McAfee

# wirelesshomenetworksecurity

# Benutzerhandbuch

McAfee®

## INFORMATIONEN ZUR LIZENZ

### Lizenzvereinbarung

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 DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. FALLS ZUTREFFEND, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE ODER AN DIE STELLE ZURÜCKGEBEN, AN DER SIE DAS PRODUKT ERWORBEN HABEN.

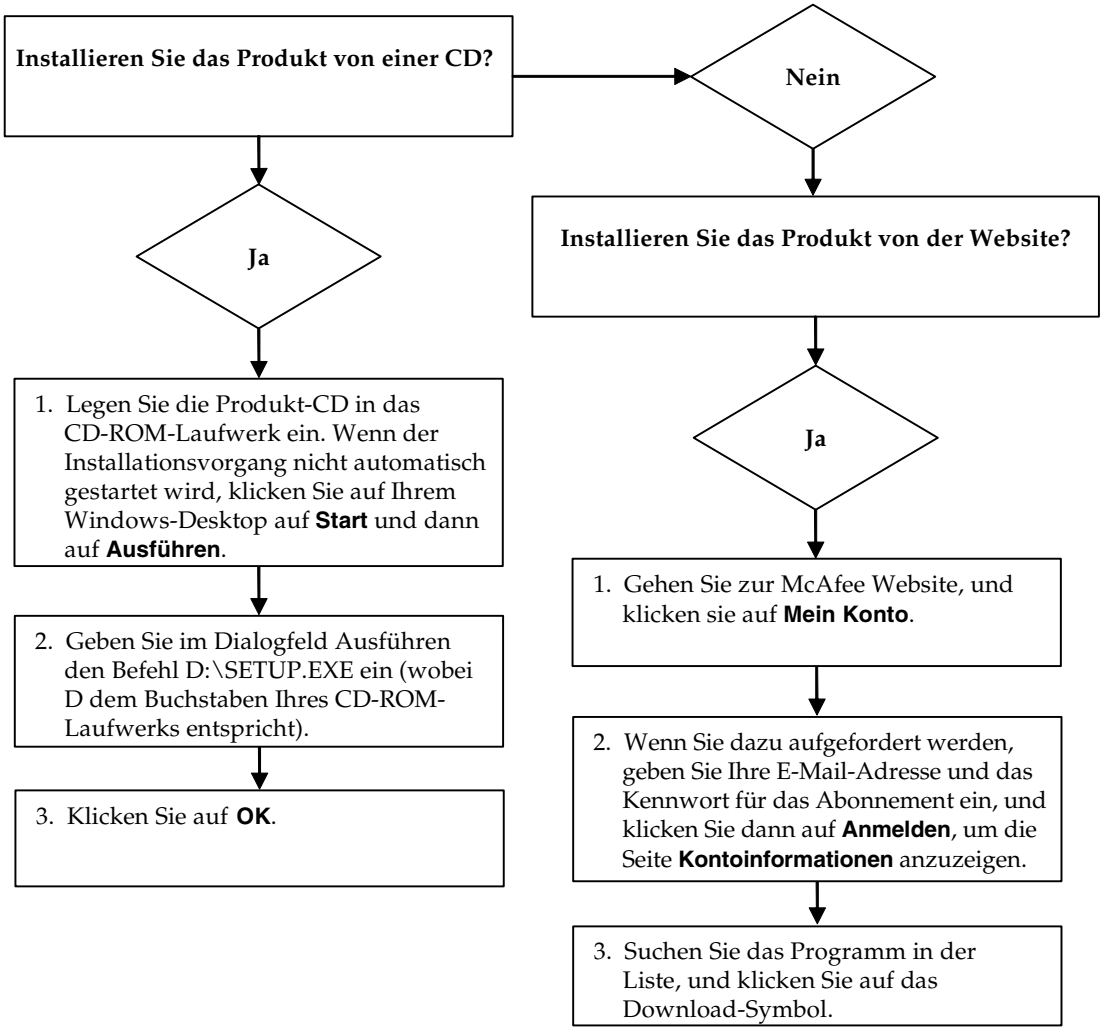
### Hinweise

Dieses Produkt enthält oder enthält möglicherweise:

♦ 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. Bei Software, die GPL unterliegt und in ausführbarem Binärformat an andere Personen weitergegeben wird, muss diesen Benutzern auch der Quellcode zur Verfügung gestellt werden. Der Quellcode der GPL unterliegenden Software ist auf dieser CD einsehbar. Falls Lizenzen für kostenlose Software verlangen, dass McAfee Rechte für die Nutzung, das Kopieren oder die Modifikation eines Softwareprogramms gewährt, die 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 des Lizenzvertrags für diese Software erhalten Sie unter www.python.org. ♦ Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002. ♦ Von Andrew Lumsdaine entwickelte Software, 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, urheberrechtlich geschützt 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 das Produkt von einer CD oder einer Website aus installieren, sollten Sie diese praktische Referenzseite ausdrucken.**



## 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 Benutzerhandbuchs, das Sie öffnen möchten.

## Registrierungsvorteile

Es wird empfohlen, 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. Weitere Vorteile sind:

- KOSTENLOSER elektronischer 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://de.mcafee.com/.
- Umtauschgarantie von 60 Tagen für Ihre Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr ab dem Zeitpunkt der Installation bei Kauf der SpamKiller-Software

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

  Preisangaben für ein zusätzliches Jahr Inhalts-Updates erhalten Sie unter http://de.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.

Für erfahrene Benutzer stehen außerdem erweiterte Optionen zur Verfügung, zum Beispiel eine Schlüsselwortsuche und unsere strukturierte Hilfe. 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. Außerdem gibt es noch die Möglichkeit von telefonischem Support, über den Sie hier mehr Informationen finden können:

http://www.mcafeehilfe.com/.

# Inhalt

# Erste Schritte 1

Willkommen bei McAfee Wireless Home Network Security. Dieses Programm bietet umfassenden Schutz für Ihr drahtloses Netzwerk, Ihre persönlichen Daten und Ihren Computer.

Das Programm ist für Computer mit drahtlosen Verbindungen ausgelegt. Wenn Sie es auf Computern installieren, die per Kabel mit Ihrem Netzwerk verbunden sind, steht auf den verkabelten Computern nicht der volle Funktionsumfang zur Verfügung.

Durch Verschlüsselung Ihrer persönlichen, privaten Daten bei der Übertragung sorgt McAfee Wireless Home Network Security für optimalen Datenschutz in Ihrem geschützten drahtlosen Netzwerk und verhindert, dass Hacker auf Ihre Informationen zugreifen.

## Verwenden von McAfee Wireless Home Network Security

Beachten Sie Folgendes, bevor Sie Ihr Netzwerk schützen.

- Kabelverbindungen – Computer, die per Kabel mit dem Router verbunden sind, müssen nicht geschützt werden, da per Kabel übertragene Signale nicht abgefangen werden können.
- Drahtlose Verbindungen – Computer mit drahtloser Verbindung sollten geschützt werden, da ihre Daten abgefangen werden können. Ein Netzwerk muss mithilfe eines drahtlosen Computers geschützt werden, denn nur ein drahtloser Computer kann einem anderen drahtlosen Computer Zugriff gewähren.

### Schützen Ihres Netzwerks

Bei einer kabelgebundenen Verbindung müssen Sie das Netzwerk nicht schützen.

1. Installieren Sie auf Ihrem drahtlosen Computer den drahtlosen Adapter, und aktivieren Sie ihn. Der drahtlose Adapter kann eine Karte sein, die seitlich im Computer eingesteckt ist, oder er kann am USB-Anschluss angeschlossen sein. Viele neuere Computer sind mit einem integrierten Drahtlosadapter ausgerüstet, so dass Sie keinen installieren müssen.

2 Installieren Sie Ihren drahtlosen Router oder Zugriffspunkt (mithilfe von Zugriffspunkten wird die Reichweite erweitert), und stellen Sie sicher, dass er eingeschaltet und aktiviert ist. Eine umfassendere Definition eines Routers und Zugriffspunktes finden Sie im *Glossar* auf Seite 47.

3 Installieren Sie McAfee Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk. Auf Computern, die per Kabel verbunden sind, müssen Sie die Software nicht installieren. Siehe *Installieren von Wireless Home Network Security* auf Seite 15.

4 Schützen Sie das Netzwerk von einem der drahtlosen Computer aus. Siehe *Schützen drahtloser Netzwerke* auf Seite 28.

5 Melden Sie sich von den anderen drahtlosen Computern aus am Netzwerk an. Siehe *Schützen anderer Computer* auf Seite 27.

# Grundlegendes zu Wireless Home Network Security

Wie viele andere auch, nutzen Sie zu Hause ein drahtloses Netzwerk, weil es einfach und bequem ist. Mit einem solchen Netzwerk haben Sie in jedem Zimmer und sogar im Garten Zugang zum Internet – ohne die Kosten und Probleme, die mit Kabeln verbunden sind. Dank der Drahtlostechnik können Sie Angehörigen und Freunden ganz einfach den Zugriff auf das Netzwerk ermöglichen.

Allerdings ist diese Bequemlichkeit mit einigen Sicherheitsrisiken verbunden. In drahtlosen Netzwerken werden die Daten per Funk übertragen, und diese Funksignale machen an den Wänden Ihrer Wohnung nicht halt. Mit speziellen Antennen können Unbefugte auf Ihr drahtloses Netzwerk zugreifen und Ihre Daten noch aus mehreren Kilometern Entfernung abfangen.

Zum Schutz Ihres drahtlosen Netzwerks und Ihrer Daten müssen Sie den Zugriff auf das Netzwerk beschränken und die Daten verschlüsseln. Zwar sind in Ihrem drahtlosen Router oder Zugriffspunkt Sicherheitsstandards integriert, doch besteht die Schwierigkeit darin, die Sicherheitseinstellungen richtig zu aktivieren und zu verwalten. Mehr als 60 Prozent aller drahtlosen Netzwerke sind nicht in einem ausreichend hohen Maße (etwa durch Verschlüsselung) geschützt.

## Wireless Home Network Security macht Ihnen die Arbeit leicht

McAfee Wireless Home Network Security aktiviert die Sicherheitseinstellungen in Ihrem drahtlosen Netzwerk und schützt die übertragenen Daten mit einem einfachen, mit einem Klick zu bewältigenden Vorgang, bei dem automatisch ein starker Verschlüsselungsschlüssel generiert wird. Die meisten Schlüssel, die für Nutzer leicht zu merken sind, können von Hackern mühelos geknackt werden. Indem sich der Computer den Schlüssel für Sie "merkt", kann Wireless Home Network Security Schlüssel verwenden, die fast unmöglich zu knacken sind.

Außerdem generiert und verteilt diese Software, während sie unauffällig im Hintergrund ausgeführt wird, alle paar Minuten einen neuen Verschlüsselungsschlüssel, so dass selbst der entschlossenste Hacker aufgeben muss. Berechtigte Computer, etwa jene von Familienangehörigen und Freunden, die auf das drahtlose Netzwerk zugreifen möchten, erhalten den starken Verschlüsselungsschlüssel sowie alle verteilten Schlüssel.

Diese Lösung bietet umfassende Sicherheit und kann dennoch mühelos vom Besitzer eines drahtlosen Netzwerks zu Hause implementiert werden. Mit einem Klick können Sie Hacker davon abhalten, Ihre drahtlos übertragenen Daten zu stehlen. Hacker können keine Trojaner oder andere bösartige Programme in Ihr Netzwerk einschleusen. Sie können Ihr drahtloses Netzwerk auch nicht als Ausgangspunkt für Spam- oder Virenangriffe missbrauchen. Selbst Gelegenheits-Freeloader können nicht auf das drahtlose Netzwerk zugreifen; dadurch können Sie auch nicht irrtümlich für illegale Film- oder Musik-Downloads angeklagt werden.

Andere Lösungen bieten weder die Einfachheit noch die umfassende Sicherheit von Wireless Home Network Security. Das Filtern von MAC-Adressen oder das Deaktivieren der SSID-Übertragung gewährt nur oberflächlichen Schutz. Selbst unerfahrene Hacker können diese Mechanismen mit frei erhältlichen Tools aus dem Internet umgehen. Andere Hilfsmittel wie VPNs schützen nicht das drahtlose Netzwerk an sich, somit ist es nach wie vor anfällig für eine Vielzahl von Angriffen.

McAfee Wireless Home Network Security ist das erste Programm, das Ihr drahtloses Heimnetzwerk wirklich umfassend absichert.

# Funktionen

Diese Version von Wireless Home Network Security bietet die folgenden Funktionen:

- Ständig aktiver Schutz – Erkennt und schützt automatisch gefährdete drahtlose Netzwerke, zu denen Sie eine Verbindung herstellen.
- Leicht verständliche Benutzeroberfläche – Ermöglicht Ihnen den Schutz des Netzwerks, ohne dass Sie schwierige Entscheidungen treffen oder komplizierte technische Begriffe kennen müssen.
- Starke automatische Verschlüsselung – Gewährt ausschließlich Familienangehörigen und Freunden Zugriff auf das Netzwerk und schützt Ihre Daten bei der Übertragung.
- Reine Softwarelösung – Wireless Home Network Security funktioniert mit einem herkömmlichen drahtlosen Router oder Zugriffspunkt und mit normaler Sicherheitssoftware. Sie müssen keine zusätzliche Hardware erwerben.

- Automatische Schlüsselrotation – Selbst die entschlossensten Hacker können Ihre Daten nicht abfangen, da der Schlüssel ständig geändert wird.
- Hinzufügen von Netzwerkbenutzern – Sie können Ihren Familienangehörigen und Freunden mühelos Zugriff auf das Netzwerk gewähren.
- Intuitives Verbindungs-Tool – Das Tool für drahtlose Verbindungen ist intuitiv zu bedienen und informativ. Es zeigt Details zur Signalstärke und zum Sicherheitsstatus an.
- Ereignisprotokollierung und Warnungen – Leicht verständliche Berichte und Warnungen bieten erfahrenen Benutzern weitere Informationen zum drahtlosen Netzwerk.
- Aussetzmodus – Hiermit können Sie die Schlüsselrotation vorübergehend aussetzen, damit bestimmte Anwendungen ohne Unterbrechung ausgeführt werden können.
- Kompatibilität mit anderer Hardware - Wireless Home Network Security aktualisiert sich selbst automatisch mit den neuesten Modulen für drahtlose Router oder Zugriffspunkte der am häufigsten verwendeten Marken. Dazu gehören: Linksys®, NETGEAR®, D-Link®, Belkin® und andere.

# Systemanforderungen

- Microsoft® Windows 98SE, Windows Me, Windows 2000 oder Windows XP
- PC mit Pentium-kompatiblem Prozessor

  Windows 98 oder Windows 2000: 133 MHz oder höher

  Windows Me: 150 MHz oder höher

  Windows XP (Home und Professional): 300 MHz oder höher
- RAM

  Windows 98SE, Me oder 2000: 64 MB

  Windows XP (Home und Professional): 128 MB
- 50 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.

**Drahtloses Netzwerk**

- Herkömmlicher drahtloser Netzwerkadapter
- Herkömmlicher drahtloser Router oder Zugriffspunkt, darunter die meisten Modelle von Linksys®, NETGEAR®, D-Link® und Belkin®

# Verwenden von McAfee SecurityCenter

McAfee SecurityCenter ist Ihre Anlaufstelle für alle Sicherheitsbelange. Sie können SecurityCenter mithilfe des McAfee-Symbols in der Windows-Taskleiste oder vom Windows-Desktop aus starten.

**HINWEIS**
Wenn Sie weitere Informationen zu den Funktionen anzeigen möchten, klicken Sie im Dialogfenster **SecurityCenter** auf **Hilfe**.

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 der Funktionen von Wireless Home Network Security zu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol .
2. Zeigen Sie auf **Wireless Network Security**, und klicken Sie auf die Funktion, die Sie verwenden möchten.

# Installieren von Wireless Home Network Security 2

In diesem Kapitel werden die Installation von Wireless Home Network Security und die ersten Schritte zum Schützen Ihres Netzwerks beschrieben.

Achten Sie beim Installieren von Wireless Home Network Security auf Folgendes.

- Installieren Sie die Software auf allen drahtlosen Computern.
- Auf Computern, die per Kabel verbunden sind, müssen Sie die Software nicht installieren.

## Installieren von einer CD

1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein. Wenn der Installationsvorgang nicht automatisch gestartet wird, klicken Sie auf Ihrem Windows-Desktop auf **Start** und dann auf **Ausführen**.
2. Geben Sie im Dialogfeld **Ausführen** den Befehl D:\SETUP.EXE ein (wobei D dem Buchstaben Ihres CD-ROM-Laufwerks entspricht).
3. Klicken Sie auf **OK**.
4. Gehen Sie zu *Verwenden des Konfigurationsassistenten* auf Seite 16.

## Installieren von der Website

Wenn Sie Wireless Home Network Security von der Website aus installieren, müssen Sie die Installationsdatei speichern. Mithilfe dieser Datei wird Wireless Home Network Security auf anderen Computern installiert.

1. Gehen Sie zur McAfee Website, und klicken sie auf **Mein Konto**.
2. Wenn Sie dazu aufgefordert werden, geben Sie die E-Mail-Adresse und das Kennwort für das Abonnement ein, und klicken Sie dann auf **Anmelden**, um die Seite **Kontoinformationen** anzuzeigen.
3. Suchen Sie Ihr Programm in der Liste, und klicken Sie auf **Ziel speichern unter**. Die Installationsdatei wird auf Ihrem Computer gespeichert.

## Installieren mithilfe der Installationsdatei

Wenn Sie das Installationspaket heruntergeladen haben (also über keine CD verfügen), müssen Sie die Software auf allen drahtlosen Computern installieren. Nachdem das Netzwerk geschützt worden ist, kann mit drahtlosen Computern ohne Eingabe des Schlüssels keine Verbindung zum Netzwerk hergestellt werden. Führen Sie einen der folgenden Schritte aus:

- Laden Sie das Installationspaket auf alle drahtlosen Computer herunter, bevor Sie das Netzwerk schützen.
- Kopieren Sie die Installationsdatei auf einen USB-Speicherstick oder eine beschreibbare CD, und installieren Sie die Software auf den anderen drahtlosen Computern.
- Schließen Sie, falls das Netzwerk bereits geschützt ist, ein Kabel am Router an, um die Datei herunterzuladen. Sie können auch auf **Aktuellen Schlüssel anzeigen** klicken, um den aktuellen Schlüssel anzuzeigen und damit eine Verbindung zum drahtlosen Netzwerk herzustellen.

Befolgen Sie nach der Installation von Wireless Home Network Security auf allen drahtlosen Computern die Anweisungen auf dem Bildschirm. Wenn Sie auf **Fertig stellen** klicken, wird der Konfigurationsassistent geöffnet. Gehen Sie zu *Verwenden des Konfigurationsassistenten* auf Seite 16.

# Verwenden des Konfigurationsassistenten

Mit dem Konfigurationsassistenten können Sie die folgenden Aufgaben ausführen:

- Schützen des Netzwerks von einem der drahtlosen Computer aus. Weitere Informationen finden Sie unter *Schützen drahtloser Netzwerke* auf Seite 28.

  Wenn Wireless Home Network Security den richtigen zu schützenden Router oder Zugriffspunkt nicht ermitteln kann, werden Sie aufgefordert, den Vorgang zu wiederholen oder abzubrechen. Rücken Sie näher an den Router bzw. Zugriffspunkt heran, den Sie schützen möchten, und klicken Sie dann auf **Wiederholen**.
- Anmelden an einem geschützten Netzwerk (bei Vorhandensein von nur einem drahtlosen Computer ist dieser Schritt nicht erforderlich). Weitere Informationen finden Sie unter *Verwalten drahtloser Netzwerke* auf Seite 19.
- Herstellen einer Verbindung zu einem Netzwerk. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 20.

Falls der drahtlose Adapter nicht erkannt wird oder der drahtlose Router oder Zugriffspunkt nicht eingeschaltet ist, werden Sie benachrichtigt.

# Verwenden der Seite "Zusammenfassung" 3

Wenn Sie den Status Ihrer Verbindung anzeigen möchten, klicken Sie mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Zusammenfassung** aus. Die Seite **Zusammenfassung** wird angezeigt (Abbildung 3-1).


**Abbildung 3-1. Seite "Zusammenfassung"**

## Anzeigen Ihrer Verbindung

Der Fensterbereich **Verbindung** zeigt den Status Ihrer Verbindung an. Wenn Sie eine Überprüfung Ihrer drahtlosen Verbindung durchführen möchten, klicken Sie auf **Sicherheitsscan**.

- Status – Zeigt an, ob Sie verbunden oder getrennt sind. Wenn Sie verbunden sind, wird der Name des Netzwerks angezeigt.
- Sicherheit – Der Sicherheitsmodus des Netzwerks.
- Geschwindigkeit – Die Verbindungsgeschwindigkeit Ihrer drahtlosen Netzwerkkarte.
- Dauer – Die Dauer Ihrer Verbindung zu diesem Netzwerk.
- Signalstärke – Die Stärke des Signals der drahtlosen Verbindung.

# Anzeigen Ihres geschützten drahtlosen Netzwerks

Der Fensterbereich **Geschütztes drahtloses Netzwerk** enthält Informationen zu Ihrem Netzwerk.

- Verbindungen heute – Gibt an, wie oft Benutzer am aktuellen Tag eine Verbindung zu diesem Netzwerk hergestellt haben.
- Schlüsselrotationen heute – Gibt an, wie oft der Schlüssel am aktuellen Tag geändert wurde, einschließlich der Zeit seit der letzten Änderung.
- Schlüsselrotation ausgesetzt – Die Schlüsselrotation in Ihrem Netzwerk ist ausgesetzt. Klicken Sie auf **Schlüsselrotation fortsetzen**, um die Rotation fortzusetzen und sicherzustellen, dass das Netzwerk vollständig vor Hackern geschützt ist.
- In diesem Monat gesicherte Computer – Gibt an, wie viele Computer im laufenden Monat gesichert wurden.
- Computer – Wenn Sie mit einem geschützten Netzwerk verbunden sind, werden alle im Netzwerk befindlichen Computer sowie der Zeitpunkt angezeigt, zu dem diese jeweils zum letzten Mal verbunden waren.

  – Der Computer ist verbunden.

  – Der Computer kann ohne Anmeldung am Netzwerk erneut eine Verbindung herstellen.

  – Der Computer ist nicht verbunden. Der Computer muss sich am Netzwerk neu anmelden, weil der Schlüssel aktualisiert wurde.

Klicken Sie auf **Netzwerkereignisse anzeigen**, um Netzwerkereignisse anzuzeigen. Siehe *Anzeigen von Ereignissen* auf Seite 23.

Klicken Sie auf **Aktuellen Schlüssel anzeigen**, um den Schlüssel anzuzeigen.

Wenn Sie drahtlose Geräte, die von Wireless Home Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), gehen Sie folgendermaßen vor.

1. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**.
2. Notieren Sie den Schlüssel.
3. Klicken Sie auf **Schlüsselrotation aussetzen**. Durch Aussetzen der Schlüsselrotation wird verhindert, dass die Verbindung zu manuell mit dem Netzwerk verbundenen Geräten getrennt wird.
4. Geben Sie den Schlüssel im Gerät ein.

Klicken Sie auf **Schlüsselrotation fortsetzen**, wenn Sie diese Geräte nicht mehr benötigen. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vor Hackern vollständig geschützt ist.

# Verwalten drahtloser Netzwerke 4

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Verfügbare drahtlose Netzwerke** aus, um drahtlose Netzwerke auszuwählen, zu denen Sie eine Verbindung herstellen oder an denen Sie sich anmelden möchten. Die Seite **Verfügbare drahtlose Netzwerke** wird angezeigt (Abbildung 4-1).


**Abbildung 4-1. Seite "Verfügbare drahtlose Netzwerke"**

Wenn Sie mit einem geschützten drahtlosen Netzwerk verbunden sind, werden die gesendeten und empfangenen Informationen verschlüsselt. Hacker können die im geschützten Netzwerk übertragenen Daten nicht abfangen und auch keine Verbindung zu Ihrem Netzwerk herstellen.

– Das Netzwerk ist geschützt.

– Das Netzwerk ist mithilfe von WEP- oder WPA-PSK-Sicherheit geschützt.

– Das Netzwerk ist ungeschützt; Sie können dennoch eine Verbindung dazu herstellen (nicht empfohlen).

# Verbinden mit einem Netzwerk

Wählen Sie zum Herstellen einer Verbindung zu einem Netzwerk das gewünschte Netzwerk aus, und klicken Sie auf **Verbinden**. Wenn Sie für Ihren Router oder Zugriffspunkt einen vorinstallierten Schlüssel manuell konfiguriert haben, müssen Sie auch den Schlüssel eingeben.

Wenn das Netzwerk geschützt ist, müssen Sie sich anmelden, bevor Sie eine Verbindung mit dem Netzwerk herstellen können. Damit Sie sich anmelden können, muss Ihnen ein bereits mit dem Netzwerk verbundener Benutzer die Berechtigung dazu erteilen.

Wenn Sie sich an einem Netzwerk anmelden, können Sie die Verbindung mit dem Netzwerk erneut herstellen, ohne sich wieder anmelden zu müssen. Sie können auch anderen Benutzern die Berechtigung erteilen, sich an diesem Netzwerk anzumelden.

# Trennen einer Netzwerkverbindung

Klicken Sie zum Trennen einer bestehenden Verbindung zu einem Netzwerk auf **Trennen**.

# Verwenden erweiterter Optionen

Klicken Sie auf **Erweitert**, wenn Sie erweiterte Verbindungsoptionen verwenden möchten. Das Dialogfeld **Erweiterte Eigenschaften für drahtloses Netzwerk** wird angezeigt. In diesem Dialogfeld haben Sie die folgenden Möglichkeiten:

- Ändern der Reihenfolge der Netzwerke, zu denen automatisch eine Verbindung hergestellt wird – Das Netzwerk an erster Stelle in der Liste ist das Netzwerk, zu dem Sie zuletzt eine Verbindung hergestellt haben. Zu diesem Netzwerk versucht Wireless Home Network Security als Erstes, eine Verbindung herzustellen. Wählen Sie zum Verschieben eines Netzwerks das gewünschte Netzwerk aus, und klicken Sie auf **Nach oben** oder **Nach unten**. Wenn Sie zum Beispiel den Standort gewechselt haben und das Netzwerk, mit dem Sie zuletzt verbunden waren, weit entfernt ist und kein starkes Signal aufweist, können Sie ein Netzwerk mit einem stärkeren Signal an die erste Stelle der Liste setzen.
- Entfernen bevorzugter Netzwerke – Entfernen Sie Netzwerke aus dieser Liste. Wenn Sie beispielsweise versehentlich eine Verbindung zum Netzwerk Ihres Nachbarn hergestellt haben, wird es nun in der Liste aufgeführt. Wählen Sie das Netzwerk aus, und klicken Sie auf **Entfernen**, um es aus der Liste zu löschen.

- Ändern von Netzwerkeigenschaften – Wenn es beim Herstellen einer Verbindung zu einem ungeschützten Netzwerk zu Problemen kommt, können Sie dessen Eigenschaften ändern. Beachten Sie, dass diese Option nur für Netzwerke gilt, die nicht geschützt sind. Wählen Sie ein Netzwerk aus, und klicken Sie auf **Eigenschaften**, um dessen Eigenschaften zu ändern.
- Hinzufügen von Netzwerken ohne SSID-Übertragung – Wenn Sie beispielsweise eine Verbindung zum drahtlosen Netzwerk eines Freundes herstellen möchten, dieses aber nicht in der Liste aufgeführt wird, können Sie auf **Hinzufügen** klicken und die entsprechenden Informationen eingeben. Beachten Sie, dass das hinzugefügte Netzwerk nicht durch Wireless Home Network Security geschützt werden kann.

# Konfigurieren von Optionen 5

Klicken Sie zum Konfigurieren von Optionen mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie dann **Optionen** aus. Die Seite **Optionen** wird angezeigt (Abbildung 5-1).


**Abbildung 5-1. Seite "Optionen"**

## Anzeigen von Ereignissen

Alle von Wireless Home Network Security durchgeführten Aktionen werden in Ereignisprotokollen vermerkt. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**. Die Informationen werden standardmäßig in chronologischer Reihenfolge angezeigt.

Im Feld **Ereignisse für das Netzwerk** können Sie auswählen, welche Art von Ereignissen angezeigt werden soll (unabhängig davon werden alle Ereignisse weiterhin protokolliert). Außerdem können Sie gegebenenfalls Ereignisse für jedes beliebige Netzwerk anzeigen, zu dem Sie gehören (falls Sie zu mehr als einem Netzwerk gehören).

Wenn ein Ereignis eintritt, wird eine Warnung mit einer kurzen Beschreibung angezeigt. Weitere Informationen zu Warnungen finden Sie unter *Grundlegendes zu Warnungen* auf Seite 31.

# Konfigurieren erweiterter Einstellungen

Dieser Abschnitt richtet sich an erfahrene Benutzer. Klicken Sie auf **Erweiterte Einstellungen**, um Sicherheits-, Warnungs- und sonstige Einstellungen zu konfigurieren.

Nachdem Sie eine Einstellung geändert haben, klicken Sie auf **OK**, damit die Änderungen wirksam werden. Beachten Sie, dass nach dem Klicken auf **OK** bei allen verbundenen Computern die Verbindung vorübergehend (einige Minuten) getrennt wird.

## Konfigurieren von Sicherheitseinstellungen

Verwenden Sie die Registerkarte **Sicherheitseinstellungen**, um Ihre Sicherheitseinstellungen zu ändern.

- Name des geschützten drahtlosen Netzwerks – Das ist der Name des derzeit geschützten Netzwerks. Wenn Sie den Namen eines Netzwerks ändern, wird es in der Liste **Verfügbare drahtlose Netzwerke** angezeigt, und Sie müssen dann eine neue Verbindung zu dem Netzwerk herstellen. Siehe *Verwalten drahtloser Netzwerke* auf Seite 19.

- Sicherheitsmodus – Das ist der aktuelle Sicherheitsmodus. Wenn Sie die Standardsicherheit (WEP) ändern möchten, wählen Sie WPA-PSK TKIP aus, um eine stärkere Verschlüsselung zu erhalten. Stellen Sie sicher, dass die Router, Zugriffspunkte und drahtlosen Adapter, die eine Verbindung zum Netzwerk herstellen, diesen Modus unterstützen. Andernfalls kann keine Verbindung hergestellt werden. Weitere Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 41.

- Automatische Schlüsselrotation aktivieren – Zum Aussetzen der Schlüsselrotation müssen Sie diese Option deaktivieren. Zum Ändern der Häufigkeit der Schlüsselrotation müssen Sie den Schieberegler verschieben. Weitere Informationen zur Schlüsselrotation finden Sie unter *Anzeigen Ihres geschützten drahtlosen Netzwerks* auf Seite 18.

- Benutzernamen oder Kennwort ändern – Sie können aus Sicherheitsgründen den standardmäßigen Benutzernamen oder das standardmäßige Kennwort für den drahtlosen Router oder Zugriffspunkt ändern, indem Sie ihn bzw. es auswählen und auf **Benutzernamen oder Kennwort ändern** klicken. Die Standardanmeldeinformationen haben Sie beim Anmelden und Konfigurieren Ihres Routers oder Zugriffspunktes angegeben.

## Konfigurieren von Warnungseinstellungen

Verwenden Sie die Registerkarte **Warnungseinstellungen**, um Ihre Warnungseinstellungen zu ändern.

Wählen Sie die Art der Ereignisse aus, bei denen Sie gewarnt werden möchten, und klicken Sie auf **OK**. Wenn Sie auf bestimmte Arten von Ereignissen nicht aufmerksam gemacht werden möchten, müssen Sie die entsprechenden Kontrollkästchen deaktivieren.

## Konfigurieren weiterer Einstellungen

Verwenden Sie die Registerkarte **Weitere Einstellungen**, um weitere Einstellungen zu ändern.

- Schlüssel in Klartext anzeigen – Für Netzwerke, die nicht durch Wireless Home Network Security geschützt sind. Schlüssel für ungeschützte Netzwerke, die in der Liste **Verfügbare drahtlose Netzwerke** aufgeführt sind, können in Klartext statt als Sternchen angezeigt werden. Wenn Sie Schlüssel in Klartext anzeigen, werden die Schlüssel aus Sicherheitsgründen verworfen.
- Alle gespeicherten Schlüssel verwerfen – Für Netzwerke, die nicht durch Wireless Home Network Security geschützt sind. Hierbei werden alle Schlüssel gelöscht, die gespeichert wurden. Hinweis: Wenn Sie diese Schlüssel löschen, müssen Sie erneut einen Schlüssel eingeben, wenn Sie eine Verbindung zu WEP- oder WPA-PSK-Netzwerken herstellen.
- Netzwerk verlassen – Für Netzwerke, die durch Wireless Home Network Security geschützt sind. Sie können Ihre Zugriffsrechte für ein geschütztes drahtloses Netzwerk aufgeben. Wenn Sie beispielsweise ein Netzwerk verlassen möchten und nicht vorhaben, später noch einmal eine Verbindung zu diesem Netzwerk herzustellen, können Sie es in der Liste auswählen und auf **Netzwerk verlassen** klicken.
- Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen – Beim Herstellen einer Verbindung wird eine Benachrichtigung angezeigt.

# Widerrufen des Zugriffs auf das Netzwerk

So verhindern Sie, dass Computer auf das Netzwerk zugreifen, die angemeldet sind, aber derzeit keine Verbindung zum Netzwerk haben:

1. Klicken Sie auf **Zugriff widerrufen**. Das Dialogfeld **Zugriff widerrufen** wird angezeigt.
2. Klicken Sie auf **Widerrufen**.

Die Schlüsselrotation für das Netzwerk wird zurückgesetzt. Die aktuell verbundenen Computer erhalten den neuen Schlüssel und bleiben verbunden. Computer, die derzeit nicht verbunden sind, erhalten den aktualisierten Schlüssel nicht und müssen sich neu anmelden, bevor sie eine Verbindung herstellen können.

Wenn Sie den Zugriff für einen Computer widerrufen, kann der Computer erst nach erneuter Anmeldung wieder eine Verbindung zum geschützten Netzwerk herstellen. Dazu muss auf dem Computer Wireless Home Network Security installiert sein (siehe *Installieren von Wireless Home Network Security* auf Seite 15), und dann muss der Computer mit dem geschützten Netzwerk verbunden und dort angemeldet werden (siehe *Verbinden mit einem Netzwerk* auf Seite 20).

# Reparieren von Sicherheitseinstellungen

Reparieren Sie die Sicherheitseinstellungen nur dann, wenn Sie Probleme mit Ihrem drahtlosen Netzwerk haben. Weitere Informationen finden Sie unter *Keine Verbindung möglich* auf Seite 41.

Gehen Sie zum Reparieren der Einstellungen für Router oder Zugriffspunkte im aktuellen Netzwerk folgendermaßen vor.

1. Klicken Sie auf **Sicherheitseinstellungen reparieren**. Das Dialogfeld **Reparieren** wird angezeigt.
2. Klicken Sie auf **Reparieren**.
3. Klicken Sie auf **Schließen**, wenn der Vorgang abgeschlossen ist.

Wenn keine Verbindung zu den Netzwerkroutern oder -zugriffspunkten hergestellt werden kann, wird eine Fehlermeldung angezeigt. Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang. Wenn das Kennwort für den Router oder Zugriffspunkt geändert wurde, werden Sie zur Eingabe des neuen Kennworts aufgefordert.

# Schützen anderer Computer

Klicken Sie auf **Anderen Computer schützen**, um weitere Informationen zum Schützen anderer Computer und zum Gewähren von Zugriff auf das geschützte Netzwerk zu erhalten.

So schützen Sie einen anderen Computer:

1. Installieren Sie McAfee Wireless Home Network Security auf dem Computer, den Sie schützen möchten.
2. Klicken Sie auf dem Computer, den Sie schützen möchten, mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Verfügbare drahtlose Netzwerke** aus. Die Seite **Verfügbare drahtlose Netzwerke** wird angezeigt.
3. Wählen Sie ein geschütztes Netzwerk aus, an dem Sie sich anmelden möchten, und klicken Sie auf **Verbinden**. Beachten Sie, dass Ihnen ein bereits mit dem Netzwerk verbundener Benutzer die Berechtigung zum Anmelden erteilen muss.

   Wenn Sie sich an einem Netzwerk anmelden, können Sie die Verbindung mit dem Netzwerk erneut herstellen, ohne sich wieder anmelden zu müssen. Sie können auch anderen Benutzern die Berechtigung erteilen, sich an diesem Netzwerk anzumelden.
4. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Wenn Sie drahtlose Geräte, die von Wireless Home Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), gehen Sie folgendermaßen vor.

1. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**.
2. Notieren Sie den Schlüssel.
3. Klicken Sie auf **Schlüsselrotation aussetzen**. Durch Aussetzen der Schlüsselrotation wird verhindert, dass die Verbindung zu manuell mit dem Netzwerk verbundenen Geräten getrennt wird.
4. Geben Sie den Schlüssel im Gerät ein.

Klicken Sie auf **Schlüsselrotation fortsetzen**, wenn Sie diese Geräte nicht mehr benötigen. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vor Hackern vollständig geschützt ist.

# Rotieren des Schlüssels

Klicken Sie auf **Sicherheitsschlüssel manuell rotieren**, um den Sicherheitsschlüssel für das Netzwerk zu rotieren.

# Schützen drahtloser Netzwerke

Gehen Sie zum Schützen eines Routers oder Zugriffspunktes folgendermaßen vor.

1. Klicken Sie auf **Drahtlosen Router/Zugriffspunkt schützen**. Das Dialogfeld **Drahtloses Netzwerk schützen** wird angezeigt. Wenn der Router oder Zugriffspunkt nicht in der Liste aufgeführt wird, klicken Sie auf **Aktualisieren**.
2. Wählen Sie den zu schützenden Router oder Zugriffspunkt aus, und klicken Sie auf **Schützen**.

# Aufheben des Schutzes drahtloser Netzwerke

Sie müssen mit dem drahtlosen Router oder Zugriffspunkt verbunden sein, dessen Schutz Sie aufheben möchten.

Gehen Sie zum Aufheben des Schutzes eines Routers oder Zugriffspunktes folgendermaßen vor.

1. Klicken Sie auf **Schutz für drahtlosen Router/Zugriffspunkt aufheben**. Das Dialogfeld **Schutz für drahtloses Netzwerk aufheben** wird angezeigt. Wenn der Router oder Zugriffspunkt nicht in der Liste aufgeführt wird, klicken Sie auf **Aktualisieren**.
2. Wählen Sie den Router oder Zugriffspunkt aus, dessen Schutz Sie aufheben möchten, und klicken Sie auf **Schutz aufheben**.

# Aktualisieren von Wireless Home Network Security 6

Wenn Sie mit dem Internet verbunden sind, prüft Wireless Home Network Security alle vier Stunden, ob Software-Updates zur Verfügung stehen, lädt diese dann automatisch herunter und installiert wöchentliche Updates, ohne Sie bei der Arbeit zu unterbrechen. Das Herunterladen dieser Updates beeinträchtigt die Leistung Ihres Systems nur minimal.

Bei einem Produktupdate erhalten Sie eine entsprechende Benachrichtigung. Sie können dann entscheiden, ob Wireless Home Network Security aktualisiert werden soll.

## Automatisches Prüfen auf Updates

McAfee SecurityCenter ist so konfiguriert, dass es bei bestehender Internetverbindung alle vier Stunden automatisch nach Updates für Ihre McAfee-Dienste sucht und Sie dann durch entsprechende Meldungen und akustische Signale benachrichtigt. Standardmäßig werden verfügbare Updates automatisch von SecurityCenter heruntergeladen und installiert.

**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 alle Programme, bevor Sie den Neustart durchführen.

## Manuelles Prüfen auf Updates

Zusätzlich zur automatischen Suche nach Updates, die bei einer bestehenden Internetverbindung durchgeführt wird, können Sie auch jederzeit manuell nach Updates suchen.

So prüfen Sie manuell, ob Updates für Wireless Home Network Security verfügbar sind:

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 **Aktualisierungen**. Das Dialogfeld **SecurityCenter-Updates** wird angezeigt.

3 Klicken Sie auf **Jetzt prüfen**.

Wenn ein Update vorhanden ist, wird das Dialogfeld **McAfee SecurityCenter** angezeigt. Klicken Sie zum Fortfahren auf **Aktualisieren**.

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

4 Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden. Das Update wird automatisch vom **Update-Assistenten** installiert.

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 alle Programme, bevor Sie den Neustart durchführen.

# Grundlegendes zu Warnungen 7

Warnungen werden bei bestimmten Ereignissen angezeigt. Sie informieren Sie über Änderungen im Netzwerk.

## Computer gesichert

Ein Benutzer, der Zugriff auf das geschützte Netzwerk besitzt, hat einem anderen Benutzer Zugriff gewährt. Beispiel: Der Benutzer "Lance" hat dem Benutzer "Mercks" Zugriff gewährt. Beide können nun das drahtlose Netzwerk "CoppiWAP" nutzen.

## Computer getrennt

Ein Benutzer hat die Netzwerkverbindung getrennt. Weitere Informationen finden Sie unter *Trennen einer Netzwerkverbindung* auf Seite 20.

## Computer verbunden

Ein Benutzer hat eine Verbindung zum Netzwerk hergestellt. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 20.

## Drahtloser Router/Zugriffspunkt geschützt

Ein drahtloser Router oder Zugriffspunkt wurde in Ihrem Netzwerk geschützt. Weitere Informationen finden Sie unter *Schützen drahtloser Netzwerke* auf Seite 28.

## Fehler bei der Schlüsselrotation

Fehlerursache:

- Die Anmeldeinformationen für Ihren Router oder Zugriffspunkt wurden geändert. Wenn Sie wissen, wie die Anmeldeinformationen lauten, finden Sie weitere Informationen unter *Reparieren von Sicherheitseinstellungen* auf Seite 26.
- Die Firmware-Version Ihres Routers oder Zugriffspunktes wurde geändert, und die neue Version wird nicht unterstützt. Weitere Informationen finden Sie unter *Keine Verbindung möglich* auf Seite 41.

- Ihr Router oder Zugriffspunkt ist nicht verfügbar. Stellen Sie sicher, dass der Router oder Zugriffspunkt eingeschaltet und an das Netzwerk angeschlossen ist.
- Fehler durch doppelte Administratoren. Weitere Informationen finden Sie unter *Fehler durch doppelte Administratoren* auf Seite 37.

Bei Problemen mit dem Herstellen einer Verbindung zum Netzwerk finden Sie weitere Informationen unter *Reparieren von Sicherheitseinstellungen* auf Seite 26.

## Häufigkeit der Sicherheitsschlüsselrotation geändert

Der Häufigkeit der Sicherheitsschlüsselrotation für das Netzwerk wurde geändert. McAfee Wireless Home Network Security ändert automatisch den Verschlüsselungsschlüssel für das Netzwerk. Das erschwert Hackern, Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk herzustellen.

## Kennwort geändert

Ein Benutzer hat den Benutzernamen oder das Kennwort für einen Router oder Zugriffspunkt im Netzwerk geändert. Weitere Informationen finden Sie unter *Konfigurieren von Sicherheitseinstellungen* auf Seite 24.

## Netzwerkeinstellungen geändert

Ein Benutzer ist im Begriff, die Sicherheitseinstellungen des Netzwerks zu ändern. Unter Umständen wird während dieses Vorgangs die Verbindung kurz unterbrochen. Mindestens eine der folgenden Einstellungen wird geändert:

- Name des Netzwerks
- Sicherheitsmodus
- Häufigkeit der Schlüsselrotation
- Status der automatischen Schlüsselrotation

## Netzwerkkonfiguration geändert

Ein Benutzer hat den Sicherheitsmodus für das Netzwerk geändert. Weitere Informationen finden Sie unter *Konfigurieren von Sicherheitseinstellungen* auf Seite 24.

## Netzwerk repariert

Ein Benutzer hat aufgrund von Problemen beim Herstellen einer Verbindung versucht, das Netzwerk zu reparieren.

## Netzwerk umbenannt

Ein Benutzer hat das Netzwerk umbenannt. Sie müssen die Verbindung mit dem Netzwerk neu herstellen. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 20.

## Schlüsselrotation ausgesetzt

Ein Benutzer hat die Schlüsselrotation ausgesetzt. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vor Hackern vollständig geschützt ist.

## Schlüsselrotation fortgesetzt

Ein Benutzer hat die Schlüsselrotation fortgesetzt. Durch die Schlüsselrotation wird verhindert, dass Hacker auf das Netzwerk zugreifen.

## Schutz für drahtlosen Router/Zugriffspunkt aufgehoben

Ein drahtloser Router oder Zugriffspunkt wurde aus dem Netzwerk entfernt. Weitere Informationen finden Sie unter *Aufheben des Schutzes drahtloser Netzwerke* auf Seite 28.

## Sicherheitsschlüssel rotiert

Der Sicherheitsschlüssel für das Netzwerk wurde geändert. McAfee Wireless Home Network Security ändert automatisch den Verschlüsselungsschlüssel für das Netzwerk. Das erschwert Hackern, Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk herzustellen.

## Zugriff widerrufen

Ein Benutzer hat den Netzwerkschlüssel aktualisiert. Weitere Informationen finden Sie unter *Widerrufen des Zugriffs auf das Netzwerk* auf Seite 25.

# Problembehandlung 8

In diesem Abschnitt werden Verfahren zur Problembehandlung für McAfee Wireless Home Network Security und Hardware von Drittanbietern beschrieben.

## Installation

In diesem Abschnitt wird erklärt, wie Installationsprobleme behoben werden.

### Auf welchen Computern muss diese Software installiert werden?

Installieren Sie McAfee Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk (im Gegensatz zu anderen McAfee-Anwendungen können Sie diese Software auf mehreren Computern installieren).

Auf Computern ohne drahtlosen Adapter können Sie die Software installieren (müssen dies aber nicht tun). Auf diesen Computern ist die Software nicht aktiv, weil sie keinen entsprechenden Schutz benötigen. Den Router oder Zugriffspunkt müssen Sie von einem der drahtlosen Computer aus schützen (siehe *Schützen drahtloser Netzwerke* auf Seite 28), um das Netzwerk zu sichern.

### Drahtloser Adapter wird nicht erkannt

Wenn der drahtlose Adapter nach dem Installieren und Aktivieren nicht erkannt wird, müssen Sie den Computer neu starten. Wird der Adapter anschließend immer noch nicht erkannt, sollten Sie folgendermaßen vorgehen:

1. Öffnen Sie das Dialogfeld **Eigenschaften von Drahtlose Netzwerkverbindung**.
2. Deaktivieren Sie das Kontrollkästchen **MWL-Filter**, und aktivieren Sie es anschließend wieder.
3. Klicken Sie auf **OK**.

Wenn das nicht funktioniert, wird der drahtlose Adapter möglicherweise nicht unterstützt. Aktualisieren Sie den Adapter, oder erwerben Sie einen neuen. Eine Liste der unterstützten Adapter finden Sie unter http://www.mcafee.com/de/router. Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 41.

## Mehrere drahtlose Adapter

Wenn in einer Fehlermeldung steht, dass mehrere drahtlose Adapter installiert sind, müssen Sie alle bis auf einen deaktivieren oder vom Netzwerk trennen. Wireless Home Network Security funktioniert nur mit einem drahtlosen Adapter.

## Kein Download auf drahtlose Computer möglich, da das Netzwerk bereits sicher ist

Installieren Sie, falls Sie über eine CD verfügen, McAfee Wireless Home Network Security von der CD auf allen drahtlosen Computern.

Wenn Sie die Software auf einem drahtlosen Computer installiert und das Netzwerk geschützt haben, bevor Sie die Software auf allen anderen Computern installiert haben, verfügen Sie über folgende Optionen.

- Heben Sie den Schutz des Netzwerks auf (siehe *Aufheben des Schutzes drahtloser Netzwerke* auf Seite 28). Laden Sie dann die Software herunter, und installieren Sie sie auf allen drahtlosen Computern. Schützen Sie Ihr Netzwerk dann wieder (siehe *Schützen drahtloser Netzwerke* auf Seite 28).
- Zeigen Sie den Netzwerkschlüssel an (siehe *Anzeigen Ihres geschützten drahtlosen Netzwerks* auf Seite 18). Geben Sie dann den Schlüssel auf Ihrem drahtlosen Computer ein, um eine Verbindung zum Netzwerk herzustellen. Laden Sie die Software herunter, installieren Sie sie, und melden Sie sich vom drahtlosen Computer aus am Netzwerk an (siehe *Schützen anderer Computer* auf Seite 27).
- Laden Sie die ausführbare Datei auf den Computer herunter, der bereits mit dem Netzwerk verbunden ist, und speichern Sie sie auf einem USB-Speicherstick, oder brennen Sie sie auf eine CD, damit Sie sie auf den anderen Computern installieren können.

# Schützen oder Konfigurieren des Netzwerks

In diesem Abschnitt wird die Behandlung von Problemen erläutert, die beim Schützen oder Konfigurieren eines Netzwerkes auftreten.

## Nicht unterstützter Router oder Zugriffspunkt

Wenn es in einer Fehlermeldung heißt, dass der drahtlose Router oder Zugriffspunkt unter Umständen nicht unterstützt wird, konnte das Gerät von McAfee Wireless Home Network Security nicht konfiguriert werden, weil es nicht erkannt oder gefunden wurde.

Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Home Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Router und Zugriffspunkte aus). Wenn der Router oder Zugriffspunkt in der Liste unter http://www.mcafee.com/de/router aufgeführt wird und dieser Fehler dennoch auftritt, liegen Kommunikationsprobleme zwischen Ihrem Computer und dem Router oder Zugriffspunkt vor. Lesen Sie *Keine Verbindung möglich* auf Seite 41, bevor Sie das Netzwerk wieder schützen.

## Aktualisieren der Firmware des Routers oder Zugriffspunktes

Wenn es in einer Fehlermeldung heißt, dass die Firmware-Version des drahtlosen Routers oder Zugriffspunktes nicht unterstützt wird, wird zwar das Gerät unterstützt, nicht aber dessen Firmware-Version. Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Home Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Firmware-Versionen aus).

Wenn Sie über die neueste Version von Wireless Home Network Security verfügen, sollten Sie die Website des Herstellers des Routers oder Zugriffspunktes aufrufen bzw. sich an dessen Support wenden und eine unter http://www.mcafee.com/de/router aufgelistete Firmware-Version installieren.

## Fehler durch doppelte Administratoren

Nach dem Konfigurieren des Routers oder Zugriffspunktes müssen Sie sich von der Administrationsoberfläche abmelden. Geschieht das nicht, verhält der Router oder Zugriffspunkt sich in einigen Fällen so, als würde er weiterhin von einem anderen Computer konfiguriert werden. Es wird dann eine Fehlermeldung angezeigt.

Wenn Sie sich nicht abmelden können, ziehen Sie das Stromkabel Ihres Routers oder Zugriffspunktes heraus, und stecken Sie es dann wieder ein.

## Netzwerk als ungesichert angezeigt

Wenn das Netzwerk als ungesichert angezeigt wird, ist es nicht geschützt. Sie müssen das Netzwerk schützen (siehe *Schützen drahtloser Netzwerke* auf Seite 28), um es zu sichern. Beachten Sie, dass McAfee Wireless Home Network Security nur mit kompatiblen Routern und Zugriffspunkten funktioniert (siehe http://www.mcafee.com/de/router).

## Keine Reparatur möglich

Gehen Sie folgendermaßen vor, wenn bei der Reparatur Fehler auftreten. Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang.
- Ziehen Sie das Stromkabel des Routers oder Zugriffspunktes, und stecken Sie es dann wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und reparieren Sie ihn.
- Verlassen Sie mithilfe der erweiterten Optionen das Netzwerk auf allen Computern, setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie ihn dann.

# Verbinden von Computern mit Ihrem Netzwerk

In diesem Abschnitt wird die Behandlung von Problemen erläutert, die beim Verbinden von Computern zum Netzwerk auftreten.

## Warten auf Autorisierung

Wenn Sie sich an einem geschützten Netzwerk anzumelden versuchen und der Computer vergeblich auf Autorisierung wartet, sollten Sie Folgendes überprüfen.

- Ein drahtloser Computer mit bestehendem Zugriff auf das Netzwerk ist eingeschaltet und mit dem Netzwerk verbunden.
- An diesem Computer ist jemand anwesend, der Zugriff erteilen kann, wenn Ihr Computer angezeigt wird.
- Die Computer befinden sich innerhalb der Reichweite der Funkwellen.

Wenn **Zugriff gewähren** auf dem Computer mit bestehendem Zugriff auf das Netzwerk nicht angezeigt wird, müssen Sie versuchen, den Zugriff von einem anderen Computer aus zu gewähren.

Falls keine anderen Computer verfügbar sind, müssen Sie den Schutz des Netzwerks vom Computer mit vorhandenem Zugriff aus aufheben und das Netzwerk vom Computer ohne Zugriff aus schützen. Melden Sie sich anschließend von dem Computer aus am Netzwerk an, der das Netzwerk ursprünglich schützte.

## Gewähren von Zugriff für einen unbekannten Computer

Wenn Sie von einem unbekannten Computer eine Anforderung zum Gewähren von Zugriff erhalten, sollten Sie überprüfen, woher sie stammt. Möglicherweise versucht ein Unbefugter, auf Ihr Netzwerk zuzugreifen.

# Verbinden mit einem Netzwerk oder dem Internet

In diesem Abschnitt wird die Behandlung von Problemen beim Herstellen einer Verbindung zu einem Netzwerk oder dem Internet erläutert.

## Schlechte Verbindung zum Internet

Wenn Sie keine Verbindung herstellen können, schließen Sie den Computer mit einem Kabel an das Netzwerk an, und stellen Sie dann eine Verbindung zum Internet her. Ist immer noch keine Verbindung möglich, sollten Sie die folgenden Punkte überprüfen:

- Ihr Modem ist eingeschaltet.
- Ihre PPPoE-Einstellungen (siehe *Glossar* auf Seite 47) sind korrekt.
- Ihre DSL- oder Kabelleitung ist aktiv.

Verbindungsprobleme, etwa mit der Geschwindigkeit und der Signalstärke, können auch durch Funkstörungen verursacht werden. Wechseln Sie den Kanal Ihres schnurlosen Telefons, beseitigen Sie mögliche Störquellen, oder stellen Sie Ihren drahtlosen Router, Zugriffspunkt oder Computer an einem anderen Ort auf.

## Kurze Unterbrechung der Verbindung

Wenn Ihre Verbindung kurz unterbrochen wird (z. B. während eines Online-Spiels), kann das daran liegen, dass die Schlüsselrotation kurze Verzögerungen im Netzwerk verursacht: Setzen Sie die Schlüsselrotation vorübergehend aus. Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

## Verbindungsverlust bei Geräten (nicht beim Computer)

Wenn beim Einsatz von McAfee Wireless Home Network Security einige Geräte die Verbindung verlieren, setzen Sie die Schlüsselrotation aus.

## Aufforderung zur Eingabe des WEP- oder WPA-Schlüssels

Wenn Sie zum Herstellen einer Verbindung zum Netzwerk einen WEP- oder WPA-Schlüssel eingeben müssen, haben Sie wahrscheinlich die Software nicht auf Ihrem Computer installiert. Für eine ordnungsgemäße Funktionsweise muss Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk installiert sein. Siehe *Schützen oder Konfigurieren des Netzwerks* auf Seite 37.

## Keine Verbindung möglich

Wenn Sie keine Verbindung herstellen können, gehen Sie folgendermaßen vor: Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Vergewissern Sie sich, falls Sie keine Verbindung zu einem geschützten Netzwerk herstellen, dass Sie über den richtigen Schlüssel verfügen. Geben Sie ihn erneut ein.
- Ziehen Sie den Stecker des drahtlosen Adapters, und stecken Sie ihn wieder ein. Oder deaktivieren Sie den Adapter, und aktivieren Sie ihn dann wieder.
- Schalten Sie den Router oder Zugriffspunkt aus und wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Vergewissern Sie sich, dass der drahtlose Router oder Zugriffspunkt verbunden ist, und reparieren Sie die Sicherheitseinstellungen (siehe *Reparieren von Sicherheitseinstellungen* auf Seite 26).

  Wenn bei der Reparatur Fehler auftreten, finden Sie weitere Informationen unter *Keine Reparatur möglich* auf Seite 38.
- Starten Sie den Computer neu.
- Aktualisieren Sie den drahtlosen Adapter, oder erwerben Sie einen neuen. Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 41. Beispiel: Im Netzwerk kommt WPA-PSK TKIP-Sicherheit zum Einsatz, und der drahtlose Adapter unterstützt den Sicherheitsmodus des Netzwerks nicht (das Netzwerk zeigt WEP an, obwohl es auf WPA eingestellt ist).
- Wenn Sie nach dem Aktualisieren des drahtlosen Routers oder Zugriffspunktes keine Verbindung herstellen können, haben Sie möglicherweise auf eine nicht unterstützte Version aktualisiert. Vergewissern Sie sich, dass der Router oder Zugriffspunkt unterstützt wird. Wenn Sie dies nicht der Fall ist, sollten Sie eine unterstützte Version installieren oder warten, bis ein Update von Wireless Home Network Security verfügbar ist.

## Aktualisieren des drahtlosen Adapters

Gehen Sie zum Aktualisieren Ihres Adapters folgendermaßen vor:

1. Klicken Sie auf dem Desktop auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie dann **Systemsteuerung** aus.
2. Doppelklicken Sie auf das Symbol **System**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
3. Wählen Sie die Registerkarte **Hardware** aus, und klicken Sie dann auf **Geräte-Manager**.
4. Doppelklicken Sie in der Liste **Geräte-Manager** auf den Adapter.

5 Wählen Sie die Registerkarte **Treiber** aus, und notieren Sie sich den Treiber, der bei Ihnen installiert ist.

6 Gehen Sie zur Website des Adapterherstellers, und überprüfen Sie, ob ein Update verfügbar ist. Treiber sind meist im Support- oder Download-Bereich zu finden.

7 Wenn ein Treiber-Update verfügbar ist, folgen Sie den Anweisungen auf der Website, um das Update herunterzuladen.

8 Gehen Sie zurück zur Registerkarte **Treiber**, und klicken Sie auf **Aktualisieren**. Ein Windows-Assistent wird angezeigt.

9 Folgen Sie den Anweisungen auf dem Bildschirm.

## Schwaches Signal

Wenn Ihre Verbindung unterbrochen wird oder sehr langsam ist, ist möglicherweise das Signal zu schwach. Gehen Sie wie folgt vor, um das Signal zu verbessern.

- Stellen Sie sicher, dass die drahtlosen Geräte nicht durch Metallobjekte wie Öfen, Rohre oder große Haushaltsgeräte blockiert werden. Funksignale werden stark abgeschwächt, wenn sie durch solche Objekte hindurch verlaufen.
- Wenn das Signal durch Wände gelangen muss, sollten Sie sicherstellen, dass dies nicht im spitzen Winkel geschieht. Je länger der Weg innerhalb der Wand ist, desto schwächer wird das Signal.
- Verfügt der drahtlose Router oder Zugriffspunkt über zwei Antennen, sollten Sie die beiden Antennen nach Möglichkeit rechtwinklig zueinander ausrichten (eine vertikal und eine horizontal im 90-Grad-Winkel).
- Einige Hersteller verwenden Hochleistungsantennen. Richtantennen haben eine größere Reichweite, während omnidirektionale Antennen (Rundstrahler) die größte Flexibilität bieten. Richten Sie sich beim Installieren der Antenne nach den entsprechenden Anweisungen des Herstellers.

Führen diese Schritte nicht zum Erfolg, sollten Sie dem Netzwerk einen Zugriffspunkt hinzufügen, der sich näher an dem Computer befindet, zu dem Sie eine Verbindung herstellen möchten. Wenn Sie den zweiten Zugriffspunkt mit demselben Netzwerknamen (SSID) und einem anderen Kanal konfigurieren, sucht der Adapter automatisch das stärkste Signal und stellt die Verbindung über den entsprechenden Zugriffspunkt her.

## Windows kann die drahtlose Verbindung nicht konfigurieren

Wenn Sie eine Meldung erhalten, dass Windows die drahtlose Verbindung nicht konfigurieren kann, können Sie sie ignorieren. Verwenden Sie Wireless Home Network Security, um Verbindungen zu drahtlosen Netzwerken herzustellen und die Netzwerke zu konfigurieren. Stellen Sie sicher, dass im Windows-Dialogfeld **Eigenschaften von Drahtlose Netzwerkverbindung** auf der Registerkarte **Drahtlosnetzwerke** das Kontrollkästchen **Windows zum Konfigurieren der Einstellungen verwenden** deaktiviert ist.

## Windows zeigt keine Verbindung an

Wenn Sie verbunden sind, das Netzwerksymbol von Windows jedoch ein X anzeigt (d. h. keine Verbindung), so können Sie das ignorieren. Ihre Verbindung ist einwandfrei.

# Andere Probleme

In diesem Abschnitt wird die Behandlung sonstiger Probleme erläutert.

## Bei Verwendung anderer Programme lautet der Netzwerkname anders

Dass der Name des Netzwerks in anderen Programmen anders angezeigt wird (etwa mit _SafeAaf als Bestandteil des Namens), ist völlig normal. Wireless Home Network Security kennzeichnet Netzwerke mit einem Code, wenn sie geschützt sind.

## Probleme beim Konfigurieren drahtloser Router oder Zugriffspunkte

Wenn beim Konfigurieren des Routers oder Zugriffspunktes oder beim Hinzufügen mehrerer Router im Netzwerk ein Fehler auftritt, müssen Sie sich vergewissern, dass alle Router und Zugriffspunkte über eine eigene IP-Adresse verfügen.

Wenn der Name des drahtlosen Routers oder Zugriffspunktes im Dialogfeld **Drahtlosen Router/Zugriffspunkt schützen** aufgeführt wird, Sie jedoch bei dessen Konfiguration eine Fehlermeldung erhalten, müssen Sie überprüfen, ob der Router oder Zugriffspunkt unterstützt wird. Eine Liste der unterstützten Router und Zugriffspunkte finden Sie unter http://www.mcafee.com/de/router.

Wenn der Router oder Zugriffspunkt konfiguriert ist, sich aber scheinbar nicht im richtigen Netzwerk befindet (es werden zum Beispiel keine anderen Computer im LAN angezeigt), müssen Sie sicherstellen, dass Sie den richtigen Router oder Zugriffspunkt konfiguriert haben, und nicht den Ihres Nachbarn. Ziehen Sie das Stromkabel des Routers oder Zugriffspunktes, und vergewissern Sie sich, dass die Verbindung unterbrochen wird. Wenn Sie den falschen Router oder Zugriffspunkt konfiguriert haben, heben Sie dessen Schutz wieder auf, und schützen Sie dann den richtigen Router oder Zugriffspunkt.

Wenn Sie den Router oder Zugriffspunkt nicht ordnungsgemäß konfigurieren oder hinzufügen können, er aber unterstützt wird, liegt das unter Umständen daran, dass Sie Änderungen durchgeführt haben, die nun eine ordnungsgemäße Konfiguration verhindern.

- Folgen Sie den Anweisungen des Herstellers zum Konfigurieren Ihres drahtlosen Routers bzw. Zugriffspunktes für DHCP oder zum Festlegen der richtigen IP-Adresse. In einigen Fällen ist ein Konfigurations-Tool im Lieferumfang des Produkts enthalten.
- Setzen Sie den Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und versuchen Sie erneut, das Netzwerk zu reparieren. Möglicherweise haben Sie den Administrationsport am Router oder Zugriffspunkt geändert oder die drahtlose Administration deaktiviert. Stellen Sie sicher, dass Sie die Standardkonfiguration verwenden und dass die drahtlose Konfiguration aktiviert ist. Eine weitere Möglichkeit besteht darin, dass die http-Administration deaktiviert ist. Stellen Sie in diesem Fall sicher, dass sie aktiviert ist.
- Wenn der drahtlose Router oder Zugriffspunkt nicht in der Liste drahtloser Router oder Zugriffspunkte aufgeführt wird, die geschützt und zu denen Verbindungen hergestellt werden sollen, müssen Sie die SSID-Übertragung aktivieren und sicherstellen, dass der Router oder Zugriffspunkt aktiviert ist.
- Falls Sie getrennt werden oder keine Verbindung herstellen können, ist möglicherweise die MAC-Filterung aktiviert. Deaktivieren Sie sie.
- Wenn zwischen zwei Computern mit drahtloser Verbindung zum Netzwerk keine Netzwerkvorgänge möglich sind (zum Beispiel die Freigabe von Dateien oder das Drucken auf freigegebenen Druckern), müssen Sie überprüfen, ob die Isolierung von Zugriffspunkten nicht aktiviert ist. Sie verhindert, dass drahtlose Computer über das Netzwerk miteinander in Verbindung treten können.

## Ersetzen von Computern

Wenn der Computer, der das Netzwerk geschützt hat, ersetzt wurde ist und es keine anderen Computer mit Zugriff gibt (d. h. Sie können nicht auf das Netzwerk zugreifen), setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie das Netzwerk erneut.

## Software funktioniert nach dem Aktualisieren des Betriebssystems nicht

Wenn Wireless Home Network Security nach dem Aktualisieren von Betriebssystemen nicht mehr funktioniert, müssen Sie es deinstallieren und dann neu installieren.

# Glossar 9

**802.11**

Eine Reihe von IEEE-Standards für Funk-LANs. 802.11 legt eine Schnittstelle für den Funkverkehr zwischen einem drahtlosen Client und einer Basisstation oder zwischen zwei drahtlosen Clients fest. Zu den verschiedenen Spezifikationen von 802.11 gehören die Standards 802.11a (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band), 802.11b (für Netzwerke mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band), 802.11g (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 2,4 GHz-Band) sowie und 802.11i (eine Reihe von Sicherheitsstandards für alle drahtlosen Ethernet-Netzwerke).

**802.11a**

Eine Erweiterung von 802.11 für Funk-LANs zum Senden von Daten mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

**802.11b**

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 11 Mbit/s im 2,4 GHz-Band bietet. 802.11b gilt derzeit als Standard für drahtlose Netzwerkverbindungen.

**802.11g**

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 54 Mbit/s im 2,4 GHz-Band bietet.

**802.1x**

Wird von Wireless Home Network Security nicht unterstützt. Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken, wird aber vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet. Dieser Standard bietet eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Außerdem bietet 802.1x dynamische, benutzer- und sitzungsspezifische WEP-Schlüssel, wodurch der bei statischen WEP-Schlüsseln übliche Verwaltungsaufwand und die Sicherheitsrisiken beseitigt werden.

## A

### Authentifizierung

Der Vorgang des Identifizierens eines bestimmten Benutzers, meist anhand von Benutzername und Kennwort. Mit der Authentifizierung wird sichergestellt, dass es sich bei einem Benutzer auch wirklich um denjenigen handelt, der er oder sie zu sein vorgibt. Über die Zugriffsrechte dieses Benutzers sagt die Authentifizierung jedoch nichts aus.

## B

### Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums übertragen werden kann. Bei digitalen Geräten wird die Bandbreite meist in Bit pro Sekunde (Bit/s) oder Byte pro Sekunde angegeben. Bei analogen Geräten wird die Bandbreite als Taktzahl pro Sekunde bzw. Hertz (Hz) angegeben.

### Brute-Force-Angriff

Eine Vorgehensweise nach dem Fehler-Treffer-Prinzip, die auch unter dem Begriff "Brute-Force-Cracking" bekannt ist. Dabei versuchen entsprechende Programme, verschlüsselte Daten (z. B. Kennwörter) mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien zu entschlüsseln. Brute-Force-Anwendungen probieren nacheinander alle möglichen Kombinationen von zulässigen Zeichen aus – wie bei einem Safe, bei dem alle Zahlenkombinationen ausprobiert werden, um ihn zu öffnen, was genauso eine strafbare Handlung ist. Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großen Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt.

## C

### Chiffrierter Text

Das sind Daten, die verschlüsselt wurden. Chiffrierter Text ist nicht lesbar, solange er nicht mithilfe eines Schlüssels wieder in Klartext umgewandelt (entschlüsselt) wurde.

### Client

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

**D**

**Denial of Service, DoS**

Ein DoS-Angriff (Denial-of-Service, Dienstverweigerung) ist ein Störfall im Internet, durch den Benutzer oder Unternehmen nicht mehr auf bestimmte Ressourcen oder Dienste zugreifen können. Dabei handelt es sich meist um die Nichtverfügbarkeit eines einzelnen Netzwerkdienstes (z. B. E-Mail) oder den vorübergehenden Verlust aller Netzwerkverbindungen und -dienste. Im schlimmsten Fall kann beispielsweise eine Website, auf die täglich Millionen Benutzer zugreifen, zeitweise gezwungen sein, ihren Betrieb einstellen. Bei einem DoS-Angriff können auch Programme und Dateien in einem Computersystem zerstört werden. Auch wenn DoS-Angriffe meist absichtlich und böswillig sind, können sie manchmal auch unbeabsichtigt passieren. Ein DoS-Angriff stellt eine Art von Sicherheitsverletzung dar, die meist nicht zu einem Diebstahl von Informationen oder anderen Sicherheitsverlusten führt. Trotzdem können solche Angriffe für die Zielperson bzw. das geschädigte Unternehmen mit einem beträchtlichen Zeitaufwand und erheblichen Kosten verbunden sein.

**Drahtloser Adapter**

Enthält die Schaltkreise, mit denen ein Computer oder ein anderes Gerät mit einem (an einem drahtlosen Netzwerk angeschlossenen) drahtlosen Router kommunizieren kann. Drahtlose Adapter können entweder im Hauptschaltkreis eines Hardwaregeräts integriert sein oder sich auf einer separaten Zusatzkarte befinden, die in den entsprechenden Anschluss eines Gerätes eingesteckt wird.

**E**

**ESS (Extended Service Set)**

Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

**F**

**Firewall**

Ein System, das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. Firewalls können in Form von Hardware, Software oder einer Kombination von beiden implementiert werden. Sie werden häufig verwendet, um zu verhindern, dass nicht autorisierte Internetbenutzer auf private Netzwerke (insbesondere Intranets) zugreifen, die mit dem Internet verbunden sind. Alle Nachrichten, die in das Intranet gelangen oder dieses verlassen, verlaufen durch eine Firewall. Von dieser werden alle Nachrichten überprüft und jene blockiert, die nicht die angegebenen Sicherheitskriterien erfüllen. Firewalls werden als erste Verteidigungslinie beim Schutz privater Informationen betrachtet. Zur höheren Sicherheit können die Daten verschlüsselt werden.

## G

### Gemeinsamer geheimer Schlüssel

Siehe auch RADIUS. Schützt den sensiblen Teil von RADIUS-Nachrichten. Der gemeinsame geheime Schlüssel ist ein Kennwort, das von dem Authentifikator und dem Authentifizierungsserver auf eine bestimmte sichere Weise gemeinsam verwendet wird.

## H

### Hotspot

Ein bestimmter örtlicher Standort, an dem ein Zugriffspunkt mobilen Besuchern den Zugriff auf öffentliche Breitband-Netzwerkdienste über ein drahtloses Netzwerk ermöglicht. Hotspots befinden sich oft in der Nähe von stark frequentierten Einrichtungen, z. B. Flughäfen, Bahnhöfen, Bibliotheken, Jachthäfen, Messe-Centern und Hotels. Sie haben meist eine geringe Reichweite.

## I

### Integriertes Gateway

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

### IP-Adresse

Ein Bezeichner für einen Computer oder ein Gerät in einem TCP/IP-Netzwerk. Netzwerke, die das TCP/IP-Protokoll verwenden, leiten Nachrichten anhand der IP-Adresse des Ziels weiter. Das Format einer IP-Adresse besteht aus einer numerischen 32 Bit-Adresse, die in Form von vier, durch Punkte getrennte Zahlen geschrieben wird. Jede Zahl kann zwischen 0 und 255 liegen. Eine IP-Adresse kann zum Beispiel so aussehen: 192.168.1.100.

### IP-Spoofing

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

## J

## K

### Klartext

Nachrichten, die nicht verschlüsselt sind.

**L**

**LAN (Local Area Network)**

Ein Computernetzwerk, dass sich über ein relativ kleines Gebiet erstreckt. Die meisten LANs sind auf ein einzelnes Gebäude oder eine Gruppe von Gebäuden eingeschränkt. Per Telefonverbindungen oder Funkwellen kann ein LAN aber auch über eine beliebige Entfernung mit anderen LANs verbunden werden. Ein System aus LANs, die auf diese Weise miteinander verbunden sind, wird WAN (Wide-Area Network) genannt.

In den meisten LANs werden Workstations und PCs über normale Hubs oder Switches miteinander verbunden. Jeder Knoten (ein einzelner Computer) in einem LAN hat seine eigene CPU, mit der er Programme ausführt, kann aber auch auf Daten und Geräte (z. B. Drucker) im LAN zugreifen. Auf diese Weise können teure Geräte (z. B. Laserdrucker) sowie Daten von vielen Benutzern gemeinsam genutzt werden. Über ein LAN können Benutzer auch miteinander kommunizieren, z. B. E-Mails senden oder an Chat-Sitzungen teilnehmen.

**M**

**MAC (Media Access Control oder Message Authenticator Code)**

Für das erstgenannte von beiden siehe "MAC-Adresse". Die zweite ausgeschriebene Abkürzung (Message Authenticator Code) bezeichnet einen Code, der zum Identifizieren einer bestimmten Nachricht (z. B. einer RADIUS-Nachricht) verwendet wird. Der Code ist gewöhnlich ein kryptografisch starker Hash des Nachrichteninhalts, der einen eindeutigen Wert als Replay-Schutz enthält.

**MAC-Adresse (Media Access Control Address)**

Eine Adresse auf unterer Ebene, die einem physikalischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

**"Man-in-the-Middle"-Angriff**

Der Angreifer fängt Nachrichten bei einem öffentlichen Schlüsselaustausch ab und überträgt sie neu, wobei er den angeforderten Schlüssel durch deren eigene öffentliche Schlüssel ersetzt, so dass die beiden ursprünglichen Parteien weiterhin den Eindruck haben, direkt miteinander zu kommunizieren. Dabei verwendet der Angreifer ein Programm, dass sich dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der Angriff kann dazu dienen, einfach nur Zugriff auf die Nachrichten zu erhalten. Der Angreifer hat aber auch die Möglichkeit, die Nachrichten zu ändern, bevor er sie wieder weiterleitet. Der Begriff leitet sich von einem Ballspiel ab, bei dem mehrere Personen versuchen, sich gegenseitig den Ball zuzuwerfen, während ein einzelner Mitspieler in der Mitte versucht, den Ball abzufangen.

**N**

**Netzwerk**

Eine Gruppe von Zugriffspunkten und deren zugehörige Benutzer, gleichbedeutend einem ESS. Die Informationen über dieses Netzwerk werden in McAfee Wireless Home Network Security gepflegt. Siehe "ESS".

**NIC (Network Interface Card, Netzwerkkarte)**

Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

**Nicht autorisierter Zugriffspunkt**

Ein Zugriffspunkt, den ein Unternehmen für den Betrieb nicht autorisiert. Das Problem dabei ist, dass nicht autorisierte Zugriffspunkte oft nicht den Sicherheitsrichtlinien für WLANs (Wireless LAN, Funk-LAN) entsprechen. Ein nicht autorisierter Zugriffspunkt bietet eine offene, unsichere Schnittstelle in das Unternehmensnetzwerk von außerhalb der physikalisch kontrollierten Einrichtung.

In einem ordnungsgemäß gesicherten WLAN richten nicht autorisierte Zugriffspunkte mehr Schäden an als nicht autorisierte Benutzer. Wenn wirksame Authentifizierungsmechanismen vorhanden sind, müssen nicht autorisierte Benutzer beim Versuch, auf ein WLAN zuzugreifen, nicht unbedingt auch an wertvolle Ressourcen des Unternehmens gelangen. Zu größeren Problemen kommt es jedoch, wenn sich ein Mitarbeiter oder Hacker über den nicht autorisierten Zugriffspunkt anmeldet. Ein nicht autorisierter Zugriffspunkt erlaubt praktisch jedem, der über ein 802.11-kompatibles Gerät verfügt, den Zutritt in das Unternehmensnetzwerk. Dadurch gelangt man schnell sehr nah an geschäftskritische Ressourcen.

**O**

**P**

**PCI-Drahtlosadapter-Karte**

Verbindet einen Desktopcomputer mit einem Netzwerk. Die Karte wird in einen PCI-Erweiterungssteckplatz im Computer gesteckt.

**PPPoE**

Abkürzung für "Point-to-Point Protocol Over Ethernet". PPPoE wird von vielen DSL-Providern verwendet und unterstützt die in PPP häufig verwendeten Protokollebenen und Authentifizierung. Mit PPPoE kann eine Punkt-zu-Punkt-Verbindung in der normalen Multipoint-Ethernet-Architektur hergestellt werden.

**Protokoll**

Ein vorab vereinbartes Format zum Übertragen von Daten zwischen zwei Geräten. Aus Sicht des Benutzers besteht der einzige interessante Aspekt bei Protokollen darin, dass der Computer oder das Gerät die entsprechenden Protokolle unterstützen muss, um mit einem jeweils anderen Computer kommunizieren zu können. Das Protokoll kann entweder in der Hardware oder in der Software implementiert sein.

**Q**

**R**

**RADIUS (Remote Access Dial-In User Service)**

Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

**Roaming**

Die Fähigkeit, aus dem Empfangbereich eines Zugriffspunkts in den eines anderen zu wechseln, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

**Router**

Ein Netzwerkgerät, das Pakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden anhand interner Routingtabellen, wie das Paket weitergeleitet werden soll. Die Wahl der Schnittstelle, an die ausgehende Pakete gesendet werden, kann davon abhängen, in welcher Konstellation Quell- und Zieladresse miteinander stehen, oder sich nach den aktuellen Gegebenheiten im Netzwerkverkehr (z. B. Auslastung, Leitungskosten oder ausgefallene Leitungen) richten. Für "Router" wird manchmal auch der Begriff "Zugriffspunkt" verwendet.

**S**

**Schlüssel**

Eine Folge von Buchstaben und/oder Zahlen, mit der zwei Geräte ihre Kommunikation miteinander authentifizieren können. Dabei müssen beide Geräte über den Schlüssel verfügen. Siehe auch "WEP" und "WPA-PSK".

**SSID (Service Set Identifier)**

Der Netzwerkname für die Geräte in einem Funk-LAN-Subsystem. Das ist eine Zeichenfolge aus 32 Zeichen, die im Klartext steht und zum Kopf jedes WLAN-Pakets hinzugefügt wird. Die SSID unterscheidet WLANs voneinander. Daher müssen alle Benutzer eines Netzwerks dieselbe SSID angeben, um auf einen bestimmten Zugriffspunkt zuzugreifen. Mit einer SSID wird der Zugriff von Clientgeräten verhindert, die eine andere SSID besitzen. Die SSID wird jedoch von Zugriffspunkten standardmäßig zusammen mit dem Signal übertragen. Dadurch kann ein Hacker die SSID per "Sniffing" selbst dann ermitteln, wenn die SSID-Übertragung deaktiviert ist.

**SSL (Secure Sockets Layer)**

Ein von Netscape entwickeltes Protokoll zum Übermitteln vertraulicher Dokumente über das Internet. SSL arbeitet mit einem öffentlichen Schlüssel, mit dem die Daten verschlüsselt werden, die über die SSL-Verbindung übertragen werden. SSL wird sowohl von Netscape Navigator als auch von Internet Explorer genutzt und unterstützt. Viele Websites verwenden dieses Protokoll, wenn Benutzer vertrauliche Informationen (z. B. Kreditkartennummern) eingeben müssen. Laut Konvention beginnen URLs, die eine SSL-Verbindung erfordern, mit der Zeichenfolge "https:" anstelle von "http:".

**T**

**TKIP (Temporal Key Integrity Protocol)**

Eine schnelle Methode zum Lösen der konstruktionsbedingten Sicherheitsschwächen von WEP, speziell des Problems der Wiederverwendung von Verschlüsselungsschlüsseln. Bei TKIP werden temporäre Schlüssel nach jeweils 10.000 Paketen geändert. Auf diese Weise wird eine dynamische Verteilungsmethode erzielt, die die Sicherheit des Netzwerks beträchtlich erhöht. Der TKIP-Sicherheitsprozess beginnt mit einem temporären 128-Bit-Schlüssel, der von Clients und Zugriffspunkten gemeinsam verwendet wird. TKIP kombiniert diesen temporären Schlüssel mit der MAC-Adresse (des Clientcomputers) und fügt dann einen relativ großen Initialisierungsvektor (16 Oktetts) hinzu, um den Schlüssel zu erstellen, mit dem die Daten verschlüsselt werden. Durch diese Vorgehensweise wird sichergestellt, dass jede Station ihre Daten mit einem anderen Schlüssel-Stream verschlüsselt. TKIP führt die Verschlüsselung mit RC4 durch. WEP verwendet ebenfalls RC4.

**U**

**USB-Drahtlosadapter-Karte**

Eine erweiterbare serielle Schnittstelle mit Plug-and-Play-Funktionalität. Diese Schnittstelle bietet eine standardisierte und preisgünstige drahtlose Anschlussmöglichkeit für Peripheriegeräte wie Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Speichergeräte und Videokameras.

**V**

**Verschlüsselung**

Die Umwandlung von Daten in einen geheimen Code. Verschlüsselung ist der wirkungsvollste Weg, Datensicherheit zu erzielen. Um eine verschlüsselte Datei lesen zu können, ist Zugriff auf den geheimen Schlüssel bzw. das Kennwort erforderlich, mit dem die Daten entschlüsselt werden können. Unverschlüsselte Daten bezeichnet man als Klartext; verschlüsselte Daten werden chiffrierter Text genannt.

**VPN (Virtual Private Network)**

Ein Netzwerk, das entsteht, indem Knoten unter Verwendung von öffentlichen Leitungen neu miteinander verbunden werden. Es gibt zum Beispiel eine Reihe von Systemen, mit denen Sie Netzwerke erstellen können, die das Internet als Medium für den Datentransport verwenden. Diese Systeme setzen Verschlüsselung und andere Sicherheitsmechanismen ein, um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen und die Daten nicht abgefangen werden können.

**W**

**Wardriver**

Das sind mit Notebooks bewaffnete Eindringlinge, die mit spezieller Software und modifizierter Hardware durch die Gegend streifen, um Datenverkehr von Funk-LANs abzufangen.

**WEP (Wired Equivalent Privacy)**

Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Standard 802.11. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

**Wi-Fi (Wireless Fidelity)**

Dieser Begriff wird allgemein für alle Arten von 802.11-kompatiblen Netzwerken verwendet, sei es 802.11b, 802.11a, Dual-Band, usw. Der Begriff wird von der Wi-Fi Alliance verwendet.

**Wi-Fi Alliance**

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht und deren Ziel darin liegt, (1) allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren, und (2) den Begriff "Wi-Fi" in allen Märkten für Produkte für 802.11-basierte Funk-LANs als globalen Markennamen zu fördern. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die die gegenseitige Kompatibilität und das Wachstum dieser Branche voranbringen möchten.

Auch wenn alle Produkte der Standards 802.11a/b/g als Wi-Fi bezeichnet werden, dürfen nur die Produkte, die den Test der Wi-Fi Alliance bestanden haben, das Prädikat "Wi-Fi Certified" (eine eingetragene Marke) tragen. Produkte, die den Test erfolgreich bestanden haben, müssen ein Identifikationssiegel auf ihrer Verpackung haben, auf dem "Wi-Fi Certified" sowie das verwendete Funkfrequenzband stehen. Die Wi-Fi Alliance war früher unter der Bezeichnung Wireless Ethernet Compatibility Alliance (WECA) bekannt, änderte jedoch im Oktober 2002 ihren Namen, um die Marke "Wi-Fi" besser darstellen zu können, deren Aufbau das Ziel der Gruppe ist.

**Wi-Fi Certified**

Produkte, die von der Wi-Fi Alliance getestet und als Wi-Fi Certified (eine eingetragene Marke) zugelassen wurden, sind als miteinander vollständig kompatibel zertifiziert, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden. Üblicherweise funktionieren Wi-Fi-Produkte mit allen anderen Produkten zusammen, die dieselbe Funkfrequenz verwenden (z. B. 2,4 GHz bei 802.11b oder 11g; 5 GHZ bei 802.11a), auch wenn diese nicht das Prädikat "Wi-Fi Certified" haben.

**WLAN (Wireless Local Area Network)**

Siehe auch LAN. Ein LAN, das ein drahtloses Medium zum Verbinden verwendet. In WLANs erfolgt die Kommunikation zwischen den Knoten über hochfrequente Funkwellen anstelle von Kabeln.

**Wörterbuchangriff**

Bei diesen Angriffen wird versucht, ein Kennwort zu ermitteln, indem unzählige Wörter aus einer Liste durchprobiert werden. Dabei geben die Angreifer diese Wörter und alle ihre Kombinationen nicht selbst manuell ein, bis sie das Kennwort von jemandem ermittelt haben, sondern verwenden dafür Tools, die diesen Vorgang automatisieren.

**WPA (Wi-Fi Protected Access)**

Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen stark erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Softwareupgrade entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

**WPA-PSK**

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

**X**

**Y**

**Z**

**Zugriffspunkt**

Ein Netzwerkgerät, das 802.11-kompatiblen Clients die Verbindung zu einem LAN (Local Area Network) ermöglicht. Zugriffspunkte erweitern die physikalische Betriebsreichweite für drahtlose Benutzer. Sie werden auch als drahtlose Router bezeichnet.

# Index