



**F-Secure Internet Security
2009**

Inhalt

Kapitel 1: Erste Schritte.....7

Was muss ich nach der Installation tun?.....8	8
So können Sie prüfen, ob das Produkt einwandfrei funktioniert.....8	8
Wie wird das Produkt geöffnet?.....8	8
Wie kann ich sicherstellen, dass mein Computer geschützt ist?.....9	9
Was zeigt der Status-Tooltip an?.....9	9
So können Sie den Gesamtstatus Ihres Schutzes anzeigen.....11	11
Wie kann ich die häufigsten Aufgaben schnell ausführen?.....16	16
So scannen Sie eine Datei oder einen Ordner im Windows Explorer.....16	16
Wie können Aufgaben schnell über das Kontextmenü des Statussymbols ausgeführt werden?.....16	16

Kapitel 2: Viren und andere Malware stoppen.21

Was sind Viren und sonstige Malware?.....23	23
Viren.....23	23
Spyware.....23	23
Rootkits.....24	24
Riskware.....24	24
Was sind AntiVirus- & AntiSpy-Schutzstufen?.....25	25
Ändern der Antivirus- & AntiSpy-Schutzstufe.....25	25
Scannen des Computers in Echtzeit.....28	28
So schützt das Scannen in Echtzeit Ihren Computer.....28	28
Echtzeit-Scanning einschalten.....29	29
In Echtzeit auf Viren überprüfen.....29	29
In Echtzeit auf Spyware überprüfen.....36	36
Scannen nach verdächtigen Programmen in Echtzeit.....38	38
Web-Datenverkehr-Scanning einschalten.....46	46
Scannen des Computers zu bestimmten Zeiten.....48	48
Zu festgelegten Zeiten nach Malware scannen.....48	48

F-Secure Internet Security 2009 | Inhaltsverzeichnis

Dateien und Ordner für manuelle und geplante Scans auswählen.....	49
Welche Aktionen werden sollen, wenn Malware bei manuellen oder geplanten Scans gefunden wurde.....	52
Manuelles Scannen des Computers.....	55
Welche verschiedenen Typen des manuellen Scannens gibt es und welcher Typ sollte verwendet werden.....	55
Computer manuell auf Malware scannen.....	56
Dateien und Ordner für manuelle und geplante Scans auswählen.....	63
Welche Aktionen werden sollen, wenn Malware bei manuellen oder geplanten Scans gefunden wurde.....	66
Was ist ein Quarantäne-Repository?.....	69
Programme unter Quarantäne anzeigen.....	69
Wiederherstellen eines Programms aus der Quarantäne.....	70
Scannen Ihrer E-Mails.....	72
Wann werden E-Mail-Nachrichten und -Anhänge gescannt?.....	72
Infizierte E-Mail-Anhänge empfangener E-Mails automatisch desinfizieren oder entfernen.....	73
Senden infizierter E-Mails automatisch verhindern.....	74
Benachrichtigen, wenn in einer E-Mail ein Virus gefunden wird.....	74
Scannen komprimierter E-Mail-Anhänge.....	75
Fortschritt des E-Mail-Scannings anzeigen.....	75
Festlegen der Ports für verschiedene E-Mail-Protokolle.....	76

Kapitel 3: Sichere Verwendung des Internets.....77

Was sind Sicherheitsstufen?.....	78
Ändern der Sicherheitsstufe	79
Was ist eine Firewall?.....	80
So verfahren Sie, wenn ein Popup des Internet-Schutzschilds angezeigt wird....	80
Was sind Firewallregeln?.....	82
Firewalleinstellungen.....	102
Kontrollieren von Internetverbindungen für Anwendungen.....	106
Vorgehensweise, wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird.....	107
Verbindungen für Programme zulassen oder ablehnen.....	110
Popup-Fenster der Anwendungssteuerung ein- und ausschalten.....	111
So verfahren Sie, wenn ein Programm nicht mehr funktioniert.....	112
Verhindern von Eindringungsversuchen.....	114
Wählen Sie aus, wie Eindringungsversuche behandelt werden.....	114

F-Secure Internet Security 2009 | Inhaltsverzeichnis

Kontrollieren von DFÜ-Verbindungen	116
Vorgehensweise bei einem Popup-Fenster des Dialerschutzes.....	117
Hinzufügen, Bearbeiten oder Entfernen von Telefonnummern.....	118
Programme anzeigen, die berechtigt sind, DFÜ-Verbindungen zu beenden.....	119
DFÜ-Verbindungsversuche anzeigen.....	120
So müssen Sie vorgehen, wenn Sie über Ihr Modem keine Verbindung zum Internet herstellen können..	121
Anzeigen von Internet-Schutzschildstatus, Alarmen und Protokolldateien.....	122
Status von Internet Shield überprüfen.....	122
Prüfen Sie die aktuellen Einstellungen des Internet-Schutzschilds.....	122
Prüfen Sie die Anzahl der kürzlich erfolgten Aktionen des Internet-Schutzschilds.	123
Alarme des Internet-Schutzschilds anzeigen.....	123
Protokolldateien anzeigen.....	125
Kapitel 4: Automatische Updates.....	133
Prüfen des Update-Status.....	134
Ändern der Internetverbindungseinstellungen.....	135
Konfigurieren eines HTTP-Proxys Manuell.....	136

Installation

Themen:

- *Systemanforderungen*
- *Vor der Installation*
- *Installationsschritte*
- *Notfall-CD*
- *Technischer Support*
- *Registrieren der Lizenz*

DISCLAIMER

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:
GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2008 F-Secure Corporation. All rights reserved.

Systemanforderungen

Zur Installation und Verwendung des Produkts muss der Computer folgende Anforderungen erfüllen:

Systemanforderungen:	
Prozessor:	<ul style="list-style-type: none">• Windows Vista: Kann Windows Vista 32-Bit ausführen (Intel Pentium 4, 2 GHz oder höher empfohlen)• Windows XP/2000: Intel Pentium III 600 MHz oder höher (Intel Pentium III, 1 GHz oder höher empfohlen)
Betriebssystem:	<ul style="list-style-type: none">• Windows Vista 32 Bit und 64 Bit: Starter, Home Basic, Home Premium, Business, Ultimate, Enterprise.• Windows XP Home/Professional/Media Center Edition (SP 2 für vollständige Funktionalität erforderlich)• Windows 2000 Professional SP4 und höher (Update Rollup 1 empfohlen)
Arbeitsspeicher:	<ul style="list-style-type: none">• Windows Vista: 512 MB RAM (1 GB oder mehr empfohlen)• Windows XP/2000: 256 MB RAM (512 MB RAM oder mehr empfohlen)
Festplattenspeicher:	600 MB freier Festplattenspeicher (800 MB empfohlen)
Bildschirm:	<ul style="list-style-type: none">• Windows Vista: 16 Bit oder mehr (65.000 Farben)• Windows XP/2000: 8 Bit, 256 Farben (16 Bit, 65.000 Farben oder mehr empfohlen)
Internetverbindung:	Eine Internetverbindung ist erforderlich, um Ihr Abonnement zu bestätigen und Updates zu erhalten
Browser:	<ul style="list-style-type: none">• Windows Vista: Internet Explorer 7.0 oder neuer• Windows XP/2000: Internet Explorer 5.0 (Internet Explorer 6.0 oder höher empfohlen)

Vor der Installation

- Wenn Sie eine frühere Version von F-Secure Internet Security oder F-Secure Anti-Virus verwenden, können sie dieses Produkt direkt installieren. Befolgen Sie die Anweisungen unter *“Installationsschritte”*.
- Wenn Sie die Testversion von F-Secure Internet Security 2009 oder F-Secure Anti-Virus 2009 auf Ihrem Computer installiert und die lizenzierte Version gekauft haben, können Sie sie verwenden, nachdem Sie den Abonnementschlüssel eingegeben haben. Um den Abonnementschlüssel einzugeben, klicken Sie auf der Registerkarte *Start* auf **Erweitert...**, öffnen Sie den Zweig *Allgemein* und wählen Sie *Meine Anmeldung*.


Installationsschritte

Sie benötigen die Produkt-CD, einen gültigen Abonnementschlüssel sowie eine Internet-Verbindung.

Wenn der Computer für mehrere Benutzer freigegeben ist, müssen Sie sich mit Administratorrechten anmelden, um dieses Produkt zu installieren.


So installieren Sie die Software:

1. Legen Sie die Installations-CD ein. Die Installation sollte automatisch starten. Falls sie nicht automatisch gestartet wird, wechseln Sie zum Windows-Explorer, doppelklicken Sie auf das Symbol der CD-ROM, und doppelklicken Sie dann auf die Datei *setup.exe*, um die Installation zu starten. Das erste Installationsdialogfeld wird angezeigt.
2. Wählen Sie die Installationssprache aus und klicken Sie auf **Weiter**, um fortzufahren.
3. Lesen Sie die Lizenzvereinbarung. Um die Vereinbarung anzunehmen und fortzufahren, klicken Sie auf **Akzeptieren**.
4. Geben Sie Ihren Abonnementschlüssel ein und klicken Sie auf **Weiter**, um fortzufahren.


 *Wenn Sie das Produkt testen möchten, lassen Sie das Feld "Meine Anmeldeschlüssel" leer und klicken Sie auf **Weiter**. Wählen Sie im Dialogfeld „Testoptionen“ den Dienst aus, den Sie testen möchten.*

- Wenn Sie das Produkt auf CD in einem Geschäft erworben haben, finden Sie den Abonnementschlüssel auf dem Deckblatt des Installationsleitfadens.
- Wenn Sie das Produkt über den F-Secure eStore bezogen haben, finden Sie den Abonnementschlüssel in der Bestätigungs-E-Mail der Bestellung.

IV | F-Secure Internet Security 2009 | Installation

 *Verwenden Sie nur den im Lieferumfang des Produkts enthaltenen Abonnementschlüssel. Sie können den Abonnementschlüssel für die Anzahl von Installationen, für die Ihre Lizenz gültig ist (weitere Informationen finden Sie unter 'F-Secure Lizenz' in diesem Handbuch). Wenden Sie sich an den technischen Support von F-Secure, wenn bei der Registrierung Probleme auftreten.*

5. Wählen Sie den Installationstyp:
 - *Automatische Installation:* Das Produkt wird automatisch gestartet. Bereits vorhandene Sicherheitsprodukte werden möglicherweise automatisch ersetzt. Das Produkt wird im Standardverzeichnis installiert.
 - *Schritt-für-Schritt-Installation:* Sie können während der Installation verschiedene Auswahlen vornehmen. Sie können beispielsweise das Installationsverzeichnis ändern. Wir empfehlen jedoch, das Standardverzeichnis zu verwenden.
6. Klicken Sie auf **Weiter**.
7. Entfernen Sie die Installations-CD, nachdem die Installation abgeschlossen ist.
8. Wählen Sie für einen Neustart die Option **Jetzt neu starten (empfohlen)**.
9. Klicken Sie auf **Fertig stellen**.
10. Nach dem Neustart können Sie das Produkt für Ihren Computer einrichten. Befolgen Sie die Bildschirmanweisungen. Danach kann das Produkt verwendet werden.

 *Für weitere Informationen zu diesem Produkt können Sie auf die Online-Hilfe zugreifen, indem Sie im Produkt auf die Taste „Hilfe“ klicken. Die Online-Hilfe befindet sich ebenfalls auf der Installations-CD.*

Notfall-CD

Falls der Computer durch einen Virus infiziert ist und sich nicht mehr neu starten lässt, können Sie die Produkt-CD als Notfall-CD verwenden. Legen Sie die CD in das CD-Laufwerk ein, und starten Sie den Computer neu. Befolgen Sie nach dem Neustart des Computers die Anweisungen auf dem Bildschirm. Sie können Dateien auf Ihren Festplatten desinfizieren, oder Ihre Daten auf Disketten oder USB-Speichersticks kopieren. Sie können sie auch auf einen anderen Computer kopieren, wenn Sie über eine Netzwerkverbindung verfügen.

! **WARNUNG: Bevor Sie Daten auf einen anderen Computer kopieren, vergewissern Sie sich, dass auf diesem Computer ein aktuelles Virenschutzprogramm installiert ist, da einige Dateien unter Umständen durch einen Virus infiziert sind.**

Technischer Support

Sie können auf die Online-Hilfe zugreifen, indem Sie auf der Benutzeroberfläche der Anwendung auf **Hilfe** klicken. Ziehen Sie die Online-Hilfe zurate, bevor Sie sich an das F-Secure Online Support Center wenden. Bei Problemen oder Fragen, die nicht mit der Hilfe oder dem Online-Dienst gelöst werden können, verwenden Sie die folgenden Informationen zur Kontaktaufnahme mit F-Secure.

Deutschland

069 669 831 31

<http://support.f-secure.de>

Schweiz

084 220 40 80

<http://support.f-secure.com>

Andere Länder (Englisch)

+358 9 2520 5050

<http://support.f-secure.com>

Registrieren der Lizenz

Durch die Lizenzregistrierung sind Sie berechtigt, weitere Dienste in Anspruch zu nehmen, z. B. kostenlose Produktupdates und Produktunterstützung. Sie können Ihre Lizenz über das Formular unter folgender Adresse registrieren: www.f-secure.com/register

F-SECURE LICENSE

You are granted the right to use the product in up to three computers (1-3 installations, license validity period begins from the first installation).

License terms and conditions are supplied with your software.

Kapitel 1

Erste Schritte

Themen:

- *Was muss ich nach der Installation tun?*
- *Wie kann ich sicherstellen, dass mein Computer geschützt ist?*
- *Wie kann ich die häufigsten Aufgaben schnell ausführen?*

Was muss ich nach der Installation tun?

Nach der Installation des Produkts sollten Sie dessen ordnungsgemäße Funktionsweise überprüfen.

So können Sie prüfen, ob das Produkt einwandfrei funktioniert

Prüfen Sie nach der Installation, ob das Statussymbol des Produkts rechts unten am Bildschirm in der Windows-Systemleiste angezeigt wird.

Anzeige des Symbols:

1. Wenn Sie Windows XP verwenden, klicken Sie auf die Schaltfläche



, um die Symbole in der Systemleiste anzuzeigen.

- 2.



Prüfen Sie, ob das Symbol  in der Systemleiste angezeigt wird.

Wenn das Symbol angezeigt wird, funktioniert das Produkt einwandfrei und Ihr Computer ist geschützt.

Wie wird das Produkt geöffnet?

Sie können das Programm starten, indem Sie in der Windows-Taskleiste auf das Status-Symbol des Produkts doppelklicken.


So öffnen Sie das Produkt:

1. Wenn Sie mit Windows XP arbeiten, klicken Sie auf die Schaltfläche




, um die Symbole in der Taskleiste anzuzeigen.

- 2.

Doppelklicken Sie auf das Symbol .

Auf der Registerkarte **Start** der Benutzeroberfläche des Programms finden Sie eine Übersicht über den Schutzstatus und die installierten Produktkomponenten.

 **Tipp:** Alternativ können Sie Produkt und Hilfe über das Windows-Menü **Start** öffnen.

Wie kann ich sicherstellen, dass mein Computer geschützt ist?





Sie können das Statussymbol in der Taskleiste und die Informationen zu Produktstatus und Abonnement auf der Registerkarte **Start** überprüfen, um sich zu vergewissern, dass Ihr Computer geschützt ist.






Was zeigt der Status-Tooltip an?

Wenn Sie den Mauszeiger in der Windows-Taskleiste auf den Produktstatus bewegen, wird eine QuickInfo eingeblendet, die Aufschluss über den Produktstatus gibt.

Abhängig vom Produktstatus wird das Symbol auf unterschiedliche Art oder überhaupt nicht angezeigt.

Status-Symbole und deren Bedeutung:

Symbol	Status	Vorgehensweise
	Das Produkt funktioniert einwandfrei. Ihr Computer ist geschützt.	Sie können Ihren Computer normal verwenden.
	Download läuft. Ihr Computer ist geschützt, sobald der Download abgeschlossen ist.	Dieses Symbol wird angezeigt, wenn z. B. <i>Viren- und Spywaredefinitionen</i> oder Sicherheitsstufen heruntergeladen werden. Warten Sie, bis der Download abgeschlossen ist.
	Fehlerstatus. Ein Fehler ist aufgetreten.	Platzieren Sie Ihren Mauszeiger auf dem Symbol  , damit der Grund für den Fehler angezeigt wird. Starten Sie Ihren Computer gegebenenfalls neu.

Symbol	Status	Vorgehensweise
	Warnung. Eine Schutzfunktion, beispielsweise Echtzeit-Scanning, ist deaktiviert oder Ihre <i>Viren- und Spyware-Definitionen</i> sind veraltet. Ihr Computer ist nicht vollständig geschützt.	Bewegen Sie den Mauszeiger auf das Symbol  , um die QuickInfo zum Status anzuzeigen. Dieses Symbol wird beispielsweise angezeigt, wenn Sie die Festplatte defragmentieren, da einige Systemfunktionen dafür sorgen, dass alle Downloads angehalten werden. Aktivieren Sie die derzeit deaktivierte Funktion oder prüfen Sie, ob Updates vorhanden sind.
	Kritischer Alarmstatus (blinkendes Symbol).	Dieses Symbol wird angezeigt, wenn die <i>Viren- und Spyware-Definitionen</i> nicht kürzlich aktualisiert wurden. Aktualisieren Sie sofort die <i>Viren- und Spywaredefinitionen</i> .
	Nicht geladen. Das Produkt ist im Arbeitsspeicher Ihres Computers nicht geladen. Ihr Computer ist nicht geschützt.	Klicken Sie mit der rechten Maustaste auf das Symbol  und wählen Sie Erneut laden , um das Produkt zu aktivieren.
Kein Symbol	Das Produkt ist nicht installiert oder ein Fehler hat den Produktstart verhindert.	Starten Sie Ihren Computer neu. Falls das Symbol nicht angezeigt wird,

Symbol	Status	Vorgehensweise
		installieren Sie das Produkt neu.

So können Sie den Gesamtstatus Ihres Schutzes anzeigen

Auf der Registerkarte **Start** finden Sie eine Kurzübersicht über Ihre Sicherheitskomponenten und den Status der installierten Sicherheitskomponenten.

Im oberen Bereich der Registerkarte **Start** wird der Sicherheitsstatus Ihres Computers angezeigt. Wenn als Status beispielsweise **Geschützt** angezeigt wird, ist der Schutz Ihres Computers aktuell.

Die Sicherheitsstufen der unterschiedlichen Sicherheitskomponenten, beispielsweise "Normal" oder "Hoch", werden neben dem Namen der Komponente angezeigt.

Im unteren Bereich der Registerkarte **Start** werden das Datum und die Uhrzeit der letzten Aktualisierungsprüfung angezeigt.

Wenn Sie links auf die Registerkarten klicken, werden die Details aller Sicherheitskomponenten angezeigt.

Das Symbol zeigt den Status des Programms und seiner Sicherheitskomponenten an. Wenn Sie die Programmeinstellungen ändern, verändert sich auch das Symbol.

Die Bedeutung der einzelnen Symbole:



Eine kritische Sicherheitskomponente, beispielsweise AntiVirus & AntiSpy, arbeitet einwandfrei.



Eine der Sicherheitskomponenten wird nicht verwendet, Ihr Computer ist jedoch weiterhin geschützt.



Eine Sicherheitskomponente oder eine ihrer Funktionen ist deaktiviert und Ihr Computer ist nicht geschützt. Das Symbol wird



wieder grün, wenn Sie die Komponente erneut aktivieren.

Ihr Abonnement für den Update-Dienst ist abgelaufen.



Ein Fehlerstatus in der Software.

Wie finde ich heraus, ob meine Abonnement gültig ist?

Der Typ und der Status Ihrer Anmeldung werden auf der Seite **Meine Anmeldung** angezeigt.

Wenn Ihr Abonnement in weniger als 30 Tagen abläuft oder bereits abgelaufen ist, befindet sich auf der **Start**-Registerkarte des Produkts eine Zeile namens **Anmeldestatus**. Sie enthält das Ablaufdatum Ihres Abonnements sowie einen Link, über den Sie das Abonnement verlängern können.

So prüfen Sie die Gültigkeit Ihrer Anmeldung:


1. Klicken Sie auf der Registerkarte **Start** auf **Erweitert**.

Wenn Ihre Anmeldung abgelaufen ist, wird auf der Registerkarte **Start** **Ändern** anstelle von **Erweitert** angezeigt.

2. Wählen Sie **Allgemein** > **Meine Anmeldung**.

Der Status und das Ablaufdatum Ihrer Anmeldung werden auf der sich öffnenden Seite **Meine Anmeldung** angezeigt:

- **Gültig** - Sie besitzen eine laufende Anmeldung.
- **Gültig bis [Datum]** - Die Anmeldung ist bis zum angezeigten Datum aktiv.
- **Abgelaufen** - Der Gültigkeitszeitraum der Anmeldung ist überschritten. Sie müssen Ihre Anmeldung erneuern, um weiterhin Updates zu erhalten und das Produkt zu verwenden.

 **Hinweis:** Wenn Ihre Anmeldung abgelaufen ist, blinkt das Symbol




in Ihrer Systemleiste.

So verlängern Sie Ihr Abonnement

Wenn Ihre Anmeldung bald abläuft oder wenn Sie eine Testversion des Produkts einsetzen, können Sie Ihre Anmeldung online verlängern.

So verlängern Sie Ihre Anmeldung:

1. Klicken Sie auf der Registerkarte **Start** auf **Erweitert**.
2. Wählen Sie **Allgemein** > **Meine Anmeldung**.
3. Klicken Sie auf **Online verlängern**.
Dies öffnet eine Website, auf der Sie Ihre Lizenz verlängern oder einen neuen Abonnementschlüssel erhalten können. Folgen Sie der Anleitung auf der Seite.
4. Sobald Sie Ihren neuen Schlüssel haben, klicken Sie auf **Schlüssel ändern**.
5. Geben Sie im sich öffnenden Dialogfeld Ihren neuen Abonnementschlüssel ein und klicken Sie auf **Registrieren**.

 **Tipp:** Falls Sie Ihren Abonnementschlüssel per E-Mail erhalten haben, können Sie den Schlüssel aus der E-Mail-Nachricht kopieren und in das Feld einfügen.

Sobald der neue Abonnementschlüssel erfolgreich registriert ist, wird das neue Gültigkeitsdatum für die Anmeldung auf der Seite **Meine Anmeldung** angezeigt.

Was sind Sicherheitsinfos?

Die Seite **Sicherheitsinfos** enthält eine Liste neuer Informationen zu aktuellen Virenausbrüchen sowie andere Sicherheitsinformationen.

Die Liste zeigt:

- das Datum und die Uhrzeit des Empfangs der neuen Punkte,
- das Thema des neuen Punkts und
- ob Ihr Computer gegen die Bedrohung geschützt ist oder nicht.

Außerdem erscheint in Ihrer Systemleiste eine Sprechblase mit einer Benachrichtigung, wenn eine neue Sicherheitsinfo empfangen wird.

So zeigen Sie die detaillierte Beschreibung der Sicherheitsinfos an

Sie können eine Beschreibung der Sicherheitsbedrohung lesen und auf eine Webseite zugreifen, die weitere Informationen über die Bedrohung enthält.

So zeigen Sie die detaillierte Beschreibung der Sicherheitsinfos an:

1. Klicken Sie auf der Registerkarte **Start** auf **Erweitert**.
2. Wählen Sie **Allgemein > Sicherheitsinfos**.
3. Klicken Sie auf **Infos anzeigen**.
4. Wählen Sie ein neues Element aus und klicken Sie auf **Details**.
Das Dialogfeld **Sicherheitsinfos** wird geöffnet, in dem Sie die Sicherheitsinfo lesen können. Im Dialogfeld ist angegeben, ob Ihr Computer gegen die Bedrohung geschützt ist.
5. Klicken Sie auf **Weitere Informationen (Web)**, um mehr Informationen aus dem Internet abzurufen.

Was zeigen die Einzelheiten der Sicherheitsinfos an?

Im Dialogfeld mit den Einzelheiten zu den **Sicherheitsinfos** können Sie die Nachricht lesen und sehen, ob Ihr Computer bereits gegen die Bedrohung geschützt ist.

Das Fenster mit der detaillierten Beschreibung der Sicherheitsinfo enthält einen kurzen Beitrag zu dem von Ihnen ausgewählten Punkt. Über dem Beitrag sehen Sie, ob Ihr Computer gegen die Bedrohung geschützt ist:

Schutzstatus und empfohlene Aktion:

Schutzstatus	Vorgehensweise
"Dieser Computer ist noch nicht geschützt. Das Update wird schon bald, bei Erscheinen der Virusdefinitionen Version yyyy-mm-dd_##, verfügbar sein."	Es ist zurzeit kein Update verfügbar, mit dem Sie sich vor diesem <i>Virus</i> schützen können. Ein neues Update, das gegen den <i>Virus</i> schützt, wird so schnell wie möglich verfügbar sein. Warten Sie, bis das Update verfügbar ist.
"Dieser Computer ist nicht gegen den Virus geschützt. Jetzt aktualisieren..."	Es ist ein neues Update verfügbar, das Sie jedoch noch nicht besitzen. Klicken Sie auf Jetzt aktualisieren , um das Produkt zu aktualisieren.
"Dieser Computer ist geschützt."	Die Updates Ihrer Virendefinitionen schützen Sie gegen diese Bedrohung. Sie können Ihren Computer normal verwenden.

Schutzstatus	Vorgehensweise
"Dieser Computer kann nur mit dem Internet-Schutzschild geschützt werden. Weitere Informationen zum Schutz des Computers finden Sie in der Beschreibung."	Die in dieser Nachricht genannte <i>Malware</i> verursacht Schäden durch Netzwerkangriffe. Um Ihren Computer vor dieser Bedrohung zu schützen, ist eine entsprechende Konfiguration von Internet-Schutzschild erforderlich, die den Zugriff der Malware auf den Computer blockiert.

Was sind Benachrichtigungsfenster?

Benachrichtigungsfenster sind kurze Benachrichtigungen, die in der unteren rechten Ecke Ihres Computerbildschirms angezeigt werden.

Diese Fenster informieren Sie zu Aktionen, die Ihr Sicherheitsprodukt für den Schutz Ihres Computers unternommen hat. Sie werden beispielsweise angezeigt, wenn die Systemsteuerung die Verwendung eines Programms abgelehnt hat. Diese Benachrichtigungsfenster dienen der Information, es ist keine Aktion Ihrerseits erforderlich. Im Verlauf der Benachrichtigungsfenster werden alle Benachrichtigungsfenster angezeigt.

Wie kann ich die häufigsten Aufgaben schnell ausführen?

Sie können Dateien und Ordner im Windows Explorer scannen oder verschiedene Aufgaben über das Kontextmenü des Statussymbols ausführen.

So scannen Sie eine Datei oder einen Ordner im Windows Explorer

Sie können Datenträger, Ordner und Dateien im Windows Explorer in Bezug auf *Viren*, *Spyware* und *Riskware* scannen.

So scannen Sie einen Datenträger, einen Ordner oder eine Datei:



1. Platzieren Sie den Mauszeiger auf dem zu scannenden Datenträger, dem Ordner oder der Datei und klicken Sie mit der rechten Maustaste.
2. Wählen Sie im Kontextmenü **Ordner nach Viren und Spyware scannen**. (Der Name der Option hängt davon ab, ob Sie einen Datenträger, einen Ordner oder eine Datei scannen.)
Das Fenster **Scan-Assistent** wird geöffnet und der Scanvorgang beginnt.

Wenn ein *Virus* oder *Spyware* gefunden wird, führt Sie der **Scan-Assistent** durch die für die Bereinigung erforderlichen Schritte.

Wie können Aufgaben schnell über das Kontextmenü des Statussymbols ausgeführt werden?

Über das Produktstatussymbol in der Windows-Systemleiste lassen sich die häufigsten Aufgaben schnell ausführen.

So werden die Aufgaben ausgeführt:

1. Wenn Sie Windows XP einsetzen, klicken Sie auf das Symbol , damit die Symbole in der Systemleiste angezeigt werden.
2. Klicken Sie mit der rechten Maustaste auf das Symbol . Ein Menü mit den häufigsten Aufgaben wird geöffnet.


3. Wählen Sie die auszuführende Aufgabe im Menü aus.

Allgemeine Aufgaben:

Option	Wirkung
Öffnen [Produktname]	Öffnet die Benutzeroberfläche des Produkts, über die Sie den Status aller Produktkomponenten anzeigen und auf Produkteinstellungen zugreifen können, um die Schutzstufe zu ändern.
Historie des Fensters anzeigen	Zeigt eine Liste aller protokollierten Scanning-Ereignisse in Bezug auf die Systemsteuerung und Webdatenverkehr an.

Aufgaben im untergeordneten Menü zum Entfernen:

Option	Wirkung
Entladen und mit der aktuellen Sicherheitsstufe fortfahren	Entlädt installierte Komponenten aus dem Speicher Ihres Computers. Firewallregeln werden eingesetzt, die Ihren Computer gegen böswillige Verbindungsversuche schützen. Das Entladen kann z. B. notwendig sein, wenn Sie bestimmte Online-Spiele spielen oder andere Produkte installieren.
Entladen und gesamten Netzwerkverkehr zulassen	Hiermit können Sie komplette Produkt aus

Option	Wirkung
	<p>dem Speicher Ihres Computers entfernen und den vollständigen Netzwerkdatenverkehr durchlassen. Alle Sicherheitsfunktionen sind währenddessen deaktiviert, und Ihr Computer ist nicht geschützt.</p> <p> Hinweis: Verwenden Sie diese Option nur dann, wenn Ihr Computer nicht mit dem Internet verbunden ist.</p>

Aufgaben im Untermenü "AntiVirus & AntiSpy":

Option	Wirkung
Ziel scannen	Scannt eine bestimmte Datei oder einen Ordner in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Riskware</i> . Wählen Sie das Zielverzeichnis oder die Datei aus und klicken Sie auf OK , um den Scanvorgang zu starten.
Festplatten scannen	Scannt alle Dateien auf Ihren Festplatten in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Riskware</i> .
Schneller Malware-Scan	Scannt das System in Bezug auf <i>Malware</i> und <i>Riskware</i> .
Schnelles Rootkit-Scanning	Scannt das System in Bezug auf <i>Rootkits</i> und andere verdächtige und <i>versteckte Elemente</i> .

Option	Wirkung
Computer vollständig überprüfen	Scannt den Computer in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Rootkits</i> .

Aufgaben im Untermenü "Internet-Schutzschild":

Option	Wirkung
Gesamten Datenverkehr blockieren	Blockiert den gesamten Netzwerkdatenverkehr. Diese Option sollte nur verwendet werden, wenn Sie den Verdacht haben, dass Ihr Computer über das Netzwerk angegriffen wird.
Gesamten Datenverkehr zulassen	Lässt den gesamten Netzwerkdatenverkehr passieren. Diese Option deaktiviert die gesamte Firewall und macht den Computer ungeschützt gegenüber Netzwerkangriffen.
Alarmprotokoll	Öffnet das Dialogfeld Alarmer von Internet-Schutzschild .

Untermenü "Info":

Option	Wirkung
Info	Zeigt Produktinformationen wie z. B. die Versionsnummer an.

Kapitel 2

Viren und andere Malware stoppen

Themen:

- *Was sind Viren und sonstige Malware?*
- *Was sind AntiVirus- & AntiSpy-Schutzstufen?*
- *Scannen des Computers in Echtzeit*
- *Scannen des Computers zu bestimmten Zeiten*
- *Manuelles Scannen des Computers*
- *Was ist ein Quarantäne-Repository?*
- *Scannen Ihrer E-Mails*

Der AntiVirus- & AntiSpy-Schutz schützt Sie vor Programmen, die Ihren Computer beschädigen können, persönliche Daten stehlen oder Ihren Computer für illegale Zwecke verwenden.

AntiVirus- & AntiSpy-Schutz:

- schützt Ihren Computer in Echtzeit und im Hintergrund vor *Malware*. Ihr Computer ist daher immer vor *Malware* geschützt.
- scannt nach *Malware*, einschließlich *Viren*, *Spyware*, *Riskware* und *Rootkits*. Wenn eine solche *Malware* gefunden wird, wird sie standardmäßig sofort deaktiviert, bevor sie Schaden anrichten kann.
- scannt Ihre lokalen Festplatten, alle Wechselmedien (wie portable Laufwerke oder CDs) und heruntergeladenen Inhalte standardmäßig automatisch. Abhängig von Ihrer Produktkonfiguration werden auch alle E-Mails und der Webdatenverkehr gescannt. Antivirus & AntiSpy überwacht außerdem Ihren Computer in Bezug auf Änderungen, die auf *Malware* hinweisen können. Wenn gefährliche Systemänderungen festgestellt werden, beispielsweise Änderungen von Systemeinstellungen

oder wichtigen Systemprozessen, dann stoppt der Antivirus- & AntiSpy-Schutz die Ausführung dieser Programme, da es sich wahrscheinlich um *Malware* handelt.

- deaktiviert *Malware* indem sie unter Quarantäne gestellt wird. *Malware*, die sich in Quarantäne befindet, kann auf Ihrem Computer keinen Schaden anrichten. Sie können alle Programme oder Dateien später aus der Quarantäne entlassen, damit sie normal ausgeführt werden. Dies ist beispielsweise dann der Fall, wenn Sie das Programm oder die Datei benötigen oder versehentlich ein sicheres Programm oder eine sichere Datei unter Quarantäne gestellt haben.

Was sind Viren und sonstige Malware?

Als Malware werden Programme bezeichnet, die speziell entwickelt wurden, um Ihren Computer zu beschädigen oder ohne Ihr Wissen zu illegalen Zwecken zu verwenden oder aber um Informationen von Ihrem Computer zu stehlen.

Malware kann:

- die Kontrolle über Ihren Webbrowser übernehmen,
- Ihre Suche umleiten,
- unerwünschte Werbung einblenden,
- die von Ihnen besuchten Websites aufzeichnen,
- persönliche Informationen stehlen, wie Ihre Kontodaten,
- Ihren Computer zum Versenden von Spam benutzen und
- Ihren Computer benutzen, um andere Computer anzugreifen.

Malware kann außerdem dazu führen, dass Ihr Computer langsam und instabil wird. Der Verdacht, dass sich *Malware* auf Ihrem Computer befindet, liegt dann nahe, wenn er plötzlich sehr langsam wird und häufig abstürzt.

Viren

Ein Virus ist in der Regel ein Programm, das sich selbst an Dateien anhängt und sich ständig selbst repliziert; es kann die Inhalte anderer Dateien so verändern oder ersetzen, dass Ihr Computer dadurch beschädigt wird.

Ein *Virus* ist ein Programm, das normalerweise ohne Ihr Wissen auf Ihrem Computer installiert wird. Anschließend versucht der Virus, sich zu replizieren. Der Virus:

- verwendet einige der Systemressourcen Ihres Computers,
- kann Dateien auf Ihrem Computer verändern oder beschädigen,
- versucht wahrscheinlich, Ihren Computer zu benutzen, um andere Computer zu infizieren,
- kann zulassen, dass Ihr Computer für illegale Zwecke verwendet wird.

Spyware

Spyware sind Programme, die Ihre persönlichen Daten sammeln.

Spyware kann persönliche Daten sammeln, wie:

- Internet-Websites, die Sie besucht haben,
- E-Mail-Adressen auf Ihrem Computer,
- Passwörter oder
- Kreditkartennummern.

Spyware installiert sich fast immer selbst, ohne Ihre ausdrückliche Erlaubnis. Spyware kann wie folgt installiert werden:

- indem Sie dazu verleitet werden, eine Option in einem Popup-Fenster anzuklicken, durch die Sie umgeleitet werden, oder
- zusammen mit einem nützlichen Programm.

Rootkits

Rootkits sind Programme, die dafür sorgen, dass *Malware* schwer zu finden ist.

Rootkits verstecken Dateien und Prozesse. In der Regel, um schädliche Aktivitäten auf dem Computer zu verbergen. Wenn ein Rootkit *Malware* versteckt, ist es nicht einfach, die Malware auf Ihrem Computer zu finden.

Dieses Produkt besitzt einen Rootkit-Scanner, der gezielt nach Rootkits sucht, wodurch *Malware* sich nicht problemlos verstecken kann.

Riskware

Riskware wurde nicht speziell entwickelt, um Ihrem Computer zu schaden, sie kann Ihrem Computer aber schaden, wenn sie missbräulich verwendet wird.

Riskware ist streng genommen keine Malware. Diese Programme führen einige nützliche, aber potenziell gefährliche Funktionen durch. Beispiele für solche Programme:

- Programme für Instant Messaging, etwa IRC (Internet Relay Chat),
- Programme zur Übertragung von Dateien über das Internet von einem Computer auf einen anderen,
- oder Programme für die Internet-Telefonie, etwa VoIP (*Voice over Internet Protocol*).

Wenn Sie das Programm explizit installiert und richtig eingerichtet haben, ist es wahrscheinlich ungefährlich.

Wenn die Riskware ohne Ihr Wissen installiert wurde, wurde sie wahrscheinlich in böser Absicht installiert und sollte entfernt werden.


Was sind AntiVirus- & AntiSpy-Schutzstufen?

Antivirus & AntiSpy-Schutzstufen sind vordefinierte Gruppen von Einstellungen, die Ihnen die einfache Auswahl einer insgesamt gültigen Schutzstufe gegen *Malware* mit einem Klick ermöglichen.

Einige durch eine Schutzstufe definierte Einstellungen sind gesperrt. Diese gesperrten Einstellungen werden grau dargestellt. Um diese gesperrten Einstellungen zu ändern, müssen Sie eine weniger strenge Schutzstufe auswählen. Nur in der benutzerdefinierten Schutzstufe können alle Einstellungen geändert werden:

Fast alle Einstellungen gesperrt	Einige Einstellungen gesperrt	Keine Einstellungen gesperrt
Hoch	Normal	Benutzerdefiniert

Einstellungen, die nicht durch die Schutzstufe definiert sind, können frei geändert werden.

 **Hinweis:** Wenn Sie das Programm am Arbeitsplatz oder über Ihren Internet Service Provider installiert haben, wird das Programm möglicherweise im verwalteten Modus ausgeführt. Dies bedeutet, dass die Einstellungen remote durch einen Administrator festgelegt werden. Von einem Administrator festgelegte Einstellungen können nicht lokal durch Auswahl der benutzerdefinierten Stufe angepasst werden.

Ändern der Antivirus- & AntiSpy-Schutzstufe

Durch die Auswahl einer Schutzstufe können Sie schnell eine Gruppe von Einstellungen ändern. So können Sie auch einzelne Einstellungen ändern, die eventuell durch eine strenge Schutzstufe blockiert waren.

So ändern Sie die Schutzstufe:

1. Klicken Sie auf der Registerkarte **Start** auf **Ändern** in der Zeile für den Antivirus- & AntiSpy-Schutz.
2. Wählen Sie in der Liste eine Schutzstufe aus:

Schutzstufe	Wann Sie diese Stufe verwenden sollten
Hoch	Verwenden Sie die hohe Stufe, wenn Sie den Verdacht haben, dass Ihr Computer durch

Schutzstufe	Wann Sie diese Stufe verwenden sollten
	Malware infiziert werden könnte. Diese Stufe bietet maximalen Schutz vor Malware, sie kann aber bewirken, dass Ihr Computer langsamer wird.
Normal	Dies ist die Standardschutzstufe; Sie sollten diese Stufe verwenden, sofern keine besonderen Gründe dagegen sprechen. Die normale Schutzstufe stellt einen guten Kompromiss zwischen Schutz und Systemleistung dar.
Aus	Verwenden Sie diese Schutzstufe nur, wenn ein wichtiger Grund vorliegt. Ihr Computer ist nicht vor Malware geschützt, wenn Sie diese Stufe verwenden. Wenn Sie diese Schutzstufe verwenden müssen, sollten folgende Bedingungen bestehen: <ul style="list-style-type: none">• Sie sind nicht mit dem Internet verbunden und• Sie arbeiten mit Dateien und Anwendungen aus vertrauenswürdigen Quellen.
Benutzerdefiniert	Verwenden Sie die benutzerdefinierte Stufe, wenn Sie bestimmte Einstellungen ändern müssen, die durch die hohe oder die normale Sicherheitsstufe gesperrt sind. Diese Schutzstufe sollte nur von erfahrenen Anwendern verwendet werden.
Leistungsoptimiert	Verwenden Sie diese Schutzstufe, wenn Ihr Computer die Hardwarevoraussetzungen für dieses Produkt nicht erfüllt. In dieser Schutzstufe unkritische Antivirus- und Anti-spyfunktionen wie das Scannen von Systemsteuerung und E-Mails deaktiviert. Dadurch wird die Kapazität der Hardwareressourcen auf Ihrem Computer erhöht. Malware wird weiterhin in Echtzeit gescannt, sodass Sie davor geschützt sind.

3. Klicken Sie auf **OK** .

Scannen des Computers in Echtzeit

Echtzeit-Scanning sucht in Echtzeit nach *Malware* und sorgt so dafür, dass Ihr Computer immer geschützt ist.

So schützt das Scannen in Echtzeit Ihren Computer

Das Scannen in Echtzeit schützt Ihren Computer, indem alle Dateien überprüft werden, sobald auf sie zugegriffen wird, und indem der Zugriff auf die Dateien blockiert wird, die *Malware* enthalten.

Das Scannen in Echtzeit funktioniert wie folgt:

1. Ihr Computer versucht, auf eine Datei zuzugreifen.
2. Die Datei wird sofort auf *Malware* überprüft, bevor dem Computer der Zugriff auf die Datei gestattet wird.
3. Wenn in der Datei *Malware* gefunden wird, blockiert das Echtzeit-Scanning den Zugriff auf die Datei, sodass die *Malware* auf Ihrem Computer keinen Schaden anrichten kann. Sie werden standardmäßig gefragt, was mit der *Malware* passieren soll.

Auf diese Weise wird *Malware* erkannt und deaktiviert, bevor sie auf Ihrem Computer Schaden anrichten kann.

Wirkt sich das Scannen in Echtzeit auf die Leistung meines Computers aus?

Normalerweise bemerken Sie den Scanvorgang nicht, da er nur kurz dauert und wenig Systemressourcen benötigt. Wie lange das Scannen in Echtzeit dauert und wie viele Systemressourcen benötigt werden, hängt beispielsweise vom Inhalt, dem Speicherort und dem Typ der Datei ab.

Dateien, bei denen das Scannen länger dauert:

- Komprimierte Dateien, wie *.zip*-Dateien. Denken Sie daran, dass diese Dateien standardmäßig nicht gescannt werden.
- Dateien auf mobilen Laufwerken, wie z. B. portablen USB-Festplatten.

Das Scannen in Echtzeit kann Ihren Computer verlangsamen, wenn:

- Sie haben einen älteren Computer oder

- Sie greifen gleichzeitig auf eine große Zahl von Dateien zu. Sie öffnen z. B. ein Verzeichnis, das viele Dateien enthält, im Windows Explorer.

Echtzeit-Scanning einschalten

Schalten Sie das Echtzeit-Scanning ein, um *Malware* zu stoppen, bevor sie Ihren Computer beschädigt.

So schalten Sie das Echtzeit-Scanning ein:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie **Echtzeit-Scanning aktivieren**.
4. Klicken Sie auf **OK**.


In Echtzeit auf Viren überprüfen

Sie können Ihren Computer in Echtzeit scannen, um *Viren* zu stoppen, bevor sie Ihren Computer beschädigen.

Vorgehensweise, wenn ein Popup-Fenster mit einer Virenmeldung angezeigt wird

Wenn ein *Virus* gefunden wird, können Sie versuchen, den *Virus* aus der infizierten Datei zu entfernen, die infizierte Datei zu löschen oder die infizierte Datei in die Quarantäne zu verschieben.

Wenn ein *Virus* gefunden wird, wird das Popup-Fenster **Virus blockiert** angezeigt.

 **Hinweis:** Diese Popup-Fenster werden nicht angezeigt, wenn Sie festgelegt haben, dass *Viren* automatisch behandelt werden sollen.

So entfernen Sie den *Virus* vom Computer:


1. Lesen Sie die Informationen zu der Infektion:
 - a) Klicken Sie auf **Details**.
Das Popup-Fenster wird vergrößert und zeigt folgende Informationen:
 - Name des *Virus* und
 - Name und Pfad der infizierten Datei.
 - b) Klicken Sie auf den Namen des *Virus* (blau unterstrichen).

30 | F-Secure Internet Security 2009 | Viren und andere Malware stoppen

Eine Webseite wird geöffnet. Die Seite beschreibt den *Virus* und die damit verbundenen Sicherheitsrisiken.

2. Wählen Sie eine der folgenden Optionen:

Desinfizieren (empfohlen) Versuch, den *Virus* aus der infizierten Datei zu entfernen.

 **Hinweis:** Es ist nicht immer möglich, einen *Virus* aus einer Datei zu entfernen. Wenn der *Virus* nicht aus der infizierten Datei entfernt werden kann, wird die infizierte Datei umbenannt. Der *Virus* in der umbenannten Datei kann Ihren Computer nicht schädigen.

Infizierte Datei löschen Löschen des *Virus* und der infizierten Datei. Wählen Sie diese Option nur aus, wenn Sie sicher sind, dass die infizierte Datei keine Informationen enthält, die Sie möglicherweise benötigen.

Quarantäne Verschieben der infizierten Datei in die Quarantäne, von wo der *Virus* den Computer nicht schädigen kann. Sie können die Datei bei Bedarf später wieder aus der Quarantäne entlassen.

Keine Aktion Weiteres Blockieren des Zugriffs auf die Datei, sodass der *Virus* den Computer nicht schädigen kann. Das Popup **Virus festgestellt** wird bei jedem Scannen der Datei erneut angezeigt.

Die Auswahl der Aktion "Desinfizieren", "Löschen" oder "Quarantäne" kann eine Suche nach anderen infizierten Dateien im System einleiten. Wenn Elemente derselben Malware gefunden werden, wird die ausgewählte Aktion für alle Elemente ausgeführt. Aus diesem Grund kann der Vorgang mehrere Minuten in Anspruch nehmen.

3. Klicken Sie auf **OK**.

Dateien für Echtzeit-Scanning auswählen

Sie können wählen, welche Dateien auf Ihrem Computer in Echtzeit gescannt werden sollen.

 **Hinweis:**

Standardmäßig ist Ihr Computer ausreichend geschützt. Sie müssen diese Einstellungen nicht ändern. Diese Einstellungen müssen Sie nur in bestimmten Sonderfällen ändern.

Wenn Sie Änderungen vornehmen möchten, ist es in der Regel am einfachsten, die Sicherheitsstufe für Antivirus & Antispy zu ändern.

Welche Dateien werden in Echtzeit auf Viren gescannt?

Mithilfe von Listen, die Dateien einschließen oder ausschließen, können Sie definieren, welche Dateien auf *Viren* gescannt werden.

Die in Echtzeit auf *Viren* gescannten Dateien werden durch zwei Typen von Listen festgelegt:


- Die Liste der gescannten Dateitypen enthält entweder alle Dateien oder eine definierte Liste mit Dateitypen.
- Mit Listen von Dateien, die vom Scannen ausgeschlossen wurden, werden Ausnahmen hinsichtlich der Liste der gescannten Dateitypen definiert. Dateitypen oder Speicherorte, die sich auf der Liste der ausgeschlossenen Dateien befinden, werden auch dann nicht gescannt, wenn sie sich auf der Liste der gescannten Dateitypen befinden.

Über die Listen der gescannten Dateitypen und der ausgeschlossenen Dateien können Sie auf unterschiedliche Art definieren, welche Teile Ihres Computers gescannt werden:

- Sie können alle Dateien einschließen und dann optional die Ausschlussliste verwenden, um Laufwerke, Verzeichnisse oder Dateien auszuschließen, von denen Sie wissen, dass sie sicher sind, und nicht gescannt werden müssen.
- Sie können eine Liste von Dateitypen definieren, die gescannt werden sollen, damit nur diese Dateitypen gescannt werden.

Einschließen von Dateien in das Echtzeit-Virus-Scanning

Sie können Dateitypen hinzufügen, die in das Echtzeit-Scanning eingeschlossen werden sollen.

-  **Hinweis:** Keine Datei, die nach Typ oder Speicherort vom Scannen ausgeschlossen ist, wird gescannt, auch nicht, wenn sie in der Liste der gescannten Dateitypen enthalten ist.

So schließen Sie Dateien ein:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie unter **Scan-Optionen** eines der folgenden Elemente aus, und klicken Sie auf **Bearbeiten**:

Alle Dateien scannen Scannt alle Dateien.

Definierte Dateien scannen Scannt nur die von Ihnen definierten Dateitypen.


4. Legen Sie die zu scannenden Dateitypen fest.
 - Um einen zu scannenden Dateityp einzuschließen, geben Sie die aus drei Buchstaben bestehende Dateierweiterung in das Feld **Zur Liste hinzufügen** ein, und klicken Sie auf **Hinzufügen**.
 - Um zu verhindern, dass ein Dateityp gescannt wird, klicken Sie auf den Dateityp in der Liste. Klicken Sie anschließend auf **Entfernen**.

Um beispielsweise ausführbare Dateien beim Scannen einzuschließen, geben Sie `exe` in das Feld **Zur Liste hinzufügen** ein, und klicken Sie auf **Hinzufügen**.

5. Klicken Sie auf **OK**.
Das Dialogfeld **Zu scannende Dateitypen bearbeiten** wird geschlossen.
6. Klicken Sie auf **OK**.

Dateien nach Dateityp aus dem Echtzeit-Virenschutz ausschließen

Definieren Sie eine Ausschlussliste der Dateitypen, die nicht in Echtzeit auf *Viren* gescannt werden sollen.

-  **Hinweis:** Dateitypen in dieser Liste setzen die Liste der gescannten Dateitypen nicht außer Kraft. Wenn Sie der Liste der nach Dateityp ausgeschlossenen Dateien einen Dateityp hinzufügen, werden Dateien dieses Typs auch dann nicht gescannt, wenn sie in der Liste der gescannten Dateitypen enthalten sind.

So definieren Sie die Liste der Dateien für den Ausschluss nach Dateityp:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.

2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf **Ausschlüsse**.
4. Einen Dateityp ausschließen:
 - a) Wählen Sie die Registerkarte **Dateitypen**.
 - b) Wählen Sie **Dateien mit diesen Erweiterungen ausschließen**.
 - c) Geben Sie die Dateierweiterung, die die Dateitypen kennzeichnet, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.


Um Dateien ohne Erweiterung anzugeben, geben Sie '.' ein. Sie können den Platzhalter '?' verwenden, um ein beliebiges Zeichen zu ersetzen oder '*', um eine beliebige Anzahl von Zeichen zu ersetzen.

Um beispielsweise ausführbare Dateien auszuschließen, geben Sie `exe` in das Feld ein.
 - d) Klicken Sie auf **Hinzufügen**
5. Wiederholen Sie den vorherigen Schritt für alle anderen Erweiterungen, die vom Scannen nach Viren ausgeschlossen werden sollen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die ausgewählten Dateitypen werden aus zukünftigen Echtzeit-Scans ausgeschlossen.

Dateien nach Speicherort vom Echtzeit-Scanning ausschließen

Definieren Sie eine Ausschlussliste für Ordner oder Laufwerke, die beim Scannen nach *Viren* in Echtzeit ausgeschlossen werden sollen.


 **Hinweis:** Dateien, die sich in Ordnern oder auf Laufwerken befinden, die vom Scannen ausgeschlossen wurden, werden auch dann nicht gescannt, wenn ihr Dateityp in der Liste der gescannten Dateitypen enthalten ist.

So definieren Sie eine Liste mit Dateien, Ordnern oder Laufwerken für den Ausschluss nach Speicherort:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf **Ausschlüsse**.

34 | F-Secure Internet Security 2009 | Viren und andere Malware stoppen

4. Auszuschließende Datei, Laufwerk oder Ordner hinzufügen:
 - a) Wählen Sie die Registerkarte **Objekte** .
 - b) Wählen Sie **Objekte ausschließen (Dateien, Ordner, ...)**.
 - c) Klicken Sie auf **Hinzufügen**
 - d) Wählen Sie die Datei, das Laufwerk oder den Ordner aus, die/das/der vom Virensan ausgeschlossen werden soll.

 **Hinweis:** Bei einigen Laufwerken kann es sich um solche mit Wechselmedien handeln, wie CD- oder DVD- oder Netzlaufwerke. Netzlaufwerke und leere Wechsellaufwerke können nicht ausgeschlossen werden.
- e) Klicken Sie auf **OK** .
5. Wiederholen Sie den vorherigen Schritt, um weitere Dateien, Laufwerke oder Ordner vom Virensan auszuschließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.

Scannen der Inhalte komprimierter Dateien und Ordner in Echtzeit

Sie können nach *Viren* scannen, die sich in komprimierten Dateien und Ordnern verbergen.

So scannen Sie komprimierte Dateien in Echtzeit:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie **In komprimierten Dateien (ZIP, ARJ, LZH, ...)** **scannen** , um Archivdateien und -ordner auf Viren zu scannen, wie z. B. ZIP-Dateien.


Bei komprimierten Dateien und Ordnern dauert der Scanvorgang ein wenig länger.
4. Klicken Sie auf **OK**.

Was soll mit Viren passieren, die in Echtzeit gefunden werden?

Sie können auswählen, wie vorgegangen werden soll, wenn *Malware* in Echtzeit erkannt wird.

So wählen Sie die Standardaktion aus, die durchgeführt wird, wenn ein Virus gefunden wird:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie im Dropdown-Menü neben **Wenn ein Virus gefunden wurde** eine Option aus:

Option	Was passiert, wenn ein Virus erkannt wird
Aktion erfragen	Ein Fenster wird geöffnet, in dem Sie erfahren, dass ein <i>Virus</i> erkannt wurde, mit Details über den Virus und die infizierte Datei.
Automatisch desinfizieren	Automatisch versuchen, den <i>Virus</i> aus der infizierten Datei zu entfernen.  Hinweis: Es ist nicht immer möglich, einen <i>Virus</i> aus einer Datei zu entfernen. Wenn der <i>Virus</i> nicht aus der infizierten Datei entfernt werden kann, wird die infizierte Datei umbenannt. Der <i>Virus</i> kann in der umbenannten Datei auf Ihrem Computer keinen Schaden mehr anrichten.
Automatisch unter Quarantäne stellen	Die infizierte Datei automatisch unter Quarantäne stellen, wo der <i>Virus</i> Ihrem Computer nicht schaden kann. Sie können die infizierte Datei später bei Bedarf aus der Quarantäne befreien.
Automatisch umbenennen	Die infizierte Datei automatisch umbenennen, damit der <i>Virus</i> Ihrem Computer nicht schaden kann.
Automatisch löschen	Die infizierte Datei automatisch löschen. Die infizierte Datei wird vom Computer entfernt, sodass kein weiterer Zugriff möglich ist. Sie sollten diese Option mit Vorsicht verwenden, da hierdurch Dateien automatisch gelöscht werden können, die für Sie wichtig sind.
Nur Bericht	Blockiert den <i>Virus</i> , damit er dem Computer nicht schaden kann, führt aber keine weitere Aktion durch. Ihr Computer ist vor diesem <i>Virus</i> sicher. Jedes Mal, wenn diese Datei gescannt wird, erhalten Sie die Meldung, dass ein <i>Virus</i> gefunden wurde.

4. Klicken Sie auf **OK**.

In Echtzeit auf Spyware überprüfen

Sie können Ihren Computer in Echtzeit scannen, um *Spyware* zu deaktivieren, bevor sie Ihren Computer beschädigt.

Spyware-Scanning in Echtzeit einschalten

Schalten Sie das Echtzeit-Scanning für *Spyware* und *Riskware* ein, damit diese deaktiviert werden, bevor sie auf Ihrem Computer Schaden anrichten.

So schalten Sie das *Spyware*- und *Riskware*- Scanning ein:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie **Echtzeit-Scanning aktivieren**.
4. Wählen Sie die Registerkarte **Spywareschutz**.
5. Wählen Sie **Nach Spyware scannen**.
6. Klicken Sie auf **OK**.

Vorgehensweise beim Einblenden eines Popups wegen Spyware oder Riskware

Wenn *Spyware* oder *Riskware* entdeckt wird, können Sie diese löschen, in Quarantäne verschieben, wo sie den Computer nicht beschädigen kann, oder als sicher kennzeichnen und bei zukünftigen Scans ignorieren.


Wenn Sie für das Auffinden von *Spyware* oder *Riskware* keine automatische Aktion festgelegt haben, wird das Fenster **Spyware gefunden** geöffnet. So entfernen Sie *Spyware* oder *Riskware* von Ihrem Computer:

1. Sehen Sie sich weitere Informationen zu der *Spyware* oder *Riskware* an, um eine gute Entscheidung zu treffen:
 - a) Klicken Sie auf **Details >>**.
Das Fenster vergrößert sich und zeigt:
 - eine Beschreibung dessen, was die *Spyware* oder *Riskware* macht,
 - der Name des *Virus* und
 - der Pfadname der infizierten Datei.

- b) Klicken Sie auf den Namen der *Spyware* oder der *Riskware* (blau unterstrichen).
Eine Webseite mit einer Beschreibung der *Spyware* oder *Riskware* und weiteren Details zu den Sicherheitsrisiken wird angezeigt.

2. Wählen Sie eine der folgenden Optionen:

Quarantäne (empfohlen)	So verschieben Sie die <i>Spyware</i> oder <i>Riskware</i> in die Quarantäne, wo sie dem Computer nicht schaden kann.
Infizierte Datei löschen	Um <i>Spyware</i> oder <i>Riskware</i> zu löschen. Wählen Sie diese Option nur aus, wenn Sie sicher sind, dass Sie das Programm, in dem die <i>Spyware</i> oder <i>Riskware</i> enthalten ist, nicht mehr brauchen.
Vom Scannen ausschließen	So markieren Sie die <i>Spyware</i> oder <i>Riskware</i> als sicher, um sie bei zukünftigen Scans zu ignorieren.

-  **Hinweis:** Sie können auch "**Keine Aktion**" auswählen, was allerdings bewirkt, dass die *Spyware* oder die *Riskware* Ihrem Computer weiterhin beschädigen kann und bei jeder Verwendung ein Alarm erfolgt. Wenn Sie dem Programm nicht vertrauen, sollten Sie es unter Quarantäne stellen und löschen. Wenn Sie dem Programm vertrauen, klicken Sie auf die Option zum Ausschluss vom Scanvorgang, damit dieses Fenster nicht mehr angezeigt wird, wenn Sie auf dieses Programm zugreifen.

3. Klicken Sie auf **OK**.

4. Warten Sie, bis die *Spyware* oder die *Riskware* bearbeitet wurde, und klicken Sie anschließend auf "**OK**".

Was soll passieren, wenn Spyware in Echtzeit gefunden wird?

Sie können wählen, welche Aktion ausgeführt werden soll, wenn beim Echtzeit-Scan Spyware gefunden wird.

So legen Sie eine Aktion fest, die beim Erkennen von *Spyware* durchgeführt werden soll:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.

3. Klicken Sie auf die Registerkarte **Spywareschutz**.
4. Wählen Sie im Dropdown-Menü eine Option neben **Wenn Spyware gefunden wurde** aus:

Option **Was soll passieren, wenn Spyware oder Riskware erkannt wird?**

Aktion erfragen

Ein Fenster öffnen, in dem gefragt wird, ob Sie das Programm in die Quarantäne verschieben möchten, wo es dem Computer nicht schaden kann, oder ob es gelöscht oder als sicher gekennzeichnet und bei zukünftigen Scans ignoriert werden soll.

Nur Bericht

Bei jeder Datei, die aktuell gescannt wird, werden Sie benachrichtigt, dass *Spyware* gefunden wurde. Wenn Sie diese Option wählen, wird Spyware weder entfernt noch unter Quarantäne gestellt und kann auf Ihrem Computer noch ausgeführt werden.

5. Klicken Sie auf **OK**.

Blockieren von Tracking Cookies

Durch das Blockieren von Tracking Cookies verhindern Sie, dass Websites verfolgen, welche Sites Sie im Internet besuchen.

Tracking Cookies sind kleine Dateien, mit denen Websites aufzeichnen, welche Websites Sie besuchen. So blockieren Sie die Installation von Tracking Cookies:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie **Echtzeit-Scanning aktivieren**.
4. Wählen Sie die Registerkarte **Spywareschutz**.
5. Wählen Sie **Tracking Cookies blockieren**.
6. Klicken Sie auf **OK**.

Scannen nach verdächtigen Programmen in Echtzeit

Verhindern Sie, dass verdächtige Programme Ihr System verändern und Ihren Computer eventuell beschädigen.

Was ist die Systemsteuerung?

Die Systemsteuerung analysiert den Inhalt von Dateien und das Verhalten von Programmen und blockiert neue und noch nicht entdeckte *Viren*, *Würmer* sowie andere schädliche Programme, die versuchen, potenziell schädliche Änderungen an Ihrem Computer vorzunehmen.

Zu den möglicherweise gefährlichen Systemänderungen gehören:

- Änderung von Systemeinstellungen (Windows-Registry),
- Versuche, wichtige Systemprogramme zu beenden, wie z. B. Sicherheitsprogramme wie dieses, und
- Versuche, wichtige Systemdateien zu verändern.

Die Systemsteuerung überwacht diese Änderungen kontinuierlich und prüft jedes Programm, das versucht, das System zu ändern.

So funktioniert die Systemsteuerung

Wenn die Systemsteuerung ein Programm erkennt, das versucht, potenziell schädliche Änderungen des Systems durchzuführen, erlaubt sie die Ausführung des Programms in einer Sicherheitszone, sofern Sie das Programm nicht explizit genehmigt bzw. blockiert haben. In der Sicherheitszone kann das Programm Ihrem Computer keinen Schaden zufügen. Die Systemsteuerung analysiert, welche Änderungen das Programm durchführen möchte, und entscheidet auf dieser Grundlage, wie wahrscheinlich es ist, dass das Programm *Malware* ist.

Das Programm wird von der Systemsteuerung entweder automatisch zugelassen oder blockiert. Oder Sie werden gefragt, ob Sie das Programm entweder zulassen oder blockieren möchten. Das ist abhängig von:

- wie wahrscheinlich es ist, dass das Programm *Malware* ist, und
- welche Aktion die Systemsteuerung durchführen soll, wenn sie einen potenziell schädlichen Versuch erkennt, das System zu ändern.

Systemsteuerung einschalten

Schalten Sie die Systemsteuerung (System Control) ein, um zu verhindern, dass verdächtige Programme auf Ihrem Computer potenziell schädliche Systemänderungen vornehmen.

Bevor Sie die Systemsteuerung einschalten, müssen Sie sicherstellen, dass Service Pack 4 Roll-up 1 installiert ist, sofern Sie Windows 2000 einsetzen, oder Service Pack 2, wenn Sie Windows XP einsetzen.

So schalten Sie die Systemsteuerung ein:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Systemsteuerung**.
4. Wählen Sie unter **Einstellungen** , die Option **Systemsteuerung aktivieren** .
5. Klicken Sie auf **OK** .

Was soll unternommen werden, wenn in Echtzeit verdächtige Systemänderungen festgestellt werden?

Wenn die Systemsteuerung (System Control) erkennt, dass ein Programm versucht, wichtige Systemänderungen durchzuführen, können solche Versuche entweder automatisch zugelassen oder blockiert bzw. Ihnen zur Entscheidung übergeben werden.

So wählen Sie aus, welche Aktion die Systemsteuerung durchführt, wenn sie einen potenziell schädlichen Versuch der Systemänderung erkennt:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Seite **Systemsteuerung**.
4. Wählen Sie unter **Maßnahme bei Systemänderungsversuch** Folgendes:

Wählen Sie dies... Wenn Sie möchten, dass die Systemsteuerung...

Um Erlaubnis fragen

Immer nachfragen, ob ein Systemänderungsversuch zugelassen oder blockiert werden soll, auch wenn die Systemsteuerung das Programm als wahrscheinlich sicher erkennt.

Bei unklaren Fällen fragen (Standardoption)

nur dann fragen, ob ein Systemänderungsversuch zugelassen oder blockiert werden soll, wenn die Systemsteuerung das Programm nicht als wahrscheinlich sicher oder unsicher einstufen kann.

Automatisch: Nicht fragen

automatisch verhindern, dass Programme, die wahrscheinlich unsicher sind,

Wählen Sie dies... Wenn Sie möchten, dass die Systemsteuerung...

Systemänderungen durchführen, ohne Ihnen dabei irgendwelche Fragen zu stellen.

5. Klicken Sie auf **OK** .

Die Liste sicherer und unsicherer Programme anzeigen

Die Systemsteuerung (System Control) führt eine Liste von Programmen, die Systemänderungen durchführen dürfen (sicher) oder bei denen Systemänderungen blockiert werden (nicht sicher).

Einige Programme in der Liste sind auf der Grundlage der Analyse der Systemsteuerung ihres Verhaltens als sicher oder unsicher definiert. Einige Dateien und Programme, die für den Betrieb von Windows entscheidend sind, sind standardmäßig zugelassen und können nicht blockiert werden. Einige Programme sind auf der Grundlage der von Ihnen getroffenen Entscheidungen blockiert oder zugelassen, bei denen Sie die Systemsteuerung angewiesen haben, unbekannte Programme zuzulassen oder zu blockieren.

So zeigen Sie die Liste der zugelassenen oder blockierten Programme an:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Systemsteuerung**.
4. Klicken Sie auf **Anwendungen**.
Die Liste der Anwendungen wird angezeigt. Die Liste enthält Anwendungen, die durch Sie oder die Systemsteuerung zugelassen oder blockiert wurden.

Zulassen eines Programms, das die Systemsteuerung blockiert hat

Sie können ein Programm zulassen, für das die Systemsteuerung blockiert hat, dass es Systemänderungen vornimmt.

Manchmal verhindert die Systemsteuerung, dass ein Programm, das Sie verwenden möchten und von dem Sie wissen, dass es sicher ist, richtig funktioniert. Dies passiert, weil das Programm versucht, Systemänderungen durchzuführen, die potenziell schädlich sein können. Es kann sein, dass Sie versehentlich ein Programm blockiert haben,

42 | F-Secure Internet Security 2009 | Viren und andere Malware stoppen

als ein Popup der Systemsteuerung angezeigt wurde. Sie können ein blockiertes Programm zulassen, indem Sie seine Berechtigung in der Liste der Anwendungen ändern.

So lassen Sie ein Programm zu, das die Systemsteuerung blockiert hat:


1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Systemsteuerung**.
4. Klicken Sie auf **Anwendungen**.
Die Liste der Anwendungen wird angezeigt.
5. Klicken Sie auf die Spalte **Berechtigung**, damit die Liste nach zugelassenen und abgelehnten Programmen sortiert wird.
6. Wählen Sie das Programm aus, das Sie zulassen möchten, und klicken Sie auf **Details**.
7. Wählen Sie unter **Berechtigung** die Option **Zulassen**.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf **Schließen**.

Das von Ihnen ausgewählte Programm ist jetzt berechtigt, die beabsichtigten Systemänderungen durchzuführen.

Das Ausführen von ActiveX stoppen

ActiveX ist eine Technik, die es Programmen erlaubt, Systemänderungen auf Ihrem Computer vorzunehmen, wenn Sie mit dem Internet Explorer im Internet surfen.

Einige Websites nutzen *ActiveX*, um Programme auf Ihrem Computer zu installieren. Einige dieser Programme sind sicher und nützlich - manche Websites benötigen *ActiveX* z. B. um Videos anzuzeigen. Einige dieser Programme können *Malware* sein. Es gibt jedoch auch Webseiten, wie z. B. die Windows-Update-Seiten, die nicht ohne *ActiveX* angezeigt werden können. Wenn Sie diese Art von Webseiten anzeigen, müssen Sie *ActiveX* zulassen.

 **Hinweis:** Der *ActiveX*-Schutz funktioniert nur, wenn die Systemsteuerung eingeschaltet ist.

So verhindern Sie, dass Ihr Webbrowser *ActiveX*-Programme ausführt:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Seite **Systemsteuerung**.

4. Gehen Sie wie folgt vor:

- a) Stellen Sie sicher, dass **Systemsteuerung aktivieren** ausgewählt ist. Der *ActiveX* -Schutz funktioniert nur, wenn die Systemsteuerung eingeschaltet ist.
- b) Wählen Sie **Ausführen von allen ActiveX-Elementen verhindern** .

Der ActiveX-Schutz ist standardmäßig ausgeschaltet. Dies bedeutet, dass Ihr Webbrowser *ActiveX* -Programme ausführen kann.

5. Klicken Sie auf **OK** .

Wenn Ihr Webbrowser versucht, *ActiveX* -Programme auszuführen, erscheint ein kleines Fenster, wenn die Systemsteuerung das Ausführen von *ActiveX* verhindert.

Serverabfragen zum Verbessern der Erkennungsgenauigkeit verwenden

Durch die Verwendung von Serverabfragen kann die Erkennungsrate bei verdächtigen Programmen verbessert werden.

Wenn Sie ein eventuell verdächtiges Programm starten, stellt die Systemsteuerung eine Verbindung mit dem F-Secure-Server her. Wenn der Server das Programm als verdächtig erkennt, wird es von der Systemsteuerung blockiert. Die Systemsteuerung stellt keine Verbindung zum F-Secure-Server her, wenn Sie explizit gestattet haben, dass das Programm ausgeführt wird.

So aktivieren Sie Serverabfragen:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben der Option für das Scannen in Echtzeit auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Systemsteuerung**.
4. Aktivieren Sie unter "Einstellungen" **Serverabfragen verwenden, um die Leistung zu verbessern** .
5. Klicken Sie auf **OK**.

Bei Verwendung einer mobilen Verbindung, sollten Sie die Option für Serverabfragen deaktivieren. Wenn die Option aktiviert ist, kann der Netzwerkdatenverkehr erhöht werden.

Eine Benachrichtigung anzeigen, wenn die Systemsteuerung die Ausführung eines Programms stoppt

Ein kleiner Flyer wird angezeigt, wenn die Systemsteuerung automatisch blockiert, dass ein Programm Systemänderungen vornimmt.

Wenn ein Programm, das Sie installieren oder ausführen möchten, nicht funktioniert, kann dies daran liegen, dass die Systemsteuerung das Programm hindert, Systemänderungen durchzuführen. In diesem Fall können Sie festlegen, dass die Systemsteuerung ein kleines Fenster anzeigt, wenn ein Programm automatisch blockiert wird. So wissen Sie, warum das Programm nicht richtig funktioniert hat.

So erhalten Sie jedes Mal einen Hinweis, wenn die Systemsteuerung ein verdächtiges Programm blockiert:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Systemsteuerung**.
4. Wählen Sie **Benachrichtigung für abgelehnte Ereignisse anzeigen**
Jedes Mal, wenn die Systemsteuerung ein Programm an der Durchführung einer Systemänderung hindert, wird eine Benachrichtigung angezeigt.
5. Klicken Sie auf **OK**.

Was ist zu tun, wenn bei einem Systemänderungsversuch das Dialogfeld angezeigt wird?

Wenn die Systemsteuerung erkennt, dass ein Programm versucht, potenziell schädliche Systemänderungen durchzuführen, und nicht festgestellt werden kann, ob das Programm sicher oder unsicher ist, wird ein Dialogfeld **Systemänderungsversuch** angezeigt.

Das Dialogfeld über einen Systemänderungsversuch wird angezeigt, wenn eine der folgenden Optionen als Aktion der Systemsteuerung beim Erkennen eines potenziell schädlichen Versuchs ausgewählt ist, das System zu ändern:

- **Um Erlaubnis fragen** oder
- **Bei unklaren Fällen fragen**

Die Systemsteuerung zeigt das Dialogfeld z. B. an, wenn Sie neue Software installieren.

So entscheiden Sie, ob das Programm, das versucht, Systemänderungen durchzuführen, vertrauenswürdig ist:

1. Wenn Sie unsicher sind, aus welcher Quelle der Änderungsversuch stammt, klicken Sie auf **Details >>**, damit weitere Informationen über das Programm angezeigt werden.

Im Bereich der technischen Details sehen Sie:

- der Name des Programms, das versucht, die Änderung vorzunehmen,
- der Speicherort des Programms,
- die Änderung, die das Programm durchführen möchte, und
- eine *Risikobewertung*, die anzeigt wie wahrscheinlich es ist, dass das Programm *Malware* ist:
 - eine geringe Bewertung weist auf ein wahrscheinlich harmloses Programm hin und
 - eine hohe Bewertung weist auf ein Programm hin, das wahrscheinlich *Malware* ist.

2. Wählen Sie eine der folgenden Optionen aus:

Auswählen ...

Wenn Sie...

Ich vertraue der Anwendung. Fortfahren zulassen.

denken, dass das Programm sicher ist. Das Programm ist wahrscheinlich sicher, wenn:

- es hat eine niedrige *Risikobewertung*,
- das Dialogfeld wurde aufgrund einer von Ihnen durchgeführten Aktion angezeigt,
- Sie erkennen das Programm oder
- Sie haben das Programm von einer vertrauenswürdigen Quelle erhalten.

Ich vertraue der Anwendung nicht. Diesen Vorgang blockieren.

befürchten, dass das Programm unsicher ist. Das Programm ist wahrscheinlich unsicher, wenn:

- es hat eine hohe *Risikobewertung*,
- Sie kennen das Programm nicht oder
- Sie kennen das Programm und halten es für verdächtig.

3. Wählen Sie **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen** aus, wenn die Systemsteuerung Ihre Entscheidung für dieses Programm auch bei zukünftigen Änderungsversuchen anwenden soll.

Diese Option wird nur angezeigt, wenn Sie **Um Erlaubnis fragen** als Aktion für Systemänderungsversuche ausgewählt haben.

Wenn die Systemsteuerung dasselbe Programm noch einmal erkennt, fragt sie nicht, was passieren soll, sondern wendet Ihre frühere Entscheidung an.

4. Wenn Sie eine Probe eines Programms senden möchten, das versucht hat, Systemänderungen durchzuführen, gehen Sie wie folgt vor:
 - a) Klicken Sie auf **Beispiel an F-Secure senden**. Ein Dialogfeld wird geöffnet, das die Einreichungsbedingungen erläutert.
 - b) Lesen Sie die Bedingungen sorgfältig durch und klicken Sie auf **Akzeptieren**, wenn Sie damit einverstanden sind und die Probe einreichen möchten.

Sie möchten eine Probe senden:

- wenn die Systemsteuerung automatisch ein Programm blockiert, das Ihnen als sicher bekannt ist, oder
- wenn das Dialogfeld **Systemänderungsversuch** angezeigt wird und Sie glauben, dass das Programm *Malware* ist.


Das System sendet der F-Secure Corporation eine elektronische Kopie des Programms, das als mögliche Sicherheitsbedrohung erkannt wurde.

Web-Datenverkehr-Scanning einschalten

Scannen Sie Informationen, die Ihren Browser durchlaufen, auf *Viren*, damit Ihr Computer beim Surfen im Internet vor Viren geschützt ist.

So schalten Sie das Web-Datenverkehr-Scanning ein:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben Echtzeit-Scanning auf **Konfigurieren**.
3. Wählen Sie die Registerkarte **Virenschutz**.
4. Wählen Sie **Web-Datenverkehr überprüfen und erkannte Viren entfernen**.

 **Hinweis:** Sie können sehen, wenn das Web-Datenverkehr-Scanning eine Datei bereinigt, wenn Sie

die Option **Benachrichtigungsfenster bei Web-Datenverkehr-Scanning anzeigen** auswählen.

5. Klicken Sie auf **OK**.
6. Wenn Ihr Browser beim Ändern der Einstellung geöffnet war, müssen Sie den Browser neu starten, damit Änderung der Einstellung wirksam wird.

Beim Herunterladen einer Datei mit böartigem oder verdächtigem Inhalt wird die Datei zwar heruntergeladen, der gefährliche Inhalt wird jedoch durch Nullen ersetzt.

Scannen des Computers zu bestimmten Zeiten

Sie können Ihren Computer zu planmäßigen Zeiten scannen, um nach *Malware* in regelmäßigen Intervallen, z. B. täglich, wöchentlich oder monatlich, zu suchen.

Das Scannen nach *Malware* ist ein intensiver Prozess. Er beansprucht die volle Leistung Ihres Computers und nimmt geraume Zeit in Anspruch. Aus diesem Grund können Sie festlegen, dass das Programm Ihren Computer dann scannt, wenn Sie ihn nicht benutzen.

Zu festgelegten Zeiten nach Malware scannen

Sie können festlegen, dass das Programm den Computer in regelmäßigen Abständen scannt, beispielsweise wöchentlich, täglich oder monatlich.

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben den geplanten Scanvorgängen auf **Konfigurieren**.
3. Wählen Sie **Geplantes Scanning aktivieren**.
4. Wählen Sie die Tage aus, an denen nach *Viren* und *Spyware* gescannt werden soll.

Option	Beschreibung
Täglich	Um jeden Tag zu scannen.
Wöchentlich	Um an ausgewählten Wochentagen zu scannen. Wählen Sie rechts in der Liste die Tage aus, an denen gescannt werden soll.
Monatlich	So scannen Sie an bis zu drei Tagen pro Monat. Wählen Sie die Tage aus: <ol style="list-style-type: none">1. Wählen Sie eine Option für "Tag" aus.2. Wählen Sie in der Liste neben dem ausgewählten Tag den Tag des Monats aus.3. Wiederholen Sie diesen Schritt, wenn Sie an einem anderen Tag scannen möchten.

5. Legen Sie fest, wann das Scannen an den ausgewählten Tagen gestartet werden soll.

Option	Beschreibung
Startzeit	Der Zeitpunkt, an dem das Scannen gestartet wird. Wählen Sie einen Zeitpunkt aus, zu dem Sie den Computer voraussichtlich nicht verwenden.
Nachdem der Computer nicht benutzt wurde für	Wählen Sie eine Inaktivitätszeit aus, nach der mit dem Scannen begonnen werden soll, wenn der Computer nicht verwendet wird.

Dateien und Ordner für manuelle und geplante Scans auswählen

Sie können die Dateitypen und die Bereiche Ihres Computers auswählen, die bei manuellen und geplanten Scans geprüft werden.

- 👉 **Hinweis:** Bearbeiten Sie die Einstellungen für das manuelle Scannen, um Dateien und Ordner auszuwählen, die beim geplanten Scan überprüft werden sollen.

Einschließen von Dateien in manuelle und geplante Scans

Sie können die Dateitypen auswählen, die auf *Viren* und *Spyware* manuell oder geplant gescannt werden sollen.


1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Weilen Sie unter **Scan-Optionen** eine der folgenden Optionen aus:
 - Alle Dateien scannen** Scannen aller Dateien.
 - Definierte Dateien scannen:** Scannen aller von Ihnen festgelegten Dateitypen.
5. Zu scannende Dateitypen festlegen.

- Um einen Dateityp in den Scanvorang einzuschließen, geben Sie die aus drei Buchstaben bestehende Dateierweiterung in das Feld **Zur Liste hinzufügen** ein, und klicken Sie auf **Hinzufügen**.
- Um zu verhindern, dass ein Dateityp gescannt wird, klicken Sie auf einen Dateityp in der Liste. Klicken Sie anschließend auf **Entfernen**.

Um beispielsweise ausführbare Dateien in den Scan einzubeziehen, geben Sie `exe` in das Feld **Zur Liste hinzufügen** ein und klicken auf **Hinzufügen**.

6. Klicken Sie auf **OK**.
Das Dialogfeld **Zu scannende Dateitypen bearbeiten** wird geschlossen.
7. Klicken Sie auf **OK**.

Die von Ihnen ausgewählten Dateien werden in zukünftige manuelle und geplante Scans einbezogen.

-  **Hinweis:** Alle in der Ausschlussliste für das manuelle und geplante Scannen enthaltenen Dateitypen bzw. Speicherorte setzen die hier definierte Liste außer Kraft. Dateitypen, die in den Ausschlusslisten stehen, werden auch dann nicht gescannt, wenn sie hier definiert sind.

Dateien nach Dateityp aus manuellen und geplanten Scans ausschließen

Sie können Dateien nach dem Dateityp aus manuellen und geplanten Scans ausschließen.

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Klicken Sie auf **Ausschlüsse**.
5. Dateityp ausschließen:
 - a) Wählen Sie die Registerkarte **Dateitypen** aus.
 - b) Wählen Sie **Dateien mit diesen Erweiterungen ausschließen**.
 - c) Geben Sie eine Dateierweiterung, die den Typ der Dateien angibt, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.

Um Dateien ohne Erweiterung anzugeben, geben Sie '.' ein. Sie können den Platzhalter '?' für ein beliebiges Zeichen verwenden oder den Platzhalter '*' für eine beliebige Anzahl von Zeichen.

Um beispielsweise ausführbare Dateien auszuschließen, geben Sie in das Feld `exe` ein.

d) Klicken Sie auf **Hinzufügen**.

6. Wiederholen Sie den vorherigen Schritt für alle anderen Erweiterungen, die Sie aus dem Virenscan ausschließen möchten.
7. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
8. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die ausgewählten Dateitypen werden in Zukunft von manuellen und geplanten Scans ausgeschlossen.

Anzeigen von Anwendungen, die aus manuellen und geplanten Scans ausgeschlossen wurden

Sie können die Anwendungen anzeigen, die Sie aus manuellen und geplanten Scans ausgeschlossen haben, und diese aus der Liste der ausgeschlossenen Anwendungen entfernen, damit sie in Zukunft bei beiden Formen des Scannens wieder mitgescannt werden.

So zeigen Sie Anwendungen an, die vom manuellen oder geplanten Scannen ausgeschlossen sind:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Klicken Sie auf **Ausschlüsse**.
5. Wählen Sie die Registerkarte **Anwendungen**.
6. So stellen Sie ein, dass eine Anwendung bei zukünftigen manuellen oder geplanten Scans einbezogen wird:
 - a) Wählen Sie die Anwendung aus, die erneut in den Scan einbezogen werden soll.
 - b) Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
8. Klicken Sie zum Beenden auf **OK**.

Scannen der Inhalte komprimierter Dateien bei manuellen und geplanten Scans

Sie können nach *Viren* scannen, die sich in komprimierten Dateien verbergen.




1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Wenn Sie Archivdateien oder -ordner scannen möchten, etwa *.zip*-Dateien, wählen Sie **In komprimierten Dateien (ZIP, ARJ, LZH, ...) scannen**.
Bei komprimierten Dateien und Ordnern dauert der Scanvorgang ein wenig länger.
5. Klicken Sie auf **OK**.

Wählen Sie aus, welche Aktionen werden sollen, wenn Malware bei manuellen oder geplanten Scans gefunden wurde

Sie können festlegen, dass Sie gefragt werden, welche Aktion durchgeführt werden soll, wenn während einem manuellen oder geplanten Scan *Malware* gefunden wurde. Sie können auch eine Aktion vordefinieren, die automatisch und ohne Rückfragen ausgeführt wird.

So wählen Sie die Standardaktion aus, die bei erkannter *Malware* durchgeführt wird:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Wählen Sie eine Option aus der Liste neben **Wenn Malware gefunden wurde**:

Option	Was passiert, wenn <i>Malware</i> gefunden wurde
Aktion erfragen	<p>Bei einem manuellen Scan werden Sie nach der durchzuführenden Aktion gefragt, wenn während einem manuellen Scan <i>Malware</i> gefunden wurde.</p> <p> Hinweis: Bei geplanten Scans verhält Sie diese Option genau wie die Option Automatisch löschen.</p>
Automatisch löschen	<p>Das Programm versucht, die in infizierten Dateien gefundenen <i>Viren</i> während manueller oder geplanter Scans automatisch zu bereinigen. <i>Spyware</i> und <i>Riskware</i> werden automatisch unter Quarantäne gestellt.</p> <p> Hinweis: Nicht in jedem Fall kann ein <i>Virus</i> in einer Datei bereinigt werden. Ist dies der Fall, wird die Erweiterung der infizierten Datei geändert, sodass der <i>Virus</i> Ihren Computer nicht beschädigen kann.</p>
Automatisch unter Quarantäne stellen	<p>Das Programm stellt infizierte Dateien, die während manueller oder geplanter Scans gefunden wurden automatisch unter Quarantäne, sodass sie ihren Computer nicht beschädigen können.</p>
Automatisch löschen	<p>Alle bei manuellen oder geplanten Scans gefundenen infizierten Dateien werden automatisch von dem Programm gelöscht.</p>
Nur Bericht	<p>Alle während eines manuellen oder geplanten Scans gefundenen infizierten Dateien bleiben auf dem Computer, da das Programm die erkannte <i>Malware</i> im Scan-Bericht aufführt.</p> <p> Hinweis: Wenn das Echtzeit-Scanning nicht aktiviert ist, kann Ihr Computer nach wie vor von Malware beschädigt werden, wenn Sie diese Option auswählen.</p>

5. Klicken Sie auf **OK**.

54 | F-Secure Internet Security 2009 | Viren und andere Malware stoppen

Wenn bei zukünftigen manuellen oder geplanten Scans *Malware* gefunden wird, führt das Programm diese Option automatisch und ohne Rückfrage durch.

Manuelles Scannen des Computers

Sie können Ihren Computer manuell scannen, wenn Sie den Verdacht haben, dass sich *Malware* auf Ihrem Computer befindet.

Welche verschiedenen Typen des manuellen Scannens gibt es und welcher Typ sollte verwendet werden?


Sie können nach bestimmten Typen von *Malware* oder nur bestimmte Teile Ihres Computer scannen.

Scan-Typ	Was wird gescannt	Nach was wird gescannt	Dauer bis zum Abschluss des Scannens	Wann sollte dieser Scantyp verwendet werden
Vollständige Computerprüfung	Ihr gesamter Computer (interne und externe Festplatten)	<i>Viren</i> , <i>Spyware</i> und <i>Riskware</i>	Dauert am längsten	Wenn Sie absolut sicher sein wollen, dass keine <i>Malware</i> oder <i>Riskware</i> auf Ihrem Computer ist.
Ziel scannen	Eine bestimmte Datei, ein Ordner oder ein Laufwerk	<i>Viren</i> , <i>Spyware</i> und <i>Riskware</i>	Hängt von der Größe der gescannten Auswahl ab. Das Scannen verläuft sehr schnell, wenn Sie beispielsweise nur einen Ordner	Wenn Sie den Verdacht haben, dass sich an einem bestimmten Speicherort Ihres Computers <i>Malware</i> befindet, weil sich dort

Scan-Typ	Was wird gescannt	Nach was wird gescannt	Dauer bis zum Abschluss des Scannens	Wann sollte dieser Scantyp verwendet werden
			scannen, der nur wenige kleine Dateien enthält.	Downloads von potenziell gefährlichen Quellen, wie Peer-to-Peer File Sharing-Netzwerken, befinden.
Festplatten scannen	Alle Festplatten innerhalb Ihres Computers.	<i>Viren</i> , <i>Spyware</i> und <i>Riskware</i>		
Schneller Malware-Scan	Teile Ihres Computers	<i>Viren</i> , <i>Spyware</i> und <i>Riskware</i>	Schneller als ein vollständiger Scan	
Schnelles Rootkit-Scanning	Wichtige Systembereiche, wo verdächtige Elemente zu einem Sicherheitsproblem werden können	Versteckte Dateien, Ordner, Laufwerke oder Prozesse		

Computer manuell auf Malware scannen

Sie können den Scantyp und die Art der Bereinigung des Computers auswählen, falls *Malware* gefunden wird.

-  **Hinweis:** Wenn Sie das Programm so eingestellt haben, dass es *Viren* oder *Spyware* automatisch behandelt, erfolgt keine Rückfrage, was beim Finden eines *Virus* oder von *Spyware*

passieren soll. Das Programm führt automatisch die von Ihnen festgelegte Aktion aus.


Manuellen Scan-Typ auswählen

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von *Malware* oder einen bestimmten Bereich scannen.


Wenn Sie einen bestimmten Typ von *Malware* befürchten, können Sie nur nach diesem Typ scannen. Wenn Sie im Bezug auf einen bestimmten Bereich Ihres Computers einen Verdacht haben, dann scannen Sie nur diesen Bereich. Diese Scans verlaufen viel schneller als ein vollständiger Scan des gesamten Computers.

So starten Sie das Scannen Ihres Computers manuell:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste

auf das Symbol .

Wenn Sie das Symbol nicht finden können, ist es möglicherweise ausgeblendet. Klicken Sie zum Einblenden ausgeblendeter Symbole

in der Taskleiste auf das Symbol .

2. Wählen Sie den Scantyp aus:

Scantyp

Vollständiger Scan - alle internen und externen Festplatten des Computers auf *Viren*, *Spyware* oder *Riskware* prüfen.

Schnell ein bestimmtes Laufwerk, einen bestimmten Ordner oder eine bestimmte Datei auf *Viren*, *Spyware* oder *Riskware* prüfen.

Scannen aller internen Festplatten Ihres Computers.

Schritte

Wählen Sie **AntiVirus & AntiSpy-Schutz** ► **Computer vollständig überprüfen** .

1. Wählen Sie **AntiVirus & AntiSpy-Schutz** ► **Ziel scannen** .
2. Wählen Sie den Bereich aus, der gescannt werden soll.
3. Klicken Sie auf **OK**.

Wählen Sie **AntiVirus & AntiSpy-Schutz** ► **Festplatten scannen** .

Scantyp

Scannen Sie Ihren Computer, um sicherzustellen, dass derzeit im System Folgendes nicht ausgeführt wird: *Viren*, *Spyware* oder *Riskware*. Beim schnellen Malware-Scan wird nicht der gesamte Computer gescannt.

Scannen des gesamten Computers nach versteckten Dateien, Ordnern oder Prozessen.

Schritte

Wählen Sie [AntiVirus & AntiSpy-Schutz](#) ►
[Schneller Malware-Scan](#) .

Wählen Sie [AntiVirus & AntiSpy-Schutz](#) ►
[Schnelles Rootkit-Scanning](#) .

Der [Scan-Assistent](#) wird geöffnet.

Legen Sie fest, ob Malware automatisch von Ihrem Computer entfernt werden soll

Wenn während des Scannens *Malware* gefunden wird, kann das Programm automatisch entscheiden, wie sie von Ihrem Computer entfernt wird. Oder Sie treffen diese Entscheidung für jedes Element selbst.

1. Wählen Sie eine Option aus:

Option

[Automatische Bereinigung \(empfohlen\)](#)

[Benutzer entscheidet abhängig vom jeweiligen Element](#)

Was passieren soll


Das Programm entscheidet, wie die jeweilige *Malware* behandelt wird, um Ihren Computer automatisch zu bereinigen.

Das Programm fragt Sie bei jedem *Malware* -Element, wie Sie vorgehen möchten.

2. Klicken Sie auf [Weiter](#).

Was soll beim Erkennen eines Virus geschehen?

Wenn *Viren* gefunden werden und wenn Sie keine automatische Bearbeitung von *Viren* durch das Programm festgelegt haben, können Sie jetzt auswählen, ob diese gelöscht, desinfiziert oder unter Quarantäne gestellt werden sollen oder ob der *Virus* unbearbeitet gelassen werden soll.

 **Hinweis:** Dieser Schritt des **Scan-Assistenten** wird übersprungen, wenn Sie festgelegt haben, dass das Programm *Viren* während eines manuellen oder geplanten Scans immer automatisch behandeln soll, oder wenn Sie festgelegt haben, dass während des Scans gefundene *Malware* automatisch behandelt werden soll.

Eine Liste der infizierten Dateien und der *Viren*, die in diesen Dateien gefunden wurden, wird angezeigt. So entfernen Sie die *Viren* von Ihrem Computer:

1. Für weitere Informationen klicken Sie auf die Links in der Spalte **Infektion**, die zu weiteren Angaben zu den *Viren* und deren Gefährlichkeit führen.
2. Wählen Sie die Aktion aus, die für die einzelnen infizierten Dateien durchgeführt werden soll:

**Durchzuführende Was mit der infizierten Datei passiert
Aktion**

Löschen	Die infizierte Datei soll gelöscht werden.
Desinfizieren	Wenn möglich, wird der <i>Virus</i> aus der infizierten Datei entfernt. Anschließend kann die Datei gefahrlos verwendet werden.
Quarantäne	Die infizierte Datei wird in die Quarantäne verschoben, wo sie Ihrem Computer nicht schaden kann. Sie können die Datei später bei Bedarf aus der Quarantäne zurückholen.
Keine	Mit der infizierten Datei geschieht nichts und der <i>Virus</i> kann Ihren Computer weiterhin beschädigen.


3. Prüfen Sie die für die infizierten Dateien ausgewählten Aktionen. Sie können alle Aktionen noch ändern.
4. Klicken Sie auf **Weiter**, um die Aktionen durchzuführen.
5. Klicken Sie auf **Weiter**.

Wenn *Spyware* gefunden wird, macht der **Scan-Assistent** mit dem Schritt zur Bereinigung von *Spyware* weiter.

Was soll passieren, wenn Spyware gefunden wird?

Wenn *Spyware* gefunden wird und Sie keine automatische Verarbeitung von *Spyware* durch das Programm festgelegt haben, können Sie

auswählen, ob die gefundene *Spyware* gelöscht, desinfiziert, unter Quarantäne gestellt oder belassen werden soll.

 **Hinweis:** Dieser Schritt des **Scan-Assistenten** wird übersprungen, wenn Sie festgelegt haben, dass das Programm *Spyware* während eines manuellen oder geplanten Scans immer automatisch behandeln soll oder wenn Sie festgelegt haben, dass das Programm während des Scans gefundene *Malware* automatisch behandeln soll.

Es wird eine Liste der *Spyware* angezeigt. So entfernen Sie diese *Spyware* von Ihrem Computer:

1. Für weitere Informationen klicken Sie in der Spalte **Name** auf den jeweiligen Link, um mehr über die *Spyware* und deren Gefährlichkeit zu erfahren.
2. Wählen Sie die Aktion aus, die für die *Spyware* durchgeführt werden soll:

Durchzuführende Aktion Was mit der *Spyware* geschieht

Löschen Der *Spyware* wird gelöscht.

Quarantäne Die *Spyware* wird unter Quarantäne gestellt, wo sie Ihrem Computer nicht schaden kann. Sie können die *Spyware* später bei Bedarf aus der Quarantäne befreien.

Ausschließen Die ausgewählte *Spyware* wird zur Liste der ausgeschlossenen Anwendungen hinzugefügt. Sie erhalten zu dieser *Spyware* bei zukünftigen manuellen oder geplanten Scans keine Benachrichtigung mehr.

Keine Für die *Spyware* wird keine Aktion durchgeführt. Sie kann Ihren Computer weiterhin beschädigen.

3. Prüfen Sie die Aktionen, die für jede *Spyware* ausgewählt sind. Sie können alle Aktionen noch ändern.
4. Klicken Sie auf **Weiter** , um die ausgewählten Aktionen anzuwenden.
5. Klicken Sie auf **Weiter**.

Wenn *Riskware* gefunden wird, fährt der **Scan-Assistent** mit dem Schritt zur Bereinigung von *Riskware* fort.

Aktionen für das Auffinden von Riskware auswählen

Wird *Riskware* gefunden, können Sie wählen, ob Sie sie löschen, desinfizieren oder unter Quarantäne stellen möchten. Sie können die *Riskware* auch auf Ihrem Computer belassen.

Eine Liste der *Riskware* wird angezeigt. So entfernen Sie die *Riskware* vom Computer:

1. Wenn Sie mehr erfahren möchten, klicken Sie in der Spalte **Name** auf den jeweiligen Link, um Informationen über die *Riskware* und deren Gefährlichkeit anzuzeigen.

2. Wählen Sie die Aktion für das *Riskware* -Element aus:

Durchzuführende Was mit der *Riskware* passiert Aktion

Löschen	Der <i>Riskware</i> wird gelöscht.
Quarantäne	Die <i>Riskware</i> wird in die Quarantäne verschoben, wo sie Ihrem Computer nicht schaden kann. Sie können die <i>Riskware</i> später bei Bedarf aus der Quarantäne befreien.
Ausschließen	Die ausgewählte <i>Riskware</i> wird zur Liste der ausgeschlossenen Anwendungen hinzugefügt. Über diese <i>Riskware</i> -Anwendung erhalten Sie bei zukünftigen manuellen oder geplanten Scans keine Warnung mehr.
Keine	Mit der <i>Riskware</i> geschieht nichts, und sie kann Ihrem Computer weiterhin schaden.

3. Prüfen Sie die Aktionen, die für einzelne *Riskware* -Elemente durchgeführt werden. Sie können alle Aktionen noch ändern.
4. Klicken Sie auf **Weiter** , um die ausgewählten Aktionen durchzuführen.
5. Klicken Sie auf **Weiter**.

Im **Scan-Assistent** wird eine Übersicht des Reinigungsprozesses angezeigt.

Aktionen auswählen, die für andere verdächtige Dateien oder Programme durchgeführt werden sollen

Wird eine verdächtige Datei oder ein verdächtiges Programm gefunden, können Sie auswählen, ob diese umbenannt, ausgeschlossen oder belassen werden sollen. Sie können auch das Programm entscheiden

lassen, welche Maßnahme hinsichtlich der einzelnen gefundenen verdächtigen Elemente ergriffen wird.

Eine Liste der verdächtigen Elemente wird angezeigt. So entfernen Sie diese Elemente von Ihrem Computer:

1. Für weitere Informationen klicken Sie auf die Links in der Spalte **Name**, die zu Angaben über die Elemente und deren Gefährlichkeit führen.
2. Wählen Sie die Aktionen für verdächtige Elemente aus:

Durchzuführende Aktion	Was mit dem verdächtigen Element geschieht
-------------------------------	---

Automatisch	Das Programm entscheidet automatisch, was mit dem verdächtigen Element geschieht.
--------------------	---


Umbenennen	Das Programm benennt die Datei um, damit sie nicht gestartet werden und Ihren Computer beschädigen kann.
-------------------	--

Ausschließen	Das ausgewählte verdächtige Element wird zur Liste der ausgeschlossenen Objekte hinzugefügt. Bei zukünftigen manuellen und geplanten Scans erhalten Sie zu diesem Element keine weiteren Benachrichtigungen.
---------------------	--

Keine	Für das verdächtige Element erfolgt keine Aktion, und es kann Ihren Computer weiterhin beschädigen.
--------------	---

Prüfen Sie, wie mit Malware auf Ihrem Computer verfahren wurde

Nachdem der Scan abgeschlossen ist, können Sie einen Bericht der Scan-Ergebnisse anzeigen.

 **Hinweis:** Sie sollten diesen Bericht anzeigen, da es sich bei der von Ihnen ausgewählten Aktion nicht immer um die durchgeführte Aktion handelt. Wenn Sie beispielsweise eine infizierte Datei desinfizieren möchten, der *Virus* jedoch nicht aus der Datei entfernt werden konnte, hat das Produkt möglicherweise an der Datei eine andere Aktion ausgeführt.

So zeigen Sie den Bericht an:

1. Klicken Sie auf **Bericht anzeigen**.

Der Bericht enthält:

- Die Anzahl gefundener *Malware*
- Der Typ der gefundenen *Malware* und Links zu Beschreibungen der *Malware* im Internet.
- Die bei den einzelnen *Malware* -Elementen durchgeführten Aktionen.
- Alle Elemente, die vom Scannen ausgeschlossen wurden.
- Die beim Scannen nach *Malware* verwendeten Scanning-Engines.

2. Klicken Sie auf **Fertig stellen**, um **Scan-Assistent** zu schließen.

Dateien und Ordner für manuelle und geplante Scans auswählen

Sie können die Dateitypen und die Bereiche Ihres Computers auswählen, die bei manuellen und geplanten Scans geprüft werden.

- 👉 **Hinweis:** Bearbeiten Sie die Einstellungen für das manuelle Scannen, um Dateien und Ordner auszuwählen, die beim geplanten Scan überprüft werden sollen.

Einschließen von Dateien in manuelle und geplante Scans

Sie können die Dateitypen auswählen, die auf *Viren* und *Spyware* manuell oder geplant gescannt werden sollen.

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Wählen Sie unter **Scan-Optionen** eine der folgenden Optionen aus:

Alle Dateien scannen Scannen aller Dateien.

Definierte Dateien scannen: Scannen aller von Ihnen festgelegten Dateitypen.

5. Zu scannende Dateitypen festlegen.
 - Um einen Dateityp in den Scanvorang einzuschließen, geben Sie die aus drei Buchstaben bestehende Dateierweiterung in


das Feld **Zur Liste hinzufügen** ein, und klicken Sie auf **Hinzufügen**.

- Um zu verhindern, dass ein Dateityp gescannt wird, klicken Sie auf einen Dateityp in der Liste. Klicken Sie anschließend auf **Entfernen**.

Um beispielsweise ausführbare Dateien in den Scan einzubeziehen, geben Sie `exe` in das Feld **Zur Liste hinzufügen** ein und klicken auf **Hinzufügen**.

6. Klicken Sie auf **OK**.
Das Dialogfeld **Zu scannende Dateitypen bearbeiten** wird geschlossen.
7. Klicken Sie auf **OK**.

Die von Ihnen ausgewählten Dateien werden in zukünftige manuelle und geplante Scans einbezogen.

-  **Hinweis:** Alle in der Ausschlussliste für das manuelle und geplante Scannen enthaltenen Dateitypen bzw. Speicherorte setzen die hier definierte Liste außer Kraft. Dateitypen, die in den Ausschlusslisten stehen, werden auch dann nicht gescannt, wenn sie hier definiert sind.

Dateien nach Dateityp aus manuellen und geplanten Scans ausschließen

Sie können Dateien nach dem Dateityp aus manuellen und geplanten Scans ausschließen.

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Klicken Sie auf **Ausschlüsse**.
5. Dateityp ausschließen:
 - a) Wählen Sie die Registerkarte **Dateitypen** aus.
 - b) Wählen Sie **Dateien mit diesen Erweiterungen ausschließen**.
 - c) Geben Sie eine Dateierweiterung, die den Typ der Dateien angibt, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.

Um Dateien ohne Erweiterung anzugeben, geben Sie `'.'` ein. Sie können den Platzhalter `'?'` für ein beliebiges Zeichen verwenden oder den Platzhalter `'*'` für eine beliebige Anzahl von Zeichen.

Um beispielsweise ausführbare Dateien auszuschließen, geben Sie in das Feld `exe` ein.

d) Klicken Sie auf **Hinzufügen**.

6. Wiederholen Sie den vorherigen Schritt für alle anderen Erweiterungen, die Sie aus dem Virenscan ausschließen möchten.
7. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
8. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die ausgewählten Dateitypen werden in Zukunft von manuellen und geplanten Scans ausgeschlossen.

Anzeigen von Anwendungen, die aus manuellen und geplanten Scans ausgeschlossen wurden

Sie können die Anwendungen anzeigen, die Sie aus manuellen und geplanten Scans ausgeschlossen haben, und diese aus der Liste der ausgeschlossenen Anwendungen entfernen, damit sie in Zukunft bei beiden Formen des Scannens wieder mitgescannt werden.

So zeigen Sie Anwendungen an, die vom manuellen oder geplanten Scannen ausgeschlossen sind:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Klicken Sie auf **Ausschlüsse**.
5. Wählen Sie die Registerkarte **Anwendungen**.
6. So stellen Sie ein, dass eine Anwendung bei zukünftigen manuellen oder geplanten Scans einbezogen wird:
 - a) Wählen Sie die Anwendung aus, die erneut in den Scan einbezogen werden soll.
 - b) Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**, um das Dialogfeld **Aus Scanvorgang ausschließen** zu schließen.
8. Klicken Sie zum Beenden auf **OK**.

Scannen der Inhalte komprimierter Dateien bei manuellen und geplanten Scans

Sie können nach *Viren* scannen, die sich in komprimierten Dateien verbergen.




1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Wenn Sie Archivdateien oder -ordner scannen möchten, etwa *.zip*-Dateien, wählen Sie **In komprimierten Dateien (ZIP, ARJ, LZH, ...) scannen**.
Bei komprimierten Dateien und Ordnern dauert der Scanvorgang ein wenig länger.
5. Klicken Sie auf **OK**.

Wählen Sie aus, welche Aktionen werden sollen, wenn Malware bei manuellen oder geplanten Scans gefunden wurde

Sie können festlegen, dass Sie gefragt werden, welche Aktion durchgeführt werden soll, wenn während einem manuellen oder geplanten Scan *Malware* gefunden wurde. Sie können auch eine Aktion vordefinieren, die automatisch und ohne Rückfragen ausgeführt wird.

So wählen Sie die Standardaktion aus, die bei erkannter *Malware* durchgeführt wird:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Manuelles Scanning** unter **AntiVirus & AntiSpy-Schutz**.
4. Wählen Sie eine Option aus der Liste neben **Wenn Malware gefunden wurde**:

Option	Was passiert, wenn <i>Malware</i> gefunden wurde
Aktion erfragen	<p>Bei einem manuellen Scan werden Sie nach der durchzuführenden Aktion gefragt, wenn während einem manuellen Scan <i>Malware</i> gefunden wurde.</p> <p> Hinweis: Bei geplanten Scans verhält Sie diese Option genau wie die Option Automatisch löschen.</p>
Automatisch löschen	<p>Das Programm versucht, die in infizierten Dateien gefundenen <i>Viren</i> während manueller oder geplanter Scans automatisch zu bereinigen. <i>Spyware</i> und <i>Riskware</i> werden automatisch unter Quarantäne gestellt.</p> <p> Hinweis: Nicht in jedem Fall kann ein <i>Virus</i> in einer Datei bereinigt werden. Ist dies der Fall, wird die Erweiterung der infizierten Datei geändert, sodass der <i>Virus</i> Ihren Computer nicht beschädigen kann.</p>
Automatisch unter Quarantäne stellen	<p>Das Programm stellt infizierte Dateien, die während manueller oder geplanter Scans gefunden wurden automatisch unter Quarantäne, sodass sie ihren Computer nicht beschädigen können.</p>
Automatisch löschen	<p>Alle bei manuellen oder geplanten Scans gefundenen infizierten Dateien werden automatisch von dem Programm gelöscht.</p>
Nur Bericht	<p>Alle während eines manuellen oder geplanten Scans gefundenen infizierten Dateien bleiben auf dem Computer, da das Programm die erkannte <i>Malware</i> im Scan-Bericht aufführt.</p> <p> Hinweis: Wenn das Echtzeit-Scanning nicht aktiviert ist, kann Ihr Computer nach wie vor von Malware beschädigt werden, wenn Sie diese Option auswählen.</p>

5. Klicken Sie auf **OK**.

68 | F-Secure Internet Security 2009 | Viren und andere Malware stoppen

Wenn bei zukünftigen manuellen oder geplanten Scans *Malware* gefunden wird, führt das Programm diese Option automatisch und ohne Rückfrage durch.

Was ist ein Quarantäne-Repository?

Als Quarantäne wird ein sicheres Repository für möglicherweise schädliche Dateien bezeichnet.

Dateien, die sich in Quarantäne befinden, können sich weder verbreiten noch Ihrem Computer schaden.

Sie können *Malware*, *Spyware* und *Riskware* unter Quarantäne stellen und sie so unschädlich machen. Sie können Anwendungen oder Dateien zu einem späteren Zeitpunkt aus der Quarantäne entlassen, wenn Sie sie benötigen.

Wenn Sie ein unter Quarantäne stehendes Element nicht benötigen, können Sie es löschen. Das Löschen eines Elements aus der Quarantäne entfernt es endgültig von Ihrem Computer.

- *Malware*, die sich in Quarantäne befindet, können Sie in der Regel löschen.
- *Spyware*, die sich in Quarantäne befindet, können Sie in den meisten Fällen löschen. Es ist möglich, dass die isolierte *Spyware* Teil eines seriösen Softwareprogramms ist und das Löschen dazu führt, dass das Programm nicht mehr richtig ausgeführt werden kann. Wenn Sie das Programm auf Ihrem Computer lassen möchten, können Sie die *Spyware* aus der Quarantäne wiederherstellen.
- *Riskware*, die sich in Quarantäne befindet, kann ein seriöses Softwareprogramm sein. Wenn Sie das Programm selbst installiert und eingerichtet haben, können Sie es aus der Quarantäne wiederherstellen. Wenn die *Riskware* ohne Ihr Wissen installiert wurde, wurde sie sehr wahrscheinlich mit böser Absicht installiert und kann gelöscht werden.

Programme unter Quarantäne anzeigen

Sie können weitere Informationen zu Elementen unter Quarantäne anzeigen.

So zeigen Sie detaillierte Informationen zu Elementen unter Quarantäne an:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben **Unter Quarantäne gestellte Elemente** auf **Konfigurieren** .
Das Dialogfeld **Quarantäne** wird geöffnet.

3. Durchsuchen Sie die Kategorien **Virus** , **Spyware** und **Riskware** , um alle unter Quarantäne gestellten Elemente anzuzeigen.
 - In der Liste der unter Quarantäne gestellten Elemente (*Viren*) werden der Name des isolierten Elements sowie der Installationspfad der Datei angezeigt. Hat das unter Quarantäne gestellte Element mehrere Dateien installiert, erfolgt die Anzeige in der Liste wie folgt: *Systeminfektion*.
 - Die Liste der unter Quarantäne gestellten *Spyware* zeigt den *Spyware* -Typ und eine Liste von Anwendungen an, bei denen bekannt ist, dass sie Spyware enthalten.
 - Die Liste der unter Quarantäne gestellten *Riskware* zeigt den Dateipfad und den Namen der Elemente an.
4. Um weitere Informationen zu dem unter Quarantäne gestellten Element anzuzeigen, sind folgende Optionen verfügbar:
 - Klicken Sie auf den Namen des Elements, um die Beschreibung in der Online-Datenbank anzuzeigen.
 - Klicken Sie auf **Details**, um zusätzliche Informationen zu dem Element unter Quarantäne anzuzeigen.
5. Um das unter Quarantäne stehende Element zu löschen, wählen Sie es aus und klicken auf **Löschen**.


Wiederherstellen eines Programms aus der Quarantäne

Unter Quarantäne gestellte Elemente, die Sie benötigen, können Sie wiederherstellen.

Anwendungen oder Dateien, die Sie benötigen, können Sie aus der Quarantäne wiederherstellen. Stellen Sie keine Elemente aus der Quarantäne wieder her, wenn Sie nicht sicher sind, dass sie keine Bedrohung sind. Wiederhergestellte Elemente werden an den Originalspeicherort auf dem Computer verschoben.

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben **Unter Quarantäne gestellte Elemente** auf **Konfigurieren**.
Das Dialogfeld **Quarantäne** wird geöffnet.

3. Durchsuchen Sie die Quarantänekategorien und wählen Sie das Element aus, das Sie wiederherstellen möchten. Sie können mehrere Elemente auswählen, die wiederhergestellt werden sollen.

 **Hinweis:** Beachten Sie beim Auswählen von Dateien, dass die Namen der Dateien als Verknüpfung zur Beschreibung des Elements in der Online-Datenbank dienen.

4. Klicken Sie auf **Wiederherstellen**.
Das Produkt stellt das ausgewählte Element am Originalspeicherort auf der Festplatte wieder her und entfernt das Element aus der Quarantäneliste.

Scannen Ihrer E-Mails

Das E-Mail-Scanning schützt Sie davor, *Viren* per E-Mail zu erhalten oder zu senden.

Das E-Mail-Scanning schützt Ihren Computer vor:

- Erhalt eines *Virus*, der sich in einer Datei befindet, die als E-Mail-Anhang an Sie gesendet wird,
- versehentliches Senden eines *Virus* an jemand anderen, wenn Sie eine E-Mail mit einer angehängten Datei versenden.

Wann werden E-Mail-Nachrichten und -Anhänge gescannt?


E-Mail-Nachrichten und -Anhänge werden jedes Mal gescannt, wenn Ihr E-Mail-Programm E-Mail-Nachrichten an den Mail-Server sendet bzw. von ihm empfängt.

Beim E-Mail-Scannen werden folgende E-Mail-Nachrichten gescannt:


- E-Mail-Nachrichten, die über E-Mail-Programme wie Microsoft Outlook, Microsoft Outlook Express, Microsoft Mail oder Mozilla Thunderbird gesendet und empfangen werden, die als Programme unabhängig von Ihrem Webbrowser ausgeführt werden.

Beim E-Mail-Scannen werden folgende E-Mail-Nachrichten nicht gescannt:

- E-Mails in Webmail, einschließlich E-Mail-Anwendungen, die in Ihrem Webbrowser ausgeführt werden, wie Hotmail, Yahoo! mail oder Gmail.

 **Hinweis:** Sie müssen sicherstellen, dass die für die verschiedenen E-Mail-Protokolle (POP3, IMAP4, SMTP) verwendeten Ports ordnungsgemäß eingerichtet sind. E-Mail-Nachrichten, die über andere Ports empfangen und versendet werden, werden nicht gescannt.

Sie sind auch dann vor *Viren* geschützt, wenn die Ports nicht vorschriftsmäßig eingerichtet sind oder Sie Webmail verwenden. Wenn Sie den E-Mail-Anhang öffnen, erkennt das Echtzeit-Scanning, dass er einen Virus enthält, und blockiert den Virus, bevor er Schaden anrichten kann.

-  **Hinweis:** Das Echtzeit-Scanning schützt nur Ihren Computer, nicht Ihre Freunde. Der Virus wird nur erkannt, wenn Sie den Dateianhang öffnen. Wenn Sie den Dateianhang nicht öffnen, wissen Sie nicht, ob die E-Mail einen *Virus* enthält und so einfach eine infizierte E-Mail an Ihre Freunde weitergeleitet werden kann.

Infizierte E-Mail-Anhänge empfangener E-Mails automatisch desinfizieren oder entfernen

Sie können infizierte E-Mail-Anhänge Ihrer empfangenen E-Mails automatisch desinfizieren oder entfernen.


So desinfizieren Sie empfangene infizierte E-Mail-Anhänge automatisch:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
3. Wählen Sie die Registerkarte **Aktionen**.
4. Wählen Sie unter **Überprüfung eingehender E-Mails** die Aktion für infizierte Dateianhänge aus:

Options	Description
Desinfizieren	Den <i>Virus</i> aus dem Anhang entfernen und eine E-Mail mit der Datei, aber ohne den <i>Virus</i> senden.
Entfernen	Entfernt die Datei vollständig und sendet die E-Mail ohne angehängte Datei.
Keine	Erlaubt, dass die E-Mail mit der Datei und dem <i>Virus</i> gesendet wird.

5. Wählen Sie unter **Überprüfung eingehender E-Mails** die Aktion für deformierte Nachrichtenteile aus:

Options	Description
Entfernen	Entfernt alle falsch kodierten Teile der E-Mail und sendet diese dann.
Keine	Erlaubt, dass eine falsch kodierte E-Mail gesendet wird.

-  **Hinweis:** Eine E-Mail-Nachricht mit deformierten Nachrichtenteilen entspricht nicht den Standardregeln für die Kodierung von E-Mail-Nachrichten. Manchmal werden E-Mail-Nachrichten bewusst falsch kodiert um falsche

Informationen zu verbergen oder aus anderen bösartigen Gründen.

6. Klicken Sie auf **OK**.

Senden infizierter E-Mails automatisch verhindern

Sie können festlegen, dass von Ihnen gesendete E-Mail-Nachrichten automatisch blockiert werden, wenn eine mit einem *Virus* infizierte Datei angehängt ist.

So verhindern Sie, dass mit einem *Virus* infizierte E-Mails gesendet werden:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Aktionen**.
4. Wählen Sie unter **Scanning ausgehender E-Mails**, neben "Aktion bei infiziertem Anhang", die Option **Blockieren**.
5. Wählen Sie unter **Scanning ausgehender E-Mails**, neben "Aktion bei 'malformed' Nachrichtenteilen", die Option **Blockieren**.



Hinweis: Eine E-Mail-Nachricht mit deformierten Nachrichtenteilen entspricht nicht den Standardregeln für die Kodierung von E-Mail-Nachrichten. Manchmal werden E-Mail-Nachrichten bewusst falsch kodiert um falsche Informationen zu verbergen oder aus anderen bösartigen Gründen.

6. Wählen Sie **Blockierte E-Mails im Postausgang belassen**, wenn Sie die blockierte Nachricht im Postausgang Ihres E-Mail-Programms belassen möchten, um die Nachricht und die Datei später untersuchen zu können.
7. Klicken Sie auf **OK**.

Benachrichtigen, wenn in einer E-Mail ein Virus gefunden wird


Sie können das Programm so konfigurieren, dass ein E-Mail-Scanning-Bericht angezeigt wird, wenn in einem E-Mail-Anhang ein *Virus* gefunden wird.

So zeigen Sie einen E-Mail Scanning-Bericht an:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
3. Wählen Sie die Registerkarte **Aktionen**.
4. Wählen Sie **Bericht anzeigen, wenn Infektionen festgestellt wurden**.
5. Klicken Sie auf **OK**.

Scannen komprimierter E-Mail-Anhänge

Sie können die Inhalte komprimierter E-Mail-Anhänge scannen, wie Dateien vom Typ `.zip`.

 **Hinweis:** Wenn die komprimierte Datei passwortgeschützt ist, ist ein automatisches Scannen nicht möglich.

So scannen Sie komprimierte E-Mail-Anhänge:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
3. Wählen Sie im Feld **Scan-Optionen** die Option **In komprimierten Dateianhängen (ZIP, ARJ, LZH, ...) scannen** aus, um Archivanhänge und -ordner, etwa gezippte Anhänge, nach Viren zu durchsuchen.

Fortschritt des E-Mail-Scannings anzeigen

Das Scannen großer Dateien auf *Viren* kann geraume Zeit in Anspruch nehmen. Sie können einen Fortschrittsbalken anzeigen, der angibt, wann der *Virus*-Scan beendet sein wird.

So zeigen Sie den Fortschrittsbalken an:

1. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
2. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
3. Wählen Sie **Beim Scannen großer Dateien Verlaufsanzeige einblenden** auf der Registerkarte **Scanvorgang**.
4. Klicken Sie auf **OK**.

Festlegen der Ports für verschiedene E-Mail-Protokolle

Wenn Ihre E-Mail-Programm keinen Standardport verwendet, müssen Sie den Port verwenden, der auf E-Mail- *Viren* überprüft wurde. Anderenfalls werden diese E-Mail-Nachrichten nicht nach *Viren* gescannt.

So legen Sie die Ports fest:

1. Starten Sie Ihre E-Mail-Anwendung und prüfen Sie, welche Ports für das Senden und Empfangen von E-Mails verwendet werden. Notieren Sie die Portnummern.
2. Öffnen Sie das Produkt.
3. Klicken Sie auf die Registerkarte **AntiVirus & AntiSpy-Schutz**.
4. Klicken Sie neben E-Mail-Scanning auf **Konfigurieren**.
5. Klicken Sie auf **Protokolle**.
6. Geben Sie die Portnummern ein, die für die einzelnen E-Mail-Protokolle verwendet werden, *POP3* , *IMAP4* oder *SMTP* .
7. Klicken Sie auf **OK**.

Kapitel 3

Sichere Verwendung des Internets

Themen:

- Was sind Sicherheitsstufen?
- Was ist eine Firewall?
- Kontrollieren von Internetverbindungen für Anwendungen
- Verhindern von Eindringungsversuchen
- Kontrollieren von DFÜ-Verbindungen
- Anzeigen von Internet-Schutzschildstatus, Alarmen und Protokolldateien

Internet-Schutzschild:

- Schützt Sie vor Eindringlingen, die versuchen, ohne Ihre Genehmigung auf Ihren Computer zuzugreifen. Diese können z. B. versuchen, Ihre persönlichen Daten zu stehlen - Dateien, Passwörter oder Kreditkartennummern.
- Blockiert schädlichen Internetdatenverkehr wie *Trojaner*. Diese können z. B. Dateien auf Ihrem Computer zerstören, Ihren Computer zum Absturz bringen oder *Ports* öffnen, damit Hacker auf Ihren Computer zugreifen können.
- Blockiert schädlichen Internetdatenverkehr, wie *Spyware*. *Spyware* kann z. B. Informationen über Ihre E-Mail-Adressen, Passwörter oder Kreditkartennummern abrufen.
- Verhindert, dass bösartige *Dialer*programme Ihre Modem- oder ISDN-Verbindung verwenden, um kostenpflichtige Telefonnummern mit hohen Minutenpreisen anzuwählen.

Sobald Sie das Produkt installiert haben, sorgt das Internet-Schutzschild automatisch dafür, dass Ihr Computer geschützt ist.

Was sind Sicherheitsstufen?

Die *Sicherheitsstufen* des Internet-Schutzschilds definieren die Schutzstufe Ihres Computers.


Jede *Sicherheitsstufe* hat einen vordefinierten Satz von *Firewallregeln*, die festlegen, welcher Typ von Datenverkehr auf dem Computer zugelassen ist oder dort abgelehnt wird. Einige Stufen können Sie um eigene, selbst erstellte Regeln ergänzen.

Sicherheitsstufen definieren auch

- wenn Internetverbindungen automatisch für alle Anwendungen zugelassen sind oder
- wenn Sie jeden Verbindungsversuch in einem Popup-Fenster der Anwendungssteuerung separat zulassen oder ablehnen können.

Es gibt einige vordefinierte *Sicherheitsstufen*, die von sehr streng bis zu sehr niedrig reichen:

- Eine sehr strenge *Sicherheitsstufe* (**Alle blockieren**) blockiert in der Regel den meisten Netzwerkdatenverkehr. Dies kann dazu führen, dass Sie einige auf Ihrem Computer installierten Programme nicht verwenden können.
- Eine mittlere Stufe (**Normal**) lässt in der Regel den gesamten von Ihrem Computer ausgehenden Datenverkehr ins Internet zu. Die mittlere Stufe lehnt eventuell einige eingehende Dienste ab und erzeugt *Alarme* für diese.
- Eine sehr niedrige Stufe (**Alle zulassen**) lässt in der Regel den gesamten Netzwerkdatenverkehr zu, eingehenden wie ausgehenden, und erzeugt keine *Alarmmeldungen*. Da Ihr Computer mit dieser Stufe nicht geschützt ist, sollten Sie sie nur in Ausnahmefällen verwenden.

 **Hinweis:** Je nach dem verwendeten Produkt, können die Namen der Sicherheitsstufen abweichen.

Ihr Computer ist mit der vordefinierten *Sicherheitsstufe* sicher. Möglicherweise müssen Sie die Stufe strenger einstellen, wenn Sie z. B. Ihren Laptop außerhalb Ihres Hauses verwenden und das Internet über eine *WLAN*-Verbindung öffnen.

Sie können Ihre eigene *Sicherheitsstufe* definieren und zu dieser Ihren eigenen Satz Regeln hinzufügen. Es empfiehlt sich jedoch nur für erfahrene Benutzer, eigene Sicherheitsstufen zu definieren.

Welcher Zusammenhang besteht zwischen Sicherheitsstufen und Firewallregeln und Diensten?

Eine *Sicherheitsstufe* besteht aus verschiedenen *Firewallregeln*. Eine *Firewallregel* umfasst verschiedene *Firewalldienste*. Dienste werden durch die *Protokolle* und *Ports* definiert, die sie verwenden.

Die Sicherheitsstufe **Normal** enthält z. B. eine Firewallregel namens **Websuche**. Diese Regel erlaubt die Suche im Web. Die Regel enthält die Dienste, die für die Suche im Web erforderlich sind, wie den Dienst **HyperText Transfer Protocol (HTTP)**. Dieser Dienst verwendet TCP und Port Nummer 80.

Ändern der *Sicherheitsstufe*

Wenn Sie den Grad des Schutzes Ihres Computers anpassen möchten, ändern Sie die *Sicherheitsstufe*.

So ändern Sie die *Sicherheitsstufe*:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie neben **Internet-Schutzschild** und der aktuellen *Sicherheitsstufe* auf **Ändern**.
3. Lesen Sie sich die Beschreibung der *Sicherheitsstufe* sorgfältig durch.
4. Wählen Sie in der Liste die geeignete Stufe aus und klicken Sie auf **OK**.

Auf der Seite **Internet-Schutzschild** wird jetzt die neue *Sicherheitsstufe* angezeigt. Die *Firewallregeln* und die Einstellungen der Anwendungssteuerung ändern sich in Funktion der ausgewählten *Sicherheitsstufe*.

Was ist eine Firewall?

Die *Firewall* schützt Ihren Computer, indem Sie sicheren Internetdatenverkehr passieren lässt und unsicheren Datenverkehr blockiert.

In der Regel lässt die *Firewall* den Datenverkehr von Ihrem Computer in das Internet zu, blockiert aber den gesamten Datenverkehr aus dem Internet auf Ihren Computer, sofern Sie diesen nicht ausdrücklich zulassen. Indem eingehender Datenverkehr blockiert wird, verhindert die *Firewall*, dass *schädliche Software*, z. B. *Würmer*, auf Ihren Computer gelangen oder dass Eindringlinge auf Ihren Computer zugreifen können. Abhängig von Ihren *Alarmeinstellungen* blendet das Internet-Schutzschild einen Popup-Alarm zu den Aktionen der Firewall ein.

Ihr Computer wird durch die vordefinierten *Firewalleinstellungen* geschützt. Diese brauchen Sie in der Regel nicht anzupassen. Es kann jedoch erforderlich sein, Änderungen vorzunehmen, wenn Sie eine strenge *Sicherheitsstufe* verwenden oder wenn Sie eigene *Firewallregeln* oder Dienste hinzugefügt haben.



Vorsicht: Schalten Sie *Firewall* nicht ab. Wenn Sie dies tun, ist Ihr Computer allen Netzwerkangriffen ungeschützt ausgeliefert. Wenn ein Programm auf Ihrem Computer nicht mehr funktioniert, da es keine Verbindung zum Internet herstellen kann, ändern Sie *Firewallregeln* bzw. die Einstellungen für die Anwendungssteuerung, anstatt *Firewall* abzuschalten.

So verfahren Sie, wenn ein Popup des Internet-Schutzschilds angezeigt wird

Ein Alarm-Popup des Internet-Schutzschilds wird auf Ihrem Bildschirm angezeigt, wenn die *Firewall* auf Ihrem Computer verdächtigen Netzwerkverkehr erkennt.

Ein Popup wird angezeigt, wenn:

- der Datenverkehr passt zu einer der aktuellen *Firewallregeln* und für die Regel wurde die Alarmmeldung aktiviert oder
- auf Ihrem Computer hat ein Eindringversuch stattgefunden, und die Alarmmeldung für den Eindringenschutz wurde eingeschaltet.

Es ist nicht unbedingt erforderlich, dass Sie etwas unternehmen, da die Firewall verdächtigen Datenverkehr automatisch blockiert und Eindringungsversuche blockiert (wenn **Blockieren und Versuch protokollieren** in den Einstellungen der Intrusion Prevention eingeschaltet wurde).

Verfahren Sie wie folgt, wenn ein Alarm-Popup angezeigt wird:

1. Lesen Sie die Alarminformation.
2. Klicken Sie auf **Details >>** , um die Alarmdetails anzuzeigen.
3. Wenn Sie nicht möchten, dass weitere Alarm-Popups des Internet-Schutzschilds angezeigt werden, aktivieren Sie das Kontrollkästchen **Alarmdialogfeld nicht mehr anzeigen**.
4. Für Informationen über die Remote- *IP-Adresse* klicken Sie auf **DNS-Name**.
Zeigt, welcher *Domainname* zur *IP-Adresse* gehört, z. B. **www.beispiel.com**. Wenn der *Domainname* nicht aufgelöst werden kann, wird die Schaltfläche **DNS-Name** deaktiviert und es wird kein Domainname angezeigt.
5. Sie können für den Datenverkehr, der den Alarm ausgelöst hat, eine neue *Firewallregel* erstellen.
Diese Regel kann diese Art von Datenverkehr in Zukunft entweder zulassen oder ablehnen. Klicken Sie auf **Regel erstellen** und geben Sie die Regelinformationen ein.
6. Um das Dialogfeld **Alarmer von Internet-Schutzschild** zu schließen, klicken Sie auf **Schließen**.

Sie können Ihren Computer jetzt wieder ganz normal verwenden.

Schalten Sie die Alarm-Popups des Internet-Schutzschilds ein oder aus

Sie können auswählen, ob Alarm-Popups des Internet-Schutzschilds angezeigt werden.

So schalten Sie Alarm-Popups ein oder aus:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie auf **Alarmprotokoll**.

6. Um die Popup-Nachrichten einzuschalten, aktivieren Sie das Kontrollkästchen **Alarm-Popups anzeigen**. Um die Popups auszuschalten, deaktivieren Sie das Kontrollkästchen.
7. Klicken Sie auf **Schließen**.

Wenn Sie die Popup-Nachrichten eingeschaltet haben, wird ein Popup-Fenster angezeigt, sobald Datenverkehr mit den aktuellen Firewallregeln übereinstimmt. Dies gilt nur für Regeln, für die die Alarmprotokollierung und Popups aktiviert sind. Wenn Sie die Popup-Nachrichten abgeschaltet haben, werden diese nicht mehr angezeigt.

Was sind *Firewallregeln*?

Firewallregeln definieren, welche Art von Internetdatenverkehr zugelassen oder blockiert ist.

Jede *Sicherheitsstufe* hat einen vordefinierten Satz von *Firewallregeln*, den Sie nicht verändern können. Sie können lediglich zu einigen Stufen neue Regeln hinzufügen. Bei einigen Stufen ist es nicht möglich, eigene Regeln hinzuzufügen. Es gibt auch Stufen ohne vordefinierte Regeln, für die Sie eigene Regelsätze definieren können. Die ausgewählte Sicherheitsstufe wirkt sich auch auf die Priorität aus, die Ihre Regel im Verhältnis zu den vordefinierten Regeln erhält.

Eine *Firewall-Regel* kann auf Datenverkehr aus dem Internet auf Ihren Computer (eingehend) oder von Ihrem Computer in das Internet (ausgehend) angewendet werden. Eine Regel kann auch auf beide Richtungen gleichzeitig angewendet werden.

Eine *Firewallregel* enthält *Firewall dienste*, die den Typ des Datenverkehrs und die *Ports* festlegen, die dieser Typ von Datenverkehr verwendet. Eine Regel namens **Websuche** verwendet z. B. einen Dienst namens **HTTP**, der TCP und den *Port* Nummer 80 verwendet.

Firewallregeln definieren außerdem, ob *Alarm-Popups* des Internet-Schutzschilds über Datenverkehr, der den *Firewallregeln* entspricht, eingeblendet werden.

Wann muss eine neue *Firewallregel* hinzugefügt werden?

Möglicherweise müssen Sie eine neue Firewallregel hinzufügen, wenn Sie mit der Verwendung eines neuen Programms beginnen oder ein neues Gerät

an Ihren Computer anschließen, wie z. B. ein WLAN-Gerät oder eine IP-Kamera.

Indem alle Dienste, die das Programm oder das Gerät benötigt, zu derselben Regel hinzugefügt werden, ist es einfach:

- die Regel später ein- oder ausschalten oder
- die Regel entfernen, wenn das Programm deinstalliert oder das Gerät entfernt wird.

Sie müssen außerdem eine neue Regel hinzufügen, wenn Sie einen bestimmten Datenverkehrstyp abgelehnt haben, diesen aber für bestimmte IP-Adressen zulassen möchten. In diesem Fall besitzen Sie bereits eine allgemeine *Firewallregel*, die den Datenverkehr ablehnt. Um den Datenverkehr für bestimmte IP-Adressen zuzulassen, müssen Sie eine etwas spezifischere Zulassungsregel erstellen.

Wenn die allgemeine Regel z. B. den gesamten ausgehenden *FTP*-Datenverkehr ablehnt, dann möchten Sie möglicherweise den *FTP*-Datenverkehr zur Website Ihres Internet Service Providers dennoch zulassen, um Ihre Webseiten aktualisieren zu können. Dies erreichen Sie, indem Sie eine spezifischere Regel hinzufügen, die den *FTP*-Datenverkehr zur IP-Adresse Ihres Internet Service Providers zulässt, und indem Sie dieser Regel eine höhere Priorität zuweisen als die der allgemeinen Ablehnungsregel.

Was sind Firewalldienste?

Firewalldienste definieren den Typ des Datenverkehrs, für den eine *Firewallregel* gilt.

Netzwerkdienste, wie Websuche, *Dateifreigabe* oder *Remote-Konsolen-Zugriff*, sind Beispiele für Firewalldienste.

Ein Dienst verwendet ein bestimmtes *Protokoll* und einen bestimmten *Port*. Der HTTP-Dienst verwendet z. B. das TCP- *Protokoll* und den *Port* Nummer 80.

Ein Firewalldienst verwendet zwei Arten von Ports:

- *Ausgangspartei-Port*: der *Port* auf dem Computer, der die Verbindung initiiert.

- *Antwortpartei-Port*: der *Port* auf dem Computer, bei dem die Verbindung ankommt.

Ob es sich bei dem *Port* auf Ihrem eigenen Computer um einen *Ausgangspartei-Port* oder um einen *Antwortpartei-Port* handelt, hängt von der Richtung des Datenverkehrs ab:

- Wenn der *Firewalldienst* für ausgehenden Datenverkehr zuständig ist, dann ist der *Ausgangspartei-Port* der *Port* auf Ihrem Computer. Der *Antwortpartei-Port* ist dann der *Port* auf einem Remote-Computer.
- Wenn der *Firewalldienst* für eingehenden Datenverkehr zuständig ist, ist der *Ausgangspartei-Port* der *Port* auf einem Remote-Computer. Der *Antwortpartei-Port* ist dann der *Port* auf Ihrem eigenen Computer.

Die *Antwortpartei-Ports* werden in der Regel in der *Softwaredokumentation* angegeben. *Ausgangspartei-Port* kann in der Regel jeder *Port* über 1023 sein. Für einige Spiele müssen Sie jedoch gegebenenfalls bestimmte *Ausgangspartei-Ports* definieren. In diesem Fall werden auch diese in der *Softwaredokumentation* angegeben.

Wenn Sie eine neue *Firewallregel* erstellen, stehen Ihnen einige vordefinierte Dienste zur Verfügung, die Sie zu Ihrer Regel hinzufügen können. Sie können auch eigene Dienste erstellen und hinzufügen, falls Sie den benötigten Dienst nicht in der Dienstliste finden.

Firewalldienste anzeigen

Die vorhandenen *Firewalldienste* können Sie auf der Registerkarte **Dienste** anzeigen.

So zeigen Sie die Dienste an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Dienste**.

Folgende Informationen sind verfügbar:

Feld	Beschreibung
Beschreibung	Beschreibung des Dienstes.
Wird verwendet	Zeigt an, ob der Dienst in einer der <i>Firewallregeln</i> verwendet wird.

Feld	Beschreibung
Regelname	Wenn der Dienst in <i>Firewallregeln</i> verwendet wird, werden die Namen der Regeln angezeigt.

- Um die Details eines Dienstes anzuzeigen, wählen Sie den Dienst in der Liste aus, und klicken Sie auf **Details**. Das Dialogfeld **Dienstdetails** wird geöffnet.
- Klicken Sie nach der Ansicht der Dienstdetails auf **Schließen**.

Was sind dynamische *Firewallregeln*?

Dynamische *Firewallregeln* werden für Verbindungen von Remote-Computern zu Serverprogrammen auf Ihrem Computer erstellt.

Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird und Sie dort eine eingehende Verbindung zulassen - z. B. zu einem Peer-to-Peer-Serverprogramm auf Ihrem Computer -, erstellt die *Firewall* eine temporäre, dynamische *Firewallregel*. Diese Regel wird auf der Registerkarte **Aktivität** zur Liste der dynamischen Regeln hinzugefügt. Die Regel öffnet einen *Port* für dieses Programm und hält diesen so lange geöffnet, wie das Programm an diesem *Port* auf eingehende Verbindungen wartet.

Wenn das Programm den *Port* nicht mehr überwacht, greift die Option *Regel schließt den Port*, und die dynamische Regel wird aus der Liste der dynamischen Regeln entfernt. Abhängig von den Einstellungen für die Anwendungssteuerung wird das Popup-Fenster der Anwendungssteuerung möglicherweise nicht für alle Programme angezeigt. Wenn das Popup-Fenster nicht angezeigt wird, wird die dynamische *Firewall*-Regel automatisch für dieses Programm erstellt.

Dynamische *Firewallregeln* anzeigen

Die Registerkarte **Aktivität** zeigt die dynamischen *Firewallregeln* an, die gerade aktiv sind.

Dynamische *Firewallregeln* werden für Verbindungen von Remote-Computern zu *Server*programmen auf Ihrem Computer erstellt.

So zeigen Sie die dynamischen *Firewallregeln* an:

- Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
- Klicken Sie auf **Erweitert**.

3. Wählen Sie **Internet-Schutzschild > Firewall**.

4. Klicken Sie auf die Registerkarte **Aktivität**.

Folgende Informationen sind verfügbar:

- **Anwendung:** Der Dateiname des *Serverprogramms* auf Ihrem Computer, das gerade einen *Port* auf eingehende Verbindungen überwacht.
- **Listening-Port:** Der *Port*, den die dynamische *Firewallregel* geöffnet hat. Das *Serverprogramm* überwacht diesen *Port* auf eingehende Verbindungen.
- **Remote-Adresse:** Das *Serverprogramm* überwacht den *Port* auf Verbindungen für folgende *IP-Adressen*:
 - **0.0.0.0/0** : Alle *IPv4* - Adressen.
 - **::/0** : Alle *IPv6*- Adressen.

Wie funktioniert die Reihenfolge der Prioritäten der *Firewallregeln*?

Firewallregeln haben eine Prioritätsreihenfolge, die festlegt, in welcher Reihenfolge die Regeln auf den Netzwerkdatenverkehr angewendet werden.

Firewallregeln werden auf der Registerkarte **Regeln** als Liste angezeigt. Die *Regeln* werden von oben nach unten angewendet, wobei die erste Regel, die mit dem Datenverkehr übereinstimmt, alle nachfolgenden Regeln überschreibt. Das Hauptprinzip besteht darin, nur den erforderlichen Datenverkehr zuzulassen und den Rest zu blockieren. Daher ist die letzte Regel einer *Sicherheitsstufe* die Regel **Alles andere sperren**. Diese blockiert den gesamten Datenverkehr, den die vor ihr stehenden Regeln nicht explizit zugelassen haben.

Dynamische *Firewallregeln* werden in einer separaten Liste auf der Registerkarte **Aktivität** angezeigt. Die Priorität der dynamischen Regeln ist niedriger als die Priorität der normalen *Firewallregeln*. Dies bedeutet, dass eine dynamische Regel einen bestimmten Datenverkehr nicht zulassen kann, wenn eine *Firewallregel* diesen ablehnt. Die Priorität der dynamischen Regeln ist jedoch höher als die Priorität der vordefinierten Regel **Alles andere sperren**.


Ein Beispiel für die Funktionsweise der Prioritätenreihenfolge

- Sie haben eine Regel hinzugefügt, die den gesamten ausgehenden *FTP*-Datenverkehr ablehnt. In der Regelliste fügen Sie vor dieser Regel eine andere Regel hinzu, die eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers zulässt. Durch diese Regel ist es möglich, eine *FTP*-Verbindung mit dieser IP-Adresse herzustellen.
- Sie haben eine Regel hinzugefügt, die eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers zulässt. Vor dieser Regel fügen Sie in der Regelliste eine Regel hinzu, die den gesamten *FTP*-Datenverkehr ablehnt. Diese Regel verhindert, dass eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers hergestellt werden kann (oder zu einer beliebigen anderen IP-Adresse).

Erstellen Sie *Firewalldienste* und -regeln

Sie können eigene *Firewalldienste* und -regeln erstellen, wenn Sie bestimmten Internetdatenverkehr zulassen oder ablehnen möchten.

Wählen Sie vor dem Erstellen einer Regel die *Sicherheitsstufe*, der Sie diese Regel hinzufügen möchten.

 **Hinweis:** Es ist nicht bei allen *Sicherheitsstufen* möglich, eigene Regeln hinzuzufügen.

Erstellen Sie einen *Firewalldienst*

Sie müssen möglicherweise einen neuen *Firewalldienst* erstellen, wenn Sie z. B. ein neues Programm einsetzen, das eine Verbindung mit dem Internet benötigt und für das kein vordefinierter Dienst vorhanden ist.

Der Dienst definiert die *Protokolle* und *Ports*, die das Programm verwendet. Diese Informationen finden Sie in der Dokumentation des Programms.

So erstellen Sie einen *Firewalldienst*:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.

3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Dienste**.
5. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Neuen Dienst hinzufügen** wird geöffnet.
6. Geben Sie im Feld **Name** einen Namen für den Dienst ein.
Verwenden Sie einen möglichst aussagekräftigen Namen.
7. Wählen Sie in der Liste **Protokoll** das *Protokoll* für den Dienst aus:
 - *ICMP* (1)
 - *TCP* (6)
 - *UDP* (17)

Wenn Sie ein anderes *IP-Protokoll* verwenden möchten, geben Sie die *Protokollnummer* (0-255) in das Feld ein.

8. Wenn der Dienst das *TCP*- oder das *UDP-Protokoll* verwendet, legen Sie die *Ausgangspartei-Ports* für den Dienst fest.
Wenn in der Dokumentation des Programms keine *Ausgangspartei-Ports* angegeben sind, können Sie in der Regel eine beliebige *Port*-Nummer über 1023 verwenden.
 - a) Klicken Sie neben dem Feld **Ausgangspartei-Ports** auf **Bearbeiten**.
 - b) Fügen Sie die *Ports* hinzu:
 - Um einen einzelnen *Port* anzugeben, geben Sie die *Port* Nummer in das Feld **Einzel** ein, beispielsweise 1024 .
 - Um einen *Port* anzugeben, fügen Sie die niedrigste und die höchste *Port*-Zahl des **Bereichs** den Feldern hinzu, z. B., 1024-65535 .
 - c) Klicken Sie auf **Zur Liste hinzuf**.
 - d) Wiederholen Sie die Schritte a-c, um alle erforderlichen Ports hinzuzufügen.
 - e) Klicken Sie auf **OK**.
9. Wenn der Dienst das *TCP*- oder das *UDP-Protokoll* verwendet, legen Sie die *Antwortpatei-Ports* für den Dienst fest.
Die *Antwortpatei-Ports* werden in der Regel in der Dokumentation des Programms angegeben.
 - a) Klicken Sie neben dem Feld **Antwortpatei-Ports** auf **Bearbeiten**.
 - b) Fügen Sie die *Ports* hinzu:

- Um einen einzelnen *Port* anzugeben, geben Sie die *Port*-Nummer in das Feld **Einzel** ein.
- Um einen *Portbereich* anzugeben, geben Sie den niedrigsten und den höchsten *Port* des **Bereichs** in die Felder **Bereich** ein.

- c) Klicken Sie auf **Zur Liste hinzuf.**
- d) Wiederholen Sie die Schritte a-c, um alle erforderlichen Ports hinzuzufügen.
- e) Klicken Sie auf **OK**.

10. Wenn der Dienst das *ICMP-Protokoll* verwendet, definieren Sie den *ICMP-Typ* und den *Code* für den Dienst. Klicken Sie auf **Bearbeiten** und geben Sie die Werte in die Felder **Typ** und **Code** ein. Zulässig sind die Werte 0-255.
11. Wenn Sie diesen Dienst verwenden möchten, um eingehenden Datenverkehr zuzulassen, können Sie festlegen, ob Sie außerdem Broadcast- und Multicast-Datenverkehr zulassen wollen.
Diese Art von Datenverkehr wird durch Streaming-Programme erzeugt, wie Webradio oder Web-TV. Um sie zuzulassen, müssen Sie die Kontrollkästchen **Broadcasts zulassen** und **Multicasts zulassen** aktivieren. Normalerweise können Sie diese Kontrollkästchen deaktiviert lassen.
12. Klicken Sie im Dialogfeld **Neuen Dienst hinzufügen** auf **OK**.

Ihr neuer Dienst wird jetzt auf der Registerkarte **Dienste** in der Dienstliste angezeigt. Um den durch den Dienst definierten Datenverkehr zuzulassen oder abzulehnen, müssen Sie den Dienst zu einer *Firewallregel* hinzufügen, die ausgehende Internetverbindungen zulässt.

Erstellen einer Regel

Geben Sie einen Namen für die Regel ein und wählen Sie aus, ob die *Firewallregel* den Datenverkehr zulässt oder ablehnt.

So erstellen Sie eine Regel:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Regeln**.
5. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Neue Regel hinzufügen** wird geöffnet.


6. Geben Sie im Feld **Name** einen Namen für die Regel ein. Verwenden Sie einen möglichst aussagekräftigen Namen.
7. Wählen Sie **Ablehnen** oder **Zulassen**, um den Datenverkehr abzulehnen oder zuzulassen.
8. Um eine Regel zu erstellen, die nur gilt, wenn eine aktive DFÜ-Verbindung besteht, wählen Sie **Diese Regel nur auf DFÜ-Verbindungen anwenden**.

Diese Option ist nur dann relevant, wenn Sie Ihre Internetverbindung über ein Modem oder einen ISDN-Anschluss herstellen. Diese Option können Sie z. B. auswählen, wenn Sie einen Laptop außerhalb Ihres Heimnetzwerks verwenden und über ein Modem oder einen ISDN-Anschluss auf das Internet zugreifen. Außerhalb Ihres Hauses ist der Laptop nicht durch die Firewall des Routers geschützt, daher möchten Sie eventuell eine strengere Regel erstellen, die den gesamten unnötigen eingehenden Datenverkehr ablehnt, und diese Regel außerhalb anwenden. Normalerweise müssen Sie keine Regel erstellen. Die Standardsicherheitsstufe schützt Ihren Computer innerhalb und außerhalb Ihres Hauses.

9. Klicken Sie auf **Weiter >**.

Wählen Sie die *IP-Adressen* aus

Wenden Sie die Regel auf alle Netzwerkverbindungen an oder geben Sie die *IP-Adressen* und Netzwerke an, für die die neue Regel gilt.

 **Hinweis:** Die Optionen für IPv6 sind nur dann verfügbar, wenn Sie Microsoft Windows Vista einsetzen.

So wählen Sie die *IP-Adressen* aus:

1. Wählen Sie eine der folgenden Optionen aus:
 - Um die Regel sowohl auf *IPv4*- als auch auf *IPv6*-Adressen anzuwenden, wählen Sie **Beliebige IP-Adresse**.
 - Damit die Regel auf alle *IPv4*-Adressen angewendet wird, wählen Sie **Beliebige IPv4-Adresse**.
 - Damit die Regel auf alle *IPv6*-Adressen angewendet wird, wählen Sie **Beliebige IPv6-Adresse**.
 - Damit die Regel auf bestimmte *IP-Adressen* und Netzwerke angewendet wird, wählen Sie **Benutzerdefiniert** und klicken Sie auf **Bearbeiten**. Das Dialogfeld **Adressen** wird geöffnet.
 1. Wählen Sie im Dialogfeld **Adressen** eine der folgenden Optionen der Liste **Typ** aus:

Typ	Adressbeispiel
IP-Adresse	192.168.5.16
DNS -Name	www.example.com
IP Bereich	192.168.1.1-192.168.1.63
IP- Subnetz	192.168.88.0/29
IPv6-Adresse	2001:db8:5a3:3:1319:8a2e:370:733
IPv6-Bereich	2001:db8:1234:: - 2001:db8:1234:ffff:ffff:ffff:ffff:ffff
IPv6 Subnetz	2001:db8:1234::/48

2. Geben Sie die **Adresse** in das Feld Adresse ein.
3. Damit die Adresse zur Adressliste hinzugefügt wird, klicken Sie auf **Zur Liste hinzuf.**
4. Wiederholen Sie die Schritte a-c, um alle erforderlichen Adressen zur Adressliste hinzuzufügen.
5. Klicken Sie auf **OK**.

2. Klicken Sie auf **Weiter >**.

Wie wird ein IP- Subnetz definiert?

Wenn Sie ein IP- Subnetz definieren möchten, verwenden Sie eine *Classless Inter-Domain Routing* -(CIDR)-Notation. Dies ist eine Standardnotation, die aus einem *Netzwerkadresse* und einem *Subnetzmaske* besteht. Beispiel:


Netzwerkadresse	Subnetzmaske	CIDR-Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

Dienste und Richtung auswählen

Wählen Sie die Dienste aus, für die die *Firewall- regel* gilt, sowie die Richtung des Datenverkehrs.

So wählen Sie die Dienste und die Richtung aus:

1. Wählen Sie die Dienste aus, auf die Sie die Regel anwenden möchten:
 - Wenn Sie die Regel auf sämtlichen IP-Verkehr anwenden möchten, wählen Sie in der Liste **Gesamter IP-Verkehr** aus.
 - Wenn sich der benötigte Dienst nicht in der Liste befindet, müssen Sie ihn zuerst erstellen.

Das Symbol  wird in der Spalte **Richtung** für die ausgewählten Dienste angezeigt.

2. Wählen Sie für alle Dienste die Richtung des Datenverkehrs aus, auf die die Regel angewendet wird.

Die **Richtung** verläuft von Ihrem Computer in das Internet oder umgekehrt. Um die Richtung auszuwählen, klicken Sie auf das

Symbol  in der Spalte Richtung.

Richtung

Erklärung



Der Dienst wird in beide Richtungen zugelassen oder abgelehnt.



Der Dienst wird zugelassen oder abgelehnt, wenn er aus dem Internet auf Ihren Computer verläuft (eingehend).



Der Dienst wird zugelassen oder abgelehnt, wenn er von Ihrem eigenen Computer ins Internet verläuft (ausgehend).

3. Klicken Sie auf **Weiter >**.

Alarmoptionen auswählen

Wählen Sie aus, wie das Produkt Sie benachrichtigt, wenn die *Firewallregel* Datenverkehr zulässt oder ablehnt.

So wählen Sie die Alarmoption aus:

1. Wählen Sie eine der folgenden Optionen:
 - Wenn Sie nicht benachrichtigt werden möchten, wählen Sie **Kein Alarm**. Es werden keine *Alarme* in das Protokoll der *Alarme* eingetragen und keine *Alarm*-Popups angezeigt. Diese Option sollten Sie auswählen, wenn Sie eine Regel erstellen, die Datenverkehr zulässt.

- Wenn das Produkt *Alarme* in das **Protok** der *Alarme* eintragen soll, wählen Sie Protokoll.
- Wenn das Produkt *Alarme* in das Protokoll der *Alarme* eintragen und *Alarm-Popups* anzeigen soll, wählen Sie **Protokoll und Popup**. Denken Sie daran, dass Sie die *Alarm-Popups* außerdem im Dialogfeld **Alarme von Internet-Schutzschild** einschalten müssen.
- Geben Sie im Feld **Alarm-Text** eine Beschreibung ein, die im Protokoll der *Alarme* und in den Popups angezeigt wird.

2. Klicken Sie auf **Weiter >**.

Die Regel prüfen und übernehmen

Prüfen und übernehmen Sie die neue Regel.

Gehen Sie wie folgt vor:

1. Prüfen Sie die Zusammenfassung der Regel. Falls Sie die Regel bearbeiten müssen, klicken Sie auf **< Zurück**.
2. Wenn Sie mit Ihrer neuen Regel zufrieden sind, klicken Sie auf **Fertig stellen**.

Ihre neue Regel wird jetzt auf der Registerkarte **Regeln** angezeigt. Sie ist automatisch aktiviert. Wenn Sie mehrere Regeln erstellt haben, können Sie nun die Reihenfolge ihrer Priorität festlegen.

Definieren Sie die Prioritätsreihenfolge von Firewallregeln

Wenn Sie mehrere neue *Firewallregeln* erstellt haben, müssen Sie deren Prioritätsreihenfolge festlegen.

Dies kann auch dann erforderlich sein, wenn z. B. eine Regel Datenverkehr ablehnt, den Sie zulassen möchten. In diesem Fall müssen Sie eine neue zulassende Regel erstellen und diese vor die ablehnende Regel verschieben. So wird die zulassende Regel zuerst auf den Datenverkehr angewendet. Sie können lediglich die Prioritätsreihenfolge der Regeln verändern, die Sie selbst erstellt haben.

So legen Sie die Prioritätsreihenfolge fest:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Regeln**.

5. Klicken Sie mit der rechten Maustaste auf die Regel, die Sie verschieben möchten, halten Sie die Maustaste gedrückt, und ziehen Sie die Regel an die neue Position in der Tabelle.

Die Regeln werden jetzt in ihrer neuen Prioritätsreihenfolge auf den Datenverkehr angewendet.

Einen Port öffnen

Sie können einen Port durch die Firewall öffnen, wenn Sie einen Teil des Internetverkehrs zulassen möchten und die Portnummer wissen, die Sie öffnen möchten.

Sie können eventuell nicht Ihre eigenen Regeln zu allen Sicherheitsstufen hinzufügen. Wählen Sie die *Sicherheitsstufe* aus, zu der Sie die neue Regel hinzufügen möchten, bevor Sie den Port öffnen.

Wenn Sie einen Port durch eine Firewall öffnen, erstellen Sie eine neue Firewallregel und zwei neue Dienste.

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Einen Port öffnen**.
3. Geben Sie im Feld **Name** einen Namen für die neue Firewallregel ein.
4. Legen Sie im Feld **Port-Adresse** den Antwortport für die Regel fest. Der Antwortport wird normalerweise in der Produktdokumentation erwähnt.
5. Klicken Sie auf **OK**.

Die neue Regel wird der Liste mit Firewallregeln hinzugefügt und zwei neue Dienste werden auf der Firewalldienstliste für TCP- und UDP-Protokolle mit der angegebenen Portnummer erstellt.

Eine Firewallregel ein- oder ausschalten

Sie können eine *Firewallregel* vorübergehend ausschalten, um Datenverkehr zuzulassen, den die Regel ablehnt.

Sie können die Regeln ein- bzw. ausschalten, die Sie selbst erstellt haben.

So schalten Sie eine Regel ein oder aus:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.

4. Klicken Sie auf die Registerkarte **Regeln**.
5. Führen Sie einen der folgenden Schritte durch:
 - Wenn Sie eine Regel abschalten möchten, müssen Sie das Häkchen in der Spalte **Aktiviert** entfernen.
 - Wenn Sie die Regel einschalten möchten, aktivieren Sie das Kontrollkästchen.

Abhängig von Ihrer Auswahl ist die Firewallregel nun ein- bzw. ausgeschaltet.

Anzeigen der *Firewallregeln*




Sie können die gerade aktiven *Firewallregeln* anzeigen, um herauszufinden, wie die *Firewall* den Datenverkehr auf Ihrem Computer zulässt oder blockiert.

Jede Sicherheitsstufe besitzt einen eigenen Satz aktiver *Firewallregeln*. So zeigen Sie die Regeln an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Regeln**.

Sie können eine Regelliste anzeigen, die folgende Informationen enthält:

Feld	Beschreibung
Aktiviert	Wenn das Kontrollkästchen aktiviert ist, ist die Regel aktuell aktiv. Wenn das Kontrollkästchen leer ist, ist die Regel aktuell deaktiviert.
Name/Kommentar	Name der Regel. Es gibt zwei Typen von Regeln: <ul style="list-style-type: none">• Vordefinierte Regeln: Diese Regeln werden grau dargestellt. Sie sind für die aktuell ausgewählte <i>Sicherheitsstufe</i> vordefiniert.• Ihre eigenen Regeln: Wenn Sie Ihre eigenen Regeln hinzugefügt haben, werden

Feld	Beschreibung
	diese über der Zeile Ihre Regeln werden hier hinzugefügt in Schwarz dargestellt.
Typ	Regeltyp: <ul style="list-style-type: none"> •  : Diese Regel lässt den Datenverkehr zu. •  : Diese Regel lehnt den Datenverkehr ab. •  : Diese Regel generiert Alarme im Alarmprotokoll und zeigt möglicherweise ein Alarm-Popup an, wenn die Regel Netzwerkdatenverkehr zulässt oder ablehnt.
Remote-Host	<i>IP-Adressen</i> und Netzwerke, für die die Regel gilt. Wenn die Regel für alle <i>IP-Adressen</i> gilt, enthält dieses Feld einen der folgenden Werte: <ul style="list-style-type: none"> • 0.0.0.0/0, ::/0: Die Regel gilt für alle <i>IPv4</i>- und <i>IPv6</i>-Adressen. • 0.0.0.0/0: Die Regel gilt für alle <i>IPv4</i>-Adressen. • ::/0: Die Regel gilt für alle <i>IPv6</i>-Adressen.

5. Um die Einzelheiten einer Regel anzuzeigen, wählen Sie in der Liste eine Regel aus und klicken Sie auf **Details**.

- Wenn die Regel vordefiniert wurde, wird das Dialogfeld **Regeldetails** geöffnet, auf dem die vordefinierte Regel angezeigt wird. Klicken Sie auf **OK**, nachdem Sie die Details gelesen haben.
- Wenn Sie die Regel selbst hinzugefügt haben, wird das Dialogfeld **Regeldetails** geöffnet. Klicken Sie auf **Weiter >**, bis das

Dialogfeld mit der Zusammenfassung der Regel angezeigt wird. Klicken Sie auf **Abbrechen**, nachdem Sie die Details gelesen haben.

Einzelheiten der *Firewallregel*

Zu den Einzelheiten der *Firewallregel* gehören der Name und der Typ der Regel, die *IP-Adressen* und Dienste, für die die Regel gilt, sowie die Alarmeinstellungen.

Das Dialogfeld **Regeldetails** enthält folgende Informationen:

Feld	Beschreibung
Name	Name der Regel.
Typ	Typ der Regel, der definiert, ob die Regel den Netzwerkdatenverkehr zulässt oder ablehnt.
Remote-Adresse	<p><i>IP-Adressen</i> und Netzwerke, für die die Regel gilt. Wenn die Regel für alle <i>IP-Adressen</i> gilt, enthält das Feld einen der folgenden Werte:</p> <ul style="list-style-type: none"> • 0.0.0.0/0, ::/0: Die Regel gilt für alle <i>IPv4</i>- und <i>IPv6</i>-Adressen. • 0.0.0.0/0: Die Regel gilt für alle <i>IPv4</i>-Adressen. • ::/0: Die Regel gilt für alle <i>IPv6</i>-Adressen.
Dienste	<p>Die Spalte Dienst enthält die <i>Firewalldienste</i>, die in der Regel enthalten sind.</p> <p>Die Spalte Richtung zeigt an, ob die Regel für eingehende Dienste (ein), ausgehende Dienste (aus) oder für beide gilt.</p>
Alarmausgabe	Zeigt, ob die Regel Alarmmeldungen generiert und Alarm-Popups einblendet.

Feld	Beschreibung
Alarmtext	Wenn die Regel Alarme generiert, ist dies der Alarmtext, der im Alarmprotokoll sowie im Popup-Fenster angezeigt wird.

Ändern einer Firewallregel

Sie können nur eine *Firewallregel* ändern, die Sie selbst erstellt haben.

So ändern Sie eine Regel:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Regeln**.
5. Wählen Sie die Regel aus und klicken Sie auf **Details**.
Das Dialogfeld **Regeldetails** wird geöffnet.
6. Nehmen Sie schrittweise die erforderlichen Änderungen vor. Klicken Sie auf **Weiter >**, um zum jeweils nächsten Schritt zu gelangen.
7. Prüfen Sie im Dialogfeld **Regeldetails** Ihre Änderungen.
8. Wenn die Regel in Ordnung ist, klicken Sie auf **Fertig stellen**.

Ihre Änderungen werden auf die Regel angewendet.

Beispiele zum Erstellen von Firewallregeln

Eine neue Firewallregel erstellen Sie, wenn Sie ein neues Netzwerkspiel spielen oder Dateien in Ihrem Heimnetzwerk freigeben möchten.


So erstellen Sie eine Regel für ein Netzwerkspiel

Dieses Beispiel zeigt, wie Sie *Firewalldienste* und eine *Firewallregel* für ein imaginäres Netzwerkspiel namens Game_1 erstellen.

Um die *Firewalldienste* zu erstellen, müssen Sie wissen, welche *Protokolle* das Spiel verwendet. Sie müssen außerdem wissen, welche *Ports* das Spiel für eingehende Verbindungen vom Spiele-Server an Ihren Computer verwendet. In diesem Fall liegen folgende Daten vor:

Protokoll	Porttyp	Standort	Ports
UDP	Ausgangspartei	Game-Server	1024
UDP	Antwortpartei	Eigener Computer	8889, 9961
TCP	Ausgangspartei	Spiele-Server	1025

Protokoll	Porttyp	Standort	Ports
TCP	Antwortpartei	Eigener Computer	17475, 9961

 **Hinweis:** Sie müssen keine Firewalldienste oder eine Firewallregel für ausgehende Verbindungen von Ihrem Computer zum Spiele-Server erstellen.

So erstellen Sie die Dienste und eine Regel für die eingehenden Verbindungen:


1. Fügen Sie den neuen Dienst wie folgt hinzu:

Schritt	Beispiel
Geben Sie einen Namen für den ersten Dienst ein	Service_Game_1_UDP
Wählen Sie das <i>Protokoll</i> aus	UDP
Geben Sie die <i>Ausgangspartei-Port</i> ein	1024
Geben Sie die <i>Antwortpartei-Ports</i> ein	8889, 9961
Geben Sie einen Namen für den zweiten Dienst ein	Service_Game_1_TCP
Wählen Sie das zweite <i>Protokoll</i> aus	TCP
Geben Sie die <i>Ausgangspartei-Port</i> ein	1025
Geben Sie die <i>Antwortpartei-Ports</i> ein	17475, 9961

Nachdem Sie die Dienste hinzugefügt haben, werden diese in der Dienstliste angezeigt.

2. Fügen Sie eine neue *Firewallregel* wie folgt hinzu:

Schritt	Beispiel
Geben Sie einen Namen für die Regel ein	Rule_Game_1
Wählen Sie den Regeltyp aus	Zulassen
Wählen Sie die <i>IP-Adressen</i> aus	Beliebige Adresse
Wählen Sie die Dienste aus	Service_Game_1_UDP, Service_Game_1_TCP

Schritt	Beispiel
Wählen Sie die Richtung aus	 (vom Internet an Ihren Computer)
Wählen Sie den <i>Alarmtyp</i> aus	Kein <i>Alarm</i>

Nachdem Sie die Regel hinzugefügt haben, wird diese aktiv und in der Regelliste angezeigt.

So erstellen Sie eine Regel für die gemeinsame Nutzung von Dateien in einem Heimnetzwerk

In diesem Beispiel wird eine neue *Firewallregel* für die Windows-Dateifreigabe erstellt, um Dateien auf den Computern eines Heimnetzwerks gemeinsam zu nutzen.

Wenn Sie in Ihrem Netzwerk einen *Router* verwenden, prüfen Sie die DHCP-Einstellungen (Dynamic Host Configuration Protocol) Ihres Routers, um den IP-Adressbereich zu ermitteln, der Ihrem Heimnetzwerk zugewiesen ist. Weitere Informationen finden Sie in der Dokumentation Ihres Routers.

Der Bereich für die *IP-Adresse* für Heimnetzwerke ist in der Regel 192.168.1.1 - 192.168.1.254. Wenn Sie Dateien auf all Ihren Computern freigeben möchten, müssen Sie auf allen Computern dieselbe Regel erstellen.

So erstellen Sie die Regel:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Regeln**.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie einen Namen ein und wählen Sie den Regeltyp aus:



Schritt	Beispiel
Geben Sie einen Namen für die Regel ein	FileSharing
Wählen Sie den Regeltyp aus	Zulassen

7. Wählen Sie die *IP-Adressen* aus:

Schritt	Beispiel
1. Klicken Sie auf Benutzerdefiniert .	192.168.1.1 -
2. Klicken Sie auf Bearbeiten .	192.168.1.254
3. Wählen Sie IP-Bereich und geben Sie die Adressen Ihrer Computer in das Feld ein.	
4. Klicken Sie auf Zur Liste hinzuf.	

8. Wählen Sie die Dienste und die Richtung aus:

Schritt	Beispiel
Wählen Sie die von der Windows-Dateifreigabe verwendeten Dienste aus	<ul style="list-style-type: none"> • SMB über TCP/IP (TCP) • SMB über TCP/IP (UDP) • Windows-Dateifreigabe und Netzwerkdrucker • Windows-Netzwerksuche

Wählen Sie für beide Dienste die Richtung aus  ←  (vom Internet auf Ihren Computer)

9. Wählen Sie den Alarmtyp aus:


Schritt	Beispiel
Wählen Sie den Alarmtyp aus	Kein <i>Alarm</i>

10. Prüfen Sie die Zusammenfassung der Regel und klicken Sie auf **Fertig stellen**.

Ihre neue Regel wird auf der Registerkarte **Regeln** in der Regelliste angezeigt. Sie ist automatisch aktiviert.

11. Prüfen Sie, ob die Regel funktioniert.

Verwenden Sie hierbei die Windows-Dateifreigabe, um einen Ordner oder eine Datei freizugeben, und prüfen Sie, ob Sie von allen Computern auf die Datei oder den Ordner zugreifen können.

-  **Tipp:** Wenn Sie den Drucker in Ihrem Heimnetzwerk freigeben möchten, dann erstellen Sie eine ähnliche Regel. In diesem Fall müssen Sie lediglich eine Regel erstellen, die auf dem Computer, an dem der Drucker angeschlossen ist, eingehenden Datenverkehr zulässt.

Firewalleinstellungen

Auf der Registerkarte **Einstellungen** können Sie die *IPv6*-Einstellungen und die Alarmstufe ändern sowie den gesamten Datenverkehr zwischen Computern in einem Heimnetzwerk zulassen.

Die Registerkarte **Einstellungen** enthält außerdem das Feld **IP-Fragmente blockieren, die kürzer sind als**. Die *Firewall* blockiert *IP-Paket*fragmente, die kürzer sind als der in diesem Feld angezeigte Grenzwert. Kurze *IP-Paket*fragmente weisen möglicherweise auf einen *Fragmentationsangriff* hin, der Ihren Computer zum Absturz bringen kann. Sie sollten den in diesem Feld angegebenen Grenzwert möglichst nicht ändern.

Ändern Sie die *IPv6*-Einstellungen

Auf der Registerkarte **Einstellungen** können Sie festlegen, wie die *Firewall* den *IPv6*-Datenverkehr behandelt.

Wenn Sie Microsoft Windows Vista als Betriebssystem einsetzen, können Sie entweder den gesamten *IPv6*-Datenverkehr blockieren oder normale *Firewallregeln* auf den Datenverkehr anwenden. Wenn Sie ein anderes Betriebssystem einsetzen, können Sie den gesamten *IPv6*-Datenverkehr entweder blockieren oder zulassen.

So ändern Sie die *IPv6*-Einstellungen:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Um festzulegen, wie die *Firewall* den *IPv6*-Datenverkehr behandelt, wählen Sie in der Liste **Filteroptionen für IPv6-Datenverkehr auswählen** eine der folgenden Optionen aus:
 - Wenn Sie Microsoft Windows Vista verwenden:
 - **Blockieren:** Blockiert den gesamten *IPv6*-Datenverkehr. Es empfiehlt sich, diese Option aktiviert zu lassen.

- **Normal:** Normale *Firewallregeln* definieren, ob der *IPv6*-Datenverkehr zugelassen oder blockiert ist. Diese Option können Sie auswählen, wenn Sie auf Ihrem Computer das *IPv6*-Protokoll verwenden.
- Wenn Sie ein anderes Betriebssystem einsetzen:
 - **Blockieren:** Der gesamte *IPv6*-Datenverkehr wird blockiert. Es empfiehlt sich, diese Option aktiviert zu lassen.
 - **Zulassen:** Lässt den gesamten *IPv6*-Datenverkehr zu. Diese Option können Sie auswählen, wenn Sie auf Ihrem Computer das *IPv6*-Protokoll einsetzen.
 - 👉 **Hinweis:** Den gesamten *IPv6*-Datenverkehr zuzulassen, stellt ein Sicherheitsrisiko dar, weil auf den *IPv6*-Datenverkehr keine *Firewallregeln* angewendet werden.

6. Klicken Sie auf **OK**.

Ihre Änderungen der *IPv6*-Einstellungen sind jetzt aktiv.

So kann eine Internetverbindung gemeinsam genutzt werden

Wenn Sie eine Internetverbindung Ihres Computers mit Ihrem restlichen Heimnetzwerk verwenden möchten, müssen Sie dem gesamten Datenverkehr zwischen diesen Computern gestatten, die Firewall zu passieren.

👉 **Hinweis:**

Lassen Sie den gesamten Datenverkehr nur dann die Firewall passieren, wenn Sie die Gemeinsame Internetnutzung von Windows verwenden. Wenn Sie andere Ressourcen freigeben möchten - wie Laufwerke, Dateien oder Drucker - sollten Sie hierfür neue Firewallregeln erstellen.

Sie können den gesamten Datenverkehr durch die Firewall passieren lassen, indem Sie die Verbindung zwischen dem Heimnetzwerk und dem Computer mit der Internetverbindung als vertrauenswürdig definieren. Sie können eine *Vertrauenswürdige Netzwerkschnittstelle* definieren, wenn:


- Sie haben einen Computer mit einer Internetverbindung.

- Dieser Computer besitzt zwei *Netzwerkkarten*: Eine für die Internetverbindung und die andere für die Verbindung mit dem Heimnetzwerk.
- Sie haben auf dem Computer, der die Internetverbindung besitzt, in Windows die Gemeinsame Nutzung der Internetverbindung aktiviert.
- Sie haben Ihr Produkt mit dem Internet-Schutzschild auf allen Computern installiert. So können Sie sicher sein, dass Sie kein Risiko eingehen, wenn Sie zwischen Ihren Computern eine vertrauenswürdige Schnittstelle definieren.

Um die vertrauenswürdige Netzwerkschnittstelle zu definieren, müssen Sie die Netzwerkkarte (Adapter) auswählen, über die der Computer mit dem Heimnetzwerk verbunden ist.

So wählen Sie die Netzwerkkarte auf dem Computer mit der Internetverbindung aus:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Firewall**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Wählen Sie in der Liste **Vertrauenswürdiger Netzwerkadapter** die *Netzwerkkarte* (Adapter) aus, über die Ihr Computer mit dem Heimnetzwerk verbunden ist. Die *IP-Adresse* des Computers wird im Feld **IP-Adresse** angezeigt.

 **Hinweis:** Da die *Firewall* den Datenverkehr über die ausgewählte Netzwerkschnittstelle zulässt, müssen Sie sicherstellen, dass Sie nicht die Internetschnittstelle als vertrauenswürdige auswählen. Andernfalls schützt die Firewall Ihren Computer nicht mehr.

6. Klicken Sie auf **OK**.

Die *Firewall* lässt nun den gesamten Datenverkehr zwischen dem Computer mit der Internetverbindung und Ihrem Heimnetzwerk zu. Sie können das Internet jetzt von allen Computern aus nutzen.

Wie sieht es bei Verwendung einer digitalen TV-Karte aus?

Wenn Sie eine digitale TV-Karte verwenden und das Fernsehbild friert ein, dann müssen Sie auch

die Schnittstelle zum Fernseher als vertrauenswürdig definieren.

Kontrollieren von Internetverbindungen für Anwendungen

Die Anwendungssteuerung verhindert, dass schädliche Programme eine Verbindung mit dem Internet herstellen.

Die Anwendungssteuerung schützt Sie hauptsächlich vor ausgehenden Bedrohungen, die durch Programme auf Ihrem Computer verursacht werden. Im Normalfall öffnet die Anwendungssteuerung ein Popup-Fenster, sobald ein Programm versucht, eine Verbindung zum Internet herzustellen. In diesem Popup-Fenster können Sie die Verbindung dann zulassen oder ablehnen:

- Wenn Sie darauf vertrauen, dass das Programm sicher ist, können Sie die Verbindung zulassen. Sie können z. B. davon ausgehen, dass das Programm sicher ist, wenn Sie es gerade selbst gestartet haben. Wenn Sie die Verbindung zulassen, öffnet die *Firewall* für das Programm einen *Port* und lässt die Verbindung so lange zu, wie das Programm gestartet ist. Wenn Sie das Programm beenden, schließt die Firewall den *Port*.
- Wenn Sie dem Programm nicht vertrauen, müssen Sie die Verbindung ablehnen. Ein Programm kann z. B. unsicher sein, wenn Sie es nicht kennen oder nicht selbst installiert haben.

Abhängig von Ihren Einstellungen für die Anwendungssteuerung werden möglicherweise keine Popup-Fenster für Programme angezeigt, die von der Systemsteuerung als sicher eingestuft werden. Diese Programme sind berechtigt, automatisch eine Verbindung zum Internet herzustellen.

Die Anwendungssteuerung fragt Sie außerdem, ob Sie Verbindungen aus dem Internet zu den Programmen auf Ihrem Computer zulassen möchten. Dies ist z. B. der Fall, wenn Sie Skype verwenden.

- 👉 **Hinweis:** Schalten Sie die Anwendungssteuerung nicht aus, wenn ein Programm auf Ihrem Computer nicht funktioniert. Dies reduziert die Schutzstufe Ihres Computers. Ändern Sie stattdessen die Einstellungen der Anwendungssteuerung oder die *Firewallregeln*.

Was ist der Unterschied zwischen der Firewall und der Anwendungssteuerung?

Eine Firewall bietet grundlegenden Schutz auf Netzwerkebene, wohingegen Sie mithilfe der Anwendungskontrolle die Verwendung bestimmter Programme steuern können. Die Firewall schützt Sie vor Bedrohungen, die durch Verbindungen aus dem Internet mit Ihrem Computer verursacht werden (eingehende Verbindungen). Die Firewall gestattet bzw. verweigert Verbindungen auf der Grundlage der von den Verbindungen verwendeten IP-Adressen.

Die Anwendungssteuerung schützt Sie in erster Linie vor Bedrohungen, die durch Verbindungen von Ihrem Computer ins Internet verursacht werden (ausgehende Verbindungen). Die Anwendungssteuerung gestattet bzw. verweigert Verbindungen auf der Grundlage der Programme, die die Verbindungen erstellen.

Vorgehensweise, wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird

Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird, müssen Sie entscheiden, ob Sie den Verbindungsversuch für das im Popup angegebene Programm zulassen oder ablehnen möchten.

Popups der Anwendungssteuerung können auf schädliche Aktivitäten hinweisen, wie auf *Trojaner*, *Würmer* oder *Spyware*. Andererseits werden auch Popups angezeigt, wenn Sie die Programme auf Ihrem Computer normal verwenden.

So lassen Sie einen Verbindungsversuch zu oder lehnen diesen ab:

1. Prüfen Sie im Popup-Fenster die Informationen über den Verbindungsversuch.
2. Um die Details des Verbindungsversuchs anzuzeigen - wie den Namen des Programms und die IP-Adresse des Remote-Computers - klicken Sie auf **Details >>**.
3. Wenn Sie möchten, dass für das aktuelle Programm in Zukunft keine Popups mehr angezeigt werden, aktivieren Sie das Kontrollkästchen **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen**.
4. Lassen Sie die Verbindung entweder zu oder lehnen Sie sie ab:
 - Klicken Sie auf **Zulassen**, wenn Sie sicher sind, dass der Verbindungsversuch sicher ist. Sie können die Verbindung in den folgenden Fällen zulassen:

Popup-Typ	Beschreibung	Klicken Sie auf Zulassen wenn...
Neuer Verbindungsversuch (ausgehend)	Ein <i>Client</i> -Programm auf Ihrem Computer versucht, eine Verbindung zum Internet herzustellen.	Sie haben dieses Programm zum ersten Mal selbst gestartet.
Geänderte Anwendung (ausgehend)	Ein <i>Client</i> -Programm auf Ihrem Computer versucht, eine Verbindung zum Internet herzustellen, es wurde aber seit der letzten Verbindung geändert.	Sie haben das Programm seit seiner letzten Verwendung auf Ihrem Computer aktualisiert.
Neue Serveranwendung (eingehend)	Ein Programm auf Ihrem Computer versucht als <i>Server</i> zu agieren und möchte anfangen, eingehende Verbindungen zu erwarten.	Sie haben das <i>Server</i> programm selbst auf Ihrem Computer gestartet.
Geänderte Anwendung (eingehend)	Ein <i>Server</i> programm auf Ihrem Computer möchte auf eingehende Verbindungen warten, es wurde aber seit dem	Sie haben das <i>Server</i> programm seit der letzten Verwendung auf Ihrem Computer aktualisiert.

Popup-Typ	Beschreibung	Klicken Sie auf Zulassen wenn...
	letzten Verbindungsversuch geändert.	

- Klicken Sie auf **Ablehnen**, wenn Sie nicht sicher sind, ob der Verbindungsversuch sicher ist.

Abhängig von der ausgewählten Aktion wird die **Anwendungen** entweder zugelassen oder abgelehnt. Wenn Sie das Kontrollkästchen **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen** aktiviert haben, wird das Programm auf der Registerkarte Verbindung zur Liste der zugelassenen bzw. abgelehnten Programme hinzugefügt. Es werden für dieses Programm keine Popup-Fenster über Verbindungsversuche mehr angezeigt.

Sichere und unsichere Programme und Verbindungsversuche

Bevor Sie in einem Popup-Fenster der Anwendungssteuerung eine Verbindung zulassen, sollten Sie prüfen, ob das Programm sicher ist.

Welche Programme und Verbindungsversuche können als sicher angesehen werden?

- Ein bekanntes Programm, das Sie selbst gestartet haben.
- Microsoft Windows-Betriebssystem, das für die Updatedienste eine Verbindung zum Internet herstellt.

Welche Programme und Verbindungsversuche sollten als unsicher angesehen werden?

- Alle Programme, die Sie von einer unbekanntem Quelle erhalten haben.
- Alle Programme, die Sie nicht selbst installiert haben oder die Sie nicht kennen.
- Alle Programme, die Sie als sicher ansehen, die aber versuchen, eine Verbindung zum Internet herzustellen oder als *Server* zu agieren, ohne dass Sie sie gestartet haben.

Verbindungen für Programme zulassen oder ablehnen

Sie können Internetverbindungen für Programme auf der Registerkarte **Anwendungen** zulassen oder ablehnen.

Sie können z. B. eine Verbindung für ein Programm zulassen, die Sie versehentlich im Popup-Fenster der Anwendungssteuerung abgelehnt haben.


Standardmäßig enthält die Registerkarte **Anwendungen** die folgenden Programme:

- Wenn die Option **Bei neuen Anwendungen nachfragen** aktiviert ist: Programme, die Sie zugelassen oder abgelehnt haben und für die Sie im Popup-Fenster der Anwendungssteuerung die Option **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen** ausgewählt haben.
- Wenn die Option **Neue Anwendungen zulassen und protokollieren** aktiviert ist: zugelassene Programme.
- Das Programm, das Sie auf dieser Registerkarte manuell zur Liste der Programme hinzugefügt haben.

Diese Registerkarte enthält keine automatisch zugelassenen Betriebssystemprogramme oder Programme, die die Systemsteuerung als sicher einstuft.

So lassen Sie die Verbindung für ein Programm zu oder lehnen diese ab:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Anwendungssteuerung**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie das Programm aus und klicken Sie auf **Details**.
Das Dialogfeld **Anwendungsdetails** wird geöffnet.
6. Wählen Sie unter **Client-Verbindung (ausgehend)** eine passende Option:
 - **Ablehnen**: Wenn Sie ablehnen möchten, dass das Programm eine Verbindung mit dem Internet herstellt, wenn es das nächste Mal gestartet wird.
 - **Zulassen**: Wenn Sie zulassen möchten, dass das Programm eine Verbindung mit dem Internet herstellt, wenn es das nächste Mal gestartet wird.

- **Auffordern:** Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt werden soll, wenn das Programm das nächste Mal versucht, eine Verbindung mit dem Internet herzustellen. In diesem Popup-Fenster können Sie die Verbindung entweder zulassen oder ablehnen.
7. Wählen Sie unter **Server-Verbindung (eingehend)** eine geeignete Option:
- **Ablehnen:** Wenn Sie Verbindungen aus dem Internet zu dem Programm ablehnen möchten.
 - **Zulassen:** Wenn Sie Verbindungen aus dem Internet zu dem Programm zulassen möchten.
 - **Auffordern:** Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt werden soll, wenn das nächste Mal versucht wird, eine Verbindung aus dem Internet zu dem Programm herzustellen. In diesem Popup-Fenster können Sie die Verbindung entweder zulassen oder ablehnen.
8. Klicken Sie auf **OK**.
-  **Tipp:** Sie können Internetverbindungen für ein neues Programm bereits ablehnen oder zulassen, bevor Sie beginnen, es zu verwenden. Hierzu klicken Sie auf die Schaltfläche **Hinzufügen** und wählen die Programmdatei aus. Anschließend können Sie für das Programm eingehende oder ausgehende Verbindungen entweder zulassen oder ablehnen.

Popup-Fenster der Anwendungssteuerung ein- und ausschalten

Sie können die Popup-Fenster der Anwendungssteuerung ein- bzw. ausschalten.

Wenn Sie Popup-Fenster der Anwendungssteuerung ausschalten, lässt das Produkt automatisch Verbindungen für alle Programme zu.

So schalten Sie die Popup-Fenster der Anwendungssteuerung ein oder aus:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Anwendungssteuerung**.
4. Klicken Sie auf die Registerkarte **Einst**.

5. Wählen Sie eine der folgenden Optionen:

- **Neue Anwendungen zulassen und protokollieren:** Wählen Sie diese Option, wenn Sie die Popup-Fenster der Anwendungssteuerung ausschalten möchten.
- **Bei neuen Anwendungen nachfragen:** Wählen Sie diese Option, wenn Sie die Popup-Fenster der Anwendungssteuerung einschalten möchten. Sobald ein neues Programm zum ersten Mal versucht, eine Verbindung herzustellen, wird ein Popup-Fenster eingeblendet.

6. Wenn für Programme, die von der Systemsteuerung als sicher eingestuft werden, keine Popup-Fenster der Anwendungssteuerung angezeigt werden sollen, wählen Sie **Keine Aufforderung für Anwendungen, die durch die Systemsteuerung identifiziert wurden**.

Lassen Sie dieses Kontrollkästchen möglichst aktiviert.

7. Klicken Sie auf **OK**.

Abhängig von Ihrer Auswahl, sind die Popup-Fenster der Anwendungssteuerung nun entweder ein- oder ausgeschaltet.

So verfahren Sie, wenn ein Programm nicht mehr funktioniert

Wenn Sie ein neues Programm zum ersten Mal einsetzen, z. B. ein Netzwerkspiel, funktioniert es möglicherweise nicht, wenn es keine Verbindung zum Internet herstellen kann.

Dies kann z. B. aus folgenden Gründen passieren:

- Ihre aktuelle *Sicherheitsstufe* ist sehr streng und lehnt Internetverbindungen für die meisten Ihrer Programme ab, auch für das gerade verwendete Netzwerkspiel.
- Sie haben ein Popup-Fenster der Anwendungssteuerung übersehen und das Popup ist noch im Hintergrund aktiv.
- Sie haben die Verbindung in dem Popup versehentlich abgelehnt.

Gehen Sie wie folgt vor, um sicherzustellen, dass das Programm eine Verbindung mit dem Internet herstellen kann:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Prüfen Sie neben dem **Internet-Schutzschild** die aktuelle *Sicherheitsstufe*.

Wenn es eine sehr strenge Stufe ist, stellen Sie sie auf eine weniger strenge ein:


- a) Klicken Sie auf **Ändern**.
 - b) Lesen Sie sorgfältig die Beschreibung der *Sicherheitsstufe*.
 - c) Wählen Sie eine geeignete Sicherheitsstufe aus und klicken Sie auf **OK**.
3. Starten Sie das Programm und prüfen Sie, ob es jetzt funktioniert.
4. Wenn das Programm nicht funktioniert, schalten Sie die Popups der Anwendungssteuerung vorübergehend aus, um sämtliche Verbindungen für neue Programme zuzulassen.
- a) Klicken Sie hierfür neben der **Anwendungssteuerung** auf **Ändern**.
Die Seite mit den erweiterten Einstellungen für die **Anwendungssteuerung** wird angezeigt.
 - b) Wählen Sie **Neue Anwendungen zulassen und protokollieren** aus, und klicken Sie auf **OK**.
5. Starten Sie das Programm und prüfen Sie, ob es jetzt funktioniert.
6. Wenn das Programm funktioniert, schalten Sie die Popups der Anwendungssteuerung wieder ein.
- a) Klicken Sie hierfür neben der **Anwendungssteuerung** auf **Ändern**.
Die Seite mit den erweiterten Einstellungen für die **Anwendungssteuerung** wird geöffnet.
 - b) Wählen Sie **Bei neuen Anwendungen nachfragen** aus, und klicken **OK**.

Verhindern von Eindringungsversuchen

Intrusion Prevention schützt Sie vor Netzwerkangriffen, die sich gegen offene *Ports* Ihres Computers richten.

Intrusion Prevention verwendet vordefinierte Regeln, mit denen Netzwerkangriffe erkannt werden. Diese Regeln enthalten Informationen über bekannten böartigen Datenverkehr. Wenn die Intrusion Prevention Datenverkehr erkennt, der mit einer Regel übereinstimmt, wird der Datenverkehr blockiert (sofern die Option **Blockier. und protok** aktiviert ist) und im *Alarm*protokoll des Internet-Schutzschilds ein Alarm erzeugt. Sofern Sie entsprechende Einstellungen vorgenommen haben, wird außerdem ein Alarm-Popup des Internet-Schutzschilds angezeigt.

Intrusion Prevention erkennt und verhindert böartigen Datenverkehr der durch Netzwerkwürmer wie den Wurm Sasser verursacht wird. Der Wurm Sasser infiziert ungeschützte Systeme, indem er am TCP-Port 445 böartigen Datenverkehr an den Microsoft-Dienst für die Netzwerkfreigabe sendet. Dieser Dienst wird für die Freigabe von Druckern in einem Netzwerk verwendet. Der Wurm öffnet eine TCP-Verbindung zu dem Port und sendet böartigen Datenverkehr über den Port. Der Datenverkehr verursacht einen Overflow und sorgt unter Umständen dafür, dass das gesamte System abstürzt.

 **Hinweis:** Schalten Sie die Intrusion Prevention nicht aus. Sonst verringert sich die Schutzstufe Ihres Computers.

Welcher Unterschied besteht zwischen der Firewall und Intrusion Prevention?

Im Unterschied zur Firewall blockiert Intrusion Prevention nur Datenverkehr, der als böartig eingestuft wird, und lässt den übrigen Datenverkehr den Port passieren. Die Firewall lässt entweder den gesamten Datenverkehr über den Port zu oder blockiert ihn.

Wählen Sie aus, wie Eindringungsversuche behandelt werden

Auf der Registerkarte **Eindringenschutz** können Sie auswählen, wie Eindringungsversuche behandelt werden.

Die Eindringungsversuche können entweder automatisch blockiert und protokolliert oder lediglich protokolliert werden.

So wählen Sie aus, wie Eindringungsversuche behandelt werden:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Eindringenschutz**.
4. Wählen Sie eine der folgenden Optionen:
 - **Blockieren und Versuch protokollieren**: Wählen Sie diese Option, wenn Sie Eindringversuche sowohl blockieren als auch protokollieren möchten. Die Versuche werden blockiert, und die Informationen zu den Versuchen werden im Dialogfeld **Alarme von Internet-Schutzschild** angezeigt.
 - **Protokollieren**: Wählen Sie diese Option aus, wenn Sie nur die Eindringversuche protokollieren möchten. Die Informationen über die Versuche werden im Dialogfeld **Alarme von Internet-Schutzschild** angezeigt.
5. Wenn Sie möchten, dass ein Popup-Fenster mit einem **Alarm von Internet-Schutzschild** angezeigt wird, wenn ein Eindringungsversuch vermutet wird, wählen Sie **Alarm anzeigen, wenn ein Eindringungsversuch vermutet wird**.
6. Klicken Sie auf **OK**.

Auf der Seite **Internet-Schutzschild** werden jetzt die geänderten Einstellungen für Intrusion Prevention angezeigt.


Kontrollieren von *DFÜ-Verbindungen*

Der *Dialerschutz* verhindert, dass böswillige *Dialerprogramme* Verbindungen zu kostenpflichtigen Telefonnummern mit einem hohen Minutenpreis herstellen.

Böswillige *Dialerprogramme* versuchen möglicherweise, Ihre Internetverbindung zu schließen und eine neue *DFÜ-Verbindung* zu einer anderen Telefonnummer herzustellen. Die Verbindung zu dieser Nummer kann sehr teuer sein und kommt dem Hersteller des *Dialerprogramms* zugute.

Durch den Einsatz des *Dialerschutzes* können Sie verhindern, dass diese böswilligen *Dialerprogramme* Verbindungen beenden und neue herstellen. Der *Dialerschutz* verhindert außerdem, dass versehentlich falsche oder mit hohen Kosten verbundene Nummern angewählt werden. Sie können sicherstellen, dass *DFÜ-Verbindungen* sicher sind, indem Sie folgende Definitionen vornehmen:

- die Nummern, zu denen Programme eine *DFÜ-Verbindung* herstellen können und
- die Programme, die berechtigt sind, *DFÜ-Verbindungen* zu beenden.

 **Hinweis:** Der *Dialerschutz* ist für Benutzer, die für ihre Internetverbindung ein Modem oder eine *ISDN-Verbindung* verwenden.

Virus & Spy Protection erkennt die böswilligen *Dialerprogramme* als *Spyware* und kann diese von Ihrem Computer entfernen. Wenn ein neues böswilliges *Dialerprogramm* nicht erkannt wird, verhindert der *Dialerschutz*, dass dieses *Dialerprogramm* *DFÜ-Verbindungen* herstellt.

Wenn Sie den Verdacht haben, dass sich auf Ihrem Computer ein nicht erkannter *Dialer* befindet, können Sie die *Dialerdatei* als Muster an F-Secure schicken. Anschließend aktualisiert F-Secure die *Viren- und Spyware-Definitionsdatenbanken* und Sie können Ihren Computer erneut scannen. Der *Dialer* wird dann erkannt und kann von Ihrem Computer entfernt werden.

Vorgehensweise bei einem Popup-Fenster des Dialerschutzes

Wenn das Popup-Fenster " **Neuer Verbindungsversuch**" angezeigt wird, können Sie die *DFÜ-Verbindung* entweder zulassen oder ablehnen.

So lassen Sie eine *DFÜ-Verbindung* zu oder lehnen diese ab:

1. Prüfen Sie den Namen des Programms.
2. Prüfen Sie die Telefonnummer.
3. Lassen Sie die *DFÜ-Verbindung* entweder zu oder lehnen Sie sie ab:
 - Wenn die Nummer in Ordnung ist (der Ihres Service Providers entspricht) und das Programm von Ihnen selbst gestartet wurde:
 1. Wählen Sie **Diese Einstellung für die Zukunft speichern**.
 2. Klicken Sie auf **Zulassen**.
 - Wenn die Nummer falsch ist oder wenn die Verbindung automatisch hergestellt wurde:
 1. Wählen Sie **Diese Einstellung für die Zukunft speichern**.
 2. Klicken Sie auf **Ablehnen**.

Die Verbindung wird auf der Grundlage der von Ihnen getroffenen Entscheidung zugelassen oder abgelehnt. Die Nummer und die Informationen über das Programm werden auf der Registerkarte **Nummernliste** zur Liste hinzugefügt. Anschließend:

- Wenn Sie die Verbindung zugelassen haben, wird kein Popup mehr angezeigt, wenn erneut ein Programm versucht, eine *DFÜ-Verbindung* zu dieser Nummer herzustellen.
- Wenn Sie die Verbindung abgelehnt haben und ein Programm versucht, eine *DFÜ-Verbindung* zu dieser Nummer herzustellen, wird das Popup **Abgelehnter Verbindungsversuch** angezeigt. **Schließen** Sie das Popup-Fenster, indem Sie auf Schließen klicken.

Hinweis:

Möglicherweise wird ein Popup **Verbindung schließen** angezeigt, wenn ein Programm versucht, eine *DFÜ-Verbindung* zu schließen. Wenn es sich bei dem Programm um das handelt, das Sie selbst

beendet haben, können Sie das Schließen der *DFÜ-Verbindung* zulassen. Klicken Sie hierzu auf **Zulassen**. Wenn es sich nicht um das Programm handelt, das Sie selbst beendet haben, müssen Sie das Schließen ablehnen, indem Sie auf **Ablehnen** klicken. Das Ablehnen des Beendigungsversuchs stellt sicher, dass kein schädliches *Dialer*programm Ihre Internetverbindung beendet und eine neue Verbindung zu einer anderen Nummer herstellt.




Hinzufügen, Bearbeiten oder Entfernen von Telefonnummern

Zu der Liste der Telefonnummern auf der Registerkarte **Nummernliste** können Sie Nummern hinzufügen, wenn Sie *DFÜ-Verbindungen* zu diesen Nummern zulassen oder ablehnen möchten.

So fügen Sie eine neue Nummer zur Liste hinzu:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Dialerschutz**.
4. Klicken Sie auf die Registerkarte **Nummernliste**.
5. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Nummer/Bereich hinzufügen** wird geöffnet.
6. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Nummer ein.
7. Geben Sie im Feld **Nummer** die Telefonnummer ein:
 - Folgende Zeichen dürfen verwendet werden: #*1234567890.
 - Sie können eine Vorwahl und eine Landesvorwahl verwenden, z. B. 040-1234567, 00 358 9 123 4567.
 - Sie können andere Zeichen, wie Leerzeichen oder Bindestriche verwenden, um die Nummern zu strukturieren. Der Dialerschutz ignoriert jedoch andere als die oben aufgeführten Zeichen. Er behandelt z. B. 09-1234567 als dieselbe Nummer wie 091234567.
 - Mithilfe der folgenden Platzhalter können Sie einen Nummernbereich eingeben:
 - "?" ersetzt eine einzelne Zahl. Um z. B. die *DFÜ-Verbindung* zu bestimmten Servicenummern abzulehnen, geben Sie 0900?234567 ein.
 - "X" oder "x" ersetzt eine oder mehrere Zahlen. Sie können diese Platzhalter verwenden, wenn Sie z. B.

DFÜ-Verbindungen ins Ausland ablehnen möchten. Wenn Sie normalerweise eine Auslandsverbindung mit "00" beginnen, geben Sie "00x" ein, um alle *DFÜ-Verbindungen* ins Ausland abzulehnen.

8. Wählen Sie aus, ob Sie die *DFÜ-Verbindungsversuche* ablehnen oder zulassen möchten:
 - Wählen Sie **Abgelehnt**, um alle Versuche, eine *DFÜ-Verbindung* zu der eingegebenen Nummer herzustellen, abzulehnen.
 - Wählen Sie **Zugelassen**, um *DFÜ-Verbindungen* mit der eingegebenen Nummer zuzulassen.
 9. Klicken Sie auf **OK**.
Auf der Registerkarte **Nummernliste** werden die Telefonnummer bzw. der Nummernbereich sowie die ausgewählte Aktion angezeigt:
 - Wenn Sie eine Nummer zulassen, wird vor der Nummer das Symbol  angezeigt.
 - Wenn Sie die Nummer abgelehnt haben, wird vor der Nummer das Symbol  angezeigt.
 10. Wenn Sie die Prioritätsreihenfolge der Nummern ändern möchten, klicken Sie auf eine Nummer in der Liste, halten Sie die Maustaste gedrückt, und ziehen sie die Nummer an die neuen Position in der Tabelle.
-  **Hinweis:** Auf der Registerkarte **Nummernliste** befinden sich möglicherweise einige vordefinierte Nummern, falls Ihr Service Provider *DFÜ-Verbindungen* zu bestimmten Nummern abgelehnt oder zugelassen hat. Diese Nummern können Sie nicht entfernen.

Programme anzeigen, die berechtigt sind, *DFÜ-Verbindungen* zu beenden

Auf der Registerkarte **Einstellungen** können Sie die sicheren Programme anzeigen, die berechtigt sind *DFÜ-Verbindungen* zu beenden.

Diese Registerkarte zeigt folgende Programme:

- Sichere Programme, die jederzeit berechtigt sind, *DFÜ-Verbindungen* zu beenden, wie z. B. der von Ihnen verwendete Webbrowser.
- Programme, bei denen Sie gefragt werden, ob Sie das Beenden der *DFÜ-Verbindung* zulassen oder ablehnen möchten. Die Registerkarte zeigt die Programme, bei denen Sie zugelassen haben, dass sie *DFÜ-Verbindungen* beenden.

Diese Registerkarte zeigt nicht die abgelehnten Programme an. Wenn Sie das Beenden der Verbindung für eine Anwendung in einem Popup-Fenster abgelehnt haben, kann die Verbindung erst dann getrennt werden, wenn Sie den Computer neu starten. Wenn Sie die Trennung der *DFÜ-Verbindung* durch eine Anwendung zugelassen haben, kann die Anwendung die Verbindung jederzeit trennen. Sie müssen diese Option nicht erneut auswählen.

So zeigen Sie die Programme an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Dialerschutz**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
Diese Registerkarte zeigt eine Liste der Programme, die berechtigt sind, *DFÜ-Verbindungen* zu beenden.

DFÜ-Verbindungsversuche anzeigen

Wenn Sie die Protokollierung des Dialerschutzes aktivieren, können Sie die Versuche, eine *DFÜ-Verbindung* herzustellen, sehen, die das Produkt erkannt hat.

Die Protokollierung des Dialerschutzes ist standardmäßig deaktiviert.

So schalten Sie die Protokollierung ein:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Dialerschutz**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Wählen Sie **Dialerschutz-Protokoll aktivieren**, um die Protokollierung einzuschalten.
6. Klicken Sie auf **Protokoll anzeigen**, um das erstellte Protokoll anzuzeigen.

Sie können folgende Informationen anzeigen:


- Versuche, *DFÜ-Verbindungen* herzustellen oder zu beenden.
- Ob die Versuche zugelassen oder abgelehnt wurden.
- Gewählte Telefonnummern.

So müssen Sie vorgehen, wenn Sie über Ihr Modem keine Verbindung zum Internet herstellen können

Wenn die *DFÜ-Verbindung* zu Ihrem Internet Service Provider (oder einer anderen Telefonnummer) nicht mehr funktioniert, überprüfen Sie, ob Sie nicht versehentlich die Verbindungen zu dieser Nummer abgelehnt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Dialerschutz**.
4. Klicken Sie auf die Registerkarte **Nummernliste**.
5. Prüfen Sie, ob sich die Nummer, die Sie anwählen möchten, in der Liste befindet. Wenn dies der Fall ist und wenn die Nummer

abgelehnt wird (das Symbol  steht davor), verfahren Sie wie folgt:

- a) Wählen Sie die Nummer aus.
- b) Klicken Sie auf **Bearbeiten**.
- c) Wählen Sie **Zugelassen**.
- d) Klicken Sie auf **OK**.

Das Symbol vor der Nummer wurde in  geändert.

Testen Sie, ob die Verbindung zu der Nummer jetzt hergestellt werden kann.

Anzeigen von Internet-Schutzschildstatus, Alarmen und Protokolldateien


Indem Sie Internet-Schutzschildstatus, Alarme und Protokolldateien anzeigen, können Sie ermitteln, wie das Internet-Schutzschild Ihren Computer schützt.

Status von Internet Shield überprüfen

Sie können den Status der zugehörigen Komponenten auf der erweiterten **Internet-Schutzschild**-Seite anzeigen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie links im Navigationsbereich **Internet-Schutzschild** aus.
4. Auf dieser Seite sehen Sie, ob Komponenten des Internet-Schutzschields, wie z. B. die Anwendungssteuerung, aktiviert bzw. deaktiviert sind.

 **Hinweis:** Deaktivieren Sie keine Komponenten, es sei denn, dies ist unbedingt erforderlich.

Prüfen Sie die aktuellen Einstellungen des Internet-Schutzschields

Die aktuellen Einstellungen des **Internet-Schutzschields** können Sie auf der Seite Internet-Schutzschild prüfen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Sie können folgende Einstellungen anzeigen:
 - Neben dem **Internet-Schutzschild** wird die aktuelle *Sicherheitsstufe* angezeigt.
 - Neben den Komponenten des Internet-Schutzschields werden deren aktuelle Einstellungen angezeigt. Die Einstellung für die Anwendungssteuerung kann z. B. **Auffordern** oder **Zulassen und protokollieren** sein.

Prüfen Sie die Anzahl der kürzlich erfolgten Aktionen des Internet-Schutzschilds

Auf der Seite [Internet-Schutzschild](#) können Sie die Anzahl der aktuellen Alarme sowie der blockierten Programme prüfen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte [Internet-Schutzschild](#).
2. Folgende Informationen werden angezeigt:
 - **Anwendungen zugelassen/abgelehnt:** Zeigt die Anzahl der Programme, für die das Erstellen von Verbindungen zugelassen oder blockiert wurde.
 - **Aktuelle Alarme:** Zeigt die Anzahl der Alarme, die das Internet-Schutzschild seit dem Start des Computers erzeugt hat. Klicken Sie auf [Ansicht](#), um eine Liste der Alarme anzuzeigen.
 - **Zuletzt gesend. Alarm:** Zeigt den Zeitpunkt des zuletzt gesendeten Alarms des Internet-Schutzschilds. Klicken Sie auf [Details](#), um Einzelheiten des Alarms anzuzeigen. Folgende Informationen werden angezeigt:
 - Zeitpunkt des zuletzt gesendeten *Alarms*, die *IP-Adresse* und der Dienst, der den *Alarm* erzeugt hat, und ob der Datenverkehr eingehend oder ausgehend war.
 - **Top 5 blockierte Adressen** zeigt die 5 *IP-Adressen*, die innerhalb von 24 Stunden die meisten *Alarme* erzeugt haben. Die *Firewall* hat den Datenverkehr von Ihrem Computer an diese *IP-Adressen* und von diesen IP-Adressen an Ihren Computer blockiert.
 - **Top 5 blockierte Dienste** zeigt die 5 Dienste, die innerhalb von 24 Stunden die meisten *Alarme* erzeugt haben. Diese Dienste haben Datenverkehr erzeugt, den die *Firewall* blockiert hat.

Klicken Sie nach der Anzeige der Informationen auf [Schließen](#).

Alarme des Internet-Schutzschilds anzeigen

Sie können eine Liste aller vom Internet-Schutzschild erzeugten Alarme anzeigen.

Die Liste enthält Alarme, die von der Firewall und Intrusion Prevention ausgelöst wurden.

So zeigen Sie die Liste an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie neben **Aktuelle Alarme** auf **Ansicht**.
Das Dialogfeld **Alarme von Internet-Schutzschild** wird geöffnet und zeigt folgende Informationen an:

Feld	Beschreibung
Zeit	Zeitpunkt des Alarms.
Remote-Adresse	<i>IP-Adresse</i> des Computers, von dem Datenverkehr empfangen wurde bzw. an den Datenverkehr gesendet wurde.
Treffer	Zeigt, wie oft ein ähnlicher Alarm erzeugt wurde.
Beschreibung	Ein Alarmtext, der für die <i>Firewallregel</i> hinzugefügt wurde. Wenn der Alarm wegen eines Eindringungsversuchs ausgelöst wurde, enthält das Feld eine Information über das <i>Muster</i> des Eindringungsversuchs.

3. Um Alarmdetails anzuzeigen, wählen Sie den Alarm aus und klicken Sie auf **Details**.
4. Um zum vorherigen oder zum nächsten Alarm zu gelangen, klicken Sie auf die Schaltfläche **< Zurück** oder **Weiter >**.
5. Klicken Sie nach der Ansicht der Details auf **Schließen**, um das Dialogfeld mit den Details der **Alarme von Internet-Schutzschild** zu schließen.
6. Klicken Sie auf **Schließen**, um das Dialogfeld mit der Liste der **Alarme von Internet-Schutzschild** zu schließen.

Internet-Schutzschild - Alarminformationen

Ein Alarm des Internet-Schutzschilds enthält bestimmte Informationen über den Datenverkehr, der den Alarm ausgelöst hat.

Ein Alarm des Internet-Schutzschilds enthält folgende Informationen:

Feld	Beschreibung
Beschreibung	Ein Alarmtext, der für die <i>Firewallregel</i> hinzugefügt wurde. Wenn der Alarm durch einen Eindringungsversuch ausgelöst wurde, zeigt der Alarm Informationen über das <i>Muster</i> des Eindringungsversuchs an.
Aktion	Zeigt, was passiert ist, z. B., dass die <i>Firewall</i> den Datenverkehr blockiert oder zugelassen hat.
Zeit	Das Datum und den Zeitpunkt, zu dem der Alarm generiert wurde.
Richtung	Zeigt, ob der Datenverkehr eingehend oder ausgehend ist (von einem Remote-Computer an Ihren Computer oder umgekehrt).
Protokoll	Das verwendete <i>IP-Protokoll</i> .
Dienste	Zeigt die <i>Firewalldienste</i> , mit denen der Datenverkehr übereinstimmte.
Remote-Adresse	Die <i>IP-Adresse</i> des Remote-Computers.
Remote-Port	Der <i>Port</i> auf dem Remote-Computer.
Lokale Adresse	Die <i>IP-Adresse</i> Ihres eigenen Computers.
Lokaler Port	Der <i>Port</i> auf Ihrem eigenen Computer.

Protokolldateien anzeigen

Informationen über die Aktionen des Internet-Schutzschilds und den Netzwerkdatenverkehr werden in Protokolldateien gesammelt.

Es gibt zwei Protokolldateien, das *Aktionsprotokoll* und das *Paketprotokoll*, die Sie auf der Seite [Protokollfunktion](#) für die Anzeige öffnen können. Auf dieser Seite wird außerdem der Speicherort der

Dateien angezeigt. Protokolldateien sind in erster Linie für erfahrene Benutzer gedacht, die mit Computernetzwerken vertraut sind.

Aktionsprotokoll

Das *Aktionsprotokoll* ist eine Textdatei (`action.log`), in der automatisch Informationen über die Aktionen des Internet-Schutzschilds gesammelt werden. Es ist hilfreich, das *Aktionsprotokoll* zu öffnen, wenn ein Programm keine Verbindung zum Internet herstellen kann und Sie prüfen möchten, ob die Anwendungssteuerung den Verbindungsaufbau verweigert. Die Maximalgröße der Datei beträgt 10 MB. Sobald die Datei voll ist, werden die alten Protokolleinträge gelöscht.

Paketprotokoll

Das *Paketprotokoll* sammelt Informationen über den *IP*-Netzwerkverkehr. Standardmäßig ist die Paketprotokollierung deaktiviert. Sie können die Paketprotokollierung einschalten, wenn Sie Ihren eigenen Satz *Firewallregeln* erstellt haben und prüfen möchten, wie diese den Datenverkehr blockieren. Sie können es außerdem aktivieren, wenn Sie bössartige Netzwerkaktivitäten befürchten.

Die Informationen werden in 10 Dateien gesammelt (`packetlog.0`-`packetlog.9`). Jedes Mal, wenn Sie die Protokollierung einschalten, wird das *Paketprotokoll* in einer neuen Datei gespeichert. Wenn die zehnte Datei voll ist, wird das Protokoll wieder in der ersten Datei gespeichert. So können Sie sich die vorhergehenden Protokolle ansehen, während ein neues Protokoll erstellt wird.

Zusätzlich zum *IP*-Datenverkehr sammelt das *Paketprotokoll* auch Informationen über andere Typen von Netzwerkdatenverkehr, z. B. über die *Protokolle*, die Ihr *lokales Netzwerk* (LAN) benötigt. Zu diesen Informationen gehören z. B. die *Routing*-Daten.

Das *Paketprotokoll* ist im *Hexadezimalformat* und unterstützt das *tcpdump*-Format. So können Sie die *Protokolldateien* auch in einem Programm für die *Paketprotokollierung* öffnen, das nicht ihr standardmäßiger Viewer für das *Paketprotokoll* ist. Sie können außerdem ein Programm zur Netzwerk-Protokoll-Analyse verwenden, um die Inhalte weiter zu analysieren.

Das Aktionsprotokoll anzeigen

Wenn ein Programm, beispielsweise ein Netzwerkspiel, nicht funktioniert, können Sie im Aktionsprotokoll prüfen, ob die

Anwendungssteuerung, die das Programm daran gehindert hat, eine Internetverbindung herzustellen.

So zeigen Sie das *Aktionsprotokoll* an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Protokollfunktion**.
4. Klicken Sie auf **Aktionsprotokoll anzeigen**.

Das *Aktionsprotokoll* wird im standardmäßigen Texteditor oder in einem Anzeigeprogramm wie z. B. Notepad geöffnet.

Aktionsprotokoll - Beispiele

Das *Aktionsprotokoll* enthält Informationen über geöffnete Verbindungen und Änderungen der *Firewallregeln*.

Öffnen einer Verbindung

Das folgende Beispiel zeigt einen Protokolleintrag, der erstellt wird, wenn Sie den Internet Explorer starten und eine Verbindung zu einem *HTTP-Server* herstellen:

Datum	Zeit	Typ	Interner Grund	Programm
2007-03-07	T13:07:15 +02:00	Info	appl control	C:\PROGRA~1\INTERN~1\iexplore.exe

Steuerungs- aktion	Netzwerk- aktion		Remote- IP-Adresse	Remote- Port
zulassen	nach außen verbinden	6	10.0.1.14	80

Verbindung wird empfangen

Das folgende Beispiel zeigt einen Protokolleintrag, der erzeugt wird, wenn ein Programm auf Ihrem Computer als *Server* für andere Computer agiert. Diese anderen Computer können über den von der Anwendungssteuerung auf Ihrem Computer geöffneten *Port* eine Verbindung zu diesem *Server-Programm* herstellen (dynamische *Firewallregel*):

Datum	Zeit	Typ	Interner Grund	Programm
-------	------	-----	----------------	----------

2007-03-04	T13:08:15+02:00	Info	appl control	unbekannt
------------	-----------------	------	--------------	-----------

Steuerungs- aktion	Netzwerk- aktion	Protokoll	Remote- IP-Adresse	Lokaler Port
-----------------------	---------------------	-----------	-----------------------	-----------------

zulassen	empfangen	17	10.0.1.146	138
----------	-----------	----	------------	-----

Hinzufügen und Entfernen einer dynamischen *Firewallregel*

Das folgende Beispiel zeigt zwei *Firewallregel*-Protokolleinträge:

- Der erste Eintrag zeigt, dass die Anwendungssteuerung eine dynamische *Firewallregel* hinzugefügt hat. Diese Regel erlaubt eine temporäre, eingehende Verbindung für ein Programm.
- Der zweite Eintrag zeigt, dass die Anwendungssteuerung die dynamische *Firewallregel* entfernt hat und dass die Verbindung beendet wurde.

Datum	Zeit	Warnungstyp	Regeltyp	Aktion	Minimaler Adressbereich für Remote-IP-Adresse
-------	------	-------------	----------	--------	---

2007-03-05	T13:06:59+02:00	Info	dynamische Regel	hinzugefügt	0.0.0.0
------------	-----------------	------	------------------	-------------	---------

2007-03-05	T13:07:23+02:00	Info	dynamische Regel	entfernt	0.0.0.0
------------	-----------------	------	------------------	----------	---------

Maximaler Adressbereich für Remote-IP-Adresse	Remote-Port-Bereich (von)	Remote-Port-Bereich (bis)	Lokaler Port-Bereich (von)	Lokaler Port-Bereich (bis)	Regel-aktion
---	---------------------------	---------------------------	----------------------------	----------------------------	--------------

255.255.255.0	0	65535	371	371	zulassen
---------------	---	-------	-----	-----	----------

Maximaler Adressbereich für Remote-IP-Adresse	Remote-Port-Bereich (von)	Remote-Port-Bereich (bis)	Lokaler Port-Bereich (von)	Lokaler Port-Bereich (bis)	Regelaktion
255.255.255.0	0	65535	371	371	zulassen

Paketprotokollierung zur Überwachung des Netzwerkdatenverkehrs verwenden

Sie können bei Bedarf die Paketprotokollierung starten, um Informationen über den *IP*-Datenverkehr im Netzwerk aufzuzeichnen.

Paketprotokollierung starten

Wenn Sie den Verdacht haben, dass bösartige Netzwerkaktivitäten stattfinden, oder wenn z. B. ein Netzwerkspiel nicht mehr funktioniert, können Sie die Paketprotokollierung starten.

So starten Sie die Protokollierung:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild > Protokollfunktion**.
4. Verwenden Sie die vorgeschlagenen Werte für die **Protokollzeit** und die Dateigröße der Felder **Protokollzeit** und **Maximalgröße der Protokolldatei**. Sie können die Werte ansonsten auch ändern.
5. Klicken Sie auf **Protokollierung starten**. Zur Liste der Protokolldateien wird eine neue Datei hinzugefügt. Die Größe der Datei steigt an, je mehr Informationen gesammelt werden. Wenn die Liste bereits 10 Protokolldateien enthält, wird das nächste Protokoll in eine vorhandene Datei geschrieben.
6. Um die Protokollierung manuell zu stoppen, klicken Sie auf **Protokollierung anhalten**. Die Protokollierung wird automatisch nach Ablauf der vorgegebenen Protokollzeit beendet bzw. wenn die Maximalgröße der Protokolldatei erreicht ist.

Eine neue Protokolldatei wird erzeugt und zur Liste der Protokolldateien hinzugefügt.

Betrachten Sie das *Paketprotokoll*

Nachdem Sie ein *Paketprotokoll* erstellt haben, können Sie es öffnen und anzeigen.

So zeigen Sie das *Paketprotokoll* an:

1. Klicken Sie auf die Registerkarte **Internet-Schutzschild**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie **Internet-Schutzschild** > **Protokollfunktion**.
4. Wählen Sie das *Paketprotokoll* aus, das Sie anzeigen möchten, und klicken Sie auf **Details**.

Der standardmäßige *Paketprotokoll* -Viewer wird geöffnet. Im oberen Fensterbereich werden alle protokollierten Verbindungen angezeigt.

Sie können folgende Informationen anzeigen:

Feld	Beschreibung
Zeit	Zeit in Sekunden ab dem Augenblick, in dem die Protokollierung begann. Wenn die definierte Protokollierungszeit 60 Sekunden beträgt, liegt die Startzeit für das erste <i>Paket</i> nahe bei 0 Sekunden, und die Startzeit für das letzte <i>Paket</i> nahe bei 60 Sekunden.
Verwerfen (Verz.)	<p>Zeigt, ob <i>Fiirewall</i> den <i>Paket</i> durchgelassen oder verworfen hat, und zeigt die Richtung von <i>Paket</i> :</p> <ul style="list-style-type: none">• Nein : Zugelassen: <i>Paket</i> .• Ja : Verwarf <i>Paket</i> .• Eingehend : Eingehendes <i>Paket</i> .• Ausgehend : Ausgehendes <i>Paket</i> . <p>Diese Informationen sind nicht verfügbar, wenn Sie die Datei in einem anderen Paketprotokollierungsprogramm anzeigen als dem standardmäßigen <i>Paketprotokoll</i> -Viewer.</p>

Feld	Beschreibung
Protokoll	Das verwendete <i>IP-Protokoll</i> .
Ursprung	Ursprungs- <i>IP-Adresse</i> des <i>Pakets</i> .
Ziel	Ziel- <i>IP-Adresse</i> des <i>Pakets</i> .
ID	<i>IP Paket</i> -Kopfzeileninformationen: Kennung des <i>Pakets</i> .
TTL	<i>IP Paket</i> Header-Informationen: der Wert <i>Gültigkeitsdauer</i> des <i>Pakets</i> definiert die Anzahl der Netzwerkgeräte, die das <i>Paket</i> durchlaufen kann, bevor es verworfen wird.
Len	<i>IP Paket</i> Header-Informationen: Gesamtlänge des <i>Pakets</i> .
Beschreibung	Beschreibung des <i>Pakets</i> .

Im rechten Fensterbereich werden die Datenverkehrstypen und die zugehörigen Definitionen angezeigt.

Im unteren Fensterbereich werden die Informationen in den Formaten *Hexadezimal* und *ASCII* angezeigt.

Wenn Sie alle Arten von Netzwerkverkehr anzeigen möchten (und nicht nur *IP* -Datenverkehr), müssen Sie das Kontrollkästchen **Nicht-IP-Datenverkehr filtern** deaktivieren.

Kapitel 4

Automatische Updates

Themen:

- *Prüfen des Update-Status*
- *Ändern der Internetverbindungseinstellung*

Das Produkt lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind. Es erkennt den Netzwerkverkehr und stört auch bei einer langsamen Netzwerkverbindung nicht die Internetnutzung.

Prüfen des Update-Status


Datum und Uhrzeit der letzten Aktualisierung anzeigen.

Wenn die automatischen Updates aktiviert sind, sorgen diese dafür, dass das Produkt bei jeder Verbindung mit dem Internet automatisch aktualisiert wird.

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Klicken Sie auf die Registerkarte **Automatische Updates**.
2. **Letzte Update-Prüfung** zeigt den Zeitpunkt des letzten Updates an.
3. Klicken Sie auf **Jetzt prüfen**.


Der F-Secure Agent für automatische Updates stellt eine Verbindung mit dem Internet her und sucht nach den neuesten Updates. Falls der Schutz nicht aktuell ist, ruft er die neuesten Updates ab.



 **Hinweis:** Wenn Sie ein Modem verwenden oder eine ISDN-Verbindung zum Internet haben, muss die Verbindung aktiv sein, um nach Updates zu suchen.

Ändern der Internetverbindungseinstellungen

Sie können konfigurieren, wie Ihr Computer eine Verbindung mit dem Internet herstellt, um Updates automatisch zu empfangen.

So ändern Sie die Einstellungen für Ihre Internetverbindung:

 **Hinweis:** Normalerweise ist es nicht erforderlich, die Standardeinstellungen zu ändern.

1. Klicken Sie auf die Registerkarte **Automatische Updates**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Verbindung**.
4. Wählen Sie in der Liste **Internetverbindung** aus, wie Ihr Computer mit dem Internet verbunden ist.
 - Wählen Sie **Ständige Verbindung voraussetzen**, wenn Sie eine permanente Netzwerkverbindung haben.
 -  **Hinweis:** Falls Ihr Computer keine ständige Netzwerkverbindung besitzt und bei Bedarf eine DFÜ-Verbindung herstellt, kann die Option **Ständige Verbindung voraussetzen** zu mehreren Einwahlversuchen führen.
 - Wählen Sie **Verbindung erkennen**, um Updates nur dann abzurufen, wenn das Produkt eine aktive Netzwerkverbindung erkennt.
 - Wählen Sie **Datenverkehr erkennen**, um Updates nur dann abzurufen, wenn das Produkt anderen Netzwerkverkehr erkennt.
 -  **Tipp:** Falls Sie eine ungewöhnliche Hardwarekonfiguration besitzen, die dafür sorgt, dass mit der Einstellung **Verbindung erkennen** auch dann eine aktive Netzwerkverbindung erkannt wird, wenn keine vorhanden ist, wählen Sie stattdessen **Datenverkehr erkennen**.
5. Wählen Sie in der Liste **HTTP-Proxy** aus, ob Ihr Computer für die Internetverbindung einen *Proxy-Server* verwendet.
 - Wählen Sie **Kein HTTP-Proxy** aus, wenn Ihr Computer direkt mit dem Internet verbunden ist.

- Wählen Sie **HTTP-Proxy manuell konfigurieren** aus, um die *HTTP-Proxy*-Einstellungen zu konfigurieren.
- Wählen Sie **HTTP-Proxy des Browsers verwenden** aus, um die *HTTP-Proxy*-Einstellungen zu verwenden, die in Ihrem Browser konfiguriert sind.

Konfigurieren eines HTTP-Proxys Manuell

Sie können den vom Produkt für die Verbindung zum Internet verwendeten HTTP-Proxy konfigurieren.

So konfigurieren Sie den HTTP-Proxy:

1. Klicken Sie auf die Registerkarte **Automatische Updates**. **Letzte Update-Prüfung** zeigt den Zeitpunkt des letzten Updates an.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf **Verbindung**.
4. Wählen Sie **HTTP-Proxy manuell konfigurieren**.
5. Klicken Sie auf **Konfigurieren**.
6. Geben Sie die Adresse und die Portnummer des HTTP-Proxys ein.
7. Wählen Sie **Zulassen, dass Updates auf Proxy zwischengespeichert werden**, wenn sich in demselben Netzwerk mehrere Installationen des Produkts befinden und Sie die Updates mehrfach verwenden möchten.
8. Wenn für den Proxy-Server eine Benutzerauthentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Proxy erfordert Benutzerauthentifizierung** und geben Sie den Benutzernamen und das Passwort für den Proxy-Server ein.