SECURING WIRELESS NETWORKS GUIDE

TIPS AND TRICKS ON HOW TO SHIELD YOUR HOME NETWORK FROM INTRUDERS

BOGDAN BOTEZATU
E-THREATS ANALYSIS AND COMMUNICATION TEAM

HOME USERS

bitdefender

Inhaltsverzeichnis

Warum Funk statt Kabel?

Funkverbindungen eignen sich hervorragend, um große Gebiete abdecken, ohne in aufwendige Verkabelung investieren zu müssen, um strukturelle Veränderungen an Gebäuden zu integrieren und um Unordnung zu vermeiden. Sie wurden in der Vergangenheit jedoch oft wegen mangelnder Sicherheit kritisiert, da Daten frei in Form von Radiowellen durch die Luft übertragen werden, auch wenn dies oft verschlüsselt geschieht.

Dieser Leitfaden erklärt den fachmännischen Umgang mit Funknetzwerken sowie Vorkehrungen zur WLAN Sicherheit, die Sie an Ihrem Router oder ihrer Basisstation vornehmen können, um Ihr Netzwerk vor dem Zugriff Unbefugter zu schützen.

Die augenfälligsten Vorteile eines Funknetzwerks (nach der Norm 802.11b/g/n) zu Hause oder in kleineren Büros sind die geringen Hardware-Anschaffungskosten (Basisstation oder Router und Netzwerkkarten), die Leichtigkeit der Installation (es müssen keine Kabel verlegt und Wände durchbohrt werden) und die Bewegungsfreiheit. Der serienmäßige Einbau von Funkadaptern in Laptops, Netbooks und einigen Handys hat ebenfalls die Verbreitung von Funknetzwerken begünstigt.

Auch wenn die Daten zwischen Client und Basisstation oder Router ungehindert ausgetauscht werden und prinzipiell jedem Client im Empfangsgebiet zugänglich sind, ist es dennoch sicherer, das WLAN-Netzwerk gut einzurichten.

Wo genau ist mehr Sicherheit nötig?

Standardmäßig werden Router und Basisstationen höchstens mit rudimentären Sicherheitsmerkmalen ausgeliefert. Die meisten Router und Basisstationen werden über eine Browser-basierte Oberfläche verwaltet, die über die IP-Adresse des Geräts aufgerufen wird. Wenn die Oberfläche aufgerufen wird, fragt das Gerät nach einem werksseitig eingestellten Benutzernamen und Passwort, die normalerweise beim selben Modell immer dieselben sind und die im Internet gefunden werden können.

Administratorenzugang und Fernanmeldung

Die meisten Geräte verfügen über eine Vielzahl von Funktionen und Technologien, die es auch Laien ermöglichen, sie unkompliziert in Betrieb zu nehmen. Der verbreitetste Fehler ist, das Gerät so zu belassen, wie es gekauft wurde, da es ja wunderbar funktioniert. Es sollte auf jeden Fall sofort nach dem Anschließen und Einschalten das voreingestellte Passwort geändert werden.

Durch gezieltes Sichern des WLAN-Verwaltungsbereichs wird verhindert, dass Unbefugte die Netzwerkeinstellungen verändern oder Zugriffsprotokolle löschen, um unerkannt zu bleiben, während sie auf fremde WLAN-Netzwerke zugreifen.

Um den Zugriff auf den Verwaltungsbereich noch weiter zu erschweren, sollte der Besitzer des WLAN-Geräts den Drahtloszugriff deaktivieren. An den meisten Routern und Basisstationen können autorisierte Benutzer Einstellungen verändern, indem sie einfach die IP-Adresse des WLAN-Geräts in die Browser-Adresszeile eingeben – auch wenn sie sich nicht im selben Gebäude befinden.

Das WPA2-Protokoll ist deutlich sicherer als der veraltete WEP-Verschlüsselungsstandard.

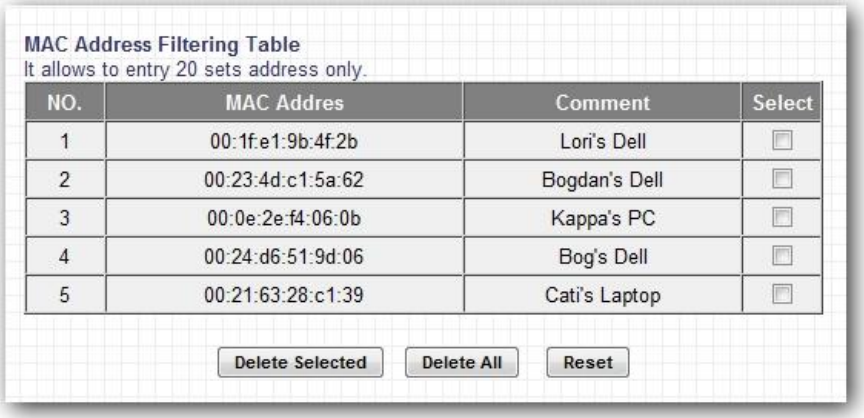
Diese Funktion ist für Systemadministratoren enorm praktisch, wenn sie z. B. nachts ein Verbindungsproblem beheben müssen, da sie sich ganz bequem von zu Hause aus einwählen können; sie birgt aber gleichzeitig die Gefahr, dass Unbefugte über die IP-Adresse der öffentlichen Geräteoberfläche auf das WLAN-Gerät zugreifen könnten.

Wenn sich in einem Router keine Liste vertrauenswürdiger IP-Adressen [1] mit Zugriffsrechten auf den Verwaltungsbereich anlegen lässt, ist es sicherer, den WLAN-Zugriff auf die Verwaltungsoberfläche zu deaktivieren.

WLAN schützen durch Verschlüsselung des drahtlosen Netzwerkverkehrs

Neben der Absicherung der Verwaltungsoberfläche des Drahtlosgeräts sollte man natürlich auch für einen Schutz der WLAN-Verbindung selbst sorgen. Wie oben erwähnt unterscheiden sich WLAN-Netzwerke von kabelgebundenen Netzwerken, die durch ihre abgeschirmte Datenübertragung automatisch nach außen hin sicher sind, dadurch, dass das Funksignal durch den freien Raum übertragen wird und nur durch die Sendeleistung des Geräts begrenzt wird. Je nach Größe des Empfangsgebiets versuchen eventuell Dutzende von Computern, unbefugt Zugang zu Ihrem Netzwerk zu erlangen oder, noch schlimmer, die unverschlüsselt übertragenen Daten auszulesen.

[1] Manche Router können automatische Berechtigungen zum Zugriff auf den Verwaltungsbereich nur erteilen, wenn die IP-Adresse des Clients einen bestimmten Wert hat oder innerhalb eines festgelegten IP-Bereichs liegt. Anfragen von anderen IP-Adressen werden automatisch abgelehnt.



MAC Address Filtering Table

It allows to entry 20 sets address only.

NO.	MAC Addres	Comment	Select
1	00:1f:e1:9b:4f:2b	Lori's Dell	☐
2	00:23:4d:c1:5a:62	Bogdan's Dell	☐
3	00:0e:2e:f4:06:0b	Kappa's PC	☐
4	00:24:d6:51:9d:06	Bog's Dell	☐
5	00:21:63:28:c1:39	Cati's Laptop	☐

Delete Selected | Delete All | Reset

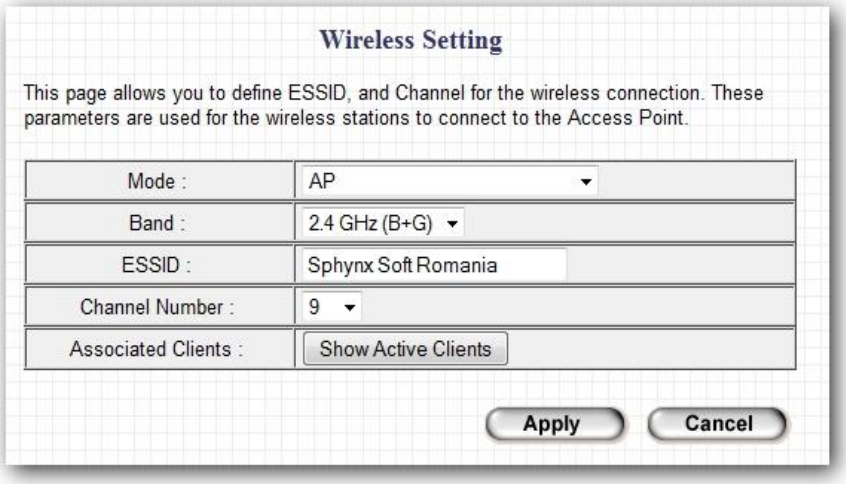
MAC-Filter bewirken, dass der Router nur Clients zulässt, die bereits als vertrauenswürdig definiert wurden.

Deshalb sollten Sie Ihr WLAN-Netzwerk schützen, indem Sie einen Zugangsschlüssel festlegen. Um die Kosten gering zu halten und die Einrichtung zu erleichtern, werden Netzwerkgeräte für den Heimgebrauch meist mit zwei eingebauten Verschlüsselungsprotokollen ausgeliefert, und zwar WEP (Wired Equivalent Privacy) und WPA/WPA2 (Wi-Fi Protected Access).

Beide Protokolle basieren auf der sogenannten Ein-Faktor-Authentifizierung in Form von voreingestellten Schlüsseln, die als Passwörter fungieren. Sie unterscheiden sich aber im Hinblick auf die Sicherheit. WEP entstand 1997 als Teil des 802.11-Protokolls, gilt inzwischen aber als überholt, weil es zu leicht geknackt werden kann. WPA und WPA2 bieten ein hohes Maß an Sicherheit, ohne allzu viel Konfiguration zu erfordern. Deshalb sind sie für Heimnetzwerke die beste Wahl.

In manchen Fällen ist der Einsatz von WPA nicht möglich – meist dann, wenn die im Netzwerk verwendete Hardware vor Einführung dieses Standards angeschafft wurde. Wenn Sie ein solches älteres Gerät besitzen, sollten Sie beim Hersteller nachfragen, ob es inzwischen neuere Firmware gibt, die WPA unterstützt.

Gibt es keine, sollten Sie zum Schutz Ihres WLAN-Netzwerks zumindest den WEP Schutz verwenden, als die Verbindung ganz ungeschützt zu lassen. Sie sollten sich in dem Fall aber darüber im Klaren sein, dass Ihre Daten eventuell von Eindringlingen abgefangen werden könnten. Es wäre also sinnvoller, etwa 30 € für einen neuen WLAN-Router auszugeben, der WPA/WPA2 unterstützt.



SSID-Signale zeigen an, dass ein Funknetzwerk in der Nähe ist. Dies kann von potenziellen Eindringlingen ausgenutzt werden.

MAC-Adressen definieren

Eine weitere Möglichkeit, Unbefugten den Zugriff auf Ihr WLAN-Netzwerk zu verweigern, sind Listen mit bestimmten Computern, denen der Zugriff ausdrücklich erlaubt wurde. Die meisten Router und Basisstationen für Heimnetzwerke unterstützen die Anlegung von Listen mit sogenannten MAC-Adressen (Media-Access-Control-Adressen); der Router bzw. die Basisstation akzeptiert dann nur Verbindungsversuche von Netzwerkkarten mit diesen MAC-Adressen.

Bei einigen Drahtlosadaptern kann der Benutzer die MAC-Adresse allerdings bei Bedarf ändern, weshalb die MAC-Filterung allein auch kein völlig sicherer Schutz ist. Sie ist jedoch eine zusätzliche Barriere, die zusammen mit einem sicheren WPA-Schlüssel in Ihrem Netzwerk solide WLAN-Sicherheit bietet.

Die drei oben beschriebenen Schritte sind die verbreitetsten Maßnahmen, um ein WLAN-Netzwerk gegen den Zugriff Unbefugter (wie z. B. Nachbarn oder WLAN-Raubnutzer) abzusichern. Im folgenden Abschnitt zeigen wir Ihnen, wie Sie ihr Netzwerk verbergen können, damit potenzielle Eindringlinge es gar nicht erst finden.

SSID-Signal unterbinden

Damit Benutzer die verschiedenen Funknetzwerke in ihrer Umgebung auseinanderhalten können, senden Router und Basisstationen automatisch ein Signal mit ihrem Namen (auch ESSID, SSID oder Service Set ID genannt). Das ist für den Eigentümer des Netzwerks zwar praktisch, für einen Eindringling aber auch, denn der Router „schreit“ gewissermaßen, und zieht so die Aufmerksamkeit auf sich. Durch das Deaktivieren des SSID-Signals wird der Router (und alle mit ihm verbundenen Clients) für alle, die nicht wissen, dass ein aktives WLAN-Netzwerk in der Nähe ist, unsichtbar.

SSID-Signale zeigen an, dass ein Funknetzwerk in der Nähe ist. Dies kann von potenziellen Eindringlingen ausgenutzt werden.

Sendeleistung reduzieren

Wie bei jedem Gerät, das Funksignale sendet, hängt die Größe des vom Router bzw. von der Basisstation abgedeckten Empfangsgebiets direkt von der Sendeleistung des Geräts ab. Die Werkseinstellungen reichen meist, um nicht nur die eigene Wohnung, sondern auch noch ein gutes Stück außerhalb der Wohnung – wie das Treppenhaus oder den Bürgersteig vor dem Haus – abzudecken, wodurch ein Eindringling in der Nähe über einen Laptop versuchen kann, in Ihr WLAN-Netzwerk einzubrechen. Wenn Sie die Sendeleistung senken, verhindern Sie damit, dass Ihr Netzwerk außerhalb Ihrer Wohnung erreichbar ist.

Hochwertige Router und Basisstationen für den Heimeinsatz haben Einstellungen, über die sich die Sendeleistung reduzieren lässt. Es gibt jedoch keinen einzig wahren Wert, der den besten Kompromiss zwischen Leistung und WLAN-Sicherheit gewährleistet.

Eine Erhöhung der WLAN-Sendeleistung kann mit einer Verminderung der WLAN-Sicherheit einhergehen und ungebetene Gäste in Ihr Netzwerk locken, eine zu starke Senkung kann sich allerdings negativ auf die Übertragungsgeschwindigkeit innerhalb des Netzwerks auswirken.

Auch an Geräten, die keine solche Funktion direkt in der Firmware haben, kann die Sendeleistung verändert werden. Sie können einfach die Antenne (oder eine der Antennen, wenn das Gerät mehrere hat) abnehmen. Dadurch wird das Signal schwach genug, um Eindringlinge abzuwimmeln, reicht aber immer noch, um die gewünschte Übertragungsgeschwindigkeit im WLAN-Netzwerk aufrechtzuerhalten.

Das Empfangsgebiet hängt auch davon ab, wo genau der Router steht. Grundsätzlich sollten Router/Basisstationen nicht am Fenster stehen, denn Funksignale werden durch Glas nicht so stark unterbrochen wie durch Beton.

Die Bitdefender-Firewall entdeckt automatisch ungesicherte Netzwerke und empfiehlt dem Besitzer entsprechende Sicherheitsmaßnahmen.

Risiken bei Betrieb von und Verbindung mit ungesicherten Netzwerken

Ungesicherte WLAN-Netzwerke sind grundsätzlich problematisch. Abgesehen von einigen Ausnahmen, in denen sie sich gegen den Eindringling wenden, birgt ein ungesichertes Netzwerk für den Betreiber ein großes Risiko im Hinblick auf Datensicherheit.

Heimnetzwerke basieren auf Vertrauen, d. h. es gibt keine aufwendigen Authentifizierungsmechanismen, die den Zugang bestimmter Benutzer steuern. Heimnetzwerkbetreiber machen sogar alles so zugänglich wie möglich, damit die verschiedenen Computer im Haushalt ungehindert Daten austauschen können.

Netzwerkfreigaben mit Lese- und Schreibberechtigungen, über die private Daten wie Fotos oder Dokumente verfügbar sind, sind die häufigste Schwachstelle in Heimnetzwerken. Wenn sich Unbefugte in ein ungesichertes WLAN-Netzwerk einschleichen, erhalten sie auch Zugriff auf die Netzwerkfreigaben; sie können also problemlos Dokumente, Fotos, Musik, Videos und Software kopieren. Wenn die Netzwerkfreigaben mit Schreibberechtigung ausgestattet sind, kann ein Eindringling sogar Dateien oder ganze Ordner löschen oder sogar Schadsoftware – als normale Dateien getarnt – einschleusen.

Paket-Sniffing und das Mitschneiden des Datenverkehrs sind weitere Risiken ungesicherter Netzwerke. In einem Funknetzwerk werden Daten ungehindert durch die Luft übertragen. Ein Computer entscheidet selbst, welche Datenpakete er verarbeitet und welche nicht, da Letztere nicht für ihn bestimmt sind. Ein bösartiger „Netzwerkteilnehmer" kann über spezielle Programme sämtlichen Datenverkehr abhören und so z. B. Chat-Gespräche oder Anmeldedaten, die nicht über SSL-Verbindungen übertragen werden, und vieles mehr mitschneiden.

Sidejacking (oder Session Hijacking) ist eine Unterart des Paket-Sniffing, die jedoch deutlich effizienter ist als das ziellose Abhören von Verbindungen in der Hoffnung auf Benutzernamen und Passwörter, die im Nur-Text-Format gesendet werden. Beim Sidejacking werden Cookies abgefangen, die zwischen authentifizierten Benutzern und Websites ausgetauscht werden. Das funktioniert sogar bei Web-Diensten, die Benutzernamen und Passwörter per SSL verschlüsseln, bevor sie gesendet werden. Wenn die Cookies einmal in falsche Hände gelangen, kann sich ein Angreifer bei den entsprechenden Online-Diensten als der Benutzer ausgeben, ohne dass der Bestohlene überhaupt etwas davon merkt.

Ungesicherte WLAN-Netzwerke sind auch ideale Kanäle für **illegale Aktivitäten**. Kriminelle nutzen offene Netzwerke z. B. um mit gestohlenen Kreditkarten Käufe zu tätigen, andere Netzwerke zu hacken oder über Tauschbörsen Musik, Filme oder Software herunterzuladen, wobei sie ihre Identität hinter der des ungesicherten WLAN-Netzwerks verstecken. Wenn dann die Polizei Ermittlungen anstellt, werden sie nicht beim tatsächlichen Täter, sondern beim Eigentümer des ungeschützten WLAN-Netzwerks landen. Offene WLAN-Netzwerke werden auch oft missbraucht, um riesige Mengen an Spam-Mails zu versenden, was ebenfalls Ermittlungen und sogar das Abschalten des Internet-Zugangs zur Folge haben kann.

Sich mit einem ungesicherten Netzwerk zu verbinden, kann aber ebenso riskant sein, denn der ungeschützte Datenverkehr zwischen dem eigenen Computer und dem Router oder der Basisstation kann von Kriminellen leicht abgehört und mitgeschnitten werden. Es können auch **Netzwerkfreigaben offengelegt werden**, die im Netzwerk angelegt sind, oder Würmer von anderen Systemen im WLAN-Netzwerk können den eigenen Rechner infizieren.

WLAN-Sicherheitstipps – Surfen an Hotspots

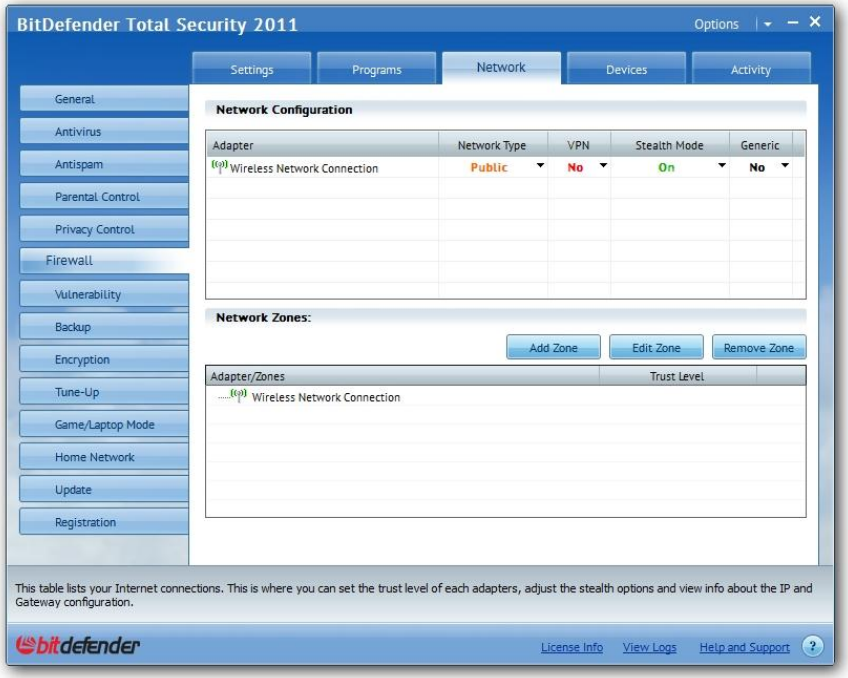
Hotspots sind heutzutage so weit verbreitet, dass man in nahezu jedem Café, Park oder Flughafen kostenlosen Internet-Zugang hat.

Die Verbindung mit einem ungesicherten Hotspot kann jedoch mehr Ärger als Freude machen, wenn man nicht einige grundlegende Vorsichtsmaßnahmen trifft. Hier geben wir Ihnen ein paar Hinweise, wie Sie sicher anonym surfen können.

Denken Sie daran, wenn Sie ein ungesichertes WLAN-Netzwerk nutzen, dass Sie nicht wissen, wer Ihre Nachbarn sind. Unter ihnen könnten Angreifer sein, die Port-Scans durchführen, um **Sicherheitslücken** zu finden und auszunutzen. Um das Risiko gering zu halten, sollten Sie eine Firewall auf Ihrem Gerät installiert haben, die Verbindungsversuche aus dem Netzwerk filtern kann.

Öffentliche Netzwerke eignen sich nicht zum Austausch vertraulicher Daten. Es besteht die Gefahr, dass andere im selben WLAN-Netzwerk versuchen, den Netzwerkverkehr von und zu den anderen Netzwerkteilnehmern auf wertvolle Informationen wie Benutzernamen, Passwörter, Chat-Gespräche oder Kreditkartennummern abzuhorchen. Wir empfehlen Ihnen, sich gut zu überlegen, welche Dienste Sie über Hotspots nutzen, und sich **so wenig wie möglich bei Online-Diensten anzumelden**.

Netzwerkfreigaben sind ein weiterer Punkt, der bei der Verbindung zu anderen Netzwerken gut bedacht werden sollte, denn Unvorsichtige laufen Gefahr, Unbefugten unwissentlich Zugang zu privaten Daten zu verschaffen. Netzwerkfreigaben sollten daher immer deaktiviert werden, bevor eine Verbindung zu einem Hotspot hergestellt wird.



Bitdefender verbirgt den Computer automatisch vor den anderen Clients im Netzwerk, wenn das Netzwerkprofil "öffentlich" ist.

Wie kann Bitdefender Ihnen helfen?

2001 war Bitdefender der weltweit erste Anbieter von Virenschutz-Software mit einer eingebauten Firewall-Funktion. Die 2011er-Produkte der Bitdefender-Produktfamilien „Internet Security“ und „Total Security“ verfügen über eine verbesserte Firewall, die Schutz in ungesicherten WLAN-Netzwerken bietet.

Um die Einrichtung zu erleichtern, verfügt die Bitdefender-Firewall über vier voreingestellte Netzwerktypen: vertrauenswürdig, Heim/Büro, öffentlich und nicht vertrauenswürdig.

Darüber hinaus aktiviert die Firewall bei der Verbindung zu öffentlichen WLAN-Netzwerken automatisch den **Unsichtbar-Modus**, der den eigenen Computer automatisch vor anderen Teilnehmern im Netzwerk versteckt und so das Risiko reduziert, dass der Datenverkehr abgehört oder Schadsoftware eingeschleust wird.

Und selbst beim Einsatz im eigenen Heimnetzwerk ist die Firewall praktisch. Denn sie gibt jedes Mal eine Benachrichtigung aus, wenn sich ein neuer Computer mit dem Netzwerk verbindet.

Das hilft besonders dabei, zu erkennen, ob die neuen Verbindungsversuche von erwünschten oder unerwünschten oder gar bösartigen Teilnehmern kommen.

bitdefender