McAfee®

virusscan®

Benutzerhandbuch

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von McAfee, Inc., ihren Lieferanten oder zugehörigen Tochtergesellschaften in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (UND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. sind eingetragene Marken oder Marken von McAfee, Inc. und/oder von ihren Tochterunternehmen in den USA und/oder anderen Ländern. Rot in Verbindung mit Sicherheit ist ein Wahrzeichen von McAfee-Markenprodukten. Alle anderen hier erwähnten eingetragenen und nicht eingetragenen Marken sind ausschließlich Eigentum ihrer jeweiligen Inhaber.

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, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI AUF DER WEBSITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESEM VERTRAG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. FALLS ZUTREFFEND, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE, INC., ODER AN DIE STELLE ZURÜCKGEBEN, VON DER SIE DAS PRODUKT ERWORBEN HABEN.

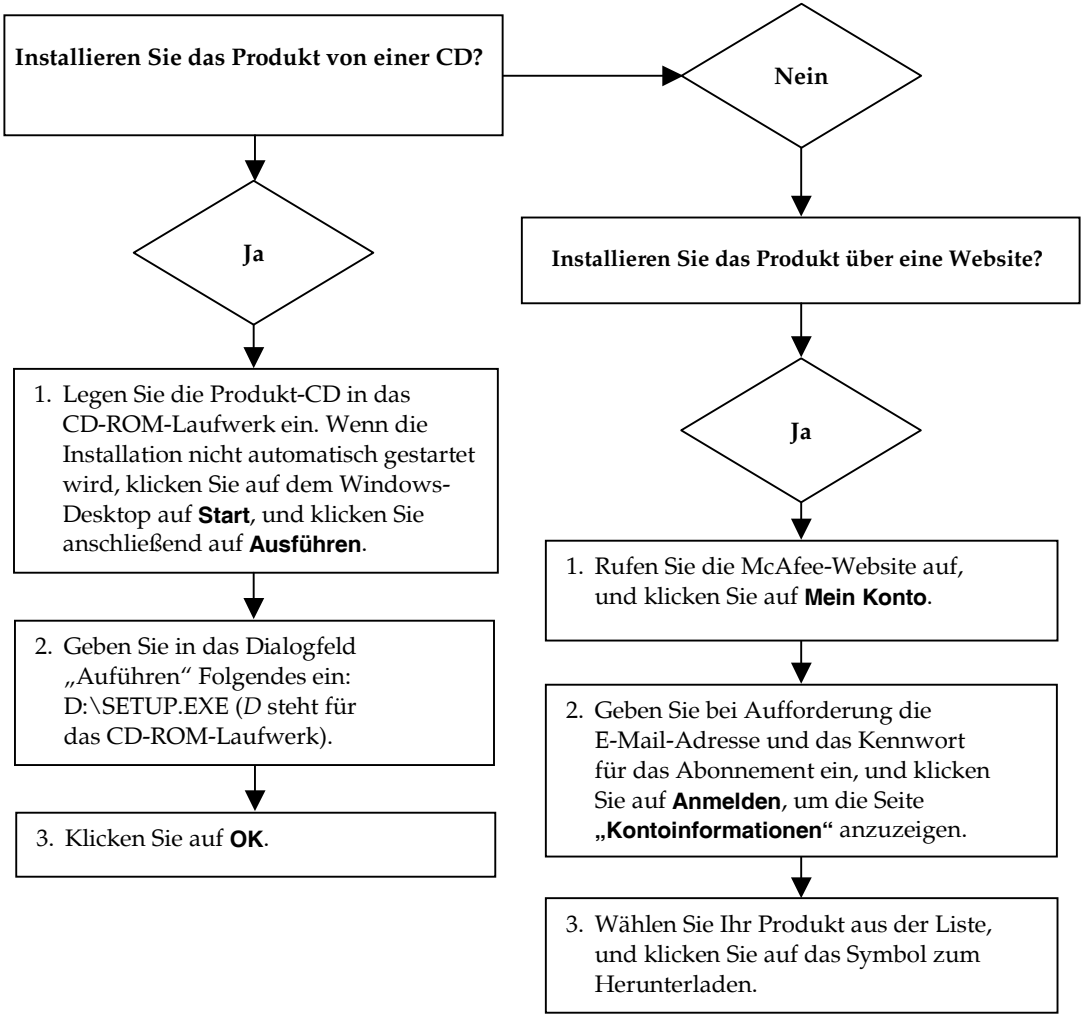
Zubehör

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, Inc. 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. ♦ Software, ursprünglich geschrieben von Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software, ursprünglich geschrieben von Robert Nordier Copyright © 1996-7 Robert Nordier. ♦ Software, geschrieben von Douglas W. Sauder. ♦ Von der Apache Software Foundation entwickelte Software (http://www.apache.org/). Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode („ICU"), Copyright © 1995-2002 International Business Machines Corporation und andere. ♦ Von CrystalClear Software, Inc. entwickelte Software, 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 der Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter www.python.org. ♦ Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002. ♦ Software, geschrieben 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. ♦ Von Indiana University Extreme! Lab entwickelte Software (http://www.extreme.indiana.edu/). ♦ Software, urheberrechtlich geschützt von International Business Machines Corporation und anderen, © 1995-2003. ♦ Von der University of California, Berkeley und deren Mitwirkenden entwickelte Software. ♦ Von Ralf S. Engelschall, <rse@engelschall.com>, entwickelte Software für die Verwendung im mod_ssl-Projekt (http://www.modssl.org/). ♦ 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 dazu finden Sie unter 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. Aktualisierungen, Dokumentation und Versionsverlauf dazu finden Sie unter 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 Website ausführen, sollten Sie diese praktische Referenzseite ausdrucken.



McAfee behält sich das Recht vor, Upgrade- und Support-Pläne sowie die entsprechenden Richtlinien jederzeit ohne Ankündigung zu ändern. McAfee und seine Produktnamen sind eingetragene Marken von McAfee, Inc. und/oder von seinen Tochterunternehmen in den USA und/oder anderen Ländern.
© 2005 McAfee, Inc. Alle Rechte vorbehalten.

Weitere Informationen

Zum Anzeigen der Benutzerhandbücher auf der Produkt-CD muss Acrobat Reader installiert sein. Andernfalls installieren Sie das Programm jetzt von der McAfee-Produkt-CD.

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 dann auf **Suchen**.
3. Suchen Sie den Ordner mit den Handbüchern (Manuals), und doppelklicken Sie auf die PDF-Datei des gewünschten Benutzerhandbuchs.

Registrierungsvorteile

McAfee empfiehlt, die im Produkt beschriebenen, einfachen Schritte zu befolgen, um Ihre Registrierung direkt an uns zu senden. Durch die Registrierung wird sichergestellt, dass Ihnen im angemessenen Zeitrahmen professionelle technische Unterstützung zur Verfügung steht. Außerdem profitieren Sie von:

- KOSTENLOSEM elektronischen Support
- Updates für Virusdefinitionsdateien (DAT-Dateien) für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der VirusScan-Software

  Preisangaben für ein zusätzliches Jahr Virussignaturen erhalten Sie unter http://www.mcafee.com/.
- Garantie von 60 Tagen für Austausch der Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der SpamKiller-Software

  Preisangaben für ein zusätzliches Jahr Filter-Updates erhalten Sie unter http://www.mcafee.com/.
- McAfee Internet Security Suite-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der MIS-Software

  Preisangaben für ein zusätzliches Jahr Inhalts-Updates erhalten Sie unter http://www.mcafee.com/.

Technischer Support

Technischen Support erhalten Sie unter

http://www.mcafeehilfe.com.

Unsere Support-Site ermöglicht Ihnen rund um die Uhr den Zugriff auf einen benutzerfreundlichen Antwort-Assistenten, 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 und kostenlos einen qualifizierten Support-Mitarbeiter erreichen. Sie können sich auch hier über die telefonischen Support-Möglichkeiten informieren:

http://www.mcafeehilfe.com.

Inhalt

Schnellreferenz iii

1 Erste Schritte 7

Neue Funktionen 7
Systemanforderungen 8
Testen von VirusScan 9
Testen von ActiveShield 9
Testen von Scan 10
McAfee SecurityCenter 12

2 McAfee VirusScan 13

ActiveShield 13
Aktivieren bzw. Deaktivieren von ActiveShield 13
Konfigurieren von ActiveShield-Optionen 14
Übersicht über Sicherheitswarnungen 24
Manuelles Überprüfen des Computers 27
Manuelles Überprüfen auf Viren und andere Bedrohungen 27
Automatisches Überprüfen auf Viren und andere Bedrohungen 31
Übersicht über Bedrohungserkennungen 33
Verwalten von Dateien unter Quarantäne 34
Erstellen einer Rettungsdiskette 36
Einrichten des Schreibschutzes für eine Rettungsdiskette 37
Verwenden einer Rettungsdiskette 38
Aktualisieren einer Rettungsdiskette 38
Automatisches Melden von Viren 38
Weiterleiten von Informationen an die World Virus Map 38
Anzeigen der World Virus Map 40
Aktualisieren von VirusScan 41
Automatisches Prüfen auf Updates 41
Manuelles Prüfen auf Updates 41

Index 43

Erste Schritte 1

Willkommen bei McAfee VirusScan.

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, verdächtigen Skripts, Hybridangriffen und anderen Bedrohungen.

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 anderen Bedrohungen.

Quarantäne: Verschlüsselt 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 Würmer und verdächtige Skripts verursacht werden.

Neue Funktionen

Diese Version von VirusScan enthält folgende neue Funktionen:

- **Erkennung und Entfernung von Spyware und Adware**
  VirusScan identifiziert und entfernt Spyware, Adware und andere Programme, die Ihre Privatsphäre verletzen und die Leistung Ihres Computers beeinträchtigen.
- **Tägliche automatische Updates**
  Tägliche automatische VirusScan-Updates schützen Sie vor den neuesten identifizierten und nicht identifizierten Computerbedrohungen.
- **Schnelles Scannen im Hintergrund**
  Schnelle, im Hintergrund ausgeführte Scans identifizieren und zerstören Viren, trojanische Pferde, Spyware, Adware, Dialer und andere Bedrohungen, ohne Sie bei der Arbeit zu unterbrechen.

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

- **Erkennung und Bereinigung an mehreren Eintrittspunkten**
  VirusScan führt die Überwachung und Bereinigung an den Haupteintrittspunkten des Computers durch: E-Mail, Anlagen von Instant Messages und Internetdownloads.

- **Überwachung von E-Mails auf wurmähnliche Aktivitäten**
  WormStopper™ überwacht den Computer auf verdächtiges Massen-Mail-Verhalten und verhindert, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten.

- **Überwachung von Skripts auf wurmähnliche Aktivitäten**
  ScriptStopper™ überwacht den Computer auf verdächtige Skriptausführungen und verhindert, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten.

- **Kostenloser technischer Support per Instant Messaging und E-Mail**
  Der live bereitgestellte technische Support bietet leicht zugängliche und schnelle Beratung mithilfe von Instant Messaging und E-Mail.

Systemanforderungen

- Microsoft® Windows 98, Windows Me, Windows 2000 oder Windows XP
- PC mit Pentium-kompatiblem Prozessor
  Windows 98, 2000: 133 MHz oder höher
  Windows Me: 150 MHz oder höher
  Windows XP (Home und Professional): 300 MHz oder höher
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home und Professional): 128 MB
- 40 MB Festplattenspeicher
- Microsoft® Internet Explorer 5.5 oder höher

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

Unterstützte E-Mail-Programme

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Unterstützte Instant Messaging-Programme:

- AOL Instant Messenger 2.1 oder höher
- Yahoo Messenger 4.1 oder höher
- Microsoft Windows Messenger 3.6 oder höher
- MSN Messenger 6.0 oder höher

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

HINWEIS
Zum Testen von ActiveShield über die Registerkarte **VirusScan** klicken Sie in SecurityCenter auf VirusScan testen, um online Fragen und Antworten mit den folgenden Schritten anzuzeigen.

So testen Sie ActiveShield:

1. Rufen Sie http://www.eicar.com/ in Ihrem Webbrowser 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** 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 möglichen Bedrohungen umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Übersicht über Sicherheitswarnungen* auf Seite 24.

Testen von Scan

Bevor Sie Scan testen können, müssen Sie ActiveShield deaktivieren, um zu verhindern, dass die Testdateien 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**, 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** 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 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**, und klicken Sie dann auf **Scan**.
2. Navigieren Sie über die Verzeichnisstruktur im linken Bereich 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 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 **Scan**, dass alle Optionen aktiviert sind.
4. Klicken Sie unten rechts im Dialogfeld auf **Scan**.

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

Wenn Sie sehen möchten, wie Scan mit möglichen Bedrohungen umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Übersicht über Bedrohungserkennungen* auf Seite 33.

McAfee SecurityCenter

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**, 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 Datei erkennen, wird automatisch versucht, diese zu bereinigen. Wenn ActiveShield den Virus nicht bereinigen kann, können Sie die Datei unter Quarantäne stellen oder löschen.

Aktivieren bzw. Deaktivieren von ActiveShield

ActiveShield wird standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol auf 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**, 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 Bedrohungen 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 14).

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**, 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 Bedrohungen geschützt.

Konfigurieren von ActiveShield-Optionen

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

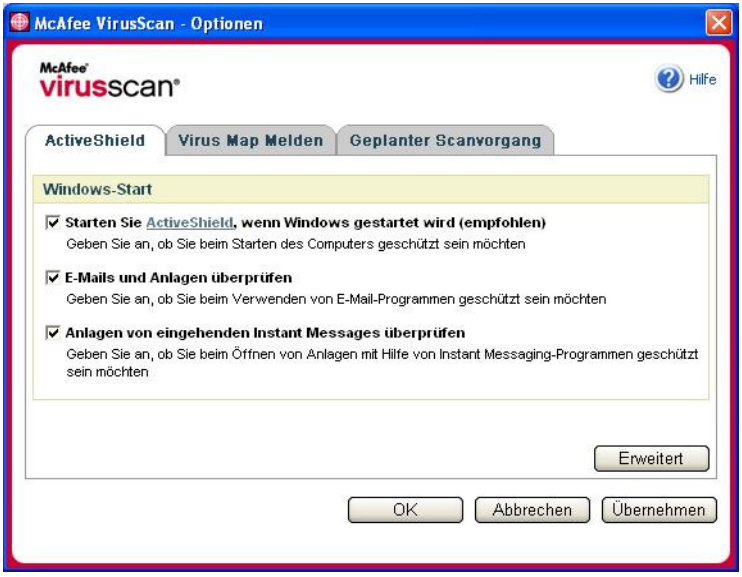


Abbildung 2-1. ActiveShield-Optionen

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 der **Update-Assistent** ActiveShield ggf. vorübergehend beenden, um neue Dateien zu installieren. Wenn Sie vom **Update-Assistenten** aufgefordert werden, auf **Fertig stellen** 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**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **VirusScan-Optionen** wird geöffnet (Abbildung 2-1 auf Seite 14).

2. Aktivieren Sie das Kontrollkästchen **ActiveShield ausführen, 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 Schutz vor Bedrohungen. 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**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **VirusScan-Optionen** wird geöffnet (Abbildung 2-1 auf Seite 14).

2. Deaktivieren Sie das Kontrollkästchen **ActiveShield ausführen, 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 Überprüfung von E-Mails und die automatische Bereinigung über die Option **E-Mails und Anlagen überprüfen** (Abbildung 2-1 auf Seite 14) aktiviert.

Wenn diese Option aktiviert ist, führt ActiveShield automatisch die Virenprüfung 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 jedoch beim Öffnen von ActiveShield geprüft.

Wenn Sie die Option **E-Mails und Anlagen überprüfen** deaktivieren, werden die E-Mail-Scan-Optionen und die WormStopper-Optionen (Abbildung 2-2 auf Seite 17) 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 wurde, 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 potentiellen Bedrohung durchgeführt wurden.

Ausgehende E-Mails

Wenn eine ausgehende E-Mail-Nachricht oder Anlage infiziert wurde, 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.

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

Deaktivieren der Prüfung von E-Mails

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**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **E-Mail-Scan** (Abbildung 2-2).
3. Deaktivieren Sie das Kontrollkästchen **Eingehende E-Mail-Nachrichten** oder **Ausgehende E-Mail-Nachrichten**, und klicken Sie auf **OK**.

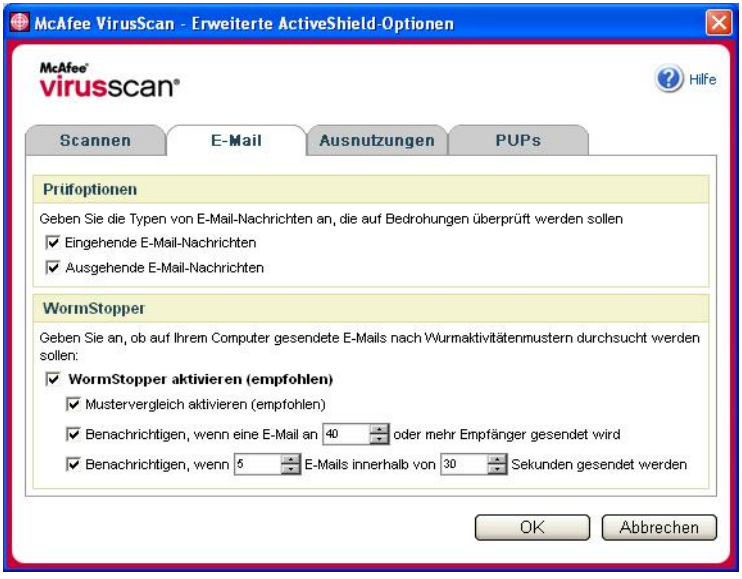


Abbildung 2-2. Erweiterte ActiveShield-Optionen - Registerkarte „E-Mail“

Prüfen auf Würmer

VirusScan überwacht den Computer auf verdächtige Aktivitäten, die möglicherweise darauf hinweisen, dass Ihr Computer akut gefährdet ist. Durch VirusScan werden Viren und andere Bedrohungen beseitigt, durch WormStopper™ hingegen wird der weiteren Verbreitung von Viren und Würmern vorgebeugt.

Computerwürmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Ohne WormStopper bemerken Sie Würmer unter Umständen erst, wenn durch ihr unkontrolliertes Fortpflanzen Systemressourcen belegt und dadurch die Leistung beeinträchtigt oder Tasks angehalten werden.

Durch den WormStopper-Schutzmechanismus werden verdächtige Aktivitäten erkannt, gemeldet und blockiert. Zu verdächtigen Aktivitäten auf dem Computer zählt Folgendes:

- 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 Standardoption **WormStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte Optionen** verwendet wird, überwacht WormStopper die E-Mail-Aktivität auf verdächtige Muster und gibt eine Warnung aus, wenn eine festgelegte Anzahl an E-Mails oder Empfängern innerhalb eines festgelegten Intervalls überschritten wird.

So konfigurieren Sie ActiveShield zur Überprüfung von gesendeten E-Mail-Nachrichten auf wurmähnliche Aktivitäten:

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

   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 die 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 bevorzugte Einstellung ersetzen.

Diese Option kann automatisch aktiviert werden, nachdem zum ersten Mal ein potentieller Wurm erkannt wurde (ausführliche Informationen finden Sie unter *Verwalten potentieller Würmer* auf Seite 25):

- Automatische Blockierung verdächtiger, ausgehender E-Mails

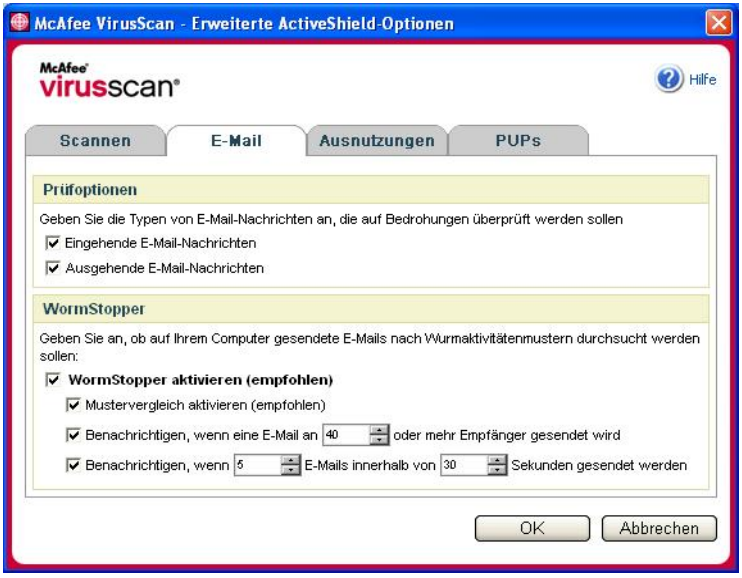


Abbildung 2-3. Erweiterte ActiveShield-Optionen - Registerkarte „E-Mail“

Prüfen 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 14) aktiviert.

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

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

HINWEIS

Aus Sicherheitsgründen kann die automatische Bereinigung von Instant Messages-Anlagen nicht deaktiviert werden.

Wenn eine eingehende Instant Messages-Anlage infiziert wurde, 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**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4 auf Seite 20).
3. Klicken Sie auf **Alle Dateien (empfohlen)** und dann auf **OK**.

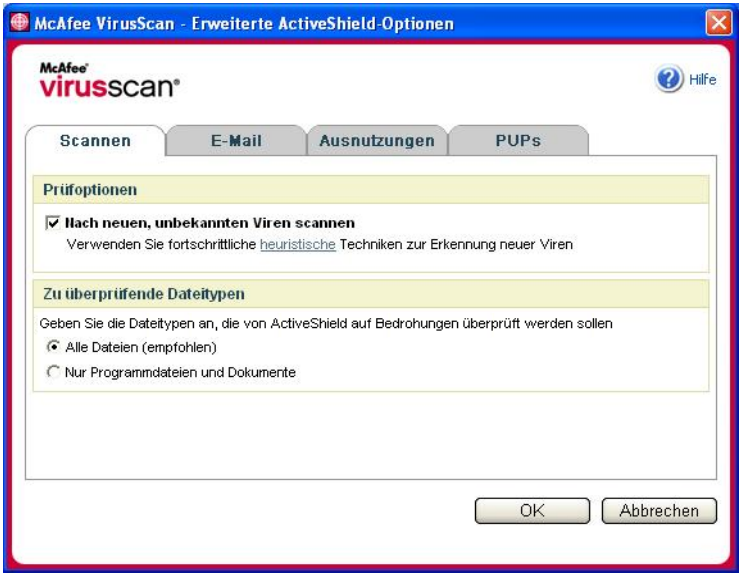


Abbildung 2-4. Erweiterte ActiveShield-Optionen - Registerkarte „Scannen“

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 jeweils neueste 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**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4).
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 (empfohlen)** verwendet wird, werden erweiterte heuristische Techniken verwendet, anhand derer eine Übereinstimmung zwischen den Dateien und Signaturen bekannter Viren ermittelt werden soll. Gleichzeitig 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**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4).
3. Klicken Sie auf **Nach neuen, unbekannten Viren scannen (empfohlen)** und dann auf **OK**.

Prüfen auf Skripts

VirusScan überwacht den Computer auf verdächtige Aktivitäten, die möglicherweise darauf hinweisen, dass Ihr Computer akut gefährdet ist. Durch VirusScan werden Viren und andere Bedrohungen beseitigt; durch ScriptStopper™ hingegen wird verhindert, dass trojanische Pferde Skripts ausführen, mit denen Viren weiterverbreitet werden.

Ein trojanisches Pferd ist ein verdächtiges Programm, das als nützliche Anwendung getarnt ist. Trojanische Pferde sind keine Viren, da sie sich nicht fortpflanzen, können aber eine ähnlich destruktive Wirkung entfalten wie Viren.

Durch den ScriptStopper-Schutzmechanismus werden verdächtige 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.

Wenn Sie ActiveShield so einstellen, dass die Standardoption **ScriptStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte Optionen** verwendet wird, überwacht ScriptStopper die Skriptausführung auf verdächtige Muster und gibt eine Warnung aus, wenn eine festgelegte Anzahl an E-Mails oder Empfängern innerhalb eines festgelegten Intervalls überschritten wird.

So konfigurieren Sie ActiveShield für die Prüfung von ausgeführten Skripts auf wurmähnliche Aktivitäten:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Ausnutzungen** (Abbildung 2-5).
3. Klicken Sie auf **ScriptStopper aktivieren (empfohlen)** und dann auf **OK**.

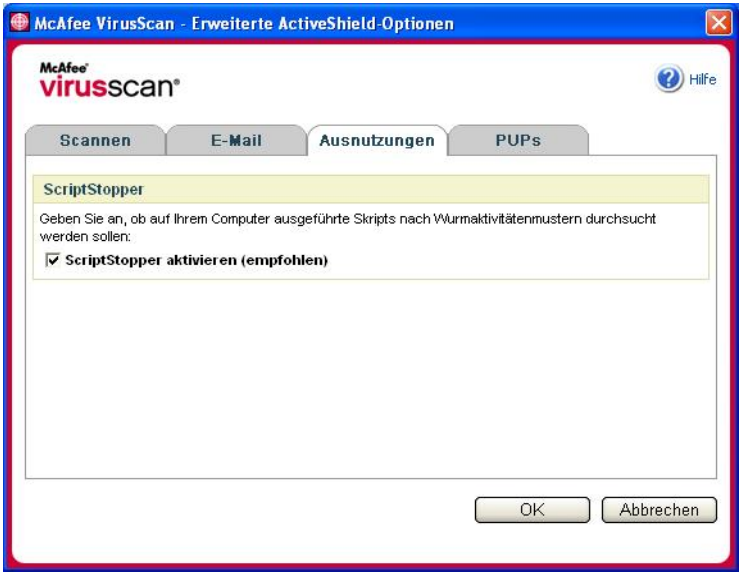


Abbildung 2-5. Erweiterte ActiveShield-Optionen - Registerkarte „Ausnutzungen“

Prüfen auf möglicherweise unerwünschte Programme (PUPs)

HINWEIS
Wenn McAfee AntiSpyware auf Ihrem Computer installiert ist, verwaltet es alle Aktivitäten von möglicherweise unerwünschten Programmen. Öffnen Sie McAfee AntiSpyware zur Konfiguration der Optionen.

Wenn Sie ActiveShield so konfigurieren, dass die standardmäßige Option **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** im Dialogfeld **Erweiterte Optionen** aktiviert ist, erkannt, blockiert und entfernt der Schutz vor möglicherweise unerwünschten Programmen (PUP) rasch Spyware, Adware und andere Programme, die Ihre persönlichen Daten ohne Ihre Zustimmung sammeln und weiterleiten.

So konfigurieren Sie ActiveShield für die Überprüfung auf PUPs:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **PUPs** (Abbildung 2-6).
3. Klicken Sie auf **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** und dann auf **OK**.

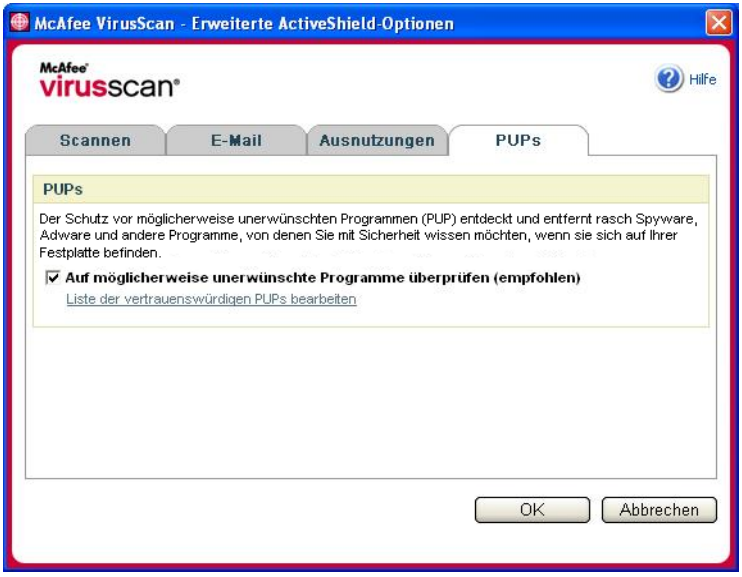


Abbildung 2-6. Erweiterte ActiveShield-Optionen - Registerkarte „PUPs“

Übersicht über Sicherheitswarnungen

Wenn ActiveShield einen Virus findet, wird eine Viruswarnung ausgegeben, die Abbildung 2-7 ähnelt. Bei den meisten Viren, Trojanern und Würmern versucht ActiveShield automatisch, die Datei zu bereinigen, und zeigt eine Warnung an. Bei möglicherweise unerwünschten Programmen (PUPs) erkannt ActiveShield die Datei, blockiert sie automatisch und zeigt eine Warnung an.



Abbildung 2-7. Viruswarnung

Anschließend können Sie angeben, wie mit infizierten Dateien, infizierten E-Mails, verdächtigen Skripts, potentiellen Würmern oder PUPs verfahren werden soll, und ob erkannte Dateien zu Forschungszwecken an die McAfee AVERT-Laboratorien übermittelt werden sollen.

Wenn ActiveShield eine verdächtige Datei erkennt, werden Sie aufgefordert, den Computer sofort vollständig zu überprüfen, um zusätzlichen Schutz zu gewährleisten. Wenn Sie die Aufforderung zum Überprüfen Ihres Computers nicht ausblenden, werden Sie solange in regelmäßigen Abständen daran erinnert, bis Sie die Überprüfung durchführen.

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 **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 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 Bedrohungen auffordert. Klicken Sie auf **Scan**, um den Quarantäneprozess abzuschließen.

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

Verwalten infizierter E-Mails

Standardmäßig wird bei der E-Mail-Überprüfung automatisch versucht, infizierte E-Mail-Nachrichten zu bereinigen. Es wird eine Warnungsdatei in die eingehende E-Mail aufgenommen, die Sie darüber informiert, ob die E-Mail-Nachricht bereinigt, unter Quarantäne gestellt oder gelöscht wurde.

Verwalten verdächtiger Skripts

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

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die Beschreibung der Aktivität anzuzeigen, die mit dem verdächtigen Skript in Verbindung steht.
- Mit **Dieses Skript anhalten** können Sie die Ausführung des verdächtigen Skripts unterbinden.

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

- Klicken Sie auf **Dieses Mal alle Skripts zulassen** , um alle in einer einzelnen Datei enthaltenen Skripts dieses eine Mal auszuführen.
- Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Skript ausführen zu lassen.

Verwalten potentieller Würmer

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:

- Klicken Sie auf **Weitere Informationen**, um die Empfängerliste, die Betreffzeile, den Nachrichtentext und die Beschreibung der verdächtigen Aktivität anzuzeigen, die mit der infizierten E-Mail-Nachricht in Verbindung steht.
- Mit **E-Mail anhalten** können Sie verhindern, dass die verdächtige E-Mail gesendet wird. Löschen Sie sie aus der Nachrichtenwarteschlange.

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.

Verwalten von PUPs

Wenn ActiveShield ein möglicherweise unerwünschtes Programm (PUP) erkennt und blockiert, können Sie sich ausführlicher informieren und das Programm dann entfernen, wenn Sie nicht beabsichtigt hatten, es zu installieren:

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die empfohlene Vorgehensweise für dieses PUP anzuzeigen.
- Klicken Sie auf **PUP entfernen**, um das Programm zu entfernen, wenn Sie nicht beabsichtigt hatten, es zu installieren.

  Es wird eine Bestätigungsmeldung angezeigt.

  - Wenn Sie (a) das PUP nicht erkennen oder (b) das PUP nicht als Teil einer Programmgruppe installiert oder den Lizenzvertrag in Verbindung mit solchen Programmen nicht akzeptiert haben, klicken Sie auf **OK**, um das Programm mithilfe der Entfernungsmethode von McAfee zu entfernen.

  - Klicken Sie andernfalls auf **Abbrechen**, um den automatischen Entfernungsvorgang zu beenden. Wenn Sie Ihre Meinung später ändern, können Sie das Programm mithilfe des Deinstallationsprogramms des Herstellers manuell entfernen.
- Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Programm dieses Mal zu blockieren.

Wenn Sie (a) das PUP erkennen oder (b) das PUP als Teil einer Programmgruppe installiert oder den Lizenzvertrag in Verbindung mit solchen Programmen akzeptiert haben, können Sie es ausführen.

- Klicken Sie auf **Dieses PUP als vertrauenswürdig einstufen**, um das Programm in die Liste der vertrauenswürdigen Programme aufzunehmen und seine Ausführung immer zuzulassen.

  Nähere Informationen dazu finden Sie unter *Verwalten von vertrauenswürdigen PUPs*.

Verwalten von vertrauenswürdigen PUPs

Die Programme, die Sie zur Liste der vertrauenswürdigen PUPs hinzufügen, werden von McAfee VirusScan nicht erkannt.

Wenn ein PUP erkannt und zur Liste der vertrauenswürdigen PUPs hinzugefügt wird, können Sie es später bei Bedarf wieder aus der Liste entfernen.

Wenn die Liste der vertrauenswürdigen PUPs voll ist, müssen Sie einige Objekte aus der Liste entfernen, bevor Sie einem weiteren PUP vertrauen können.

So entfernen Sie ein Programm aus der Liste der vertrauenswürdigen PUPs:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **PUPs**.
3. Klicken Sie auf **Liste der vertrauenswürdigen PUPs bearbeiten**, aktivieren Sie das Kontrollkästchen vor dem Dateinamen, und klicken Sie auf **Entfernen**. Klicken Sie auf **OK**, wenn Sie die gewünschten Objekte entfernt haben.

Manuelles Überprüfen des Computers

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

Manuelles Überprüfen auf Viren und andere Bedrohungen

So überprüfen Sie Ihren Computer:

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

Das Dialogfeld **Scan** wird geöffnet (Abbildung 2-8).

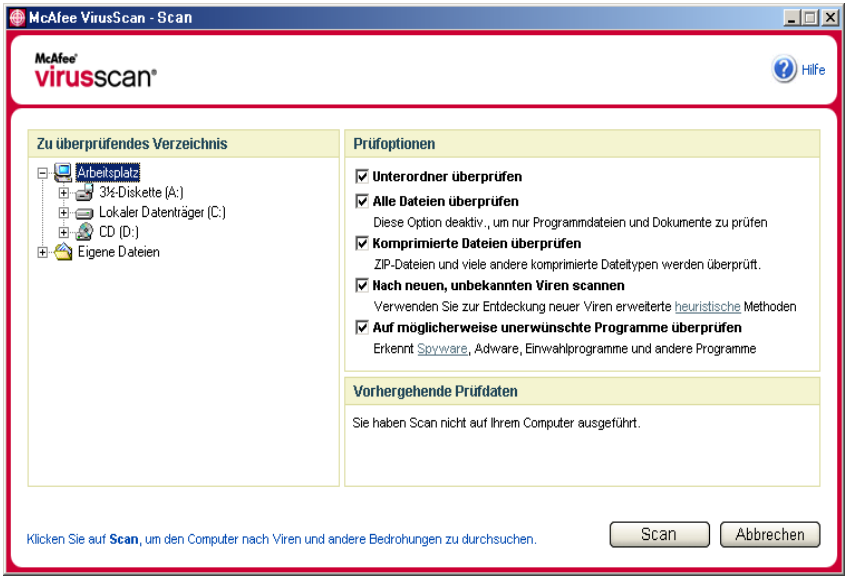


Abbildung 2-8. Dialogfeld „Scan“

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

3 Wählen Sie die **Prüfoptionen** aus. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 2-8):

- **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: Wenn Sie das Kontrollkästchen **Unterordner überprüfen** deaktivieren, werden ausschließlich die Dateien in Abbildung 2-9 durchsucht. Die Ordner und ihr Inhalt werden nicht überprüft. Wenn sie ebenfalls durchsucht werden sollen, belassen Sie das Kontrollkästchen aktiviert.

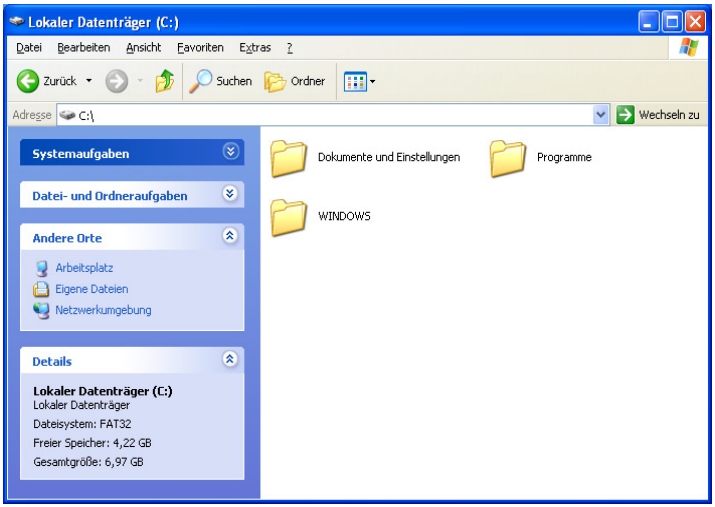


Abbildung 2-9. Inhalt lokaler Datenträger

- **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 Dateien in ZIP-Dateien und anderen komprimierten Dateien aufzuspüren. 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 wiederum in eine weitere ZIP-Datei eingefügt, um Anti-Virus-Scanner zu umgehen. Wenn Sie diese Option aktiviert belassen, kann Scan diese Viren ermitteln.
- **Nach neuen, unbekannten Viren scannen** : Verwenden Sie diese Option, um die neuesten Viren zu ermitteln, für die es möglicherweise noch kein Gegenmittel gibt. Diese Option verwendet erweiterte heuristische Techniken, anhand derer eine Übereinstimmung zwischen den Dateien und Signaturen bekannter Viren ermittelt werden soll. Gleichzeitig wird versucht, anhand bestimmter Anzeichen nicht identifizierte Viren in den Dateien zu ermitteln.

Bei diesem Scan-Verfahren 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 ergreifen wie bei einem bekannten Virus.

Diese Option bietet eine äußerst gründliche Prüfung, die jedoch zeitaufwendiger als eine normale Prüfung ist.

- **Auf möglicherweise unerwünschte Programme überprüfen** : Mit dieser Option können Sie Spyware, Adware und anderen Programme, die Ihre persönlichen Daten ohne Ihre Zustimmung weiterleiten und sammeln, erkennen.

  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, desto länger dauert die Überprüfung.

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

Nach Abschluss der Überprüfung wird in einer Zusammenfassung angezeigt, wie viele Dateien überprüft und erkannt wurden, wie viele möglicherweise unerwünschte Programme gefunden wurden und wie viele infizierte Dateien automatisch bereinigt wurden.

5 Klicken Sie auf **OK**, um die Zusammenfassung zu schließen und die Liste der erkannten Dateien im Dialogfeld **Scan** anzuzeigen (Abbildung 2-10).

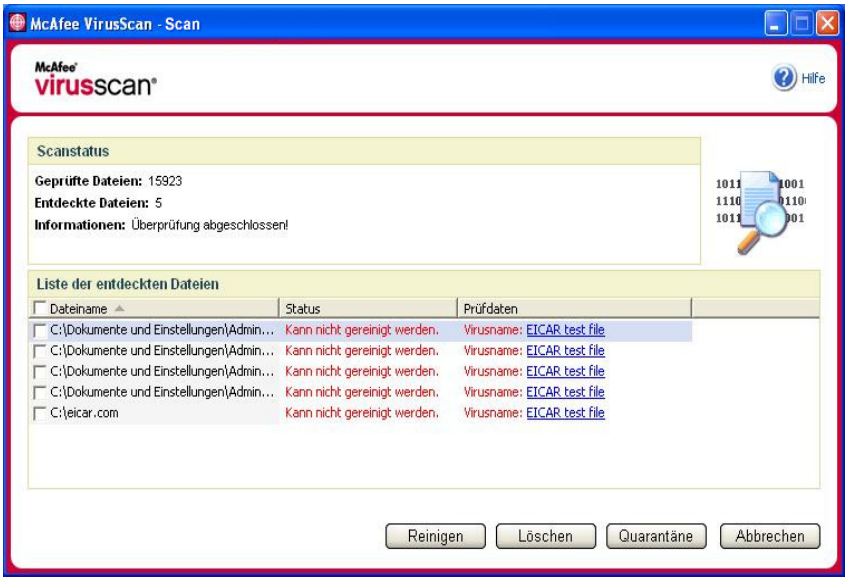


Abbildung 2-10. Prüfergebnisse

HINWEIS
Unter **Geprüfte Dateien** zählt Scan komprimierte Dateien (ZIP, CAB usw.) jeweils 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 andere Bedrohungen 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 *Übersicht über Bedrohungserkennungen* auf Seite 33.

Prüfen über Windows-Explorer

VirusScan ermöglicht die Verwendung eines Kontextmenüs, mit dem ausgewählte Dateien, Ordner oder Laufwerke über Windows-Explorer auf Viren und andere Bedrohungen 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 soll, und klicken Sie dann auf **Scan**.

Das Dialogfeld **Scan** wird angezeigt, und es wird mit der Überprüfung der Dateien begonnen. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 2-8 auf Seite 27).

Prüfen über Microsoft Outlook

VirusScan stellt ein Symbol auf der Symbolleiste bereit, 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 andere Bedrohungen 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 soll, und klicken Sie dann auf 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 **Prüfoptionen** aktiviert (Abbildung 2-8 auf Seite 27).

Automatisches Überprüfen auf Viren und andere Bedrohungen

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 andere Bedrohungen zu durchsuchen.

So planen Sie eine Prüfung:

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

   Das Dialogfeld **VirusScan-Optionen** wird geöffnet.
2. Klicken Sie auf die Registerkarte **Geplante Prüfung** (Abbildung 2-11 auf Seite 32).



Abbildung 2-11. Optionen für geplante Prüfungen

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

4 Legen Sie einen Zeitplan für die automatische Prüfung fest:

- 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**.

  b. Wählen Sie in der Liste **Task planen**, 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 Scans 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**.

  Einmalig: Geben Sie das Datum an, an dem der Scan ausgeführt werden soll.

HINWEIS
Folgende Optionen im Windows-Taskplaner werden 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 **Beginn um** die Tageszeit aus, zu der die Überprüfung des Computers erfolgen soll.

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

Das Dialogfeld **Erweiterte Planungsoptionen** wird angezeigt.

i. Geben Sie Anfangsdatum, Enddatum, Dauer und Endzeitpunkt ein, und geben Sie an, ob der Scan-Vorgang zur festgelegten Zeit beendet werden soll, wenn die Überprüfung noch nicht beendet 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 **Auf Standard setzen**. Klicken Sie andernfalls auf **OK**.

Übersicht über Bedrohungserkennungen

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 möglicherweise unerwünschtes Programm findet, können Sie versuchen, es manuell 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 erkannten 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 möglicherweise 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 verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann. (Nähere Informationen dazu finden Sie unter *Verwalten von Dateien unter Quarantäne* auf Seite 34.)

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 infizierte 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 infizierte 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* auf Seite 36.

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

Verwalten von Dateien unter Quarantäne

Mithilfe der Quarantäne-Funktion können Sie verdächtige Dateien verschlüsseln und temporär in einem Quarantäneverzeichnis unter Quarantäne stellen, bis eine angemessene Maßnahme ergriffen werden kann. Nach der Bereinigung können unter 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**, und klicken Sie dann auf **Dateien unter Quarantäne verwalten**.

Eine Liste mit Dateien unter Quarantäne wird angezeigt (Abbildung 2-12).



Abbildung 2-12. Dialogfeld „Dateien unter Quarantäne verwalten“

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 die Datei dann in der Quarantäneliste aus.

3 Klicken Sie auf **Reinigen**.

4 Wenn die Datei bereinigt ist, klicken Sie auf **Wiederherstellen**, 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 möglicherweise 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 Speicherort 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.

Erstellen einer Rettungsdiskette

Bei Rescue Disk handelt es sich um ein Dienstprogramm, das eine startfähige Diskette erstellt, über die Sie einen infizierten Computer starten und nach Viren durchsuchen können.

HINWEIS
Um die Imagedatei für die Rettungsdiskette herunterladen zu können, müssen Sie mit dem Internet verbunden sein. Rescue Disk ist nur für Computer mit FAT-Partitionen (FAT 16 und FAT 32) verfügbar und ist für NTFS-Partitionen nicht erforderlich.

So erstellen Sie eine Rettungsdiskette:

1 Legen Sie eine nicht infizierte Diskette in Laufwerk A eines nicht infizierten Computers ein. Verwenden Sie Scan, wenn Sie sicherstellen möchten, dass der Computer und die Diskette nicht von einem Virus befallen sind. (Nähere Informationen dazu finden Sie unter *Manuelles Überprüfen auf Viren und andere Bedrohungen* auf Seite 27.)

2 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Rettungsdiskette erstellen**.

Das Dialogfeld **Rettungsdiskette erstellen** wird angezeigt (Abbildung 2-13).

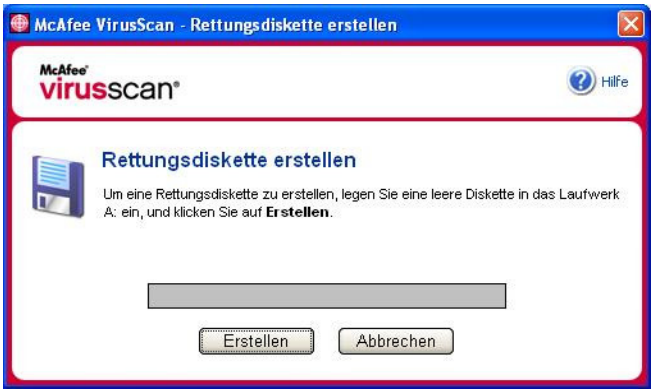


Abbildung 2-13. Dialogfeld „Rettungsdiskette erstellen“

3 Klicken Sie auf **Erstellen**, um die Rettungsdiskette zu erstellen.

Wenn Sie zum ersten Mal eine Rettungsdiskette erstellen, werden Sie in einer Meldung darüber informiert, dass die Imagedatei für die Rettungsdiskette heruntergeladen werden muss. Klicken Sie auf **OK**, um die Komponente jetzt herunterzuladen, oder auf **Abbrechen** für einen späteren Download.

Es wird eine Warnung angezeigt, die Sie darüber informiert, dass der Inhalt der Diskette verloren geht.

4 Klicken Sie auf **Ja**, um die Rettungsdiskette zu erstellen.

Der Status für diesen Vorgang wird im Dialogfeld **Rettungsdiskette erstellen** angegeben.

5 Wenn die erfolgreiche Erstellung einer Rettungsdiskette gemeldet wird, klicken Sie auf **OK**, und schließen Sie dann das Dialogfeld **Rettungsdiskette erstellen**.

6 Nehmen Sie die Rettungsdiskette aus dem Laufwerk, versehen Sie sie mit einem Schreibschutz, und bewahren Sie den Datenträger an einem sicheren Ort auf.

Einrichten des Schreibschutzes für eine Rettungsdiskette

So richten Sie den Schreibschutz für eine Rettungsdiskette ein:

1 Drehen Sie die Diskette mit der Beschriftungsseite nach unten (die runde Metallplatte ist sichtbar).

2 Suchen Sie den Riegel für den Schreibschutz. Verschieben Sie den Riegel so, dass die Öffnung sichtbar ist.

Verwenden einer Rettungsdiskette

So verwenden Sie eine Rettungsdiskette:

1. Schalten Sie den infizierten Computer aus.
2. Legen Sie die Rettungsdiskette in das Laufwerk ein.
3. Schalten Sie den Computer wieder ein.

   Es wird ein graues Fenster mit verschiedenen Optionen geöffnet.
4. Wählen Sie die Option, die Ihren Bedürfnissen am ehesten entspricht, indem Sie die Funktionstasten (F2, F3 usw.) drücken.

   HINWEIS
   Wenn Sie keine dieser Tasten drücken, wird das Programm Rescue Disk nach 60 Sekunden automatisch gestartet.

Aktualisieren einer Rettungsdiskette

Es empfiehlt sich, Ihre Rettungsdiskette regelmäßig zu aktualisieren. Befolgen Sie dazu die Anweisungen zum Erstellen einer neuen Rettungsdiskette.

Automatisches Melden von Viren

Informationen zu Viren können anonym an die World Virus Map gesendet werden. Nehmen Sie das Angebot, diese kostenlose, sichere Funktion zu nutzen an: Entweder automatisch während der Installation von VirusScan (im Dialogfeld **Informationen an Virus Map weiterleiten**) oder jederzeit auf der Registerkarte **Informationen an Virus Map weiterleiten** im Dialogfeld **VirusScan-Optionen**.

Weiterleiten von Informationen an die World Virus Map

So melden Sie Vireninformationen an die World Virus Map:

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

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

2 Klicken Sie auf die Registerkarte **Informationen an Virus Map weiterleiten** (Abbildung 2-14).



Abbildung 2-14. Optionen für die Weiterleitung von Informationen an Virus Map

3 Übernehmen Sie die Standardeinstellung **Ja, ich möchte teilnehmen**, um die Informationen anonym an McAfee zu senden. Ihre Informationen werden bei der Berechnung der weltweiten Erkennungsrate in der World Virus Map berücksichtigt. Wählen Sie andernfalls **Nein, ich möchte nicht teilnehmen**. Ihre Informationen werden in diesem Falle nicht gesendet.

4 Wenn Sie in den USA leben, wählen Sie den Bundesstaat aus, und geben Sie die Postleitzahl (Zip-Code) für den Standort Ihres Computers ein. Wenn Sie nicht in den USA leben, versucht VirusScan automatisch das Land auszuwählen, in dem sich der Computer befindet.

5 Klicken Sie auf **OK**.

Anzeigen der World Virus Map

Auch wenn Sie keine Informationen an die World Virus Map senden, können Sie die neuesten globalen Erkennungsraten über das McAfee-Symbol auf der Windows-Taskleiste anzeigen.

So zeigen Sie die World Virus Map an:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **World Virus Map**.

  Die Webseite mit der **World Virus Map** wird angezeigt (Abbildung 2-15).

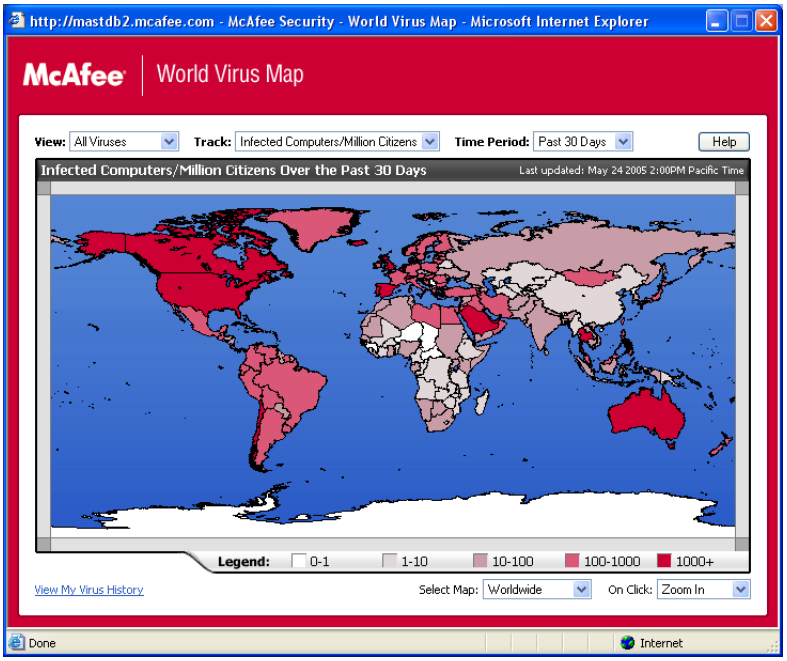


Abbildung 2-15. World Virus Map

Standardmäßig wird auf der World Virus Map die Anzahl der Computer angezeigt, die weltweit in den letzten 30 Tagen infiziert wurden. Außerdem sehen Sie, wann die gemeldeten Daten zuletzt aktualisiert wurden. Sie können die Ansicht der World Virus Map so ändern, dass die Anzahl der infizierten Dateien angezeigt wird, oder den Zeitraum modifizieren, um nur die Ergebnisse der letzten sieben Tage oder der letzten 24 Stunden anzuzeigen.

Im Abschnitt **Virus Tracking** finden Sie eine Auflistung der gesamten durchsuchten Dateien, der infizierten Dateien und der infizierten Computer, die seit dem angegebenen Datum gemeldet wurden.

Aktualisieren von VirusScan

Wenn Sie mit dem Internet verbunden sind, ermittelt VirusScan alle vier Stunden, ob Updates zur Verfügung stehen, lädt sie automatisch herunter und installiert wöchentliche Virusdefinitions-Updates, ohne Sie bei der Arbeit zu unterbrechen.

Virusdefinitionsdateien sind maximal 100 KB groß und beeinträchtigen die Systemleistung während des Downloads folglich nur geringfügig.

Bei einem Produktupdate oder Virusausbruch erhalten Sie eine entsprechende Benachrichtigung. Sie können nach der Benachrichtigung VirusScan aktualisieren, um den Ausbruch des Virus zu verhindern.

Automatisches Prüfen auf Updates

McAfee SecurityCenter ist so konfiguriert, dass alle vier Stunden automatisch nach Updates für Ihre gesamten McAfee-Dienste gesucht wird, sofern Sie mit dem Internet verbunden sind, und Sie durch Warnmeldungen und akustische Signale benachrichtigt werden. Standardmäßig lädt SecurityCenter automatisch alle verfügbaren Updates herunter und installiert sie.

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

Manuelles Prüfen auf Updates

Zusätzlich zum automatischen Suchen nach Updates, das alle vier Stunden durchgeführt wird (vorausgesetzt, eine Internetverbindung besteht), haben Sie außerdem jederzeit die Möglichkeit, manuell nach Updates zu suchen.

So suchen Sie manuell nach VirusScan-Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, und klicken Sie dann auf **Updates**.

   Das Dialogfeld **SecurityCenter-Updates** wird geöffnet.
3. Klicken Sie auf **Jetzt prüfen**.

   Wenn ein Update vorhanden ist, wird das Dialogfeld **VirusScan-Updates** geöffnet (Abbildung 2-16 auf Seite 42). Klicken Sie auf **Aktualisieren**, um fortzufahren.

Wenn keine Updates verfügbar sind, werden Sie in einem Dialogfeld darüber informiert, dass VirusScan auf dem neuesten Stand ist. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

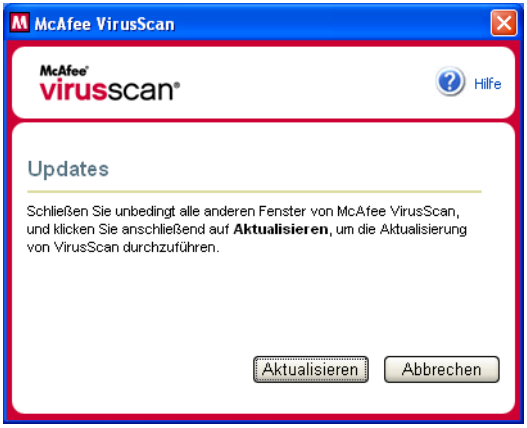


Abbildung 2-16. Dialogfeld „Updates“

4 Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden. Der **Update-Assistent** installiert das Update automatisch.

5 Klicken Sie nach Abschluss der Update-Installation auf **Fertig stellen**.

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

Index

A

ActiveShield
- aktivieren, 13
- anhalten, 15
- ausschließliches Prüfen von Programmdateien und Dokumenten, 21
- deaktivieren, 14
- Prüfen aller Dateien, 20
- Prüfen aller Dateitypen, 20
- Prüfen auf möglicherweise unerwünschte Programme (PUPs), 23
- Prüfen auf neue, unbekannte Viren, 21
- Prüfen auf Skripts, 21
- prüfen auf Würmer, 18
- Prüfen von Anlagen eingehender Instant Messages, 19
- Prüfen von E-Mails und Anlagen, 16
- Prüfoptionen, 14
- standardmäßige Scan-Einstellung, 15, 18 to 23
- starten, 15
- testen, 9
- Virus bereinigen, 24

aktualisieren
- einer Rettungsdiskette, 38
- VirusScan
  - automatisch, 41
  - manuell, 41

Alle Dateien überprüfen, Option (Scan), 28

Anlagen eingehender Instant Messages
- automatisch bereinigen, 19
- Prüfung, 19

Auf möglicherweise unerwünschte Programme überprüfen, Option (Scan), 29

AVERT, Übermitteln verdächtiger Dateien, 36

E

Einrichten des Schreibschutzes für eine Rettungsdiskette, 37

E-Mails und Anlagen
- automatisch bereinigen
  - aktivieren, 16
- Prüfung
  - aktivieren, 16
  - deaktivieren, 17
  - Fehler, 17

Erste Schritte mit VirusScan, 7

Erstellen einer Rettungsdiskette, 36

I

in Liste der vertrauenswürdigen Programme aufnehmen
- PUPs, 26

K

Komprimierte Dateien überprüfen, Option (Scan), 28

Konfigurieren
- VirusScan
  - ActiveShield, 13
  - Scan, 27

L

Liste der erkannten Dateien (Scan), 29, 33

Liste der vertrauenswürdigen Programme bearbeiten, 26

Liste der vertrauenswürdigen PUPs, 26

M

McAfee SecurityCenter, 12

Microsoft Outlook, 31

Möglicherweise unerwünschte Programme (PUPs), 23
- bereinigen, 33
- entfernen, 26

erkennen, 33
löschen, 34
unter Quarantäne stellen, 34
vertrauenswürdig, 26
Warnungen, 26

N

Nach neuen, unbekannten Viren scannen, Option (Scan), 28
Neue Funktionen, 7

P

Planen von Prüfungen, 31
Prüfoptionen
ActiveShield, 14, 20 to 21
Scan, 27
Prüfung
alle Dateien, 20, 28
auf möglicherweise unerwünschte Programme (PUPs), 23
auf neue, unbekannte Viren, 28
auf Skripts, 21
auf Würmer, 18
komprimierte Dateien, 28
nur Programmdateien und Dokumente, 21
Planen automatischer Prüfungen, 31
über die Microsoft Outlook-Symbolleiste, 31
über Windows-Explorer, 30
Unterordner, 27

Q

Quarantäne
Bereinigen von Dateien, 34 to 35
Hinzufügen von verdächtigen Dateien, 34
Löschen von Dateien, 34
Löschen von verdächtigen Dateien, 35
Übermitteln verdächtiger Dateien, 36
Verwalten von verdächtigen Dateien, 34
Wiederherstellen von bereinigten Dateien, 34 to 35

R

Rettungsdiskette
aktualisieren, 38
Einrichten des Schreibschutzes, 37
erstellen, 36
verwenden, 34, 38

S

Scan
Alle Dateien überprüfen, Option, 28
Auf möglicherweise unerwünschte Programme überprüfen, Option, 29
automatisches Prüfen, 31
Bereinigen eines Virus oder eines möglicherweise unerwünschten Programms, 33
Komprimierte Dateien überprüfen, Option, 28
Löschen eines Virus oder eines möglicherweise unerwünschten Programms, 34
manuelles Prüfen, 27
manuelles Prüfen über die Microsoft Outlook-Symbolleiste, 31
manuelles Prüfen über Windows-Explorer, 30
Nach neuen, unbekannten Viren scannen, Option, 28
Quarantäne für einen Virus oder ein möglicherweise unerwünschtes Programm, 34
testen, 10 to 11
Unterordner überprüfen, Option, 27
Schnellreferenz, iii
ScriptStopper, 21
Skripts
anhalten, 25
Warnungen, 25
zulassen, 25
Systemanforderungen, 8

T

Technischer Support, 34
Testen von VirusScan, 9
Trojaner
erkennen, 33
Warnungen, 24

U

Übermitteln verdächtiger Dateien an AVERT, 36
Unterordner überprüfen, Option (Scan), 27
Update-Assistent, 15

V

Vertrauenswürdige Programme, 26
Verwenden einer Rettungsdiskette, 38
Viren
  Anhalten potentieller Würmer, 25
  Anhalten verdächtiger Skripts, 25
  automatisches Melden, 38, 40
  bereinigen, 24, 33
  Entfernen von PUPs, 26
  erkennen, 33
  Erkennung mit ActiveShield, 24
  löschen, 24, 33
  Löschen infizierter Dateien, 25
  Quarantäne für infizierte Dateien, 24
  unter Quarantäne stellen, 24, 33
  Warnungen, 24
  Zulassen verdächtiger Skripts, 25
VirusScan
  automatisches Aktualisieren, 41
  automatisches Melden von Viren, 38, 40
  Erste Schritte, 7
  manuelles Aktualisieren, 41
  Planen von Prüfungen, 31
  Prüfen über die Microsoft Outlook-Symbolleiste, 31
  Prüfen über Windows-Explorer, 30
  testen, 9

W

Warnungen
  bei infizierten Dateien, 24
  bei infizierten E-Mails, 25
  bei potentiellen Würmern, 25
  bei PUPs, 26
  bei verdächtigen Skripts, 25
  bei Viren, 24
Windows-Explorer, 30
World Virus Map
  anzeigen, 40
  melden, 38
WormStopper, 18
Würmer
  anhalten, 25
  erkennen, 24, 33
  Warnungen, 24 to 25