für den DSL-Anschluss mit dem Splitter.

Zum Konfigurieren verbinden Sie den LAN-Netzwerkanschluss Ihres Computers über ein Netzwerkkabel mit dem Router. Der dafür geeignete Anschluss am Router heisst meist "LAN 1". Öffnen Sie mit einem Webbrowser die Konfigurationsoberfläche des Routers.

Geben Sie dazu in die Adresszeile Ihres Browsers die Standard-IP-Adresse des Geräts ein. In vielen Fällen ist das die Adresse `192.168.1.1`. Die nötigen Angaben finden Sie im Handbuch. Nach dem Öffnen der Weboberfläche werden Sie nach einem Benutzernamen und Passwort gefragt. Die Voreinstellungen finden Sie im Handbuch des Routers. Gelegentlich stehen sie auch auf der Rückseite des Geräts.

Ändern Sie als Erstes das Passwort. Damit verhindern Sie, dass sich ein Hacker über ein ungeschütztes Funknetz an Ihrem Router anmeldet. Verwenden Sie dabei ein möglichst kompliziertes und schwer zu erratendes Passwort.

DHCP einrichten

Ein DHCP-Server (Dynamic Host Configuration Protocol) weist in einem Netzwerk den angeschlossenen Computern automatisch eine IP-Adresse zu. In der Regel ist bei Routern ein DHCP-Server enthalten. Das erhöht Ihren Komfort – Sie müssen lediglich die Zugangsdaten für das Internet eingeben, damit alle angeschlossenen Rechner und sogar Live-CDs automatisch Zugriff auf das Internet erhalten.

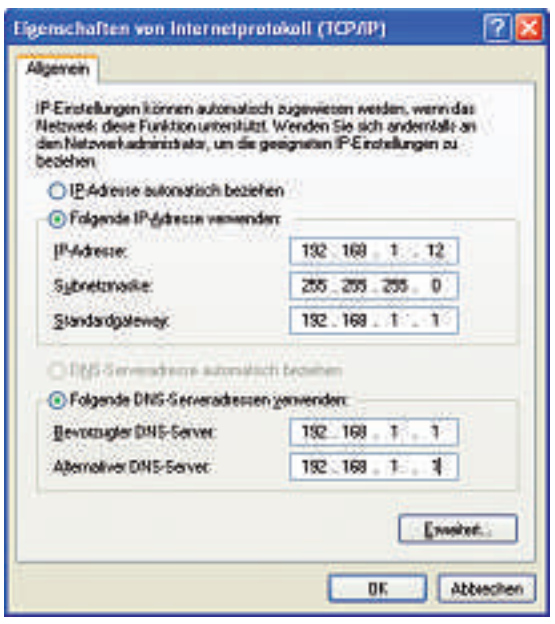
Aber ein DHCP-Server ist auch ein Risiko: Fremde Nutzer im Empfangsbereich bekommen auf diesem Weg ebenfalls automatisch eine IP-Adresse zugewiesen und erhalten damit Zugang zu Ihrem Funknetzwerk.

Feste IP-Adressen verwenden

Erschweren Sie Hackern die unerlaubte Nutzung Ihres Funknetzes, indem Sie den DHCP-Server abschalten und die IP-Adressen manuell vergeben.

Rufen Sie *Start*, *Systemsteuerung*, *Netzwerk- und Internetverbindungen*, *Netzwerkverbindungen* auf, um eine feste IP-Adresse auf Ihrem PC einzustellen. Klicken Sie mit der rechten Maustaste auf *LAN-Verbindung* und wählen Sie *Eigenschaften* aus.

Es öffnet sich ein Fenster, in dem Sie unter *Diese Verbindung verwendet folgende Elemente* den Punkt *Internetprotokoll (TCP/IP)* markieren. Klicken Sie auf *Eigenschaften*. Es öffnet sich ein weiteres Fenster, in dem Sie *Folgende IP-Adresse verwenden* auswählen und anschliessend darunter eine freie IP-Adresse eintragen.

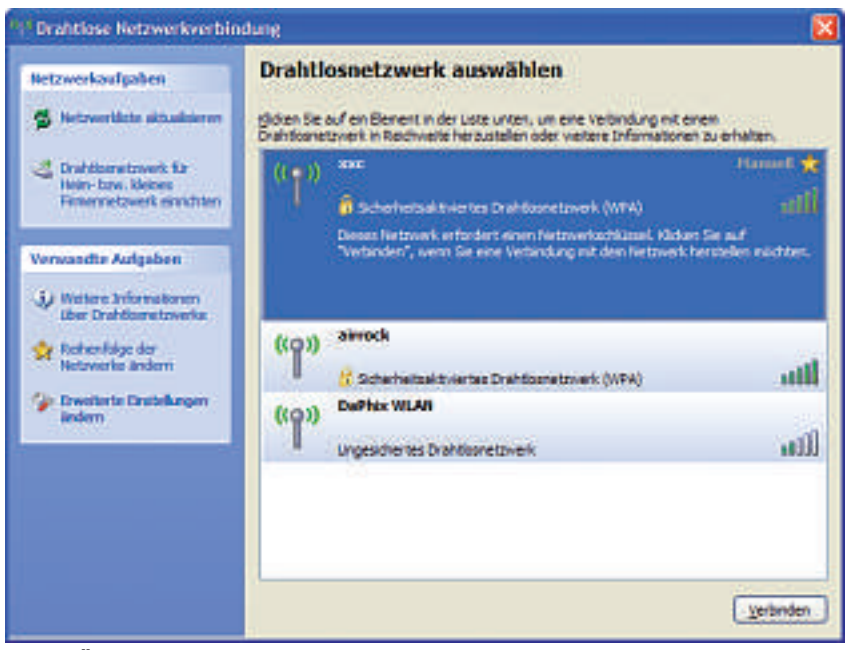


Feste IP-Adresse einrichten: In diesem Fenster richten Sie eine feste IP-Adresse für Ihren Windows-PC ein.

Wenn Ihr Router beispielsweise die IP-Adresse `192.168.1.1` verwendet, stehen Ihnen in der Regel Adressen von `192.168.1.2` bis `192.168.1.253` zur Verfügung. Bei der Zuteilung der Adressen an die einzelnen Geräte ist zu beachten, dass jede IP-Adresse nur einmal vergeben werden darf.

Hinter *Subnetzmaske* tragen Sie `255.255.255.0` ein und hinter *Standardgateway* die Adresse Ihres Routers, beispielsweise `192.168.1.1`. Diese Adresse tragen Sie ebenfalls hinter *Bevorzugter DNS-Server* und *Alternativer DNS-Server* ein.

Bestätigen Sie abschliessend zwei Mal mit *OK*, um die Änderungen zu aktivieren.



WLAN-Übersicht: Wählen Sie Ihr Funknetz mit einem Doppelklick aus, tragen Sie Ihren Zugangsschlüssel ein und klicken Sie auf die Schaltfläche "Verbinden".

WLAN-Verbindung einrichten

Um sich mit Ihrem WLAN-Router zu verbinden, müssen Sie dort noch die bestmögliche Verschlüsselung einstellen sowie ein Passwort festlegen. Verwenden Sie unbedingt WPA oder WPA2 (Wi-Fi Protected Access) und vergeben Sie einen komplizierten Schlüssel, der die maximale Länge von 63 Zeichen voll ausschöpft.

Tragen Sie den Schlüssel in der Verwaltungsoberfläche Ihres WLAN-Routers ein und speichern Sie ihn ausserdem in einer Textdatei, die Sie per USB-Stick auf Ihren WLAN-Client übertragen. Das Abtippen eines so langen komplizierten Schlüssels wäre viel zu fehlerträchtig.

Lassen Sie dann Ihren PC beziehungsweise Ihr Notebook nach Ihrem Funknetz suchen, indem Sie unten rechts im System-Tray doppelt auf das WLAN-Icon klicken.

Windows öffnet das Fenster *Drahtlose Netzwerkverbindung* und zeigt alle gefundenen WLANs an. Klicken Sie doppelt auf Ihr Funknetz und tragen Sie den Zugangsschlüssel ein. Mit einem Klick auf *Verbinden* aktivieren Sie die Verbindung.

Empfangsqualität prüfen

Mit Netstumbler 0.4.0 und einem Notebook prüfen Sie die WLAN-Empfangsqualität in Ihren vier Wänden. Netstumbler funktioniert auch auf einem normalen PC, der an ein WLAN angeschlossen ist. Den können Sie aber nicht bequem durch die Wohnung tragen, um den Empfang zu prüfen.

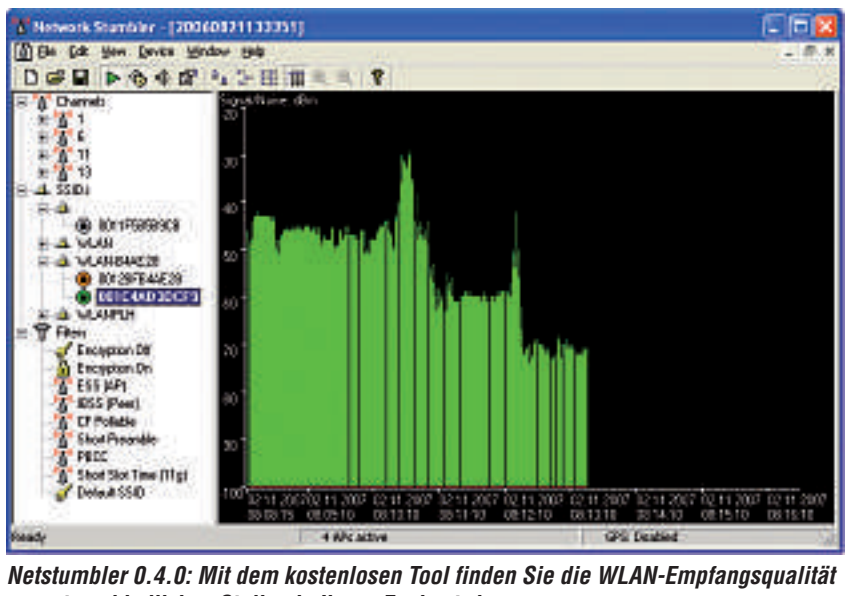
Starten Sie nach dem Download die Installation. Es öffnet sich ein Fenster mit dem *License Agreement*. Klicken Sie auf *I Agree*, um die Lizenzbedingungen des Herstellers zu akzeptieren.

Der nächste Dialog dient zur Auswahl der Komponenten. Belassen Sie die Auswahl auf *Complete* und klicken Sie auf *Next*. Nun legen Sie den Installationsordner fest und beginnen mit *Install* das Setup. Ein Klick auf *Close* schliesst den Vorgang ab.

Starten Sie Netstumbler. Sofort beginnt das Programm mit der Suche nach drahtlosen Netzen in Ihrer Umgebung. Manuell starten und beenden Sie den Suchvorgang, indem Sie auf den grünen Start-Button oben in der Netstumbler-Menüleiste klicken. Wenn Ihr WLAN-Netz eingeschaltet ist, erscheint es nach kurzer Zeit in dem grossen weissen Fensterbereich rechts. Je nach Konfiguration Ihres Netzes zeigt Netstumbler verschiedene Informationen wie den Netzwerknamen, den verwendeten Kanal, die Übertragungsgeschwindigkeit und die Verschlüsselung an.

Das kleine Symbol links zeigt die Signalstärke an. Grün bedeutet einen guten Empfang, gelb einen mittelmässigen, rot einen schwachen und grau gar keinen. Ein Vorhängeschloss steht für Verschlüsselung.

Klicken Sie links auf das kleine Pluszeichen neben *SSIDs*, um die Liste gefundener Netzwerknamen aufzuklappen. Wählen Sie Ihren Netzwerknamen aus und dann den darunter liegenden Eintrag. Im rechten Fenster erscheint die gemessene Signalstärke. Bewegen Sie sich mit Ihrem Notebook durch Ihre Räume, um Veränderungen der Signalstärke zu messen. Je stärker der grüne Balken ist, desto besser die Empfangsqualität. *Andreas Th. Fischer*



Netstumbler 0.4.0: Mit dem kostenlosen Tool finden Sie die WLAN-Empfangsqualität an unterschiedlichen Stellen in Ihrem Funknetz heraus.

INTERNET: WLAN sichern

WLAN ohne jedes Risiko

Wie schützt man ein WLAN vor Angreifern und heimlichen Mitsurfern? Welche Tricks und Tools verwenden Eindringlinge? Das müssen Sie wissen, damit Ihr Funknetz sicher bleibt.

WLANs sind allgegenwärtig. Ein bedeutender Teil ist jedoch überhaupt nicht oder nur mangelhaft gesichert. Was Sie beachten müssen und wie Sie sich wirksam gegen die Gefahr von Eindringlingen schützen, zeigen die folgenden Fragen und Antworten.

WLAN-Gefahren

Jeder WLAN-Nutzer muss sich mit den Risiken beschäftigen, die ihm drohen, wenn er sein Funknetz nicht absichert.

Frage: *Ich habe von meinem DSL-Anbieter einen WLAN-Router erhalten. Ist dieser bereits sicher konfiguriert oder muss ich selbst noch etwas ändern?*
Antwort: Vertrauen ist gut, Kontrolle ist besser. Es ist unbedingt nötig, die Konfiguration Ihres WLAN-Routers zu überprüfen und gegebenenfalls Anpassungen vorzunehmen, um eine optimale Sicherheit zu gewährleisten. Immer wieder bringen die Hersteller schlecht konfigurierte WLAN-Router auf den Markt. Das Ergebnis: Teils sind die Geräte nicht per Passwort geschützt, teils haben die Hersteller eine schwache Verschlüsselung voreingestellt, obwohl der Router eigentlich auch die sicherste Variante beherrscht.

Frage: *Was sind die grössten Gefahren bei einem nur ungenügend gesicherten WLAN?*
Antwort: Die naheliegendste Gefahr ist das Eindringen eines Angreifers in Ihr WLAN, der darüber Zugriff auf Ihren PC erhält. Auf diese Weise lassen sich Daten stehlen, beispielsweise aus freigegebenen Ordnern, oder beliebige Schädlinge einschleusen.

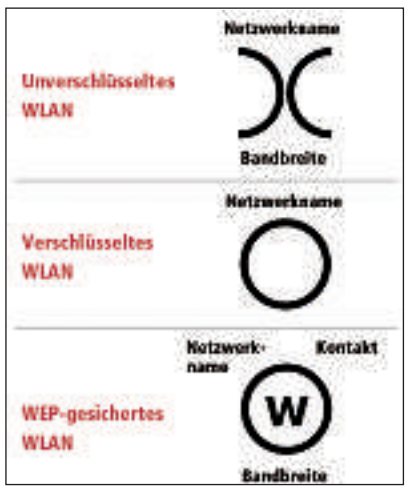
Frage: *Warum ist es problematisch, wenn jemand mein WLAN mitbenutzt?*
Antwort: Begeht der Schwarzsurfer eine Straftat über Ihre Internetverbindung, haben die Ermittler nur Ihre IP-Adresse als Information. Über diese IP-Adresse identifiziert Ihr Provider Sie, obwohl Sie gar keine illegalen Inhalte aufgerufen haben. Je nach Schwere der begangenen Tat sind eine Hausdurchsuchung und eine Beschlagnahmung Ihrer Hardware mögliche Konsequenzen.

WLAN sichern

Bereits mit wenigen Schritten lässt sich fast jedes WLAN so absichern, dass Eindringlinge keine Chance mehr haben.

Frage: *Welche Sicherheitsmassnahmen sollte ich ergreifen?*
Antwort: Es gibt mehrere Massnahmen, die jeder WLAN-Nutzer unbedingt durchführen sollte. Dazu zählen die Wahl eines neuen Passworts für Ihren Router, die Abschaltung der Fernkonfiguration, die Einrichtung einer sicheren Verschlüsselung und die Sperrung unbekannter MAC-Adressen.

Frage: *Wie erstelle ich ein sicheres Passwort und wie lang muss es mindestens sein?*



Warchalking: Mit diesen Zeichen markieren Hacker fremde WLANs.

Antwort: Die maximale Länge hängt von Ihrem Router ab. Generell gilt: Je länger es ist, desto besser. Ein sicheres Passwort sollte ausserdem Ziffern und, sofern erlaubt, Sonderzeichen enthalten. Näheres erfahren Sie im Handbuch Ihres Routers.

Frage: *Welche Verschlüsselung ist wirklich sicher vor Hackern?*
Antwort: Derzeit gelten nur WPA (Wi-Fi Protected Access) und WPA2 als sicher vor einem Angriff. WEP (Wired Equivalent Privacy) lässt sich mit im Internet frei verfügbaren Tools in kürzester Zeit knacken. Bei WPA und WPA2 ist dies nicht möglich.

Frage: *Was ist ein MAC-Filter und warum sollte ich ihn verwenden?*
Antwort: Ein MAC-Filter verhindert, dass sich neue Netzwerkgeräte an Ihrem Funknetz anmelden, ohne dass Sie es erlaubt haben. Meist meldet man seinen eigenen WLAN-Client an und aktiviert anschliessend den MAC-Filter, der dann neue Teilnehmer blockiert.

Richtig verschlüsseln: Konfigurieren Sie im WLAN-Router WPA oder WPA2 als Verschlüsselung.