McAfee®

virus scan professional™

Benutzerhandbuch

Version 9.0

McAfee®

LIZENZINFORMATIONEN

Lizenzvertrag

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

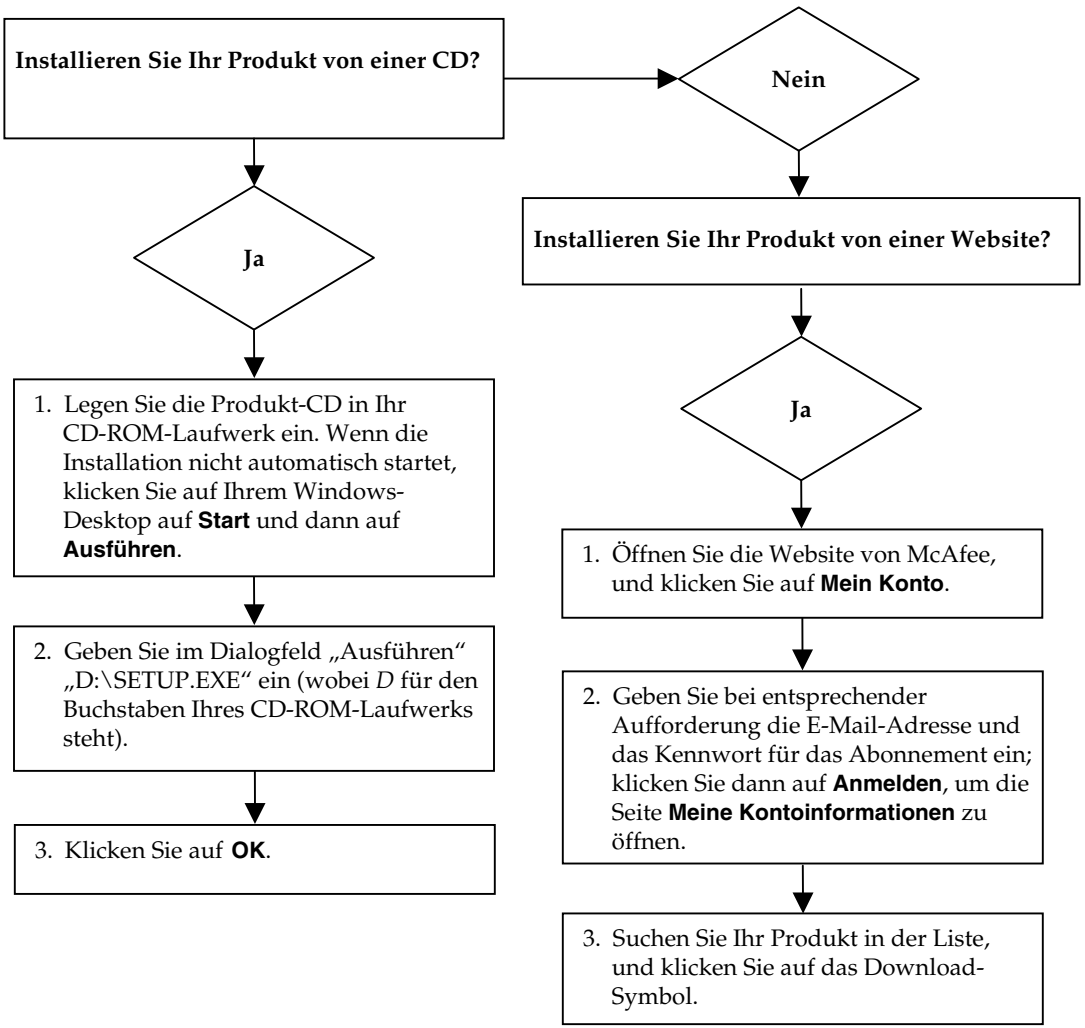
Zubehör

Im Lieferumfang dieses Produkts ist gegebenenfalls Folgendes enthalten:

♦ Software, die vom OpenSSL-Projekt zur Verwendung mit dem OpenSSL-Toolkit entwickelt wurde (http://www.openssl.org/). ♦ Kryptographie-Software, die von Eric Young entwickelt wurde, und Software, die von Tim J. Hudson entwickelt wurde. ♦ Softwareprogramme, die gemäß der GNU, General Public License (GPL) oder anderen ähnlichen Lizenzen für kostenlose Software zugelassen werden und es dem Benutzer neben anderen Rechten erlauben, bestimmte Programme oder Teile davon zu kopieren, zu modifizieren und weiterzugeben sowie auf den Quellcode zuzugreifen. Die GPL verlangt, dass grundsätzlich bei Weitergabe der Software an Dritte in einem ausführbaren binären Format im Geltungsbereich der GPL diesem Benutzer auch der Quellcode zur Verfügung gestellt werden muss. Bei Software dieser Art, die unter den Geltungsbereich der GPL fällt, wird der Quellcode ebenfalls auf der entsprechenden CD zur Verfügung gestellt. Falls Lizenzen für kostenlose Software verlangen, dass McAfee Rechte für die Nutzung, das Kopieren oder die Modifikation eines Softwareprogramms gewährt, welche über die in diesem Vertrag gewährten Rechte hinausgehen, haben Rechte dieser Art Vorrang vor den Rechten und Einschränkungen in diesem Vertrag. ♦ Von Henry Spencer entwickelte Software, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Von Robert Nordier entwickelte Software, Copyright © 1996-7 Robert Nordier. ♦ Von Douglas W. Sauder entwickelte Software. ♦ Von der Apache Software Foundation entwickelte Software (http://www.apache.org/). Eine Kopie der Lizenzvereinbarung für diese Software finden Sie unter www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode („ICU") Copyright © 1995-2002 International Business Machines Corporation und andere. ♦ Software, die von CrystalClear Software, Inc., entwickelt wurde, Copyright © 2000 CrystalClear Software, Inc., ♦ FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc., und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc., ♦ Software, urheberrechtlich geschützt von Thai Open Source Software Center Ltd. und Clark Cooper, © 1998, 1999, 2000. ♦ Software, urheberrechtlich geschützt von Expat maintainers. ♦ Software, urheberrechtlich geschützt von The Regents of the University of California, © 1989. ♦ Software, urheberrechtlich geschützt von Gunnar Ritter. ♦ Software, urheberrechtlich geschützt von Sun Microsystems®, Inc.,© 2003. ♦ Software, urheberrechtlich geschützt von Gisle Aas. © 1995-2003. ♦ Software, urheberrechtlich geschützt von Michael A. Chase, © 1999-2000. ♦ Software, urheberrechtlich geschützt von Neil Winton, © 1995-1996. ♦ Software, urheberrechtlich geschützt von RSA Data Security, Inc., © 1990-1992. ♦ Software, urheberrechtlich geschützt von Sean M. Burke, © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Martijn Koster, © 1995. ♦ Software, urheberrechtlich geschützt von Brad Appleton, © 1996-1999. ♦ Software, urheberrechtlich geschützt von Michael G. Schwern, © 2001. ♦ Software, urheberrechtlich geschützt von Graham Barr, © 1998. ♦ Software, urheberrechtlich geschützt von Larry Wall und Clark Cooper, © 1998-2000. ♦ Software, urheberrechtlich geschützt von Frodo Looijaard, © 1997. ♦ Software, urheberrechtlich geschützt von Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie der Lizenzvereinbarung für diese Software finden Sie unter www.python.org. ♦ Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002. ♦ Software, urheberrechtlich geschützt von Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software, urheberrechtlich geschützt von Simone Bordet & Marco Cravero, © 2002. ♦ Software, urheberrechtlich geschützt von Stephen Purcell, © 2001. ♦ Software, die von Indiana University Extreme! Lab entwickelt wurde (http://www.extreme.indiana.edu/). ♦ Software, urheberrechtlich geschützt von International Business Machines Corporation und anderen, © 1995-2003. ♦ Software, urheberrechtlich geschützt von University of California, Berkeley und ihren Beitragenden. ♦ Software, die von Ralf S. Engelschall <rse@engelschall.com> zur Verwendung im mod_ssl-Projekt (http://www.modssl.org/) entwickelt wurde. ♦ Software, urheberrechtlich geschützt von Kevlin Henney, © 2000-2002. ♦ Software, urheberrechtlich geschützt von Peter Dimov und Multi Media Ltd. © 2001, 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, © 2001, 2002. Dokumentation siehe http://www.boost.org/libs/bind/bind.html. ♦ Software, urheberrechtlich geschützt von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software, urheberrechtlich geschützt von Boost.org, © 1999-2002. ♦ Software, urheberrechtlich geschützt von Nicolai M. Josuttis, © 1999. ♦ Software, urheberrechtlich geschützt von Jeremy Siek, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Daryle Walker, © 2001. ♦ Software, urheberrechtlich geschützt von Chuck Allison und Jeremy Siek, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Samuel Krempp, © 2001. Updates, Dokumentation und Überarbeitungsverlauf siehe http://www.boost.org. ♦ Software, urheberrechtlich geschützt von Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Cadenza New Zealand Ltd., © 2000. ♦ Software, urheberrechtlich geschützt von Jens Maurer, © 2000, 2001. ♦ Software, urheberrechtlich geschützt von Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Ronald Garcia, © 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, Jeremy Siek und Daryle Walker, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software, urheberrechtlich geschützt von Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software, urheberrechtlich geschützt von Paul Moore, © 1999. ♦ Software, urheberrechtlich geschützt von Dr. John Maddock, © 1998-2002. ♦ Software, urheberrechtlich geschützt von Greg Colvin und Beman Dawes, © 1998, 1999. ♦ Software, urheberrechtlich geschützt von Peter Dimov, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Jeremy Siek und John R. Bandela, © 2001. ♦ Software, urheberrechtlich geschützt von Joerg Walter und Mathias Koch, © 2000-2002.

Schnellreferenz

Wenn Sie die Installation des Produkts von einer CD oder einer Website aus ausführen, empfiehlt es sich, diese praktische Referenzseite auszudrucken.



Weitere Informationen

Zum Anzeigen der auf der Produkt-CD enthaltenen Benutzerhandbücher muss auf Ihrem Computer Acrobat Reader installiert sein. Falls Sie die Anwendung noch nicht besitzen, können Sie sie jetzt von der McAfee-Produkt-CD installieren.

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

Registrierungsnutzen

Wir empfehlen Ihnen, Ihre Registrierung in einigen einfachen Schritten innerhalb des Produkts vorzunehmen und direkt an uns zu übermitteln. Durch die Registrierung wird sichergestellt, dass Ihnen im angemessenen Zeitrahmen professionelle technische Unterstützung zur Verfügung steht. Außerdem profitieren Sie von:

- KOSTENLOSEM elektronischem Support
- Updates für Virusdefinitionsdateien (.DAT) für ein Jahr nach der Installation, wenn Sie VirusScan-Software kaufen
- Informationen zum Preis für ein zusätzliches Jahr Aktualisierungen der Virusdefinitionen erhalten Sie unter http://de.mcafee.com/.
- Garantie von 60 Tagen für Austausch der Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr nach der Installation, wenn Sie SpamKiller-Software kaufen

  Informationen zum Preis für ein zusätzliches Jahr Filter-Updates erhalten Sie unter http://de.mcafee.com/.
- McAfee Internet Security Suite-Updates für ein Jahr nach der Installation, wenn Sie MIS-Software kaufen

  Informationen zum Preis für ein zusätzliches Jahr Inhaltsaktualisierungen erhalten Sie unter http://de.mcafee.com/.

Technischer Support

Technischen Support und Kundendienst erhalten Sie unter

http://www.mcafeehilfe.com/.

Unsere Support-Site ermöglicht Ihnen rund um die Uhr den Zugriff auf einen leicht zu bedienenden Antwortassistenten, der Ihnen Antworten auf die häufigsten Fragen gibt.

Die erweiterten Optionen sind für erfahrene Benutzer gedacht. Sie umfassen beispielsweise eine Schlüsselwortsuche und ein Hilfeverzeichnis. Wenn sich keine Lösung findet, können Sie außerdem KOSTENLOS auf unsere Dienste Chat Now! und E-Mail Express! zugreifen. Per Chat und E-Mail können Sie über das Internet schnell einen qualifizierten Support-Mitarbeiter erreichen, wobei Ihnen keine Kosten entstehen. Andernfalls können Sie sich unter

http://www.mcafeehilfe.com/.

über die telefonischen Support-Möglichkeiten informieren.

Telefonnummern des Notfall-Supports:

Land:	Telefonnummer:
Belgien	02 27 50 703
Brasilien	11 4196 7077
Dänemark	03 5258 321
Deutschland	06 966 404 330
Finnland	09 229 06 000
Frankreich	01 70 20 0 008
Großbritannien	020 794 901 07
Irland	01 601 55 80
Italien	02 45 28 15 10
Luxemburg	040 666 15670
Niederlande	020 504 0586
Norwegen	02 3050420
Österreich	017 908 75 810
Portugal	00 31 20 586 6430 (auf Englisch)
Schweden	08 57 92 9004
Schweiz	022 310 1033
Spanien	901-120 175 (* anteilige Gebühren)
Südafrika	011 700-8216

Inhalt

Erste Schritte 1

Willkommen bei McAfee VirusScan. McAfee VirusScan Professional Edition enthält McAfee VirusScan sowie McAfee SpamKiller und McAfee Shredder. Weitere Informationen zu diesen zusätzlichen Programmen finden Sie unter *Verwendung der Professional Edition-Software* auf Seite 39.

> **HINWEIS**
> Hierbei handelt es sich nur um einen kurzen Überblick. Weitere Informationen erhalten Sie in den Online-Hilfen für VirusScan, SpamKiller bzw. Shredder.

McAfee VirusScan ist ein Anti-Virus-Abonnementservice, der Ihnen umfassenden, zuverlässigen und stets aktuellen Virenschutz bietet. Unterstützt durch die preisgekrönte McAfee-Scan-Technologie schützt VirusScan vor Viren, Würmern, Trojanern, bösartigen Skripts und Hybridangriffen.

Das Programm umfasst folgende Funktionen:

ActiveShield – ActiveShield durchsucht alle Dateien, auf die Sie oder Ihr Computer zugreifen.

Scan – Durchsucht Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und potentiell unerwünschten Programmen.

Quarantäne – Verschlüsselt infizierte bzw. verdächtige Dateien und isoliert sie temporär in einem Ordner, bis eine angemessene Maßnahme ergriffen werden kann.

Erkennung feindseliger Aktivitäten – Überwacht den Computer auf virenähnliche Aktivitäten, die durch bösartige Skripts oder Würmer verursacht werden.

Neue Funktionen

Diese Version von VirusScan enthält folgende neue Funktionen:

- **Prüfen auf potentiell unerwünschte Programme**
  VirusScan kann Daten auf potentiell unerwünschte Programme prüfen (einschließlich Spyware, Adware und Einwahlprogramme). Dies kann beim manuellen Prüfen, beim Prüfen von ausgehenden E-Mails, von Instant Messaging (IM)-Nachrichten sowie über das Windows Explorer-Kontextmenü oder die Microsoft Outlook-Symbolleiste erfolgen.

- **Prüfen von großen ausgehenden Anlagen**
  Um der größeren Verbreitung von Breitband-Internetverbindungen Rechnung zu tragen sowie der Tatsache, dass Dienstanbieter erhöhte E-Mail-Speicher- und -Übertragungskapazitäten gewähren, ist VirusScan nun in der Lage, große E-Mail-Anlagen zu überprüfen, ohne die Zeitüberschreitungswerte von E-Mail-Programmen zu überschreiten.

- **E-Mail-Scan**
  VirusScan prüft automatisch eingehende (POP3) und abgehende (SMTP) E-Mails und E-Mail-Anlagen für den Großteil gängiger E-Mail-Clients, einschließlich Microsoft Outlook, Netscape Mail, Eudora und Pegasus.

- **Prüfen von Instant Messenger**
  VirusScan prüft automatisch eingehende Dateiübertragungen für den Großteil der Instant Messaging-Clients, einschließlich Yahoo Messenger, AOL Instant Messenger und MSN Messenger.

- **Erkennung gefährlicher Aktivität**
  VirusScan enthält ScriptStopper™ und WormStopper™, mit denen virenähnliche Aktivitäten, die durch gefährliche Skripten und Würmer verursacht werden, erkannt, gemeldet und blockiert werden können.

- **Automatische Säuberung der infizierten Datei**
  VirusScan versucht automatisch, infizierte oder verdächtige Dateien sofort nach der Erkennung zu bereinigen.

- **Geplante Scanvorgänge**
  Sie können festlegen, dass Ihr Computer in regelmäßigen, frei definierbaren Abständen automatisch auf Viren überprüft wird.

- **Dateien unter Quarantäne stellen**
  Mit Hilfe der Quarantänefunktion können Sie infizierte und verdächtige Dateien verschlüsseln und temporär in einem Ordner isolieren, bis eine angemessene Maßnahme ergriffen werden kann. Nach der Reinigung können in Quarantäne gestellte Dateien am ursprünglichen Speicherort wiederhergestellt werden.

- **Dateien an AVERT übermitteln**
  VirusScan beinhaltet nun eine Funktion, über die verdächtige Dateien direkt von der Quarantäne-Funktion aus zu Forschungszwecken an das McAfee AntiVirus Emergency Response (AVERT™) übermittelt werden können.

- **Informationen an Virus Map weiterleiten**
  Informationen zu Viren können jetzt anonym in unsere World Virus Map aufgenommen werden. Sie haben die Möglichkeit, sich automatisch für diese kostenlose und sichere Funktion anzumelden, um die aktuellsten weltweiten Infektionsraten über McAfee SecurityCenter anzeigen zu lassen.

Systemanforderungen

- Microsoft® Windows 95, 98, Me, 2000 oder XP
- PC mit Prozessor Windows 98 oder Me: Pentium 150 MHz oder höher
  Windows 2000 oder XP: Pentium 233 MHz oder höher
- RAM
  Windows 98: 32 MB (64 MB empfohlen)
  Windows Me, 2000 oder XP: 64 MB (128 MB empfohlen)
- 40 MB Festplattenspeicher
- Microsoft® Internet Explorer ab Version 5.5

HINWEIS
Sie können die neueste Version von Internet Explorer von der Microsoft-Website unter http://www.microsoft.com/worldwide/ herunterladen.

Testen von VirusScan

Bevor Sie VirusScan zum ersten Mal verwenden, sollten Sie Ihre Installation testen. Gehen Sie für das separate Testen der ActiveShield- und Scan-Funktionen wie nachfolgend beschrieben vor.

Testen von ActiveShield

So testen Sie ActiveShield:

1. Rufen Sie http://www.eicar.com/ in Ihrem Web-Browser auf.
2. Klicken Sie auf den Link **The AntiVirus testfile eicar.com**.
3. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download Area** werden vier Links angezeigt.
4. Klicken Sie auf **eicar.com**.

Wenn ActiveShield korrekt ausgeführt wird, wird die Datei **eicar.com** sofort nach Klicken auf den Link als Virus erkannt. Wenn Sie sehen möchten, wie VirusScan mit Viren umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Wenn ActiveShield einen Virus findet* auf Seite 25.

Testen von Scan

Bevor Sie Scan testen können, müssen Sie ActiveShield deaktivieren, um zu verhindern, dass infizierte Dateien von ActiveShield erkannt werden, bevor Scan sie erkennt, und anschließend die Testdateien herunterladen.

So laden Sie die Testdateien herunter:

1. Deaktivieren Sie ActiveShield. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Deaktivieren**.
2. Laden Sie die EICAR-Testdateien von der EICAR-Website herunter:
   a. Rufen Sie http://www.eicar.com/ auf.
   b. Klicken Sie auf den Link **The AntiVirus testfile eicar.com**.
   c. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download Area** werden diese Links angezeigt:

      eicar.com enthält eine Textzeile, die von VirusScan als Virus erkannt wird.

      eicar.com.txt (optional) ist dieselbe Datei, jedoch mit einem anderen Dateinamen. Diese Datei ist für diejenigen Benutzer vorgesehen, die mit dem ersten Link Probleme haben. Benennen Sie die Datei nach dem Download einfach in “eicar.com“ um.

      eicar_com.zip ist eine Kopie des Testvirus in einer mit WinZip™ komprimierten ZIP-Datei (ein WinZip-Dateiarchiv).

      eicarcom2.zip ist eine Kopie des Testvirus in einer mit WinZip komprimierten ZIP-Datei, die sich ebenfalls in einer mit WinZip komprimierten ZIP-Datei befindet.

   d. Klicken Sie auf den jeweiligen Link, um die entsprechende Datei herunterzuladen. Für jede Datei wird ein Dialogfeld für den **Dateidownload** geöffnet.
   e. Klicken Sie auf **Speichern** und auf die Schaltfläche **Neuen Ordner erstellen** und benennen Sie den Ordner anschließend in **VSO-Scan-Ordner** um.
   f. Doppelklicken Sie in jedem Dialogfeld **Speichern unter** auf **VSO-Scan-Ordner** und dann erneut auf **Speichern**.
3. Wenn Sie die Dateien heruntergeladen haben, schließen Sie den Internet Explorer.
4. Aktivieren Sie ActiveShield: Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Aktivieren**.

So testen Sie Scan:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Auf Viren überprüfen**.
2. Navigieren Sie über die Verzeichnisstruktur im linken Ausschnitt des Dialogfeldes zum **VSO-Scan-Ordner**, in dem Sie die Dateien gespeichert haben:
   a. Klicken Sie auf das Pluszeichen (**+**) neben dem Laufwerkbuchstaben C.
   b. Klicken Sie auf den **VSO-Scan-Ordner**, um ihn zu markieren (und nicht auf das Pluszeichen neben dem Ordner).

      Dadurch wird Scan angewiesen, nur diesen Ordner nach Viren zu durchsuchen. Eine noch überzeugendere Demonstration der Fähigkeiten von Scan erhalten Sie, wenn Sie die Dateien an zufällig ausgewählten Standorten auf der Festplatte speichern.
3. Vergewissern Sie sich im Bereich **Prüfoptionen** des Dialogfeldes **Auf Viren überprüfen**, dass alle Optionen aktiviert sind.
4. Klicken Sie unten rechts im Dialogfeld auf **Prüfen**.

   VirusScan durchsucht den **VSO-Scan-Ordner**. Die EICAR-Dateien, die Sie in diesem Ordner gespeichert haben, werden in der **Liste der entdeckten Dateien** aufgeführt. In diesem Fall arbeitet Scan korrekt.

Wenn Sie sehen möchten, wie Scan mit Viren umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Wenn die Scan-Funktion einen Virus oder ein potentiell unerwünschtes Programm findet* auf Seite 35.

McAfee SecurityCenter verwenden

Das McAfee SecurityCenter stellt Ihre Anlaufstelle für alle Sicherheitsbelange dar und ist über das Symbol auf der Windows-Taskleiste oder dem Windows-Desktop zugänglich. Mit diesem Programm können Sie auf folgende nützliche Dienste zugreifen:

- Kostenlose Sicherheitsanalyse für Ihren Computer.
- Starten, Verwalten und Konfigurieren aller McAfee-Abonnements über ein einziges Symbol.
- Anzeige fortwährend aktualisierter Viruswarnungen und der neuesten Produktinformationen.
- Direkte Links zu häufig gestellten Fragen und Antworten sowie Kontoinformationen auf der McAfee-Website.

HINWEIS
Um weitere Informationen zu den Funktionen anzuzeigen, klicken Sie im Dialogfenster **SecurityCenter** auf **Hilfe**.

Wenn SecurityCenter ausgeführt wird und alle auf Ihrem Computer installierten McAfee-Funktionen aktiviert sind, wird das Symbol mit dem roten M auf der Windows-Taskleiste angezeigt. Dieser Bereich, der auch die Systemuhr enthält, befindet sich in der Regel unten rechts auf dem Windows-Desktop.

Wenn auf Ihrem Computer installierte McAfee-Anwendungen deaktiviert sind, wird das McAfee-Symbol schwarz dargestellt.

So öffnen Sie McAfee SecurityCenter:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol.
2. Klicken Sie auf **SecurityCenter öffnen**.

So greifen Sie auf eine VirusScan-Funktion zu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol.
2. Zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf die zu verwendende Funktion.

McAfee VirusScan 2

ActiveShield

Nachdem ActiveShield gestartet (in den Computerspeicher geladen) und aktiviert wurde, bietet das Programm konstanten Schutz für Ihren Computer. ActiveShield durchsucht alle Dateien, auf die Sie oder Ihr Computer zugreifen. Sollte ActiveShield eine infizierte Datei entdecken, wird automatisch versucht, den Virus zu bereinigen. Wenn ActiveShield den Virus nicht bereinigen kann, können Sie die Datei unter Quarantäne stellen oder sie löschen.

Aktivieren bzw. Deaktivieren von ActiveShield

ActiveShield wird standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol in der Windows-Taskleiste), sobald Sie Ihren Computer nach erfolgreicher Installation neu starten.

Wenn ActiveShield angehalten (nicht geladen) oder deaktiviert wird (gekennzeichnet durch das schwarze Symbol), können Sie das Programm manuell starten. Sie können ActiveShield auch so konfigurieren, dass das Programm automatisch nach jedem Start von Windows ausgeführt wird.

Aktivieren von ActiveShield

So aktivieren Sie ActiveShield für die aktuelle Windows-Sitzung:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Aktivieren**. Das McAfee-Symbol wird rot dargestellt.

Wenn ActiveShield weiterhin so konfiguriert ist, dass das Programm bei jedem Neustart von Windows ausgeführt wird, werden Sie in einer Meldung darüber informiert, dass Ihr Computer jetzt vor Viren geschützt ist. Andernfalls wird ein Dialogfeld geöffnet, in dem Sie ActiveShield so konfigurieren können, dass das Programm nach jedem Neustart von Windows ausgeführt wird (Abbildung 2-1 auf Seite 16).

Deaktivieren von ActiveShield

So deaktivieren Sie ActiveShield für die aktuelle Windows-Sitzung:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Deaktivieren**.
2. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

   Das McAfee-Symbol wird schwarz dargestellt .

Wenn ActiveShield so konfiguriert ist, dass das Programm beim Start von Windows automatisch ausgeführt wird, ist Ihr Computer nach einem Neustart wieder vor Viren geschützt.

Konfigurieren von ActiveShield-Optionen

Sie können die Start- und Scan-Optionen von ActiveShield ändern. Verwenden Sie hierzu im Dialogfeld **McAfee VirusScan - Optionen** (Abbildung 2-1) die Registerkarte **ActiveShield**. Der Zugriff erfolgt über das McAfee-Symbol in der Windows-Taskleiste.

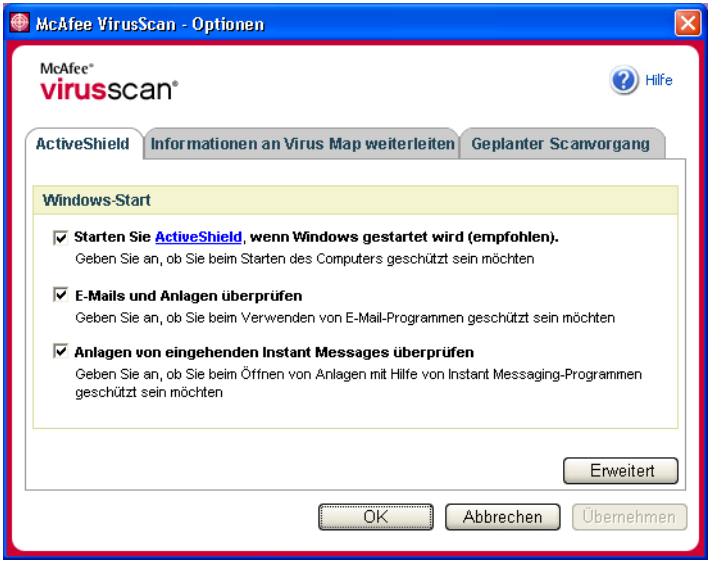


Abbildung 2-1. ActiveShield-Optionen

Starten von ActiveShield

ActiveShield wird standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol ), sobald Sie Ihren Computer nach erfolgreicher Installation neu starten.

Wenn ActiveShield angehalten ist (gekennzeichnet durch das schwarze Symbol ), können Sie das Programm so konfigurieren, dass es nach jedem Start von Windows automatisch ausgeführt wird (empfohlen).

> **HINWEIS**
> Während der Installation von VirusScan-Updates kann es dazu kommen, dass der **Update-Assistent** ActiveShield vorübergehend beendet, um neue Dateien zu installieren. Wenn Sie vom **Update-Assistenten** aufgefordert werden, auf **Beenden** zu klicken, wird ActiveShield erneut gestartet.

So starten Sie ActiveShield automatisch beim Start von Windows:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **McAfee VirusScan - Optionen** wird geöffnet (Abbildung 2-1 auf Seite 16).

2. Aktivieren Sie das Kontrollkästchen **Starten Sie ActiveShield**, **wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3. Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Anhalten von ActiveShield

> **WARNUNG**
> Mit dem Anhalten von ActiveShield verliert Ihr Computer den Virenschutz. Wenn Sie ActiveShield zu anderen Zwecken als zur Aktualisierung anhalten müssen, vergewissern Sie sich, dass keine Verbindung mit dem Internet besteht.

So verhindern Sie die automatische Ausführung von ActiveShield beim Start von Windows:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **McAfee VirusScan - Optionen** wird geöffnet (Abbildung 2-1 auf Seite 16).

2. Deaktivieren Sie das Kontrollkästchen **Starten Sie ActiveShield**, **wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3. Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Prüfen von E-Mails und Anlagen

Standardmäßig werden die E-Mail-Scan-Funktion und die automatische Bereinigungsfunktion über die Option **E-Mails und Anlagen überprüfen** (Abbildung 2-1 auf Seite 16) und **Infizierte Anlagen automatisch reinigen (empfohlen)** (Abbildung 2-2 auf Seite 20) aktiviert.

Wenn diese beiden Optionen aktiviert sind, führt ActiveShield automatisch die Virenprüfung durch und versucht, eingehende (POP3) und abgehende (SMTP) infizierte E-Mail-Nachrichten und Anlagen für den Großteil gängiger E-Mail-Clients zu reinigen. Hierzu zählen:

- Microsoft Outlook Express ab Version 4.0
- Microsoft Outlook ab Version 97
- Netscape Messenger ab Version 4.0
- Netscape Mail ab Version 6.0
- Eudora Light ab Version 3.0
- Eudora Pro ab Version 4.0
- Eudora ab Version 5.0
- Pegasus ab Version 4.0

HINWEIS

Für folgende E-Mail-Clients wird der E-Mail-Scan nicht unterstützt: Webbasierte E-Mail-Clients, IMAP, AOL, POP3 SSL und Lotus Notes. E-Mail-Anlagen werden beim Öffnen jedoch von ActiveShield geprüft.

Wenn Sie die Option **E-Mails und Anlagen überprüfen** deaktivieren, werden die E-Mail-Scan-Optionen (Abbildung 2-2 auf Seite 20) und die WormStopper-Optionen (Abbildung 2-5 auf Seite 25) automatisch deaktiviert. Bei Deaktivierung der Prüfung ausgehender E-Mails werden die WormStopper-Optionen ebenfalls automatisch deaktiviert.

Wenn Sie Ihre E-Mail-Scan-Optionen ändern, müssen Sie anschließend das E-Mail-Programm neu starten, um die Änderungen in Kraft zu setzen.

Eingehende E-Mails

Wenn eine eingehende E-Mail-Nachricht oder Anlage infiziert ist, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die infizierte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, unter Quarantäne zu stellen oder zu löschen.
- Es wird eine Warnungsdatei in die eingehende E-Mail aufgenommen, die Informationen zu den Schritten enthält, die zur Beseitigung der Infektion durchgeführt wurden.

Abgehende E-Mails

Wenn eine abgehende E-Mail-Nachricht oder Anlage infiziert ist, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die infizierte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, unter Quarantäne zu stellen oder zu löschen.
- Es wird eine Warnungsdatei in einer neuen E-Mail an Sie gesendet, die Informationen zu den Schritten enthält, die zur Beseitigung der Infektion durchgeführt wurden.

> **HINWEIS**
> Einzelheiten zu Fehlermeldungen bei der Prüfung ausgehender E-Mails finden Sie in der Online-Hilfe.

Standardmäßig prüft ActiveShield sowohl eingehende als auch ausgehende E-Mails. Bei Bedarf können Sie jedoch festlegen, dass nur die eingehende oder nur die ausgehende E-Mail von ActiveShield geprüft wird.

So deaktivieren Sie die Prüfung der eingehenden bzw. ausgehenden E-Mail:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **E-Mail-Scan** (Abbildung 2-2).
3. Heben Sie die Markierung des Kontrollkästchens **Eingehende E-Mail-Nachrichten** oder des Kontrollkästchens **Ausgehende E-Mail-Nachrichten** auf, und klicken Sie auf **OK**.

Wenn Ihr E-Mail-Server so eingestellt ist, dass E-Mails nur dann empfangen und gesendet werden, wenn Sie sich an Ihrem Computer befinden, können Sie angeben, dass Sie durch Warnungen zur Bereinigung infizierter E-Mails aufgefordert werden. Deaktivieren Sie hierzu die automatische Bereinigungsfunktion. Befolgen Sie die nachfolgenden Schritte, um die automatische Bereinigungsfunktion zu deaktivieren. Lesen Sie dann unter *Verwalten infizierter E-Mails* auf Seite 26 nach, um Informationen hinsichtlich der Reaktion auf Warnungen zu erhalten.

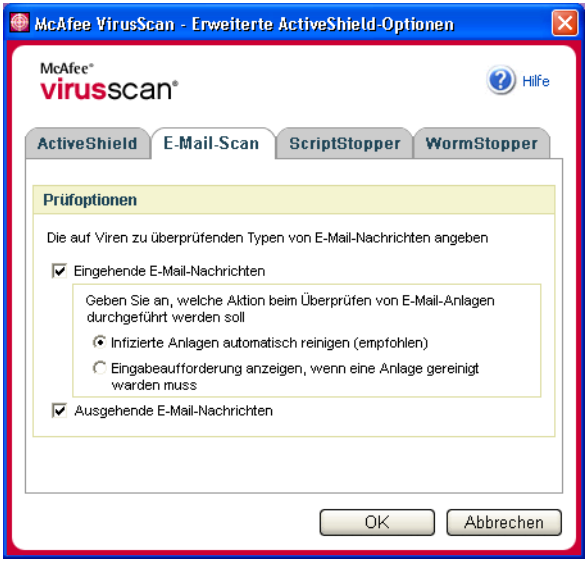


Abbildung 2-2. E-Mail-Scan-Optionen

So deaktivieren Sie die automatische Bereinigungsfunktion für infizierte E-Mails:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **E-Mail-Scan** (Abbildung 2-2).
3. Klicken Sie auf **Eingabeaufforderung anzeigen, wenn eine Anlage gereinigt werden muss**, und klicken Sie dann auf **OK**.

Überprüfen von Anlagen eingehender Instant Messages

Standardmäßig wird die Überprüfung von Instant Messages-Anlagen über die Option **Anlagen von eingehenden Instant Messages überprüfen** (Abbildung 2-1 auf Seite 16) aktiviert.

Wenn diese Option aktiviert ist, führt VirusScan automatisch die Virenprüfung durch und versucht, eingehende infizierte Instant Messages-Anlagen für den Großteil gängier Instant Messaging-Clients zu bereinigen. Hierzu zählen:

- MSN Messenger 6.0 oder höher
- Yahoo Messenger 4.1 oder höher
- AOL Instant Messenger ab Version 2.1

HINWEIS
Aus Sicherheitsgründen kann die automatische Reinigung von Instant Messages-Anhängen nicht deaktiviert werden.

Wenn eine eingehende Instant Messages-Anlage infiziert ist, führt VirusScan folgende Schritte durch:

- Es wird versucht, die infizierte Nachricht zu bereinigen
- Sie werden aufgefordert, die Nachricht, die nicht bereinigt werden kann, unter Quarantäne zu stellen oder zu löschen

Prüfen aller Dateien

Wenn Sie in ActiveShield die Standardeinstellung **Alle Dateien (empfohlen)** verwenden, werden alle Dateitypen durchsucht, auf die der Computer zugreift. Verwenden Sie diese Option, um die genaueste Prüfung durchzuführen.

So konfigurieren Sie ActiveShield für die Überprüfung aller Dateitypen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **ActiveShield** (Abbildung 2-3 auf Seite 22).
3. Klicken Sie auf **Alle Dateien (empfohlen)** und dann auf **OK**.

Abbildung 2-3. Erweiterte ActiveShield-Optionen

Ausschließliches Prüfen von Programmdateien und Dokumenten

Wenn Sie in ActiveShield die Option **Nur Programmdateien und Dokumente** auswählen, werden Programmdateien und Dokumente durchsucht, nicht jedoch andere auf Ihrem Computer verwendete Dateien. Durch die aktuellste Virussignaturdatei (DAT-Datei) wird bestimmt, welche Dateitypen von ActiveShield durchsucht werden. So lassen Sie in ActiveShield nur Programmdateien und Dokumente überprüfen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **ActiveShield** (Abbildung 2-3).
3. Klicken Sie auf **Nur Programmdateien und Dokumente** und dann auf **OK**.

Prüfen auf neue, unbekannte Viren

Wenn Sie ActiveShield so konfigurieren, dass die Standardoption **Nach neuen, unbekannten Viren scannen** verwendet wird, werden erweiterte heuristische Techniken, anhand derer eine Übereinstimmung zwischen den Dateien und Signaturen bekannter Viren ermittelt werden soll. Außerdem wird versucht, nicht identifizierte Viren in den Dateien anhand bestimmter Anzeichen zu ermitteln.

So konfigurieren Sie ActiveShield für die Prüfung auf neue, unbekannte Viren:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **ActiveShield** (Abbildung 2-3).
3. Klicken Sie auf **Nach neuen, unbekannten Viren scannen** und dann auf **OK**.

Prüfen auf Skripts und Würmer

VirusScan überwacht den Computer auf verdächtige Aktivität hin, die möglicherweise darauf hinweist, dass ihr Computer akut gefährdet ist. Durch VirusScan werden Viren bereinigt, durch ScriptStopper™ und WormStopper™ hingegen wird der weiteren Verbreitung von Viren, Würmern und Trojanern vorgebeugt.

Durch die ScriptStopper- und WormStopper-Schutzmechanismen werden bösartige Aktivitäten erkannt, gemeldet und blockiert. Zu verdächtigen Aktivitäten auf dem Computer zählt Folgendes:

- Eine Skriptausführung, die dazu führt, dass Dateien erstellt, kopiert oder gelöscht werden bzw. dass die Windows-Registrierung geöffnet wird.
- Ein Versuch, eine E-Mail an einen Großteil der Adressen in Ihrem Adressbuch weiterzuleiten.
- Versuche, mehrere E-Mail-Nachrichten in schneller Folge weiterzuleiten.

Wenn Sie ActiveShield so einstellen, dass die Standardoptionen **ScriptStopper aktivieren (empfohlen)** und **WormStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte ActiveShield-Optionen** verwendet werden, überwachen ScriptStopper und WormStopper die Skriptausführung und die E-Mail-Aktivität auf verdächtige Verfahren hin und geben eine Warnung aus, wenn eine festgelegte Anzahl an E-Mails oder Empfängern innerhalb eines festgelegten Intervalls überschritten werden.

So konfigurieren Sie ActiveShield für die Prüfung auf bösartige Skripts und Würmer:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **ScriptStopper**.
3. Klicken Sie auf **ScriptStopper aktivieren (empfohlen)** (Abbildung 2-4).

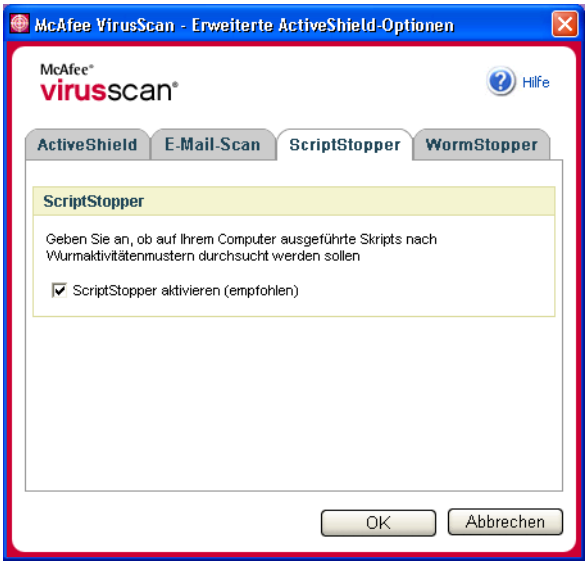


Abbildung 2-4. ScriptStopper-Optionen

4 Aktivieren Sie die Registerkarte **WormStopper**, klicken Sie auf **WormStopper aktivieren (empfohlen)**, und klicken Sie dann auf **OK** (Abbildung 2-5 auf Seite 25).

Standardmäßig sind folgende Detailoptionen aktiviert:

- Mustervergleich zur Erkennung verdächtiger Aktivität
- Warnung beim Senden einer E-Mail an 40 oder mehr Empfänger
- Warnung beim Senden von 5 oder mehr E-Mails innerhalb von 30 Sekunden

HINWEIS
Wenn Sie die Anzahl der Empfänger oder der Dauer für die Überprüfung gesendeter E-Mails ändern, kann es zu ungültigen (fehlerhaften) Erkennungen kommen. McAfee empfiehlt, die Standardeinstellung durch Klicken auf **Nein** beizubehalten. Andernfalls können Sie auf **Ja** klicken und die Standardeinstellung durch Ihre bevorzugten Einstellung ersetzen.

Diese Option kann automatisch aktiviert werden, nachdem zum ersten Mal ein potentieller Wurm entdeckt wurde (ausführliche Informationen finden Sie unter *Verwalten potentieller Würmer* auf Seite 27):

- Automatische Blockierung verdächtiger, abgehender E-Mails

Abbildung 2-5. WormStopper-Optionen

Wenn ActiveShield einen Virus findet

Wenn ActiveShield einen Virus findet, wird eine Viruswarnung ausgegeben, die Abbildung 2-6 ähnelt. Bei den meisten Viren, Trojanern und Würmern versucht ActiveShield automatisch, die Datei zu bereinigen. Anschließend können Sie angeben, wie mit infizierten Dateien, infizierten E-Mails, verdächtigen Skripts und potentiellen Würmern verfahren werden soll und ob infizierte Dateien zu Forschungszwecken an die McAfee AVERT-Laboratorien übermittelt werden sollen.

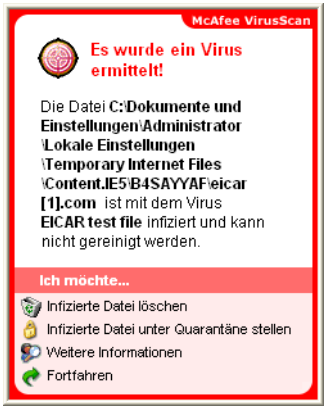


Abbildung 2-6. Viruswarnung

Verwalten infizierter Dateien

1 Wenn ActiveShield die Datei bereinigen kann, können Sie sich ausführlicher informieren oder die Warnung ignorieren:

- Klicken Sie auf **Weitere Informationen**, um den Dateinamen, den Speicherort und den Virusnamen für die infizierte Datei anzuzeigen.
- Klicken Sie auf **Aktuelle Tätigkeit fortfahren**, um die Warnung zu ignorieren und zu schließen.

2 Wenn ActiveShield die Datei nicht bereinigen kann, klicken Sie auf **Infizierte Datei unter Quarantäne stellen**, um infizierte und verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann.

Es wird eine Bestätigungsmeldung angezeigt, die Sie zum Überprüfen Ihres Computers auf Viren auffordert. Klicken Sie auf **Überprüfen**, um den Quarantäneprozess abzuschließen.

3 Wenn ActiveShield die Datei nicht unter Quarantäne stellen kann, klicken Sie auf **Infizierte Datei löschen**, um zu versuchen, die Datei zu entfernen.

Verwalten infizierter E-Mails

1 Wenn die automatische Bereingungsfunktion für E-Mails deaktiviert wurde, können Sie sich ausführlicher informieren und die E-Mail bereinigen.

a Klicken Sie auf **Weitere Informationen**, um den Dateinamen, den Virusnamen, den Infektionsstatus, den Absender und den Betreff der infizierten E-Mail anzuzeigen.

b Klicken Sie auf **Infizierte Anlage löschen**.

2 Wenn ActiveShield die E-Mail nicht bereinigen kann, klicken Sie auf **Infizierte Anlage unter Quarantäne stellen**, um infizierte und verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann.

Es wird eine Bestätigungsmeldung angezeigt, die Sie zum Überprüfen Ihres Computers auf Viren auffordert. Klicken Sie auf **Überprüfen**, um den Quarantäneprozess abzuschließen.

3 Wenn ActiveShield die E-Mail nicht unter Quarantäne stellen kann, klicken Sie auf **Infizierte Anlage löschen**, um zu versuchen, die Datei zu entfernen.

Verwalten verdächtiger Skripts

1. Wenn ActiveShield ein verdächtiges Skript erkennt, können Sie sich ausführlicher informieren und das Skript dann anhalten, wenn Sie nicht beabsichtigt hatten, es zu initiieren:

   a. Klicken Sie auf **Weitere Informationen**, um den Dateinamen, den Speicherort und die Bechreibung der Aktivität anzuzeigen, die mit dem verdächtigen Skript in Verbindung steht.

   b. Mit **Dieses Skript anhalten** können Sie die Ausführung des verdächtigen Skripts unterbinden.

2. Wenn Sie das Skript als vertrauenswürdig einschätzen, können Sie seine Ausführung zulassen:

   a. Klicken Sie auf **Dieses Mal alle Skripten zulassen**, um alle in einer einzelnen Datei enthalten Skripts dieses eine Mal auszuführen.

   b. Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Skript ausführen zu lassen.

Verwalten potentieller Würmer

1. Wenn ActiveShield einen potentiellen Wurm erkennt, können Sie sich ausführlicher informieren und die E-Mail-Aktivität dann anhalten, wenn Sie nicht beabsichtigt hatten, sie zu initiieren:

   a. Klicken Sie auf **Weitere Informationen**, um die Empfängerliste, die Betreffszeile, den Nachrichtentext und die Beschreibung der verdächtigen Aktivität anzuzeigen, die mit der infizierten E-Mail-Nachricht in Verbindung stehen.

   b. Mit **E-Mail anhalten** können Sie verhindern, dass die verdächtige E-Mail gesendet wird. Löschen Sie sie aus der Nachrichtenwarteschlange.

2. Wenn Sie die E-Mail-Aktivität als vertrauenswürdig einschätzen, klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Senden der E-Mail zuzulassen.

Manuelle Überprüfung des Computers

Mit der Scan-Funktion werden Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und potentiell unerwünschten Programmen durchsucht. Wenn bei der Überprüfung eine infizierte Datei gefunden wird, wird automatisch versucht, die Datei zu bereinigen, es sei denn, es handelt sich dabei um ein potentiell unerwünschtes Programm. Wenn Scan die Datei nicht bereinigen kann, können Sie die Datei unter Quarantäne stellen oder löschen.

Manuelle Überprüfung auf Viren und potentiell unerwünschte Programme

So überprüfen Sie Ihren Computer:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Auf Viren überprüfen**.

Das Dialogfeld **Auf Viren überprüfen** wird angezeigt (Abbildung 2-7).

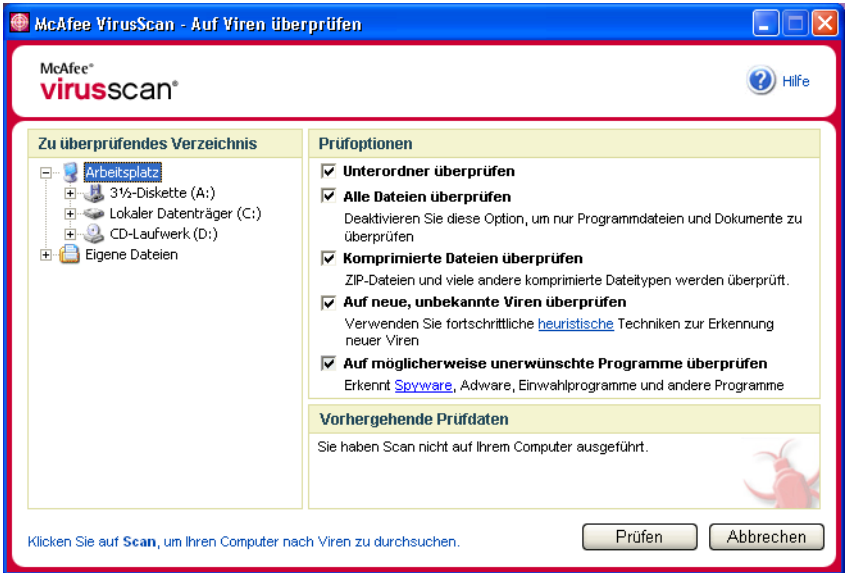


Abbildung 2-7. Auf Viren überprüfen

2 Klicken Sie auf das Laufwerk, den Ordner oder die Datei, die überprüft werden sollen.

3 Wählen Sie die gewünschten **Prüfoptionen**. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren Optionen aktiviert (Abbildung 2-7):

- **Unterordner überprüfen** – Verwenden Sie diese Option, um Dateien in Unterordnern auf Viren zu durchsuchen. Deaktivieren Sie dieses Kontrollkästchen, wenn nur die Dateien durchsucht werden sollen, die beim Öffnen eines Ordners oder Laufwerks angezeigt werden.

  Beispiel: Die Dateien in Abbildung 2-8 sind die einzigen Dateien, die durchsucht werden, wenn Sie das Kontrollkästchen **Unterordner überprüfen** deaktivieren. Die Ordner und ihr Inhalt werden nicht überprüft. Wenn sie ebenfalls durchsucht werden sollen, lassen Sie das Kontrollkästchen aktiviert.

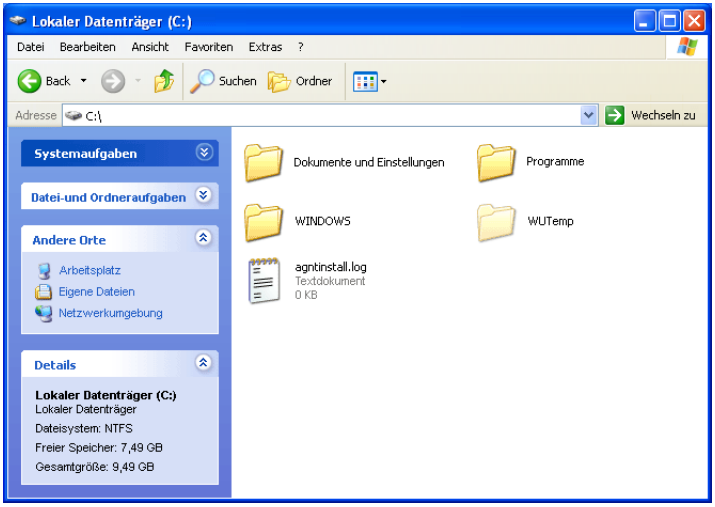


Abbildung 2-8. Inhalt lokaler Datenträger

- **Alle Dateien überprüfen** – Verwenden Sie diese Option, um eine umfassende Überprüfung aller Dateitypen zu gewährleisten. Deaktivieren Sie dieses Kontrollkästchen, um den Vorgang zu beschleunigen und nur Programmdateien und Dokumente zu durchsuchen.

- **Komprimierte Dateien überprüfen** – Verwenden Sie diese Option, um verborgene infizierte Dateien in ZIP-Dateien und anderen komprimierten Dateien einzublenden. Deaktivieren Sie dieses Kontrollkästchen, um die Überprüfung jeglicher Dateien oder komprimierter Dateien in der komprimierten Datei zu unterbinden.

  Manchmal werden Viren in eine ZIP-Datei eingesetzt und diese ZIP-Datei anschließend in eine andere ZIP eingefügt, um Anti-Virus-Scanner zu umgehen. Wenn Sie diese Option aktiviert belassen, kann Scan diese Viren ermitteln.

- **Auf neue, unbekannte Viren überprüfen** – Mit Hilfe dieser Option ermitteln Sie die neuesten Viren, für die es eventuell noch kein Gegenmittel gibt. Die Option **Auf neue, unbekannte Viren überprüfen** verwendet erweiterte heuristische Techniken, anhand derer eine Übereinstimmung zwischen den Dateien und den Signaturen bekannter Viren ermittelt werden soll. Außerdem wird versucht, nicht identifizierte Viren in den Dateien anhand bestimmter Anzeichen zu ermitteln.

  Bei diesem Scanverfahren wird auch nach charakteristischen Merkmalen in Dateien gesucht, die eine Virusinfektion prinzipiell ausschließen. Dadurch wird weitgehend verhindert, dass Scan falsche Meldungen ausgibt. Wenn mit dem heuristischen Verfahren jedoch ein Virus in einer Datei gefunden wird, sollten Sie dieselben Maßnahmen wie bei einem bekannten Virus ergreifen.

  Diese Option bietet einen äußerst gründlichen Scanvorgang, der jedoch zeitaufwendiger als ein normaler Scanvorgang ist.

- **Auf möglicherweise unerwünschte Programme überprüfen** – Verwenden Sie diese Option, um Spyware, Adware, Einwahlprogramme und andere Programme ausfindig zu machen, die nicht auf Ihrem Computer installiert werden sollten.

  HINWEIS
  Lassen Sie alle Optionen aktiviert, um die Überprüfung so gründlich wie möglich zu gestalten. Dadurch dauert die Überprüfung etwas länger, aber jede Datei im gewählten Laufwerk oder Ordner wird effektiv überprüft. Je größer die Festplatte ist und je mehr Dateien Sie haben, umso länger dauert die Überprüfung.

4 Klicken Sie auf **Prüfen**, um mit dem Überprüfen der Dateien zu beginnen.

Nach Abschluss der Scan-Funktion wird in einer Zusammenfassung angezeigt, wie viele Dateien überprüft und erkannt wurden, wie viele potentiell unerwünschten Programme gefunden wurden sowie wie viele erkannte Dateien automatisch bereinigt wurden.

5 Klicken Sie auf **OK**, um die Zusammenfassung zu schließen und die Liste der erkannten Dateien im Dialogfeld **Auf Viren überprüfen** anzuzeigen (Abbildung 2-9).

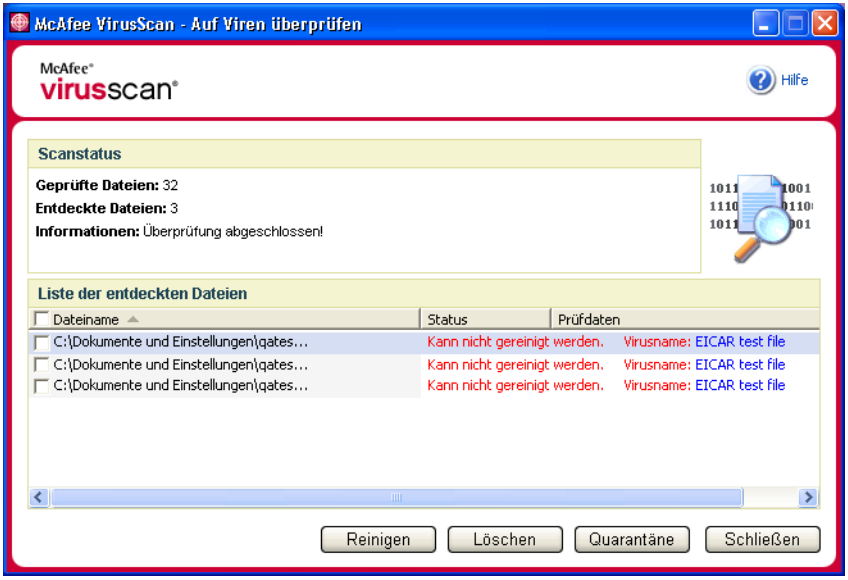


Abbildung 2-9. Scanergebnisse

HINWEIS
Innerhalb der geprüften Dateien zählt Scan eine komprimierte Datei (ZIP, CAB usw.) als eine Datei. Die Anzahl der durchsuchten Dateien kann variieren, wenn Sie Ihre temporären Internetdateien seit Ihrer letzten Überprüfung gelöscht haben.

6 Wenn Scan keine Viren oder potentiell unerwünschten Programme ermittelt, klicken Sie auf **Zurück**, um ein anderes Laufwerk oder einen anderen Ordner zur Überprüfung auszuwählen, oder auf **Schließen**, um das Dialogfeld zu schließen. Informieren Sie sich andernfalls unter *Wenn die Scan-Funktion einen Virus oder ein potentiell unerwünschtes Programm findet* auf Seite 35.

Prüfen über Windows-Explorer

VirusScan ermöglicht die Verwendung eines Kontextmenüs, mit dem ausgewählte Dateien, Ordner oder Laufwerke über Windows-Explorer auf Viren oder potentiell unerwünschte Programme geprüft werden können.

So überprüfen Sie Dateien in Windows-Explorer:

1. Öffnen Sie Windows-Explorer.
2. Klicken Sie mit der rechten Maustaste auf das Laufwerk, den Ordner oder die Datei, die überprüft werden sollen, und klicken Sie dann auf **Auf Viren überprüfen**.

   Das Dialogfeld **Auf Viren überprüfen** wird angezeigt, und es wird mit der Überprüfung der Dateien begonnen. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren Standardoptionen aktiviert (Abbildung 2-7 auf Seite 28).

Prüfen über Microsoft Outlook

VirusScan enthält ein Kontextmenü, mit dem ausgewählte Nachrichtenspeicher und die zugehörigen Unterordner, Mailbox-Ordner bzw. E-Mail-Nachrichten mit Anlagen in Microsoft Outlook 97 (oder höher) auf Viren und potentiell unerwünschte Programme überprüft werden können.

So überprüfen Sie E-Mails in Microsoft Outlook:

1. Öffnen Sie Microsoft Outlook.
2. Klicken Sie auf den Nachrichtenspeicher, Ordner oder die E-Mail-Nachricht mit Anlage, die überprüft werden sollen, und klicken Sie dann in der Symbolleiste auf das E-Mail-Scan-Symbol  .

   Der E-Mail-Scanner wird geöffnet und beginnt mit der Überprüfung von Dateien. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren Standardoptionen aktiviert (Abbildung 2-7 auf Seite 28).

Automatische Überprüfung auf Viren und potentiell unerwünschte Programme

Obwohl VirusScan Dateien überprüft, wenn Sie oder Ihr Computer darauf zugreifen, können Sie im Windows-Taskplaner die automatische Überprüfung planen, um den Computer in festgelegten Intervallen gründlich nach Viren und potentiell unerwünschten Programmen zu durchsuchen.

So planen Sie einen Scanvorgang:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **McAfee VirusScan - Optionen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Geplanter Scanvorgang** (Abbildung 2-10 auf Seite 33).

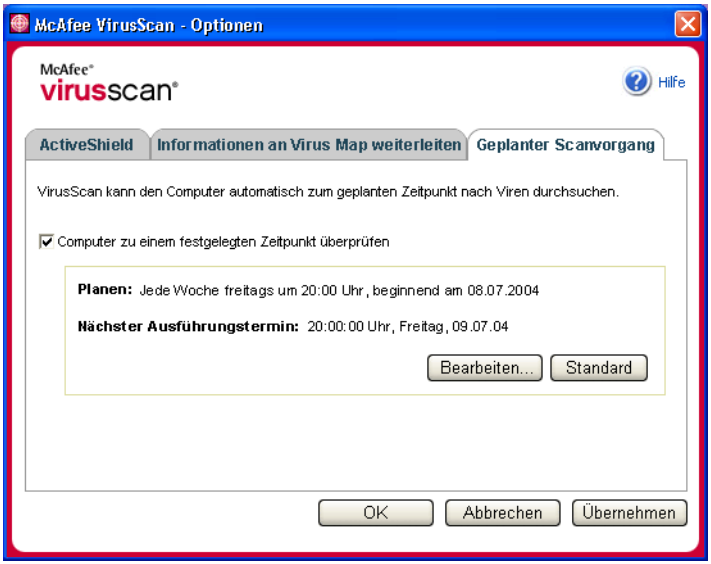


Abbildung 2-10. Optionen für geplante Scanvorgänge

3 Aktivieren Sie das Kontrollkästchen **Computer zu einem festgelegten Zeitpunkt überprüfen**, um die automatische Prüfung zu aktivieren.

4 So planen Sie eine automatische Überprüfung:

- Wenn Sie den standardmäßigen Zeitplan (freitags um 20 Uhr) akzeptieren möchten, klicken Sie auf **OK**.
- So bearbeiten Sie den Zeitplan:

  a. Klicken Sie auf **Bearbeiten**.

  Wählen Sie in der Liste **Task ausführen**, wie oft Ihr Computer überprüft werden soll, und wählen Sie dann weitere Optionen in dem darunter liegenden dynamischen Bereich aus:

  Täglich – Geben Sie die Anzahl der Tage zwischen Scanvorgängen an.

  Wöchentlich (Standardeinstellung) – Geben Sie die Anzahl der Wochen zwischen den Scans und die Wochentage an, an denen die Scans ausgeführt werden sollen.

  Monatlich – Geben Sie den Tag an, an dem der Scan ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um die Monate auszuwählen, in denen gescannt werden soll, und klicken Sie dann auf **OK**.

  Einmal – Geben Sie das Datum an, an dem der Scan ausgeführt werden soll.

  HINWEIS
  Folgende Optionen werden im Windows-Taskplaner nicht unterstützt:
  Beim Systemstart, **Im Leerlauf** und **Mehrfache Zeitpläne anzeigen**. Der letzte unterstützte Zeitplan bleibt so lange aktiv, bis Sie eine gültige Option auswählen.

  c. Wählen Sie im Feld **Startzeit** die Tageszeit aus, zu der der Computer überprüft werden soll.

  d. Wenn Sie erweiterte Optionen einstellen möchten, klicken Sie auf **Erweitert**.

  Das Dialogfeld **Erweiterte Zeitplanoptionen** wird angezeigt.

  i. Geben Sie Startdatum, Enddatum, Dauer und Endzeitpunkt ein, und geben Sie an, ob der Scanvorgang zur festgelegten Zeit beendet werden soll, wenn die Überprüfung noch nicht beeendet ist.

  ii. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

6 Wenn Sie zum standardmäßigen Zeitplan zurückkehren möchten, klicken Sie auf **Standard**. Anderenfalls klicken Sie auf **OK**.

Wenn die Scan-Funktion einen Virus oder ein potentiell unerwünschtes Programm findet

Bei den meisten Viren, Trojanern und Würmern versucht Scan automatisch, die Datei zu bereinigen. Anschließend können Sie angeben, wie mit erkannten Dateien verfahren werden soll und ob sie zu Forschungszwecken an die McAfee AVERT-Labore übermittelt werden sollen. Wenn die Scan-Funktion ein potentiell unerwünschtes Programm findet, können Sie manuell versuchen, es zu bereinigen, unter Quarantäne zu stellen oder zu löschen (Einsenden an AVERT ist nicht möglich).

So gehen Sie mit einem Virus oder potentiell unerwünschten Programm vor:

1. Wenn eine Datei in der **Liste der entdeckten Dateien** angezeigt wird, aktivieren Sie das Kontrollkästchen vor der Datei.

   HINWEIS
   Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für sämtliche Dateien durchzuführen. Sie können auch auf den Dateinamen in der Liste **Prüfdaten** klicken, um Details aus der Virus Information Library anzuzeigen.

2. Wenn es sich bei der Datei um ein potentiell unerwünschtes Programm handelt, können Sie auf **Reinigen** klicken, um sie zu bereinigen.

3. Wenn Scan die Datei nicht bereinigen kann, klicken Sie auf **Quarantäne**, um infizierte und verdächtige Dateien zu verschlüsseln und im Quarantäne-verzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann. (Weitere Informationen finden Sie unter *Verwalten von Dateien unter Quarantäne*.)

4. Wenn Scan die Datei nicht bereinigen oder unter Quarantäne stellen kann, haben Sie folgende Möglichkeiten:

   - Klicken Sie auf **Löschen**, um die Datei zu entfernen.
   - Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Maßnahmen zu ergreifen.

Wenn Scan die erkannte Datei weder bereinigen noch löschen kann, rufen Sie die Virus Information Library unter http://us.mcafee.com/virusInfo/default.asp auf. Dort finden Sie Anweisungen zum manuellen Löschen der Datei.

Wenn die erkannte Datei das Herstellen einer Internetverbindung verhindert bzw. Sie Ihren Computer nicht mehr verwenden können, starten Sie den Computer mit einer Rettungsdiskette. In vielen Fällen kann ein infizierter Computer über die Rettungsdiskette wieder gestartet werden. Nähere Informationen dazu finden Sie unter „Erstellen einer Rettungsdiskette“ in der Online-Hilfe.

Weitere Hilfe erhalten Sie vom McAfee-Kundendienst unter http://www.mcafeehilfe.com/.

Verwalten von Dateien unter Quarantäne

Mit Hilfe der Quarantäne-Funktion können Sie infizierte und verdächtige Dateien verschlüsseln und temporär in einem Quarantäneverzeichnis unter Quarantäne stellen, bis eine angemessene Maßnahme ergriffen werden kann. Nach der Reinigung können in Quarantäne gestellte Dateien am ursprünglichen Speicherort wiederhergestellt werden.

So verwalten Sie eine unter Quarantäne gestellte Datei:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan Professional**, und klicken Sie dann auf **Dateien unter Quarantäne verwalten**.

Eine Liste mit Dateien unter Quarantäne wird angezeigt (Abbildung 2-11).

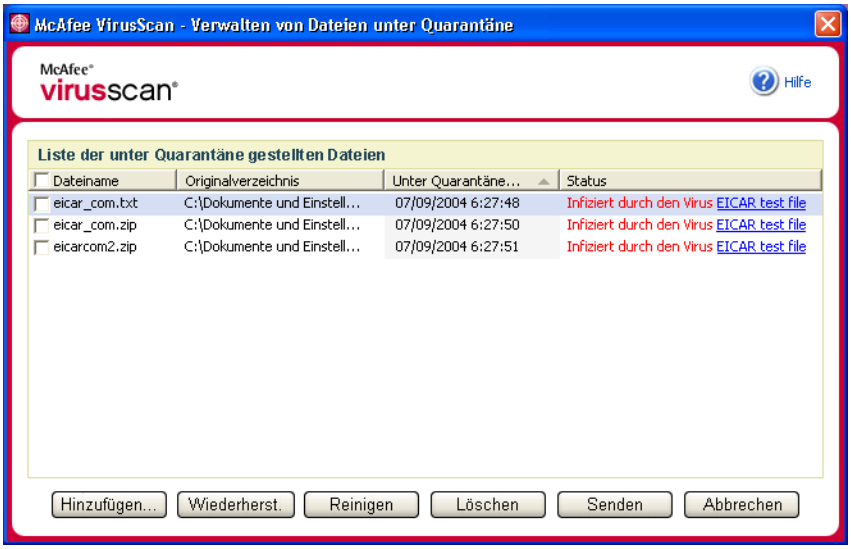


Abbildung 2-11. Verwalten von Dateien unter Quarantäne

2 Aktivieren Sie das Kontrollkästchen neben den Dateien, die bereinigt werden sollen.

HINWEIS
Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für sämtliche Dateien durchzuführen. Sie können auch auf den Virusnamen in der Liste **Status** klicken, um Details aus der Virus Information Library anzuzeigen.

Alternativ klicken Sie auf **Hinzufügen**, wählen Sie eine verdächtige Datei aus, die der Quarantäneliste hinzugefügt werden soll, klicken Sie auf **Öffnen**, und wählen Sie sie dann in der Quarantäneliste aus.

3 Klicken Sie auf **Reinigen**.

4 Wenn die Datei bereinigt ist, klicken Sie auf **Wiederherst.**, um die Datei wieder an ihren ursprünglichen Speicherort zu verschieben.

5 Wenn VirusScan den Virus nicht bereinigen kann, klicken Sie auf **Löschen**, um die Datei zu entfernen.

6 Wenn VirusScan die Datei nicht bereinigen oder löschen kann und es sich nicht um ein potentiell unerwünschtes Programm handelt, können Sie die Datei zu Forschungszwecken an das McAfee AntiVirus Emergency Response Team (AVERT™) übermitteln:

a Aktualisieren Sie die Virussignaturdateien, wenn Sie älter als zwei Wochen sind.

b Überprüfen Sie Ihr Abonnement.

c Wählen Sie die Datei aus, und klicken Sie auf **Senden**, um die Datei an AVERT zu übermitteln.

VirusScan sendet die unter Quarantäne gestellte Datei als Anlage einer E-Mail-Nachricht, die Ihre E-Mail-Adresse, Ihr Land, die Softwareversion, das Betriebssystem sowie den ursprünglichen Namen und Standort der Datei enthält. Pro Tag darf maximal eine Datei mit 1,5 MB übermittelt werden.

7 Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Maßnahmen zu ergreifen.

Verwendung der Professional Edition-Software 3

Die McAfee VirusScan Professional Edition enthält McAfee VirusScan plus zusätzliche Software, McAfee SpamKiller und McAfee Shredder.

HINWEIS
Es handelt sich hierbei nur um eine kurze Übersicht. Detaillierte Informationen finden Sie in der Online-Hilfe für VirusScan, SpamKiller oder Shredder.

Verwendung von McAfee SpamKiller

McAfee SpamKiller hilft Ihnen, Ihren E-Mail-Posteingang frei von Spam-E-Mails zu halten.

HINWEIS
McAfee SpamKiller filtert MSN/Hotmail, filtert aber derzeit weder AOL, noch Yahoo oder andere webbasierte E-Mail-Konten.

Überblick

Während der Installation haben Sie ein oder mehrere E-Mail-Konten angegeben, für die ungewollte Nachrichten blockiert werden sollen. Sie haben auch E-Mail-Adressbücher in Ihre Freunde-Liste importiert, um zu verhindern, dass Nachrichten von unbekannten Absendern blockiert werden.

So verwalten Sie Spam:

1. Öffnen Sie Ihr E-Mail-Programm wie gewöhnlich, um E-Mail-Nachrichten anzuzeigen, zu senden und zu empfangen.
2. Öffnen von SpamKiller:

   Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol  , zeigen Sie auf **SpamKiller**, und klicken Sie dann auf **Blockierte Mails anzeigen**, **Zusammenfassung anzeigen**, **Freunde anzeigen**, bzw. **Einstellungen**. Die entsprechende Seite wird eingeblendet.

   HINWEIS
   Wenn das Dialogfeld **Anmelden** erscheint, geben Sie Ihr SpamKiller-Anmeldekennwort ein, und klicken Sie dann auf **OK**.

Zusammenfassung (Seite)

Durch Klicken auf das Symbol **Zusammenfassung** im linken Bereich des Fensters wird die Seite **Zusammenfassung** geöffnet. Hier finden Sie folgende Informationen:

- **Status** zeigt an, ob der Filter aktiviert wurde, wann die Freunde-Liste zum letzten Mal aktualisiert wurde und wie viele Spam-Nachrichten heute eingegangen sind. Sie können hier den SpamKiller-Filter deaktivieren bzw. wieder aktivieren, die Freunde-Liste aktualisieren und die Registerkarte **Blockierte E-Mails** öffnen.
- **Neuer Spam** zeigt die zuletzt eingegangenen Spam-Nachrichten an, die von SpamKiller blockiert wurden (Nachrichten, die aus dem Posteingang entfernt wurden). Wenn Sie eine Nachricht wieder in Ihren Posteingang zurückholen möchten, klicken Sie auf das **Retten**-Symbol neben der Nachricht.
- **E-Mail-Übersicht** zeigt die Gesamtzahl der E-Mails, die Zahl der wegen Spam blockierten Nachrichten und den prozentualen Anteil der Spam-Nachrichten an den gesamten eingegangenen E-Mails an.
- **Neuer Spam** gibt einen Überblick über die Arten von Spam-Nachrichten, die in den letzten 30 Tagen eingegangen sind.

Microsoft Outlook- und Outlook Express-Integration

Kernfunktionen von SpamKiller können direkt von Outlook Express 6.0, Outlook 98, Outlook 2000 und Outlook XP aus genutzt werden. In der Outlook- und der Outlook Express-Symbolleiste stehen zu diesem Zweck Schaltflächen zur Verfügung, mit deren Hilfe Sie Spam blockieren, Personen zur Freunde-Liste hinzufügen und Ihre blockierten E-Mails einsehen können:

- Klicken Sie auf die Symbolschaltfläche **Nachricht blockieren**  , wenn die ausgewählte Nachricht aus Ihrem Microsoft Outlook-Posteingang entfernt und in den SpamKiller-Ordner **Blockierte E-Mails** verschoben werden soll.
- Klicken Sie auf die Symbolschaltfläche **Durch SpamKiller blockierte E-Mails anzeigen**  , wenn Sie sich die Nachrichten anzeigen lassen möchten, die aus Ihrem Microsoft Outlook-Posteingang entfernt und in den SpamKiller-Ordner **Blockierte E-Mails** verschoben wurden.
- Klicken Sie auf die Symbolschaltfläche **Freund hinzufügen**  , wenn die E-Mail-Adresse des Absenders der Nachricht zur persönlichen Freunde-Liste hinzugefügt werden soll.

Rechts von den Standardsymbolleisten in Outlook und Outlook Express erscheint eine SpamKiller-Symbolleiste. Wenn die Symbolleiste nicht zu sehen ist, vergrößern Sie entweder das Fenster Ihres E-Mail-Programms, oder klicken Sie auf die Pfeilsymbole, um weitere Symbolleisten anzuzeigen.

Wenn die SpamKiller-Symbolleiste zum ersten Mal in Ihrem E-Mail-Programm angezeigt wird, können Sie die Optionen in dieser Symbolleiste nur auf neue Nachrichten anwenden. Bereits im Posteingang vorhandene Spam-Nachrichten müssen manuell gelöscht werden.

Arbeiten mit blockierten und akzeptierten Nachrichten

Durch Klicken auf die Symbolschaltfläche **Nachrichten** haben Sie Zugriff auf die Nachrichten, die von SpamKiller blockiert bzw. akzeptiert wurden. Die Registerkarten **Blockierte E-Mails** und **Akzeptierte E-Mails** sind im Wesentlichen gleich strukturiert.

Registerkarte „Blockierte E-Mails“

Durch Klicken auf den Reiter der Registerkarte **Blockierte E-Mails** auf der Seite **Nachrichten** können Sie sich die von SpamKiller blockierten Nachrichten anzeigen lassen.

> **HINWEIS**
> Microsoft Outlook-Benutzer können sich die blockierten Nachrichten auch über Ihr Outlook-Konto anzeigen lassen. Öffnen Sie dazu Ihren Outlook-Posteingang, und klicken Sie dann auf  in der Symbolleiste von Microsoft Outlook bzw. Outlook Express.

Blockierte Nachrichten werden die Nachrichten genannt, die von SpamKiller als Spam identifiziert wurden. SpamKiller entfernt diese Nachrichten aus Ihrem Posteingang und verschiebt Sie in den Ordner **Blockierte E-Mails**.

Auf der Registerkarte **Blockierte E-Mails** werden alle Spam-Nachrichten angezeigt, die aus Ihren E-Mail-Konten entfernt wurden. Wenn Sie sich die blockierten Nachrichten für ein bestimmtes Konto anzeigen lassen möchten, klicken Sie auf dem Reiter der Registerkarte **Blockierte E-Mails** auf den nach unten zeigenden Pfeil , und wählen Sie das Konto aus, das angezeigt werden soll.

Im oberen Bereich der Seite **Nachrichten** werden die blockierten Nachrichten, nach Datum sortiert, aufgelistet. Die neueste Nachricht erscheint zuerst. Im unteren Teil wird der Text der oben ausgewählten Nachricht angezeigt.

> **HINWEIS**
> Wenn Sie als Betriebssystem Windows 2000 oder Windows XP verwenden, SpamKiller mehrere Benutzer hinzugefügt wurden und Sie sich bei SpamKiller als Benutzer mit eingeschränkten Rechten angemeldet haben, wird der Inhalt der Nachricht nicht angezeigt.

Der mittlere Fensterbereich enthält nähere Informationen zur Nachricht. Klicken Sie auf die Schaltfläche mit den nach unten zeigenden Pfeilen  , um den Fensterbereich mit den Nachrichtendetails zu erweitern und sich den Nachrichtentext und die Informationen im Nachrichten-Header im nativen Format, einschließlich aller HTML-Formatierungs-Tags, anzeigen zu lassen. Der Bereich mit den Nachrichtendetails enthält die folgenden Informationen:

- **Vorgang** beschreibt, wie SpamKiller die Spam-Nachricht behandelt hat. Vorgang ist mit der Aktion des Filters verknüpft, der die Nachricht blockiert hat.
- **Grund** erläutert, warum die Nachricht von SpamKiller blockiert wurde. Sie können auf den Grund klicken, um den Filter-Editor zu öffnen und sich den Filter anzeigen zu lassen. Der Filter-Editor zeigt an, wonach der Filter in einer Nachricht sucht und welche Maßnahmen SpamKiller gegen Nachrichten ergreift, die vom Filter als Spam erkannt werden.

- **Von** zeigt den Absender der Nachricht an.
- **Datum** zeigt das Sendedatum der Nachricht an.
- **An** zeigt an, an wen die Nachricht gesendet wurde.
- **Betreff** zeigt das Thema der Nachricht in der Betreffzeile an.

Wenn manuelle Beschwerden oder Fehlermeldungen gesendet wurden, wird in der Spalte am linken Rand für die jeweilige Nachricht eines der folgenden Symbole angezeigt:

 Eine Beschwerde über diese Nachricht wurde gesendet.

 Zeigt an, dass an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet wurde.

 Zeigt an, dass sowohl eine Beschwerde als auch eine Fehlermeldung gesendet wurden.

Registerkarte „Akzeptierte E-Mails“

Durch Klicken auf den Reiter der Registerkarte **Akzeptierte E-Mails** auf der Seite **Nachrichten** können Sie sich die von SpamKiller als erwünscht erkannten Nachrichten anzeigen lassen.

Auf der Registerkarte **Akzeptierte E-Mails** werden alle Nachrichten in den Posteingängen aller Ihrer E-Mail-Konten angezeigt. Bei MAPI-Konten enthält die Registerkarte **Akzeptierte E-Mails** jedoch keine internen E-Mails. Wenn Sie sich die akzeptierten Nachrichten für ein bestimmtes Konto anzeigen lassen möchten, klicken Sie auf dem Reiter der Registerkarte **Akzeptierte E-Mails** auf den nach unten zeigenden Pfeil  , und wählen Sie das Konto aus, das angezeigt werden soll.

HINWEIS
SpamKiller ist so eingerichtet, dass es erwünschte E-Mail-Nachrichten akzeptiert und nicht blockiert. Falls es einmal passieren sollte, dass an sich erwünschte E-Mail-Nachrichten doch blockiert wurden und auf der Registerkarte **Blokkierte E-Mails** erscheinen, können Sie diese Nachrichten in den Posteingang (und damit in die Liste auf der Registerkarte **Akzeptierte E-Mails**) zurückholen, indem Sie sie auswählen und dann auf **Diese Nachricht retten** klicken.

Im oberen Bereich der Registerkarte **Akzeptierte E-Mails** werden die akzeptierten Nachrichten, nach Datum sortiert, aufgelistet. Im unteren Bereich wird der Text der oben ausgewählten Nachricht angezeigt.

Im mittleren Bereich finden Sie Informationen dazu, ob die Nachricht von jemandem aus der Freunde-Liste stammt oder die Kriterien eines Filters erfüllt, für den als Aktion entweder **Akzeptieren** oder **Als möglichen Spam markieren** festgelegt wurde. Klicken Sie auf die Schaltfläche mit den nach unten zeigenden Pfeilen, um den Fensterbereich mit den Nachrichtendetails zu erweitern und sich den Nachrichtentext und die Informationen im Nachrichten-Header im nativen Format, einschließlich aller HTML-Formatierungs-Tags, anzeigen zu lassen.

Der Bereich mit den Nachrichtendetails enthält die folgenden Informationen:

- **Vorgang** beschreibt, wie SpamKiller die Nachricht behandelt hat.
- **Grund** erläutert, warum die Nachricht von SpamKiller markiert wurde.
- **Von** zeigt den Absender der Nachricht an.
- **Datum** zeigt das Sendedatum der Nachricht an.
- **An** zeigt an, an wen die Nachricht gesendet wurde.
- **Betreff** zeigt das Thema der Nachricht in der Betreffzeile an.

Neben einer akzeptierten Nachricht wird eines der folgenden Symbole angezeigt:

SpamKiller hat erkannt, dass der Absender der Nachricht in einer der Freunde-Listen eingetragen ist.

Die Nachricht erfüllt die Kriterien eines Filters, für den als Aktion **Als möglichen Spam markieren** festgelegt wurde.

Eine Beschwerde über diese Nachricht wurde gesendet.

Zeigt an, dass an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet wurde.

Zeigt an, dass sowohl eine Beschwerde als auch eine Fehlermeldung gesendet wurden.

Aufgaben für blockierte und akzeptierte Nachrichten

Im Bereich auf der rechten Seite der Registerkarten **Blockierte E-Mails** und **Akzeptierte E-Mails** finden Sie unter der Überschrift Ich möchte… eine Liste von Aufgaben, die Sie ausführen können:

- **Diese Nachricht blockieren** entfernt die Nachricht aus Ihrem Posteingang und verschiebt sie in den SpamKiller-Ordner für **Blockierte E-Mails**. (Diese Option erscheint nur auf der Seite **Akzeptierte E-Mails**.)
- Mit dem Symbol **Retten** können Sie eine Nachricht wieder in Ihren Posteingang zurückholen und das Dialogfeld Wiederherstellungsoptionen öffnen. (Diese Option erscheint nur auf der Seite **Blockierte E-Mails**.) Sie können den Absender automatisch zur Freunde-Liste hinzufügen lassen und somit alle Nachrichten von diesem Absender retten.

- **Diese Nachricht löschen** löscht die ausgewählte Nachricht.
- **Freund hinzufügen** ermöglicht das Hinzufügen des Namens bzw. der E-Mail-Adresse eines Absenders, einer ganzen Domäne oder einer Mailing-Liste zu einer Freunde-Liste.
- **Filter hinzufügen** ermöglicht das Erstellen eines Filters.
- **Bei McAfee melden** ermöglicht es Ihnen, McAfee über bestimmte nicht blockierte Spam-Nachrichten in Kenntnis zu setzen, die Sie empfangen haben.
- **Beschwerde senden** sendet eine Beschwerde über die Spam-Nachricht an den Administrator der Domäne des Absenders bzw. an eine andere von Ihnen angegebene E-Mail-Adresse.
- **Fehler senden** sendet eine Fehlermeldung an die in der Spam-Nachricht angegebene Antwortadresse.

Retten von Nachrichten

Wenn die Registerkarte **Blockierte E-Mails** E-Mails enthält, die eigentlich erwünscht sind, können Sie diese Nachrichten in den Posteingang zurückholen.

So retten Sie eine Nachricht:

1. Durch SpamKiller blockierte E-Mails anzeigen:
   - Klicken Sie in Spamkiller auf die Registerkarte **Nachrichten**, und klicken Sie anschließend auf die Registerkarte **Blockierte E-Mails**.
   - Klicken Sie im Posteingang von Microsoft Outlook oder Outlook Express auf die Symbolschaltfläche  , um die Registerkarte **Blockierte E-Mails** für dieses Konto zu öffnen.

   Die Registerkarte **Blockierte E-Mails** wird angezeigt.
2. Wählen Sie eine Nachricht aus, und klicken Sie anschließend auf **Diese Nachricht retten**.

   Das Dialogfeld Wiederherstellungsoptionen wird geöffnet mit folgenden ausgewählten Standardoptionen:
   - **Freund hinzufügen**
   - **Alle vom selben Absender wiederherstellen**
3. Klicken Sie auf **OK**. Der Absender wird Ihrer Freunde-Liste hinzugefügt und alle Nachrichten von diesem Absender werden wieder in Ihren Posteingang verschoben und erscheinen im Ordner **Akzeptierte E-Mails**.

Blockieren von Nachrichten

Sie können Spam-Nachrichten, die sich derzeit in Ihrem Posteingang befinden, manuell blockieren. Beim Blockieren einer Nachricht erstellt SpamKiller automatisch einen Filter, mit dem diese Nachricht aus dem Posteingang entfernt wird. Nachrichten im Posteingang können Sie sowohl von der Registerkarte **Akzeptierte E-Mails** als auch von Microsoft Outlook aus blockieren.

So blockieren Sie eine Nachricht von der Registerkarte **Akzeptierte E-Mails** aus:

1. Klicken Sie auf die Seite **Nachrichten**, und klicken Sie dann auf den Reiter der Registerkarte **Akzeptierte E-Mails**. Die Seite **Akzeptierte E-Mails** wird geöffnet, und es werden die Nachrichten angezeigt, die sich derzeit im Posteingang befinden.
2. Wählen Sie eine Nachricht aus, und klicken Sie anschließend auf **Diese Nachricht blockieren**. Die Nachricht wird aus dem Posteingang und von der Registerkarte **Akzeptierte E-Mails** entfernt, und im Ordner **Blockierte E-Mails** wird eine Kopie der Nachricht angezeigt.

So blockieren Sie eine Nachricht von Microsoft Outlook aus:

1. Öffnen Sie Ihren Posteingang von Microsoft Outlook bzw. Outlook Express. Sie können nur externe Nachrichten blockieren, also Nachrichten, die über einen Internet-Server empfangen wurden.
2. Wählen Sie eine Nachricht aus, und klicken Sie anschließend auf  . Im Ordner **Blockierte E-Mails** wird eine Kopie der Nachricht abgelegt.

Löschen von Nachrichten

Wenn SpamKiller Spam-Nachrichten findet, entfernt es diese standardmäßig aus Ihrem Posteingang und verschiebt sie in den SpamKiller-Ordner **Blockierte E-Mails**. Nach Ablauf von 15 Tagen werden dann die blockierten Nachrichten von SpamKiller automatisch aus dem Ordner **Blockierte E-Mails** gelöscht. Sie können die Häufigkeit dieser automatischen Löschvorgängen ändern oder die Nachrichten manuell entfernen.

Nachrichten aus dem Ordner **Akzeptierte E-Mails** werden von SpamKiller nicht automatisch gelöscht, weil dieser Ordner die gleichen Nachrichten wie Ihr Posteingang enthält.

Statt Spam-Nachrichten in den Ordner **Blockierte E-Mails** zu verschieben, können Sie SpamKiller auch anweisen, in der Betreffzeile der E-Mail das Tag [Spam] oder ein anderes Tag Ihrer Wahl hinzuzufügen und die Nachricht im Posteingang zu belassen. Das Markieren von Nachrichten mit Tags ist vor allem dann sinnvoll, wenn Sie die so markierten Nachrichten in einen anderen Ordner in Ihrem E-Mail-Client verschieben möchten, z. B. wenn Sie sich einen Ordner namens Müll angelegt haben. Sie können die mit Tags versehenen Nachrichten verschieben, indem Sie in Ihrem E-Mail-Client eine Regel erstellen, mit der nach Nachrichten mit dem Tag [Spam] gesucht wird und die gefundenen Nachrichten in den angegebenen Ordner verschoben werden.

So ändern Sie die Einstellung für das automatische Entfernen blockierter Nachrichten:

1. Klicken Sie im linken Fensterbereich auf das Symbol **Einstellungen**, und klicken Sie dann auf die Symbolschaltfläche **Filteroptionen**.
2. Legen Sie fest, wie SpamKiller mit Spam-Nachrichten verfahren soll:
   - **Spam im Ordner mit blockierten E-Mails speichern**: Die Spam-Nachrichten werden aus Ihrem Posteingang entfernt und in den SpamKiller-Ordner **Blockierte E-Mails** verschoben.
   - **Blockierte E-Mails beibehalten für ____ Tage**: Die blockierten Nachrichten verbleiben für die angegebene Dauer im Ordner **Blockierte E-Mails**.
   - **Spam kennzeichnen und im Posteingang beibehalten**: Die Spam-Nachrichten verbleiben in Ihrem Posteingang, wobei die Betreffzeile der Nachricht mit dem Tag **[Spam]** oder einem anderen von Ihnen festgelegten Tag versehen wird.
3. Klicken Sie auf **OK**.

So löschen Sie eine Nachricht manuell:

1. Durch SpamKiller blockierte E-Mails anzeigen:
   - Klicken Sie in Spamkiller auf die Registerkarte **Nachrichten**, und klicken Sie anschließend auf die Registerkarte **Blockierte E-Mails**.
   - Klicken Sie im Posteingang von Microsoft Outlook oder Outlook Express auf die Symbolschaltfläche  , um die Registerkarte **Blockierte E-Mails** für dieses Konto zu öffnen.

   Die Registerkarte **Blockierte E-Mails** wird angezeigt.
2. Wählen Sie eine zu entfernende Nachricht aus, und klicken Sie anschließend auf **Diese Nachricht entfernen**. Es wird ein Bestätigungsdialogfeld angezeigt.
3. Klicken Sie auf **Ja**, um die Nachricht zu löschen.

Melden von Spam-Nachrichten an McAfee

Sie können Spam-Nachrichten an McAfee senden, wo diese analysiert werden, um entsprechende Filter-Updates zu erstellen.

So melden Sie Spam-Nachrichten an McAfee:

1. Klicken Sie im linken Fensterbereich auf das Symbol **Nachrichten**, und klicken Sie dann auf den Reiter der Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails** wird geöffnet.
2. Wählen Sie eine Nachricht aus, und klicken Sie dann auf **Bei McAfee melden**. Es wird ein Bestätigungsdialogfeld angezeigt.
3. Klicken Sie auf **Ja**, um die Nachricht automatisch an McAfee zu senden.

Senden manueller Beschwerden

Sie haben die Möglichkeit, dem Absender von Spam-Nachrichten eine Beschwerde zu senden, um ihn davon abzuhalten, Ihnen weitere Spam-Nachrichten zu senden. Weitere Informationen dazu finden Sie in der Online-Hilfe unter „Senden von Beschwerden und Fehlermeldungen“.

So senden Sie eine manuelle Beschwerde:

1. Klicken Sie im linken Fensterbereich auf das Symbol **Nachrichten**, und klicken Sie dann auf den Reiter der Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Es wird eine Liste der Nachrichten angezeigt.
2. Wählen Sie die Nachricht aus, über die Sie sich beschweren möchten, und klicken Sie dann auf **Beschwerde senden**. Das Dialogfeld „Beschwerde senden“ wird geöffnet.
3. Wählen Sie denjenigen aus, dem Sie die Beschwerde senden möchten.

   WARNUNG
   In den meisten Fällen sollten Sie nicht **Absender** wählen, da der Absender durch den Empfang einer Beschwerde erfährt, dass Ihre E-Mail-Adresse gültig ist, was zu noch mehr Spam-Nachrichten von diesem Absender führen kann.
4. Klicken Sie auf **Weiter**, und befolgen Sie die angezeigten Anweisungen.

Senden von Fehlermeldungen

Sie können festlegen, dass SpamKiller eine Fehlermeldung sendet, um den Absender davon abzuhalten, Ihnen weitere Spam-Nachrichten zu senden. Weitere Informationen dazu finden Sie in der Online-Hilfe unter „Senden von Beschwerden und Fehlermeldungen“.

So senden Sie eine manuelle Fehlermeldung:

1. Klicken Sie im linken Fensterbereich auf das Symbol **Nachrichten**, und klicken Sie dann auf den Reiter der Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Es wird eine Liste der Nachrichten angezeigt.
2. Wählen Sie eine Nachricht aus, und klicken Sie anschließend auf **Fehler senden**. Daraufhin wird an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet.

Verwendung von McAfee Shredder

McAfee Shredder schützt Ihre Privatsphäre durch das schnelle und sichere Vernichten unerwünschter Dateien.

Gelöschte Dateien können von Ihrem Computer auch dann wiederhergestellt werden, nachdem Sie den Papierkorb geleert haben. Wenn Sie eine Datei löschen, kennzeichnet Windows den frei gewordenen Platz auf der Festplatte zwar als nicht mehr verwendet, die Datei ist jedoch noch vorhanden.

Warum Windows Dateireste zurücklässt

Um eine Datei dauerhaft zu löschen, müssen Sie die vorhandene Datei wiederholt mit neuen Daten überschreiben. Würde Microsoft Windows Dateien sicher löschen, wären sämtliche Dateivorgänge sehr langsam. Durch das Vernichten eines Dokuments wird nicht immer verhindert, dass das Dokument wiederhergestellt wird, da einige Programme temporäre verborgene Kopien geöffneter Dokumente erstellen. Falls Sie Dokumente, die Sie in Explorer anzeigen, lediglich vernichten, sind möglicherweise nach wie vor temporäre Kopien jener Dokumente vorhanden. Es empfiehlt sich, in regelmäßigen Abständen den freien Speicherplatz auf der Festplatte zu vernichten, um sicherzustellen, dass diese temporären Kopien dauerhaft gelöscht werden.

HINWEIS
Mit forensischen Computer-Tools, können Steuererklärungen, Lebensläufe oder andere Dokumente, die von Ihnen gelöscht wurden, wiederbeschaffen werden.

Was McAfee Shredder löscht

Mit McAfee Shredder können Sie Folgendes sicher und dauerhaft löschen:

- Eine(n) oder mehrere Dateien oder Ordner
- Einen gesamten Datenträger
- Beim Surfen im Internet hinterlassene Spuren

Dauerhaftes Löschen von Dateien in Windows-Explorer

So vernichten Sie eine Datei über Windows-Explorer:

1. Öffnen Sie Windows-Explorer, und wählen Sie die Datei oder die Dateien aus, die Sie vernichten möchten.
2. Klicken Sie mit der rechten Maustaste auf Ihre Auswahl, zeigen Sie auf **Senden an**, und wählen Sie anschließend **McAfee Shredder** aus.

Leeren des Papierkorbs unter Windows

Wenn sich in Ihrem Papierkorb Dateien befinden, bietet McAfee Shredder eine sehr sichere Methode zum Löschen des Papierkorbs.

So vernichten Sie den Inhalt des Papierkorbs:

1. Klicken Sie auf dem Windows-Desktop mit der rechten Maustaste auf **Papierkorb**.
2. Wählen Sie **Papierkorb vernichten**, und befolgen Sie die Anweisungen auf dem Bildschirm.

Anpassen der Shredder-Einstellungen

Sie können Ihre Shredder-Einstellungen anpassen:

- Festlegen der Anzahl der Vernichtungsschritte.
- Anzeigen einer Warnmeldung beim Vernichten von Dateien.
- Überprüfen der Festplatte nach Fehlern vor dem Vernichtungsvorgang.
- Hinzufügen von McAfee Shredder zum Menü **Senden an**.
- Anlegen eines Shredder-Symbols auf dem Windows-Desktop.

Wenn Sie die Shredder-Einstellungen anpassen möchten, öffnen Sie McAfee Shredder, klicken Sie auf **Eigenschaften**, und befolgen Sie die Anweisungen auf dem Bildschirm.

Index

Q

R

S

T

U

V

W

Weitere Informationen zu Produkten,
weltweiten Services und Suppert
erhalten Sie von Ihrem autorisierten
McAfee-Händler, oder wenden Sie
sich unter folgender Adresse an uns:

McAfee
International BV
PO Box 58326, 1040 HH Amsterdam
The Netherlands

de.mcafee.com

http://www.mcafeehilfe.com

NA-675-0010-GE-1