B. den Verwendungszweck) im Feld **Beschreibung**, oder ändern Sie das Kennwort im Feld **Kennwort**.

6 Klicken Sie auf **OK**.

Hinzufügen eines Kennworts

Wenn Sie Probleme haben, sich Ihre Kennwörter zu merken, können Sie diese zum Kennwortdepot hinzufügen. Das Kennwortdepot ist ein sicherer Speicherort, auf den nur Benutzer zugreifen können, denen das Kennwort für Ihr Kennwortdepot bekannt ist.

1 Öffnen Sie den Bereich "Kennwortdepot".

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Kennwort-Tresor** auf die Option **Erweitert**.

2 Geben Sie das Kennwort für Ihr Kennwortdepot in das Feld **Kennwort** ein.

3 Klicken Sie auf **Öffnen**.

4 Klicken Sie im Bereich "Kennwortdepot verwalten" auf **Hinzufügen**.

5 Geben Sie eine Beschreibung des Kennworts (z. B. wofür es gebraucht wird) in das Feld **Beschreibung** ein, und geben Sie das Kennwort anschließend in das Feld **Kennwort** ein.

6 Klicken Sie auf **OK**.

KAPITEL 35

McAfee Backup and Restore

Mit McAfee® Backup and Restore können Sie Ihre Dateien auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren und so einen Datenverlust vermeiden. Bei der lokalen Archivierung können Sie Ihre persönlichen Dateien auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren (sichern). Damit erhalten Sie eine lokale Kopie Ihrer Datensätze, Dokumente und anderen für Sie wichtigen Unterlagen, auf die Sie im Fall eines Datenverlusts zurückgreifen können.

Bevor Sie mit der Verwendung von Backup and Restore beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Backup and Restore. Stellen Sie außerdem sicher, dass genügend Archivierungsmedien vorhanden sind, um lokale Archive anlegen zu 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

Backup and Restore-Funktionen

Lokal geplante Archivierung

Schützen Sie Ihre Daten durch die Archivierung von Dateien und Ordnern auf einer CD, einer DVD, einem USB-Laufwerk, einer externen Festplatte oder einem Netzlaufwerk. Wenn Sie die erste Archivierung initiiert haben, werden automatisch inkrementelle Archivierungen für Sie ausgeführt.

Wiederherstellung mit nur einem Klick

Wenn auf Ihrem Computer Dateien oder Ordner versehentlich gelöscht oder beschädigt werden, können Sie die zuletzt gesicherten Versionen von den verwendeten Archivierungsmedien wiederherstellen.

Komprimierung und Verschlüsselung

Ihre archivierten Dateien sind standardmäßig komprimiert, wodurch Speicherplatz auf den Archivierungsmedien eingespart wird. Als zusätzliche Sicherheitsmaßnahme werden Ihre Archive standardmäßig verschlüsselt.

KAPITEL 36

Archivieren von Dateien

Mit McAfee Backup and Restore können Sie die Dateien, die sich auf Ihrem Computer befinden, wahlweise auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren. Durch diese Archivierung können Sie Ihre Daten bei Datenverlust oder Beschädigung schnell und einfach wiederherstellen.

Vor dem Archivieren legen Sie den standardmäßigen Archiv-Speicherort fest (CD, DVD, USB-Laufwerk, externe Festplatte, Netzlaufwerk). Einige Einstellungen sind bereits vordefiniert, beispielsweise die Ordner und die Dateitypen für die Archivierung; Sie können diese Einstellungen nach Bedarf ändern.

Sobald Sie die Optionen für das lokale Archiv eingerichtet haben, können Sie die Standardeinstellungen für die Ausführung von vollständigen Archivierungen oder Schnellarchivierungen durch Backup and Restore bearbeiten. Darüber hinaus können Sie jederzeit eine manuelle Archivierung ausführen.

In diesem Kapitel

Aktivieren und Deaktivieren des lokalen Archivs

Wenn Sie Backup and Restore das erste Mal starten, entscheiden Sie, ob Sie das lokale Archiv aktivieren oder deaktivieren möchten, je nachdem, wie Sie Backup and Restore verwenden möchten. Nachdem Sie sich bei Backup and Restore angemeldet und das Programm gestartet haben, können Sie die lokale Archivierung jederzeit aktivieren oder deaktivieren.

Wenn Sie keine Kopie der Dateien, die sich auf Ihrem Computer befinden, auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren möchten, können Sie das lokale Archiv deaktivieren.

Aktivieren des lokalen Archivs

Sie aktivieren das lokale Archiv, wenn Sie eine Kopie der Dateien, die sich auf Ihrem Computer befinden, wahlweise auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren möchten.

1. Klicken Sie im SecurityCenter im **Erweiterten Menü** auf **Konfiguration**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie im Bereich "Computer- & Dateikonfiguration" unter **Lokales Archiv ist deaktiviert** auf **Ein**.

Deaktivieren des lokalen Archivs

Sie deaktivieren das lokale Archiv, wenn Sie keine Kopie der Dateien, die sich auf Ihrem Computer befinden, wahlweise auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren möchten.

1. Klicken Sie im SecurityCenter im **Erweiterten Menü** auf **Konfiguration**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie im Bereich "Computer- & Dateikonfiguration" unter **Lokales Archiv ist aktiviert** auf **Ein**.

Festlegen von Archivoptionen

Bevor Sie mit der Archivierung Ihrer Dateien beginnen, müssen Sie einige Optionen für das lokale Archiv festlegen. Sie müssen beispielsweise die Überwachungs-Speicherorte und die überwachten Dateitypen festlegen. Die Überwachungs-Speicherorte sind Ordner auf dem Computer, die Backup and Restore auf neue Dateien und Dateiänderungen überwacht. Die überwachten Dateitypen (beispielsweise .doc oder .xls) werden beim Archivieren der Überwachungs-Speicherorte durch Backup and Restore erfasst. Standardmäßig werden die nachstehenden Dateitypen archiviert; Sie können jedoch auch andere Dateitypen archivieren.

- Microsoft® Word-Dokumente (.doc, .docx)
- Microsoft Excel®-Arbeitsblätter (.xls, .xlsx)
- Microsoft PowerPoint®-Präsentationen (.ppt, pptx)
- Microsoft Project®-Dateien (.mpp)
- Adobe® PDF-Dateien (.pdf)
- Textdateien (*.txt)
- HTML-Dateien (.html)
- Joint Photographic Experts Group-Dateien (.jpg, .jpeg)
- Tagged Image Format-Dateien (.tif)
- MPEG Audio Stream III-Dateien (.mp3)
- Videodateien (.vdo)

Hinweis: Die folgenden Dateitypen können nicht archiviert werden: .ost und .pst.

Sie können zwei Arten von Überwachungs-Speicherorten festlegen: über- und untergeordnete Ordner oder nur übergeordnete Ordner. Wenn Sie einen Speicherort für Ordner und Unterordner auf der obersten Ebene festlegen, archiviert Backup and Restore die überwachten Dateitypen in diesem Ordner und seinen Unterordnern. Wenn Sie einen Speicherort für Ordner auf der obersten Ebene festlegen, archiviert Backup and Restore die überwachten Dateitypen nur in diesem Ordner (nicht in seinen Unterordnern). Sie können auch Speicherorte angeben, die von der lokalen Archivierung ausgeschlossen werden sollen. Standardmäßig sind der Windows-Desktop und der Ordner "Eigene Dokumente" als Speicherorte für Ordner und Unterordner auf der obersten Ebene eingerichtet.

Sobald Sie die überwachten Dateitypen und die Überwachungs-Speicherorte festgelegt haben, richten Sie den Archiv-Speicherort ein (also die CD, die DVD, das USB-Laufwerk, das externe Laufwerk oder das Netzlaufwerk, auf dem die archivierten Dateien gespeichert werden sollen.) Sie haben jederzeit die Möglichkeit, den Archiv-Speicherort zu ändern.

Aus Sicherheitsgründen bzw. zur Einschränkung des Umfangs sind die Verschlüsselung und die Komprimierung für die archivierten Dateien standardmäßig aktiviert. Bei der Verschlüsselung wird der Inhalt der Dateien in Code umgewandelt, sodass die Textinformationen für alle Benutzer unleserlich sind, denen das Verfahren zur Entschlüsselung unbekannt ist. Bei der Komprimierung werden die Dateien so "verdichtet", dass der erforderliche Speicherplatz zum Speichern oder Übertragen auf ein Minimum reduziert wird. Auch wenn McAfee dies nicht empfiehlt, können Sie die Verschlüsselung und/oder die Komprimierung jederzeit deaktivieren.

Aufnehmen eines Speicherorts in das Archiv

Sie können zwei Arten von Überwachungs-Speicherorten für die Archivierung festlegen: über- und untergeordnete Ordner oder nur übergeordnete Ordner. Bei einem Speicherort mit über- und untergeordneten Ordnern überwacht die Datensicherung und -wiederherstellung den Inhalt des Ordners und aller Unterordner auf Änderungen. Bei einem Speicherort mit übergeordneten Ordnern überwacht die Datensicherung und -wiederherstellung lediglich den Inhalt des Ordners (nicht den der Unterordner).

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

Wie?

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Überwachungs-Speicherorte**.

3 Führen Sie einen der folgenden Vorgänge aus:

- Wenn der Inhalt eines Ordners mit allen Unterordnern archiviert werden soll, klicken Sie unter **Ordner und Unterordner auf der obersten Ebene archivieren** auf **Ordner hinzufügen**.
- Wenn nur der Inhalt eines Ordners archiviert werden soll, aber nicht der Inhalt der Unterordner, klicken Sie unter **Ordner auf der obersten Ebene archivieren** auf **Ordner hinzufügen**.
- Um eine ganze Datei zu archivieren, klicken Sie unter **Ordner auf der obersten Ebene archivieren** auf **Datei hinzufügen**.

4 Wechseln Sie im Dialogfeld "Nach Ordner suchen" (oder Öffnen) zum Ordner (oder zur Datei), der überwacht werden soll, und klicken Sie auf **OK**.

5 Klicken Sie auf **OK**.

Tipp: Wenn Backup and Restore einen Ordner überwachen soll, den Sie noch nicht erstellt haben, klicken Sie im Dialogfeld "Nach Ordner suchen" auf **Neuen Ordner erstellen**, um einen Ordner hinzuzufügen und diesen gleichzeitig als neuen Überwachungs-Speicherort festzulegen.

Festlegen der Dateitypen für die Archivierung

Sie können angeben, welche Dateitypen an den Speicherorten für Ordner und Unterordner auf der obersten Ebene archiviert werden. Wählen Sie hierzu aus einer Liste mit Dateitypen, oder fügen Sie der Liste neue Dateitypen hinzu.

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

   Wie?

   1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
   2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Dateitypen**.

3 Erweitern Sie die Listen mit den Dateitypen, und aktivieren Sie das Kontrollkästchen neben den zu archivierenden Dateitypen.

4 Klicken Sie auf **OK**.

Tipp: Soll ein neuer Dateityp in die Liste **Ausgewählte Dateitypen** aufgenommen werden, geben Sie die Dateinamenerweiterung in das Feld **Benutzerdefinierten Dateityp zu "Andere" hinzufügen** ein, klicken Sie auf **Hinzufügen** und dann auf **OK**. Der neue Dateityp wird automatisch als überwachter Dateityp eingestuft.

Ausschließen eines Speicherorts aus dem Archiv

Wenn ein bestimmter Speicherort (Ordner) und dessen Inhalt nicht online archiviert werden sollen, schließen Sie diesen Speicherort aus der Archivierung aus.

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

   Wie?

   1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
   2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Überwachungs-Speicherorte**.

3 Klicken Sie auf **Ordner hinzufügen** unter **Von der Sicherung ausgeschlossene Ordner**.

4 Wechseln Sie im Dialogfeld **Nach Ordner suchen** zum auszuschließenden Ordner. Markieren Sie diesen Ordner, und klicken Sie auf **OK**.

5 Klicken Sie auf **OK**.

Tipp: Soll Backup and Restore auch einen Ordner von der Sicherung ausschließen, den Sie noch nicht angelegt haben, dann können Sie im Dialogfeld **Nach Ordner suchen** mit der Option **Neuen Ordner erstellen** einen neuen Ordner erstellen und diesen Ordner gleichzeitig von der Sicherung ausschließen.

Ändern des Archiv-Speicherorts

Wenn Sie den Archiv-Speicherort ändern, werden die Dateien, die bislang an einem anderen Speicherort aktiviert wurden, als *Nie archiviert* aufgeführt.

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

   Wie?

   1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
   2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Archiv-Speicherort ändern**.

3 Führen Sie im Dialogfeld **Archiv-Speicherort** einen der folgenden Schritte aus:

   - Klicken Sie auf **CD/DVD-Writer auswählen**, klicken Sie in der Liste **Writer** auf das CD- oder DVD-Laufwerk Ihres Computers, und klicken Sie auf **OK**.
   - Klicken Sie auf **Festplatten-Speicherort auswählen**, wechseln Sie zu einem USB-Laufwerk, einem lokalen Laufwerk oder einer externen Festplatte, markieren Sie das Speichermedium, und klicken Sie auf **OK**.
   - Klicken Sie auf **Netzwerk-Speicherort auswählen**, wechseln Sie zu einem Netzlaufwerk, markieren Sie dieses Laufwerk, und klicken Sie auf **OK**.

4 Überprüfen Sie, ob der neue Archiv-Speicherort unter **Archiv-Speicherort auswählen** richtig aufgeführt wird, und klicken Sie dann auf **OK**.

5 Klicken Sie im Bestätigungsdialogfeld auf **OK**.

6 Klicken Sie auf **OK**.

Hinweis: Wenn Sie den Archiv-Speicherort ändern, werden zuvor archivierte Dateien in der Spalte **Status** als **Nicht archiviert** aufgeführt.

Deaktivieren der Verschlüsselung und Komprimierung für Archive

Durch das Verschlüsseln archivierter Dateien stellen Sie die Vertraulichkeit Ihrer Daten sicher. Der Inhalt der Dateien wird dabei unleserlich gemacht. Durch das Komprimieren werden archivierte Dateien auf die kleinstmögliche Größe "verdichtet". Standardmäßig sind die Verschlüsselung und die Komprimierung aktiviert; Sie können diese Optionen jedoch jederzeit deaktivieren.

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

   Wie?

   1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
   2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Erweiterte Einstellungen**.

3 Deaktivieren Sie das Kontrollkästchen **Verschlüsselung aktivieren, um die Sicherheit zu erhöhen**.

4 Deaktivieren Sie das Kontrollkästchen **Komprimierung aktivieren, um Speicherplatz zu reduzieren**.

5 Klicken Sie auf **OK**.

Hinweis: McAfee empfiehlt, die Verschlüsselung und die Komprimierung beim Archivieren der Dateien nicht zu deaktivieren.

Ausführen von vollständigen Archivierungen und Schnellarchivierungen

Es stehen zwei Arten von Archivierungen zur Auswahl: die vollständige Archivierung und die Schnellarchivierung. Bei einer vollständigen Archivierung werden alle Daten mit den angegebenen überwachten Dateitypen und an den definierten Speicherorten archiviert. Bei einer Schnellarchivierung werden nur die überwachten Dateien archiviert, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden.

Standardmäßig ist Backup and Restore so eingerichtet, dass montags um 9:00 Uhr eine vollständige Archivierung der überwachten Dateien an den Überwachungs-Speicherorten ausgeführt wird, während jeweils 48 Stunden nach der letzten vollständigen Archivierung oder Schnellarchivierung eine Schnellarchivierung startet. Dieser Zeitplan sorgt dafür, dass stets ein aktuelles Archiv der Dateien vorliegt. Soll die Archivierung in anderen Zeitabständen erfolgen, können Sie den Zeitplan jederzeit nach Bedarf anpassen.

Zudem ist jederzeit eine manuelle Archivierung des Inhalts der Überwachungs-Speicherorte möglich. Wenn Sie beispielsweise eine Datei geändert haben und die nächste vollständige Archivierung oder Schnellarchivierung mit Backup and Restore erst in einigen Stunden ansteht, können Sie die Dateien manuell archivieren. Bei einer manuellen Archivierung beginnt das Intervall für die automatischen Archivierungen wieder neu.

Darüber hinaus können Sie eine automatische oder manuelle Archivierung unterbrechen, wenn diese zu einem ungeeigneten Zeitpunkt ausgeführt wird. Wird beispielsweise eine automatische Archivierung gestartet, während Sie gerade eine ressourcenintensive Aufgabe ausführen, können Sie die Archivierung unterbrechen. Wenn Sie eine automatische Archivierung anhalten, beginnt das Intervall für die automatischen Archivierungen wieder neu.

Planen von automatischen Archivierungen

Sie können die Zeitabstände für vollständige Archivierungen und Schnellarchivierungen so einrichten, dass Ihre Daten stets geschützt sind.

1 Öffnen Sie das Dialogfeld "Einstellungen für lokales Archiv".

Wie?

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.

2 Klicken Sie auf **Allgemein**.

3 Soll täglich, wöchentlich oder monatlich eine vollständige Archivierung erfolgen, klicken Sie unter **Vollständige Archivierung alle** auf eine der folgenden Optionen:

- **Tag**
- **Woche**
- **Monat**

4 Aktivieren Sie das Kontrollkästchen neben dem Tag, an dem die vollständige Archivierung ausgeführt werden soll.

5 Klicken Sie in der Liste **Um** einen Wert für die Uhrzeit an, zu der die vollständige Archivierung gestartet werden soll.

6 Soll täglich, wöchentlich oder monatlich eine Schnellarchivierung erfolgen, klicken Sie unter **Schnellarchivierung** auf eine der folgenden Optionen:

- **Stunden**
- **Tage**

7 Geben Sie in das Feld **Schnellarchivierung alle** den gewünschten Wert für die Häufigkeit ein.

8 Klicken Sie auf **OK**.

Hinweis: Sie können eine geplante Archivierung deaktivieren, indem Sie unter **Vollständige Archivierung alle:** die Option **Manuell** auswählen.

Unterbrechen einer automatischen Archivierung

Backup and Restore archiviert automatisch die Dateien und Ordner an den Überwachungs-Speicherorten automatisch gemäß dem definierten Zeitplan. Die Ausführung einer automatischen Archivierung kann jedoch jederzeit unterbrochen werden.

1 Klicken Sie im linken Bereich auf **Archivierung unterbrechen**.

2 Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

Hinweis: Der Link **Archivierung unterbrechen** ist nur dann verfügbar, wenn gerade eine Archivierung ausgeführt wird.

Manuelles Ausführen einer Archivierung

Neben den automatischen Archivierungen, die nach einem bestimmten Zeitplan ablaufen, können Sie jederzeit eine manuelle Archivierung ausführen. Bei einer Schnellarchivierung werden nur die überwachten Dateien archiviert, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden. Bei einer vollständigen Archivierung werden die überwachten Dateitypen an allen Überwachungs-Speicherorten erfasst.

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Soll eine Schnellarchivierung ausgeführt werden, klicken Sie im linken Bereich auf **Schnellarchivierung**.
   - Soll eine vollständige Archivierung ausgeführt werden, klicken Sie im linken Bereich auf **Vollständige Archivierung**.
3. Überprüfen Sie den Speicherplatz und die Einstellungen im Dialogfeld **Archivierung starten**, und klicken Sie auf **Fortfahren**.

KAPITEL 37

Arbeiten mit archivierten Dateien

Nach dem Archivieren können Sie mithilfe von Backup and Restore mit den archivierten Dateien arbeiten. Die archivierten Dateien werden in der gewohnten Explorer-Ansicht aufgeführt, sodass Sie die gewünschten Dateien schnell und einfach auffinden. Mit zunehmendem Umfang des Archivs können Sie die Dateien sortieren oder nach bestimmten Dateien suchen. Darüber hinaus lassen sich die Dateien direkt aus der Explorer-Ansicht heraus öffnen, sodass Sie deren Inhalt betrachten können, ohne die Dateien selbst abrufen zu müssen.

Wenn die lokale Kopie einer Datei veraltet ist, fehlt oder beschädigt wurde, können Sie diese Datei aus dem Archiv abrufen. Backup and Restore liefert außerdem die notwendigen Informationen zum Verwalten der lokalen Archive und der Speichermedien.

In diesem Kapitel

Verwenden des Explorers der lokalen Archive

Im Explorer der lokalen Archive können Sie die lokal archivierten Dateien anzeigen und bearbeiten. Hier werden der Dateiname, der Typ, der Speicherort, die Größe, der Status (archiviert, nicht archiviert, Archivierung läuft) und das Datum der letzten Archivierung für die einzelnen Dateien aufgeführt. Darüber hinaus können Sie die Dateien nach diesen Kriterien sortieren.

Wenn Sie ein großes Archiv besitzen, können Sie schnell und einfach nach Dateien suchen. Geben Sie zunächst den Namen oder den Pfad der Datei (vollständig oder teilweise) ein, und verfeinern Sie dann die Suche, indem Sie die ungefähre Dateigröße und das Datum der letzten Archivierung angeben.

Eine gefundene Datei lässt sich direkt im Explorer der lokalen Archive öffnen. Backup and Restore öffnet die Datei im ursprünglichen Programm, sodass Sie Änderungen an der Datei vornehmen können, ohne den Explorer der lokalen Archive verlassen zu müssen. Die Datei wird im bisherigen Überwachungs-Speicherort auf dem Computer gespeichert und bei der automatischen Archivierung gemäß dem definierten Zeitplan berücksichtigt.

Sortieren von archivierten Dateien

Sie können die archivierten Dateien und Ordner nach den folgenden Kriterien sortieren: Dateiname, Dateityp, Größe, Status (archiviert, nicht archiviert, Archivierung läuft), Datum der letzten Archivierung, Speicherort (Pfad) auf dem Computer.

So sortieren Sie die archivierten Dateien:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im rechten Bereich auf eine Spaltenüberschrift.

Suchen nach einer archivierten Datei

Wenn Sie ein großes Repository mit archivierten Dateien besitzen, können Sie schnell und einfach nach Dateien suchen. Geben Sie zunächst den Namen oder den Pfad der Datei (vollständig oder teilweise) ein, und verfeinern Sie dann die Suche, indem Sie die ungefähre Dateigröße und das Datum der letzten Archivierung angeben.

1. Geben Sie in das Feld **Suche** oben im Fenster den Dateinamen (vollständig oder teilweise) ein, und drücken Sie die EINGABETASTE.
2. Geben Sie in das Feld **Der gesamte oder ein Teil des Pfads** den Pfad (vollständig oder teilweise) ein.
3. Geben Sie die ungefähre Dateigröße der gesuchten Datei an. Führen Sie hierzu einen der folgenden Schritte aus:
   - Klicken Sie auf **Weniger als 100 KB**, **Weniger als 1 MB** oder **Mehr als 1 MB**.
   - Klicken Sie auf **Größe in KB**, und geben Sie die ungefähre Größe in das Feld ein.
4. Geben Sie das ungefähre Datum für die letzte Archivierung der Datei an. Führen Sie hierzu einen der folgenden Schritte aus:
   - Klicken Sie auf **Diese Woche**, **Diesen Monat** oder **Dieses Jahr**.
   - Klicken Sie auf **Daten angeben**, klicken Sie in der Liste auf den Eintrag **Archiviert**, und wählen Sie dann in den Listen die ungefähren Werte für das Datum aus.
5. Klicken Sie auf **Suche**.

Hinweis: Falls Ihnen die ungefähre Größe und/oder das Datum der letzten Archivierung nicht bekannt sind, klicken Sie auf **Unbekannt**.

Öffnen einer archivierten Datei

Sie können eine archivierte Datei direkt im Explorer der lokalen Archive öffnen und so deren Inhalt betrachten.

So öffnen Sie archivierte Dateien:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im rechten Bereich auf einen Dateinamen, und klicken Sie dann auf **öffnen**.

Tipp: Alternativ doppelklicken Sie auf den Dateinamen, um eine archivierte Datei zu öffnen.

Wiederherstellen von archivierten Dateien

Wenn eine Datei beschädigt ist, fehlt oder versehentlich gelöscht wurde, können Sie die jeweils letzte Kopie dieser Datei aus einem lokalen Archiv abrufen. Achten Sie daher darauf, Ihre Dateien in regelmäßigen Abständen zu archivieren. Darüber hinaus können Sie ältere Versionen von Dateien aus einem lokalen Archiv wiederherstellen. Wenn Sie beispielsweise eine Datei in regelmäßigen Abständen archivieren und nun zu einer früheren Version der Datei zurückkehren möchten, suchen Sie die Datei im Archiv-Speicherort. Liegt das Archiv auf einer lokalen Festplatte oder einem Netzlaufwerk vor, können Sie dieses Laufwerk direkt nach der Datei durchsuchen. Falls das Archiv sich auf einer externen Festplatte oder einem USB-Laufwerk befindet, schließen Sie das Laufwerk an den Computer an, und durchsuchen Sie dann das Laufwerk nach der Datei. Falls das Archiv auf einer CD oder DVD gespeichert ist, legen Sie die CD oder DVD in das entsprechende Laufwerk am Computer ein, und durchsuchen Sie dann den Datenträger nach der Datei.

Sie können auch Dateien wiederherstellen, die Sie von einem anderen Computer aus auf einem bestimmten Computer archiviert haben. Wenn Sie beispielsweise einen Satz an Dateien auf einer externen Festplatte auf Computer A archivieren, können Sie diese Dateien auf Computer B wiederherstellen. Hierfür müssen Sie Backup and Restore auf Computer B installieren und die externe Festplatte verbinden. Durchsuchen Sie den Datenträger dann in Backup and Restore nach den Dateien. Die Dateien werden in die Liste **Fehlende Dateien** für die Wiederherstellung eingetragen.

Weitere Informationen zum Archivieren von Dateien finden Sie unter Archivieren von Dateien. Falls Sie eine überwachte Datei aus dem Archiv löschen und dieses Löschen beabsichtigt war, können Sie auch den Eintrag in der Liste **Fehlende Dateien** entfernen.

Wiederherstellen von fehlenden Dateien aus einem lokalen Archiv

Über das lokale Archiv von Backup and Restore können Sie Daten wiederherstellen, die in einem Überwachungs-Ordner auf dem lokalen Computer fehlen. Wenn beispielsweise eine Datei, die bereits archiviert wurde, aus einem Überwachungs-Ordner verschoben oder ganz gelöscht wird, können Sie die archivierte Datei aus dem lokalen Archiv wiederherstellen.

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Aktivieren Sie unten im Fenster auf der Registerkarte **Fehlende Dateien** das Kontrollkästchen neben dem Namen der wiederherzustellenden Datei.
3. Klicken Sie auf **Wiederherstellen**.

Tipp: Sollen alle Dateien in der Liste **Fehlende Dateien** wiederhergestellt werden, klicken Sie auf **Alle wiederherstellen**.

Wiederherstellen einer älteren Version einer Datei aus einem lokalen Archiv

Soll eine ältere Version einer archivierten Datei wiederhergestellt werden, nehmen Sie diese Datei in die Liste **Fehlende Dateien** auf. Anschließend stellen Sie die Datei wie gewohnt aus der Liste **Fehlende Dateien** wieder her.

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie unten im Bildschirm auf der Registerkarte **Fehlende Dateien** auf **Durchsuchen**, und wechseln Sie dann zum Speicherort des Archivs.

   Für die Namen der Archivordner gilt das folgende Format: `cre ttmmjj_hh-mm-ss_***`, wobei gilt: `ttmmjj` ist das Datum, an dem die Dateien archiviert wurden, `hh-mm-ss` ist die Uhrzeit der Archivierung, und für `***` steht entweder `Full` oder `Inc`, je nachdem, ob eine vollständige Archivierung oder eine Schnellarchivierung durchgeführt wurde.
3. Wählen Sie den Speicherort aus, und klicken Sie anschließend auf **OK**.

   Die Dateien am ausgewählten Speicherort werden in die Liste **Fehlende Dateien** aufgenommen und können wiederhergestellt werden. Weitere Informationen finden Sie unter Wiederherstellen von fehlenden Dateien aus einem lokalen Archiv (Seite 207).

Entfernen von Dateien aus der Liste "Fehlende Dateien"

Wenn eine archivierte Datei aus einem überwachungs-Ordner verschoben oder ganz gelöscht wurde, wird diese Datei automatisch in die Liste **Fehlende Dateien** aufgenommen. Damit werden Sie darauf hingewiesen, dass eine Inkonsistenz zwischen den archivierten Dateien und den Dateien in den überwachungs-Ordnern vorliegt. Falls Sie die Datei aus dem überwachungs-Ordner verschieben oder ganz löschen und dieser Vorgang beabsichtigt war, können Sie die Datei aus der Liste **Fehlende Dateien** löschen.

So entfernen Sie eine Datei aus der Liste "Fehlende Dateien":

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Aktivieren Sie unten im Fenster auf der Registerkarte **Fehlende Dateien** das Kontrollkästchen neben dem Namen der zu entfernenden Datei.
3. Klicken Sie auf **Löschen**.

Tipp: Sollen alle Dateien in der Liste **Fehlende Dateien** abgerufen werden, klicken Sie auf **Alle löschen**.

Verwalten von Archiven

Sie können jederzeit eine übersicht zu den vollständigen Archivierungen und den Schnellarchivierungen abrufen, z. B. Angaben zum Umfang der derzeit überwachten Daten, zur bereits archivierten Datenmenge und zum Umfang der Daten, die derzeit überwacht werden, jedoch noch nicht archiviert wurden. Darüber hinaus stehen Informationen zum Archivierungszeitplan bereit, beispielsweise das Datum der letzten Archivierung sowie der nächsten geplanten Archivierung.

Abrufen einer Übersicht über die Archivierungsvorgänge

Sie können jederzeit Informationen zu Ihren Archivierungsvorgängen abrufen. Informieren Sie sich beispielsweise über den prozentualen Anteil der archivierten Dateien, über den Umfang der überwachten Daten, den Umfang der bereits archivierten Daten sowie über den Umfang der Daten, die überwacht werden, jedoch noch nicht archiviert wurden. Außerdem wird das Datum der letzten Archivierung und der nächsten geplanten Archivierung angezeigt.

1 Klicken Sie auf die Registerkarte **Lokales Archiv**.

2 Klicken Sie oben im Fenster auf **Kontozusammenfassung**.

KAPITEL 38

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

Dateisäuberung	Löscht unnötige Dateien sicher und effizient mithilfe verschiedener Cleaner. Durch das Löschen dieser Dateien können Sie den Speicherplatz auf der Festplatte Ihres PCs erhöhen und seine Leistung verbessern.

KAPITEL 39

Bereinigen Ihres Computers

QuickClean löscht Dateien, die zu Datenresten auf Ihrem Computer führen können. Es leert Ihren Papierkorb und löscht temporäre Dateien, Verknüpfungen, Fragmente verloren gegangener Dateien, Registrierungsdateien, Dateien im Cache, Cookies, Dateien zum Browserverlauf, versendete und empfangene E-Mails, kürzlich verwendete Dateien, Active-X-Dateien und Dateien zu Systemwiederherstellungspunkten. QuickClean löscht diese Elemente, ohne dass davon andere wichtige Informationen betroffen sind.

Sie können alle QuickClean-Cleaner verwenden, um unnötige Dateien von Ihrem Computer zu entfernen. In der folgenden Tabelle sind die QuickClean-Cleaner beschrieben:

Name	Funktion
Papierkorb-Cleaner	Löscht Dateien im Papierkorb.
Cleaner für temporäre Dateien	Löscht Dateien, die in temporären Ordner gespeichert sind.
Kurzbefehls-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 seine Konfigurationsinformationen speichert. Die Registrierung enthält Profile für jeden Computerbenutzer und Informationen zur System-Hardware, zu installierten Programmen und Eigenschafteneinstellungen. Windows bezieht sich während seiner Ausführung ständig auf diese Informationen.

Name	Funktion
Cache-Cleaner	Entfernt Dateien aus dem Cache, die beim Browsen auf Webseiten anfallen. Diese Dateien werden üblicherweise als temporäre Dateien in einem Cache-Ordner gespeichert. Ein Cache-Ordner ist ein temporärer Speicherbereich auf Ihrem Computer. Um die Geschwindigkeit und Effizienz beim Surfen im Web 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 üblicherweise als temporäre Dateien gespeichert. Ein Cookie ist eine kleine Datei mit Informationen, wie dem Benutzernamen, dem aktuellen Datum und der Uhrzeit, die auf dem Computer einer Person gespeichert werden, die im Internet surft. Cookies werden hauptsächlich von Websites verwendet, um Benutzer zu identifizieren, die sich zuvor auf der Websites registriert oder diese besucht haben. Sie können jedoch auch eine Informationsquelle für Hacker darstellen.
Browser-Verlaufs-Cleaner	Löscht Ihren Webbrowser-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-Verlauf ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

Name	Funktion
ActiveX-Cleaner	Löscht ActiveX-Steuerlemente. ActiveX ist eine Software-Komponente, die von den Programmen oder Webseiten verwendet wird, um Funktionen hinzuzufügen, die als normaler Teil des Programms oder der Webseite erscheinen. Die meisten ActiveX-Steuerelemente sind harmlos, einige können jedoch Informationen von Ihrem Computer stehlen.
Cleaner für Systemwied-erherstellungspunkte	Löscht alte Systemwiederherstellungspunkte (außer dem neuesten) von Ihrem Computer. Systemwiederherstellungspunkte werden von Windows erstellt, um sämtliche Änderungen an Ihrem Computer zu markieren, damit Sie zu einem früheren Status zurückkehren können, falls Probleme auftreten.

In diesem Kapitel

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.

KAPITEL 40

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.

KAPITEL 41

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 42

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

Löscht Dateien und Ordner dauerhaft

Entfernt Elemente von der Festplatte Ihres Computers, damit die damit verknüpften Informationen nicht wiederhergestellt werden können. Es schützt Ihre Privatsphäre, indem Dateien und Ordner, Elemente in Ihrem Papierkorb und Ordner mit temporären Internetdateien sowie der gesamte Inhalt von Computer-Laufwerken, wie wiederbeschreibbare CDs, externe Festplatten und Disketten, sicher und dauerhaft gelöscht werden.

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 43

McAfee Network Manager

Netzwerkmanager stellt eine graphische Ansicht der Computer und andere Geräte dar, die Ihr Home-Netzwerk bilden. Sie können den Netzwerkmanager verwenden, um den Schutzstatus der verwalteten Computer in Ihrem Netzwerk remote zu verwalten und gemeldete Sicherheitslücken auf diesen Computern remote zu beheben. Wenn Sie McAfee Total Protection installiert haben, kann der Netzwerkmanager Ihr Netzwerk auch auf Eindringlinge überwachen (Computer oder Geräte, die Sie nicht erkennen oder denen Sie nicht vertrauen), die versuchen, eine Verbindung herzustellen.

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

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

Graphische Netzwerkzuordnung

Zeigen Sie eine grafische Übersicht über den Schutzstatus der Computer und Geräte an, die Ihr privates Netzwerk ausmachen. Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), erkennt die Netzwerkübersicht diese Änderungen. Sie können die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Geräten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Remote-Verwaltung

Verwalten Sie den Schutzstatus der Computer in Ihrem privaten Netzwerk. 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.

Netzwerküberwachung

Falls verfügbar, können Sie mit dem Netzwerkmanager Ihre Netzwerke überwachen und sich benachrichtigen lassen, wenn Freunde oder Eindringline eine Verbindung herstellen. Die Netzwerküberwachung ist nur verfügbar, wenn Sie McAfee Total Protection erworben haben.

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 44

Erstellen eines verwalteten Netzwerks

Um ein verwaltetes Netzwerk einzurichten, markieren Sie das Netzwerk als vertrauenswürdig (wenn Sie dies nicht schon getan haben), und fügen Sie dem Netzwerk Mitglieder (Computer) 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 jedes der Elemente 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 der Netzwerkmanager 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 der Netzwerkmanager 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 Namen 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. Sie können beispielsweise die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Elemente der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch Details anzeigen, die den in der Netzwerkzuordnung angezeigten Elementen zugeordnet sind.

Zugreifen auf die Netzwerkzuordnung

Die Netzwerkzuordnung bietet eine graphische Darstellung des Computers und der Geräte, die Ihr Home-Netzwerk ausmachen.

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

Hinweis: Wenn Sie das Netzwerk noch nicht als vertrauenswürdig markiert haben (mithilfe von McAfee Personal Firewall), werden Sie dazu aufgefordert, wenn Sie das erste Mal auf die Netzwerkzuordnung zugreifen.

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

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

Anzeigen von Details zu einem Element

Sie können detaillierte Informationen zu jedem beliebigen Element in Ihrem Netzwerk anzeigen, indem Sie diese in der Netzwerkzuordnung auswählen. Diese Informationen umfassen den Elementnamen, seinen Schutzstatus und andere Informationen, die für die Verwaltung des Elements 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 festlegen, ob Sie möchten, dass andere Computer im Netzwerk die Sicherheitseinstellungen dieses Computers verwalten.

1. Stellen Sie sicher, dass im Dialogfeld "Verwaltetes Netzwerk" das Kontrollkästchen **Zulassen, dass jeder Computer im Netzwerk die Sicherheitseinstellungen verwalten kann** aktiviert ist.
2. Klicken Sie auf **Anmelden**.
   Wenn Sie die Einladung annehmen, werden zwei Spielkarten angezeigt.
3. Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden.
4. Klicken Sie auf **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 verwalten**.
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 dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden.

6 Klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer, den Sie 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 45

Remote-Verwaltung des Netzwerks

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

In diesem Kapitel

Verwalten von Status und Berechtigungen

Ein verwaltetes Netzwerk umfasst verwaltete und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus zu verwalten, unverwaltete Mitglieder tun das nicht. 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 mit administrativen Berechtigungen eingeladen werden, ein verwalteter Computer zu werden. Ähnlich kann ein verwalteter Computer mit administrativen Berechtigungen einen anderen verwalteten Computer jederzeit zu einem unverwalteten Computer machen.

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 den Netzwerkmanager auch für die Verwaltung dieser Geräte verwenden. Sie können auch die Anzeigeeigenschaften eines Geräts in der Netzwerkzuordnung konfigurieren und verändern.

Verwalten des Schutzstatus eines Computers

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

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

Stoppen der Verwaltung des Schutzstatus eines Computers

Sie können die Verwaltung des Schutzstatus für einen verwalteten Computer in Ihrem Netzwerk stoppen. Der Computer wird dann jedoch nicht mehr verwaltet, und Sie können dessen Schutzstatus nicht remote verwalten.

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

Ändern der Berechtigungen eines verwalteten Computers

Sie können die Berechtigungen eines verwalteten Computers jederzeit ändern. Damit ändern Sie, welche Computer den Schutzstatus anderer Computer im Netzwerk verwalten 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 Kontrollkästchen, das angibt, ob dieser Computer und andere Computer im verwalteten Netzwerk den Schutzstatus der anderen Computer verwalten können.
4. Klicken Sie auf **OK**.

Verwalten eines Geräts

Sie können ein Gerät verwalten, indem Sie von der Netzwerkzuordnung aus 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-Website des Geräts anzeigt.
3. Geben Sie in Ihrem Webbrowser Ihre Anmeldeinformationen ein, und konfigurieren Sie die Sicherheitseinstellungen des Geräts.

Hinweis: Wenn es sich bei dem Gerät um einen durch Wireless Network Security geschützten drahtlosen Router oder Zugriffspunkt handelt, müssen Sie McAfee Wireless Network Security verwenden, um die Sicherheitseinstellungen eines 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 verwalten 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 Netzwerkmanager die meisten gemeldeten Probleme. Einige Sicherheitslücken erfordern jedoch möglicherweise ein manuelles Eingreifen auf dem lokalen Computer. In diesem Fall behebt Netzwerkmanager 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 keine aktuelle Version des SecurityCenter ausgeführt wird, kann deren Schutzstatus nicht remote verwaltet werden. Wenn Sie diese Computer remote verwalten möchten, müssen Sie auf allen Computern eine aktuelle Version des SecurityCenter installieren.

1. Vergewissern Sie sich, dass Sie alle Anweisungen auf dem Computer befolgen, den Sie remote verwalten möchten.
2. Sie sollten Ihre McAfee-Anmeldeinformationen bereithalten, nämlich die E-Mail-Adresse und das Kennwort, das Sie verwendet haben, als die McAfee-Software zum ersten Mal aktiviert wurde.
3. Gehen Sie in einem Browser zur McAfee-Website, und klicken Sie auf **Mein Konto**.
4. Suchen Sie nach dem zu installierenden Produkt, klicken Sie auf seine Schaltfläche **Download**, und folgen Sie den Anweisungen auf dem Bildschirm.

Tipp: Sie können auch erfahren, wie Sie die McAfee-Sicherheitssoftware auf Remote-Computern installieren, indem Sie Ihre Netzwerkzuordnung öffnen und unter **Ich möchte** auf **Meine PCs schützen** klicken.

KAPITEL 46

Überwachen Ihrer Netzwerke

Wenn Sie McAfee Total Protection installiert haben, überwacht der Netzwerkmanager Ihre Netzwerke auch auf Eindringlinge. Jedes Mal, wenn ein unbekannter Computer oder ein Gerät eine Verbindung zu Ihrem Netzwerk herstellt, werden Sie darüber benachrichtigt, damit Sie entscheiden können, ob es sich bei diesem Computer oder Gerät um einen Freund oder einen Eindringling handelt. Ein Freund ist ein Computer oder Gerät, das Sie erkennen und dem Sie vertrauen, und ein Eindringling ist ein Computer oder Gerät, das Sie nicht erkennen oder dem Sie nicht vertrauen. Wenn Sie einen Computer oder ein Gerät als Freund markieren, können Sie entscheiden, ob Sie jedes Mal benachrichtigt werden möchten, wenn dieser Freund eine Verbindung zum Netzwerk herstellt. Wenn Sie einen Computer oder ein Gerät als Eindringling markieren, warnen wir Sie automatisch jedes Mal, wenn eine Verbindung zu Ihrem Netzwerk hergestellt wird.

Wenn Sie nach der Installation oder dem Upgrade auf diese Version von Total Protection zum ersten Mal eine Verbindung zu einem Netzwerk herstellen, werden wir automatisch jeden Computer und jedes Gerät als Freund markieren, und wir werden Sie nicht benachrichtigen, wenn diese das nächste Mal eine Verbindung zu Ihrem Netzwerk herstellen. Nach drei Tagen beginnen wir damit, Sie über jeden unbekannten Computer und jedes unbekannte Gerät zu benachrichtigen, damit Sie sie selbst markieren können.

Hinweis: Die Netzwerküberwachung ist eine Funktion des Netzwerkmanagers, die nur in McAfee Total Protection verfügbar ist. Weitere Informationen zu Total Protection finden Sie auf unserer Website.

In diesem Kapitel

Anhalten der Netzwerküberwachung

Wenn Sie die Netzwerküberwachung deaktivieren, können wir Sie nicht mehr warnen, wenn Eindringlinge eine Verbindung zu Ihrem privaten Netzwerk herstellen oder über beliebige andere Netzwerke, zu denen Sie eine Verbindung herstellen.

1 Öffnen Sie den Konfigurationsbereich für "Internet und Netzwerk"

Wie?

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.

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

Erneutes Aktivieren der Benachrichtigungen für die Netzwerküberwachung

Sie können die Benachrichtigungen für die Netzwerküberwachung zwar deaktivieren, wir empfehlen dies jedoch nicht. Wenn Sie dies tun, sind wir womöglich nicht mehr in der Lage, Ihnen mitzuteilen, wenn unbekannte Computer oder Eindringlinge eine Verbindung zu Ihrem Netzwerk herstellen. Wenn Sie diese Benachrichtigungen versehentlich deaktivieren (z. B. wenn Sie das Kontrollkästchen **Diese Warnung nicht mehr anzeigen** in einer Warnung aktivieren), können Sie sie jederzeit wieder aktivieren.

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 die Option **Informationswarnungen**.

3 Vergewissern Sie sich im Fenster "Informationswarnungen", dass die folgenden Kontrollkästchen nicht ausgewählt sind:

- **Keine Warnungen anzeigen, wenn neue PCs oder Geräte eine Verbindung zum Netzwerk herstellen**
- **Keine Warnungen anzeigen, wenn Eindringlinge eine Verbindung zum Netzwerk herstellen**
- **Keine Warnungen für Freunde anzeigen, über die ich normalerweise benachrichtigt werden möchte**
- **Nicht erinnern, wenn unbekannte PCs oder Geräte erkannt werden**
- **Nicht warnen, wenn McAfee das Erkennen neuer Freunde abgeschlossen hat**

4 Klicken Sie auf **OK**.

Als Eindringling markieren

Markieren Sie einen Computer oder ein Gerät in Ihrem Netzwerk nur dann als Eindringling, wenn Sie es nicht erkennen oder ihm nicht vertrauen. Wir benachrichtigen Sie automatisch jedes Mal, wenn der Eindringling versucht, eine Verbindung zu Ihrem Netzwerk herzustellen.

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

2 Klicken Sie in der Netzwerkzuordnung auf ein Element.

3 Klicken Sie unter **Ich möchte** auf **Als Freund oder Eindringling markieren**.

4 Klicken Sie im Dialogfeld auf **Ein Eindringling**.

Als Freund markieren

Markieren Sie einen Computer oder ein Gerät in Ihrem Netzwerk nur dann als Freund, wenn Sie es erkennen und ihm vertrauen. Wenn Sie einen Computer oder ein Gerät als Freund markieren, können Sie entscheiden, ob Sie jedes Mal benachrichtigt werden möchten, wenn dieser Freund eine Verbindung zum Netzwerk herstellt.

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**.
2. Klicken Sie in der Netzwerkzuordnung auf ein Element.
3. Klicken Sie unter **Ich möchte** auf **Als Freund oder Eindringling markieren**.
4. Klicken Sie im Dialogfeld auf **Ein Freund**.
5. Um jedes Mal benachrichtigt zu werden, wenn dieser Freund eine Verbindung zum Netzwerk herstellt, wählen Sie das Kontrollkästchen **Benachrichtigen, wenn dieser Computer oder dieses Gerät eine Verbindung zum Netzwerk herstellt**.

Erkennung neuer Freunde anhalten

In den ersten drei Tagen, nachdem Sie eine Verbindung zu einem Netzwerk herstellen und diese Version von Total Protection installiert haben, markieren wir automatisch jeden Computer und jedes Gerät, über das Sie nicht benachrichtigt werden möchten, als Freund. Sie können diese automatische Markierung jederzeit innerhalb dieser drei Tage beenden, aber Sie können sie später nicht erneut starten.

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**.
2. Klicken Sie unter **Ich möchte** auf **Erkennung neuer Freunde anhalten**.

KAPITEL 47

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

Dateifreigabe

Geben Sie Dateien für andere Computer im Netzwerk ganz einfach frei. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die vollständigen oder administrativen Zugriff auf Ihr verwaltetes Netzwerk haben (Mitglieder), können Dateien, die von anderen Mitgliedern freigegeben wurden, freigeben oder darauf zugreifen.

Dateiübertragung

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

Automatisierte Druckerfreigabe

Treten Sie einem verwalteten Netzwerk bei, damit Sie sämtliche lokalen Drucker auf Ihrem Computer für andere Mitglieder freigeben können, die den aktuellen Namen des Druckers als freigegebenen Druckernamen verwenden. 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 48

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

Sie können EasyNetwork über Ihr Windows-Startmenü oder indem Sie auf das Desktop-Symbol klicken öffnen.

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

Tipp: Sie können EasyNetwork auch öffnen, indem Sie auf das McAfee EasyNetwork-Symbol in Ihrem Desktop klicken.

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 254).

Verwaltetes Netzwerk verlassen

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

1. Trennen Sie Ihren Computer vom Netzwerk.
2. Klicken Sie in EasyNetwork im Menü **Tools** auf **Netzwerk verlassen**.
3. Wählen Sie im Dialogfeld "Netzwerk verlassen" den Namen des Netzwerks, das Sie verlassen möchten.
4. Klicken Sie auf **Netzwerk verlassen**.

KAPITEL 49

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 262).
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 262).
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 264).

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 50

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

8

802.11

Ein Satz an Standards für die Datenübertragung in einem drahtlosen Netzwerk. 802.11 wird häufig als Wi-Fi bezeichnet.

802.11a

Eine Erweiterung zu 802.11, die Daten mit bis zu 54 Mbps auf dem 5-GHz-Band überträgt. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

802.11b

Eine Erweiterung zu 802.11, die Daten mit bis zu 11 Mbps auf dem 2,4-GHz-Band überträgt. Hierbei ist die Übertragungsgeschwindigkeit geringer als bei 802.11a, die Reichweite ist jedoch größer.

802.1x

Ein Standard für die Authentifizierung in Netzwerken mit oder ohne Draht. 802.1x wird häufig in drahtlosen 802.11-Netzwerken verwendet. Siehe auch Authentifizierung (Seite 268).

A

ActiveX-Steuerelement

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

Anschluss

Ein Hardware-Speicherort für das Weitergeben von Daten zu und von einem Computer. PCs verfügen über verschiedene Arten von Ports, einschließlich interner Ports für den Anschluss von Festplatten-Laufwerken, Monitoren und Tastaturen, sowie externer Ports für das Anschließen von Modems, Druckern, Mäusen und anderer Peripheriegeräte.

Archivieren

Mithilfe dieser Option können Sie eine Kopie Ihrer wichtigen Dateien auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen. Siehe auch Sichern (Seite 277).

Authentifizierung

Der Vorgang der Verifizierung der digitalen Identität des Absenders einer elektronischen Kommunikation.

B

Bandbreite

Die Datenmenge (Durchsatz), die innerhalb eines bestimmten Zeitraums übertragen werden kann.

Browser

Ein Programm, das zur Anzeige von Webseiten im Internet verwendet wird. Häufig verwendete Webbrowser sind beispielsweise Microsoft Internet Explorer und Mozilla Firefox.

Brute-Force-Angriff

Eine Hacking-Methode, die zur Suche nach Kennwörtern oder Verschlüsselungsschlüsseln verwendet wird, indem alle möglichen Zeichenkombinationen ausprobiert werden, bis die Verschlüsselung aufgebrochen wird.

C

Cache

Ein temporärer Speicherplatz auf Ihrem Computer für häufig oder kürzlich verwendete Daten. Um die Geschwindigkeit und Effizienz beim Surfen im Web zu erhöhen, kann Ihr Browser beispielsweise 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. Siehe auch Verschlüsselung (Seite 279).

Client

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

Cookie

Eine kleine Textdatei, die von zahlreichen Websites für das Speichern von Informationen zu besuchten Seiten verwendet und auf dem Computer der Person gespeichert wird, die im Web surft. Sie kann Anmelde- oder Registrierungsinformationen, Informationen zum Einkaufswagen oder Benutzervoreinstellungen enthalten. Cookies werden hauptsächlich von Websites verwendet, um Benutzer zu identifizieren, die sich zuvor auf der Websites registriert oder diese besucht haben. Sie können jedoch auch eine Informationsquelle für Hacker darstellen.

D

DAT

Erkennungsdefinitionsdateien, auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potentiell unerwünschte Programme (PUPs) identifizieren, erkennen und reparieren.

Dateifragmente

Überbleibsel einer Datei, die auf einem Datenträger verteilt sind. Dateifragmentierung tritt dann auf, wenn Dateien hinzugefügt oder gelöscht werden, und sie kann die Leistung Ihres Computers herabsetzen.

Denial-of-Service (DOS)-Angriff

Ein Typ von Angriff gegen einen Computer, Server oder ein Netzwerk, der den Datenverkehr im Netzwerk verlangsamt oder anhält. Er tritt auf, wenn ein Netzwerk mit so vielen zusätzlichen Anfragen überflutet wird, dass der reguläre Datenverkehr verlangsamt oder ganz unterbrochen wird. Ein Denial-of-Service-Angriff "überflutet" sein Ziel mit falschen Verbindungsanfragen, sodass das Ziel legitime Anfragen ignoriert.

Dialer

Software, die Internetverbindungen an einen anderen Anbieter als den standardmäßigen ISP (Internet Service Provider) des Benutzers umleitet, um zusätzliche Verbindungsgebühren für einen Inhaltsanbieter, einen Händler oder einen Dritten zu produzieren.

DNS

(Domain Name System.) Ein Datenbanksystem, das eine IP-Adresse, wie 11.2.3.44, in einen Domänennamen, wie www.mcafee.com, übersetzt.

Domäne

Ein lokales untergeordnetes Netzwerk oder eine Beschreibung für Websites im Internet. In einem Local Area Network (LAN) ist eine Domäne ein untergeordnetes Netzwerk, das aus Client- und Server-Computern besteht, die von derselben Sicherheitsdatenbank gesteuert werden. Im Internet ist eine Domäne Teil einer jeden Web-Adresse. Beispielsweise ist in www.mcafee.com "mcafee" die Domäne.

Drahtloser Adapter

Ein Gerät, das Drahtlosfunktionen zu einem Computer oder PDA hinzufügt. Es ist über einen USB-Port, eine PC-Karte (CardBus), einen Steckplatz, einen Steckplatz für Speicherkarten oder intern an den PCI-Bus angeschlossen.

E

E-Mail

Elektronische Mail. Nachrichten, die auf elektronischem Weg in einem Computer-Netzwerk versendet und empfangen werden. Siehe auch Webmail (Seite 280).

E-Mail-Client.

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

Echtzeit-Scans

Der Prozess des Scannens von Dateien und Ordnern auf Viren und andere Aktivitäten, wenn Sie oder Ihr Computer darauf zugreifen.

Ereignis

Ein Vorfall oder ein Zwischenfall in einem Computer-System oder -Programm, der von der Sicherheits-Software entsprechend vordefinierter Kriterien erkannt werden kann. Typischerweise löst ein Ereignis eine Aktion aus, wie das Senden einer Benachrichtigung oder das Hinzufügen eines Eintrags zu einem Ereignisprotokoll.

ESS

Erweiterter Dienstsatz. Zwei oder mehr Netzwerke, die ein untergeordnetes Netzwerk 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 es verlassen, passieren die Firewall, die jede Nachricht prüft und diejenigen blockiert, die nicht den angegebenen Sicherheitskriterien entsprechen.

Freigeben

Erlaubt den E-Mail-Empfängern für einen begrenzten Zeitraum den Zugriff auf ausgewählte gesicherte Dateien. 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 von Backup and Restore, 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), die bzw. der zwischen zwei kommunizierenden Parteien vor Beginn der Kommunikation freigegeben wurde. Er wird zum Schutz wichtiger Teile von RADIUS-Nachrichten verwendet. Siehe auch RADIUS (Seite 276).

H

Hotspot

Ein geografischer Ort, der von einem Wi-Fi (802.11)-Zugriffspunkt (AP) abgedeckt ist. Benutzer, die einen Hotspot mit einem drahtlosen Laptop betreten, können eine Internetverbindung herstellen, vorausgesetzt, der Hotspot ist öffentlich und es ist keine Authentifizierung erforderlich. Hotspots befinden sich häufig an sehr belebten Orten, wie Flughäfen.

I

Inhaltsklassifikationsgruppe

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

Integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunkts, Routers und einer Firewall kombiniert sind. Einige Geräte enthalten auch Sicherheitsoptimierungen und Überbrückungsfunktionen.

Intranet

Ein privates Computernetzwerk, üblicherweise innerhalb einer Organisation, auf das nur von autorisierten Benutzern zugegriffen werden kann.

IP-Adresse

(Internet Protocol-Adresse) Eine Adresse für einen Computer oder ein Gerät in einem TCP/IP-Netzwerk. 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. 192.168.1.100).

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Diese Methode wird in vielen Arten von Angriffen einschließlich dem "Session-Hijacking" verwendet. Sie wird oftmals auch dazu verwendet, die Header von E-Mails zu fälschen, damit diese E-Mails nicht mehr zurückverfolgt werden können.

Isolieren

Die erzwungene Isolierung einer Datei oder eines Ordners, die bzw. der vermutlich einen Virus, Spam, verdächtigen Inhalt oder potentiell unerwünschte Programme (PUPs) enthält, damit die Dateien oder Ordner nicht geöffnet oder ausgeführt werden können.

K

Kennwort

Ein Code (normalerweise bestehend aus Buchstaben und Ziffern), der für den Zugriff auf Ihren Computer, ein Programm oder eine Website verwendet wird.

Kennwortdepot

Ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Es ermöglicht es Ihnen, Ihre Kennwörter sicher zu speichern in dem Wissen, dass kein anderer Benutzer (auch kein Administrator) darauf zugreifen kann.

Knoten

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

Komprimierung

Ein Prozess, der Dateien in eine Form komprimiert, die den für die Speicherung oder Übertragung erforderlichen Speicherplatz minimiert.

L

LAN

Abkürzung für Local Area Network (lokales Netzwerk). 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 gemeinsam nutzen.

Launchpad

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

Liste vertrauenswürdiger Adressen

Eine Liste mit Elementen, denen Sie vertrauen und die nicht erkannt werden. Wenn Sie einem Element versehentlich misstrauen (z. B. einem potentiell unerwünschten Programm oder einer Registrierungsänderung), oder wenn Sie möchten, dass das Element wieder erkannt wird, entfernen Sie es einfach aus der Liste.

M

MAC-Adresse

Media Access Control-Adresse. Eine eindeutige Seriennummer, die einem physischen Gerät zugewiesen ist (NIC, Network Interface Card), das auf das Netzwerk zugreift.

"Man-in-the-Middle"-Angriff

Eine Methode des Abhörens und möglicherweise Bearbeitens von Nachrichten, die zwischen zwei Personen versendet werden, ohne dass die Beteiligten wissen, dass ihre Kommunikation abgehört wird.

MAPI

Messaging Application Programming Interface. Die Microsoft-Schnittstellenspezifikation, die es verschiedenen Messaging- und Arbeitsgruppenprogrammen (einschließlich E-Mail, Voice-Mail und Fax) ermöglicht, einen einzigen Client zu verwenden, wie den Exchange-Client.

Message Authentication Code (MAC)

Ein Sicherheitscode, der für das Verschlüsseln von Nachrichten verwendet wird, die zwischen Computern übertragen werden. Die Nachricht wird akzeptiert, wenn der Computer den verschlüsselten Code als gültig erkennt.

MSN

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

N

Netzwerk

Eine Sammlung IP-basierter Systeme (wie Router, Switches, Server und Firewalls), die als logische Einheit gruppiert werden. Ein "Finanznetzwerk" kann beispielsweise alle Server, Router und Systeme umfassen, die einer Finanzabteilung dienen. Siehe auch Privates Netzwerk (Seite 275).

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 graphische Darstellung des Computers und der Komponenten, die ein privates Netzwerk ausmachen.

NIC

(Network Interface Card) Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

P

Papierkorb

Ein simulierter Papierkorb für gelöschte Dateien und Ordner in Windows.

PCI-Drahtlosadapter-Karte

(Peripheral Component Interconnect) Eine Drahtlosadapter-Karte, die in einen PCI-Erweiterungssteckplatz im Computer gesteckt wird.

Phishing

Eine Methode des betrügerischen Erlangens persönlicher Informationen, wie Kennwörter, Sozialversicherungsnummern und Kreditkarteninformationen, indem gefälschte E-Mails versendet werden, die aussehen als kämen sie von vertrauenswürdigen Quellen, wie Banken oder legitimen Unternehmen. Typischerweise fordern Phishing-E-Mails die Empfänger dazu auf, auf den Link in der E-Mail zu klicken, um Kontaktdetails oder Kreditkarteninformationen zu verifizieren oder zu aktualisieren.

Plugin, Plug-in

Ein kleines Software-Programm, das Funktionen hinzufügt oder eine umfangreichere Software erweitert. Plugins ermöglichen dem Webbrowser beispielsweise 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 verfügen über ein POP3-E-Mail-Konto, auch bekannt als standardmäßiges E-Mail-Konto.

Popups

Kleine Fenster, die über anderen Fenstern auf dem Bildschirm angezeigt werden. Popup-Fenster werden oft in Webbrowsern verwendet, um Werbung anzuzeigen.

Potentiell unerwünschtes Programm (PUP)

Ein Software-Programm, das möglicherweise unerwünscht ist, obwohl die Benutzer zugestimmt haben, es herunterzuladen. Es kann die Sicherheits- oder Datenschutzeinstellungen des Computers verändern, auf dem es installiert ist. PUPs können möglicherweise Spyware, Adware und Dialer enthalten, und werden möglicherweise mit einem Programm zusammen heruntergeladen, das der Benutzer möchte.

PPPoE

Abkürzung für "Point-to-Point Protocol Over Ethernet". Eine Methode der Verwendung des Point-to-Point Protocol (PPP)-Einwahlprotokolls mit Ethernet für die Übertragung.

Privates Netzwerk

Zwei oder mehr Computer, die in einem Privathaus verbunden sind, sodass Dateien und der Internetzugriff gemeinsam genutzt werden können. Siehe auch LAN (Seite 273).

Protokoll

Ein Regelsatz, der es Computern oder Geräten ermöglicht, Daten auszutauschen. In einer Netzwerkarchitektur mit mehreren Ebenen (Open Systems Interconnection-Modell) hat jede Ebene ihre eigenen Protokolle, die angeben, wie die Kommunikation auf dieser Ebene erfolgen soll. Ihr Computer oder Ihr Gerät muss das entsprechende Protokoll unterstützen, um mit anderen Computern kommunizieren zu können. Siehe auch Open Systems Interconnection (OSI).

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 Proxy-Server (Seite 275).

Proxy-Server

Eine Firewallkomponente, die den ein- und ausgehenden Internetverkehr eines LAN (Local Area Network) verwaltet. Ein Proxy-Server 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.

Prüfung auf Anforderung

Eine geplante Prüfung ausgewählter Dateien, Anwendungen oder Netzwerkgeräte, um eine Bedrohung, eine Schwachstelle oder anderen potentiell unerwünschten Code zu finden. Die Prüfung kann sofort, zu einem geplanten Zeitpunkt in der Zukunft oder in regelmäßigen Abständen stattfinden. Siehe auch "Zugriffsscans" oder "Schwachstelle".

Pufferüberlauf

Ein Umstand, der in einem Betriebssystem oder einer Anwendung auftritt, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (temporärer Speicherplatz) zu speichern, als dieser aufnehmen kann. Ein Pufferüberlauf beschädigt den Speicher und überschreibt Daten in benachbarten Puffern.

R

RADIUS

RADIUS (Remote Access Dial-In User Service). Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern. Siehe auch Gemeinsamer geheimer Schlüssel.

Registrierung

Eine von Windows verwendete Datenbank zum Speichern der Konfigurationsinformationen für jeden Benutzer des Computers, die System-Hardware, installierte Programme und Eigenschafteneinstellungen. Die Datenbank wird in Schlüssel aufgeteilt, für die Werte festgelegt werden. Unerwünschte Programme können den Wert von Registrierungsschlüsseln ändern oder neue erstellen, um schädlichen Code auszuführen.

Reiner Text

Text, der nicht verschlüsselt ist. Siehe auch Verschlüsselung (Seite 279).

Roaming

Das Wechseln aus dem Empfangsbereich eines Zugriffspunkts in den eines anderen, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

Rootkit

Ein Satz an Tools (Programmen), die einem Benutzer Administratorzugriff auf einen Computer oder ein Computer-Netzwerk gewähren. Rootkits können Spyware und andere potentiell unerwünschten Programme umfassen, die eine zusätzliche Gefahr oder ein Datenschutzrisiko für die Sicherheit Ihres Computers und Ihrer persönlichen Daten darstellen.

Router

Ein Netzwerkgerät, das Datenpakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden, wie es auf der Grundlage der Quell- und Zieladressen und der aktuellen Verkehrbedingungen weitergeleitet werden soll. Ein Router wird gelegentlich als Zugriffspunkt 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 (Seite 280), WPA (Seite 281), WPA2 (Seite 281), WPA2-PSK (Seite 281), WPA-PSK (Seite 281).

Schwarze Liste

In Anti-Spam eine Liste der E-Mail-Adressen, von denen Sie keine Nachrichten erhalten möchten, da Sie die Nachrichten für Spam halten. In Anti-Phishing eine Liste der Websites, die als betrügerisch angesehen werden. Siehe auch Weiße Liste (Seite 280).

Server

Ein Computer oder Programm, der bzw. das Verbindungen von anderen Computern oder Programmen akzeptiert, und entsprechende Antworten ausgibt. Beispielsweise stellt Ihr E-Mail-Programm eine Verbindung zu einem E-Mail-Server her, sobald Sie E-Mails versenden oder empfangen.

Sichern

Verwenden Sie diese Option, um eine Kopie Ihrer wichtigen Dateien auf einem sicheren Online-Server zu erstellen. Siehe auch Archivieren (Seite 268).

Skript

Eine Liste mit Befehlen, die automatisch ausgeführt werden können (d. h. ohne Eingreifen des Benutzers). Anders als Programme werden Skripten typischerweise in reinem Textformat gespeichert, und bei jedem Ausführen kompiliert. Makros und Batch-Dateien werden auch als Skripten bezeichnet.

Smart-Laufwerk

Siehe USB-Laufwerk (Seite 279).

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.

SSID

Service Set Identifier. Ein Token (geheimer Schlüssel), der ein Wi-Fi (802.11)-Netzwerk identifiziert. Der SSID wird vom Netzwerkadministrator eingerichtet, und muss von den Benutzern angegeben werden, die dem Netzwerk beitreten 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 (Seite 274).

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 warnt bei Erkennung nicht autorisierter Änderungen auf Ihrem Computer und benachrichtigt Sie.

Systemwiederherstellungspunkt

Ein Bild (Image) der Inhalte im Speicher oder in einer Datenbank des Computers. Windows erstellt Wiederherstellungspunkte in regelmäßigen Abständen und wenn wichtige Systemereignisse auftreten, beispielsweise bei der Installation eines Programms oder Treibers. Sie können jedoch auch jederzeit Ihre eigenen Wiederherstellungspunkte erstellen und diese benennen.

T

Temporäre Datei

Eine von dem 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 (gesprochen tee-kip). Teil des 802.11i-Verschlüsselungsstandards für drahtlose LANs. TKIP ist die nächste Generation von WEP, das verwendet wird, um drahtlose 802.11-LANs zu schützen. TKIP bietet eine Schlüsselmischung nach Paket, eine Nachrichtenintegritätsprüfung und einen Mechanismus zum erneuten Erstellen von Schlüsseln nach dem Beheben von Fehlern im WEP.

Trojaner (Trojanisches Pferd)

Ein Programm, das sich nicht selbst vervielfacht, aber Schäden versursacht oder die Sicherheit Ihres Computers gefährdet. Typischerweise sendet Ihnen eine Einzelperson einen Trojaner per E-Mail. Der Trojaner versendet sich nicht automatisch. Sie können einen Trojaner auch von einer Website oder über ein Peer-to-Peer-Netzwerk ohne Ihr Wissen herunterladen.

U

U3

You: Einfacher, schlauer, mobil. 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 Backup and Restore innerhalb der Überwachungs-Speicherorte gesichert oder archiviert werden.

Überwachungs-Speicherorte

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

U

Unerwünschter Zugriffspunkt

Ein nicht autorisierter Zugriffspunkt. Unerwünschte Zugriffspunkte können in einem sicheren Unternehmensnetzwerk installiert werden, um den Netzwerkzugriff für nicht autorisierte Personen zu gewähren. Sie können auch erstellt werden, um es einem Angreifer zu ermöglichen, einen Man-in-the-Middle-Angriff durchzuführen.

URL

(Uniform Resource Locator) Das Standardformat für Internetadressen.

USB

Universal Serial Bus. Ein standardmäßiger Connector auf den meisten modernen Computern, der eine Verbindung zu mehreren Geräten herstellt, von Tastaturen und Mäusen bis hin zu Webcams, Scannern und Druckern.

USB-Drahtlosadapter-Karte

Eine Drahtlosadapterkarte, die an den USB-Port eines Computers angeschlossen werden kann.

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

Der Prozess des Verfügbarmachens einer gesicherten Datei im Internet. Sie können auf veröffentlichte Dateien zugreifen, indem Sie die Backup and Restore-Bibliothek durchsuchen.

Verschlüsselung

Eine Methode des Verschlüsselns von Informationen, damit nicht autorisierte Personen nicht darauf zugreifen können. Wenn die Daten verschlüsselt werden, verwendet der Prozess einen "Schlüssel" und mathematische Algorithmen. Verschlüsselte Informationen können nicht ohne den entsprechenden Schlüssel entschlüsselt werden. Viren verwenden manchmal die Verschlüsselung, um nicht erkannt zu werden.

Virus

Ein Computerprogramm, das sich selbst kopieren und einen Computer infizieren kann, ohne dass der Benutzer seine Erlaubnis gibt oder davon weiß.

VPN

Virtual Private Network. Ein Netzwerk für private Kommunikationen, das über ein Host-Netzwerk, wie das Internet, konfiguriert wird. Die über eine VPN-Verbindung übertragenen Daten werden verschlüsselt und sind somit gut geschützt.

W

Wardriver

Eine Person, die nach Wi-Fi (802.11)-Netzwerken sucht, indem sie mit einem Wi-Fi-Computer und spezieller Hardware oder Software durch Städte 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 sind auch als Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs bekannt.

Webmail

Webbasierte E-Mail. Elektronischer Mail-Service, auf den hauptsächlich über einen Webbrowser zugegriffen werden kann anstatt über einen computerbasierten E-Mail-Client wie Microsoft Outlook. Siehe auch E-Mail (Seite 270).

Weiße Liste

Eine Liste der Websites oder E-Mail-Adressen, die als sicher angesehen werden. Websites auf einer weißen Liste sind diejenigen, auf die die Benutzer zugreifen dürfen. E-Mail-Adressen auf einer weißen Liste gehören zu vertrauenswürdigen Quellen, von denen Sie Nachrichten empfangen möchten. Siehe auch Schwarze Liste (Seite 276).

WEP

Wired Equivalent Privacy. Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Wi-Fi-Standard (802.1). Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

Wi-Fi

(Wireless Fidelity) Ein Begriff, der von der Wi-Fi Alliance verwendet wird und einen Typ von 802.11-Netzwerk bezeichnet.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht. Die Wi-Fi Alliance möchte alle 802.11-basierten Produkte für die Interoperabilität zertifizieren und den Begriff Wi-Fi als globalen Markennamen auf allen Märkten und für alle 802.11-basierten drahtlosen LAN-Produkte vorantreiben. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die das Wachstum dieser Branche voranbringen möchten.

Wi-Fi Certified

Durch die Wi-Fi Alliance getestet und genehmigt. Wi-Fi-zertifizierte Produkte werden als interoperabel angesehen, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden.

WLAN

Wireless Local Area Network. Ein lokales Netzwerk (LAN), das eine drahtlose Verbindung verwendet. Ein WLAN verwendet Funkwellen auf hoher Frequenz, sodass für die Kommunikation zwischen Computern keine Kabel mehr erforderlich sind.

Wörterbuchangriff

Ein Typ von gewaltsamem Angriff, der häufig verwendete Begriffe einsetzt, 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 stark erhöht. WPA ist vom Standard 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Software-Upgrades entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entworfen wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus kann der Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren, und sollte die Passphrase auf jedem drahtlosen Computer und Zugriffspunkt regelmäßig ändern. Siehe auch WPA2-PSK (Seite 281), TKIP (Seite 278).

WPA2

Ein aktualisierter WPA-Sicherheitsstandard, der auf dem 802.11i-Standard basiert.

WPA2-PSK

Ein spezieller WPA-Modus, der WPA-PSK ähnlich ist und auf dem WPA2-Standard basiert. Eine häufig verwendete Funktion von WPA2-PSK ist, dass Geräte häufig mehrere Verschlüsselungsmodi (z. B. AES, TKIP) gleichzeitig unterstützen, während ältere Geräte üblicherweise nur jeweils einen Verschlüsselungsmodus unterstützten (d. h. alle Clients müssten denselben Verschlüsselungsmodus unterstützen).

Wurm

Ein Virus, das sich durch die Erzeugung von eigenen Duplikaten auf anderen Laufwerken, Systemen oder Netzwerken verbreitet. Ein Massenmailer-Wurm erfordert das Eingreifen des Benutzers für seine Verbreitung, d. h. der Benutzer öffnet einen Anhang oder führt eine heruntergeladene Datei aus. Die meisten E-Mail-Viren heutzutage sind Würmer. Ein sich selbst verbreitender Wurm benötigt kein Eingreifen des Benutzers, um sich zu verbreiten. Beispiele für sich selbst verbreitende Würmer sind Blaster und Sasser.

Z

Zugriffspunkt (Access Point, AP)

Ein Netzwerkgerät (häufig auch als drahtloser Router bezeichnet), das an einen Ethernet-Hub oder -Switch angeschlossen werden kann, um die physische Reichweite eines Dienstes für einen drahtlosen Router zu erweitern. Wenn drahtlose Benutzer Roaming für ihre mobilen Geräte durchführen, findet die Übertragung von einem Zugriffspunkt zu einem anderen statt, um die Konnektivität aufrecht zu erhalten.

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.

Lizenz

Copyright

KAPITEL 51

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.

Lesen Sie in den folgenden Tabellen nach, um die Websites des Supports und für Downloads von McAfee in Ihrem Land oder Ihrer Region zu finden, einschließlich der Benutzerhandbücher.

Support und Downloads

Land/Region	McAfee-Support	McAfee-Downloads
Australien	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilien	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
China (vereinfachtes Chinesisch)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp

Dänemark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Deutschland	www.mcafeehilfe.com	de.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
Griechenland	www.mcafeehelp.com	el.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
Kanada (Englisch)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (Französisch)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
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
Russland	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Schweden	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Slowakei	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Spanien	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tschechische Republik	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Türkei	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

Ungarn	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection-Benutzerhandbücher

Land/Region	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
China (vereinfachtes Chinesisch)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/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
Griechenland	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/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
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
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Slowakei	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tschechische Republik	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Ungarn	http://download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security-Benutzerhandbücher

Land/Region	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
China (vereinfachtes Chinesisch)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/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
Griechenland	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/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
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
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Slowakei	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tschechische Republik	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus-Benutzerhandbücher

Land/Region	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

China (vereinfachtes Chinesisch)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/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
Griechenland	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/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
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
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Slowakei	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf

Tschechische Republik	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan-Benutzerhandbücher

Land/Region	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
China (vereinfachtes Chinesisch)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Dänemark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Deutschland	download.mcafee.com/products/manuals/de/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
Griechenland	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Großbritannien	download.mcafee.com/products/manuals/en-uk/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
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
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Niederlande	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Schweden	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Slowakei	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tschechische Republik	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Türkei	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

In der nachfolgenden Tabelle finden Sie die Websites des McAfee Threat Center and Virus Information in Ihrem Land oder Ihrer Region.

Land/Region	Security Headquarters	Virus-Informationen
Australien	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilien	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
China (vereinfachtes Chinesisch)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Dänemark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Deutschland	www.mcafee.com/us/threat_center	de.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
Griechenland	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo

Großbritannien	www.mcafee.com/us/threat_center	uk.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
Kanada (Englisch)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (Französisch)	www.mcafee.com/us/threat_center	ca.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
Niederlande	www.mcafee.com/us/threat_center	nl.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
Russland	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Schweden	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Slowakei	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Spanien	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tschechische Republik	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Türkei	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Ungarn	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

In der nachfolgenden Tabelle finden Sie die HackerWatch-Websites in Ihrem Land oder Ihrer Region.

Land/Region	HackerWatch
Australien	www.hackerwatch.org
Brasilien	www.hackerwatch.org/?lang=pt-br
China (vereinfachtes Chinesisch)	www.hackerwatch.org/?lang=zh-cn
Dänemark	www.hackerwatch.org/?lang=da
Deutschland	www.hackerwatch.org/?lang=de
Finnland	www.hackerwatch.org/?lang=fi
Frankreich	www.hackerwatch.org/?lang=fr
Griechenland	www.hackerwatch.org/?lang=el
Großbritannien	www.hackerwatch.org
Italien	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Kanada (Englisch)	www.hackerwatch.org
Kanada (Französisch)	www.hackerwatch.org/?lang=fr-ca
Korea	www.hackerwatch.org/?lang=ko
Mexiko	www.hackerwatch.org/?lang=es-mx
Niederlande	www.hackerwatch.org/?lang=nl
Norwegen	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Russland	www.hackerwatch.org/?lang=ru
Schweden	www.hackerwatch.org/?lang=sv
Slowakei	www.hackerwatch.org/?lang=sk
Spanien	www.hackerwatch.org/?lang=es
Taiwan	www.hackerwatch.org/?lang=zh-tw
Tschechische Republik	www.hackerwatch.org/?lang=cs
Türkei	www.hackerwatch.org/?lang=tr
Ungarn	www.hackerwatch.org/?lang=hu
USA	www.hackerwatch.org

Index

C

D

E

F

G

H

I

R

S

T

U

V

W

Z