

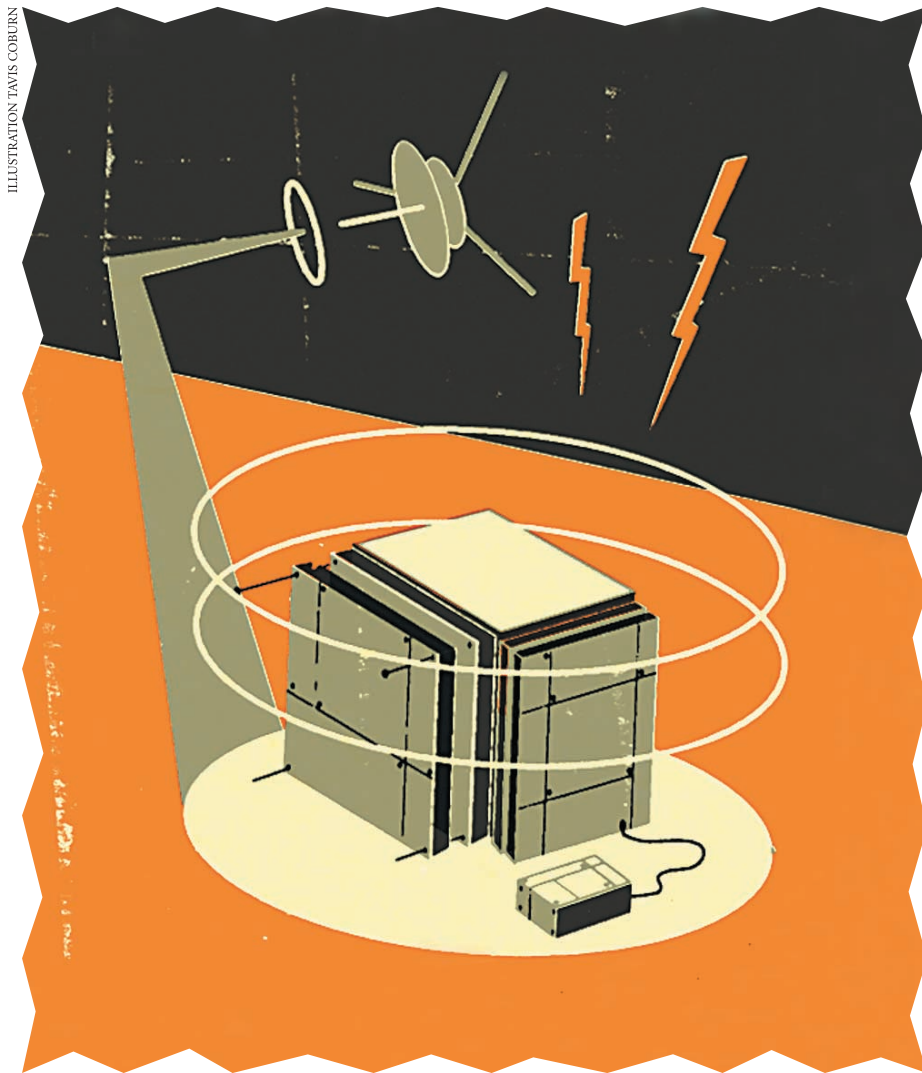


ILLUSTRATION TAVIS COBURN

WLAN abdichten

Computer mit dem kabellosen WLAN
sind Angriffen besonders ausgesetzt.
Wir zeigen, wie Sie sich schützen.

■ von Beat Rüdts

Dank günstigem Anschaffungspreis und der Integration in fast allen neuen Notebooks verbreiten sich drahtlose Netzwerke (WLAN) rasant. Es reicht schon, einen Access Point an die Breitband-Internetverbindung anzuschliessen und einen Desktop-PC oder ein Notebook mit WLAN auszurüsten (bei neuen Notebooks oft integriert), und die Verbindung steht (siehe Box «WLAN auf einen Blick, S. 62»). Die Geräte werden so ausgeliefert, dass eigentlich kein einziger Konfigurationsschritt mehr nötig ist.

Das ist allerdings wenig ratsam, da dann Ihr WLAN-Netz offen wie ein Scheunentor ist: Andere Anwender haben – sofern ebenfalls mit WLAN-fähigen Computern ausgerüstet – Zugriff auf Ihr Breitband-Internet und bei schlecht geschütztem Betriebssystem sogar auf die angeschlossenen Geräte.

Da hilft nur eines: Sie müssen Ihre drahtlose Verbindung abdichten. Unsere Sicherheitstipps verfolgen verschiedene Strategien, vom Verstecken des eigenen Computers über die Zugangskontrolle zum Netzwerk bis zur Verschlüsselung der übermittelten Daten. Am besten wenden Sie nicht nur einen Sicherheitstipp an, sondern kombinieren mehrere.

Zugang zum Access Point: Für die meisten der folgenden Schritte müssen Sie Einstellungen im Menü des Access Points ändern. Dieses Menü sieht bei jedem Hersteller etwas anders aus. Die von uns gezeigten Tipps beziehen sich auf den D-Link-Router DI-614+, der gleichzeitig auch ein Access Point ist. Das Vorgehen ist bei jedem Hersteller ähnlich, das heisst aber nicht, dass Benutzerführung und Bezeichnung der Menüpunkte gleich sind. Nehmen Sie deshalb die Betriebsanleitung Ihres Access Points zu Hilfe, um die folgenden Tipps umzusetzen.

In unserem Fall ist der Access Point über den Browser (zum Beispiel Internet Explorer) erreichbar, ins Adressfeld wird die IP-Adresse «192.168.0.1» eingegeben.

Stellen Sie als Erstes im Handbuch fest, wie Sie den Access Point auf die Werkseinstellungen zurücksetzen («Reset»). Falls etwas schief läuft, ist dies der einzige Weg, die Veränderungen rückgängig zu machen.

Passwortschutz

Weil die Hersteller in der Grundkonfiguration immer dieselben Benutzernamen und Passwörter für ihre Access Points verwenden, ist es auch ohne Hacker-Erfahrung möglich, sich in ein fremdes System einzuloggen.

Sicherheitstipp Passwort: Die erste Veränderung im Menü des Access Points muss daher ein neues Zugangspasswort sein. Sonst kann jeder, der in die Reichweite Ihres WLANs kommt, Ihre Einstellungen rückgängig machen.

Vorgehen: In unserem Beispiel befindet sich die Einstellung im Menü ADMIN im Register TOOLS. Geben Sie ins Feld «New Password» und «Confirm Password» zweimal dasselbe Passwort ein und klicken Sie anschliessend auf APPLY, [Screen 1](#).

Grenzen: Der Passwortschutz ist nur effektiv, wenn Sie einen Begriff wählen, der nicht einfach erraten werden kann (siehe auch «Geheime Schlüssel», PCtipp 3/2003, S. 42, online unter www.pctipp.ch mit WEBCODE pdf030342).

Filter einrichten

Mit Filtern erlauben Sie nur ganz bestimmten Computern den Zugang zum Netzwerk. Man unterscheidet MAC-Filter und IP-Filter. In beiden Fällen müssen Sie zuerst die Adressen der Geräte kennen, die sich im Netzwerk befinden: Sie klicken auf jedem PC, der zu Ihrem WLAN gehören soll, auf START/AUSFÜHREN und tippen ins Feld «Öffnen» den Befehl `cmd`, gefolgt von einem Klick auf OK. Im Fenster «Eingabeaufforderung» tippen Sie `ipconfig /all`, **Screen 2 A**, und drücken Enter. Windows listet alle relevanten Daten auf: Die **MAC-Adresse** finden Sie unter «Physikalische Adresse» **B** und die **IP-Adresse** unter «IP-Adresse» **C**.

Sicherheitstipp Filtern von MAC-Adresse: Hinterlegen Sie im Access Point die MAC-Adressen aller Computer (bzw. von deren Netzwerkkarten), die das WLAN benutzen dürfen. Damit schliessen Sie alle anderen Computer aus, denn die MAC-Adresse ist die fixe Nummer Ihrer Netzwerkkarte, die weltweit einmalig ist.

Vorgehen: Suchen Sie im Access-Point-Menü den Eintrag «Filter», den Sie meistens unter ERWEITERTE EINSTELLUNGEN (ADVANCED) finden. Im D-Link-Menü gibts die Auswahl zwischen «IP Filter» und «MAC Filters». Wählen Sie die zweite Möglichkeit, **Screen 3 A**. Dann markieren Sie «Only allow computers with MAC address listed...» **B**. Jetzt tragen Sie zuerst den Namen des Computers **C** und die ermittelte MAC-Adresse ins Feld hinter «MAC Address» **D** ein und klicken auf APPLY **E**.

Ist der Rechner, den Sie zulassen möchten, online, gehts noch einfacher: Wählen Sie ihn unter DHCP CLIENT aus und klicken Sie auf CLONE **F**. Die Daten werden automatisch eingetragen und Sie müssen nur noch mit APPLY bestätigen.

Grenzen: MAC-Adressen lassen sich fälschen. Mit einfachen Programmen aus dem Internet kann der Netzwerkkarte eine neue Kombination zugeteilt werden. Dazu muss der Angreifer allerdings zuerst wissen, welche Adressen im Access Point hinterlegt sind.

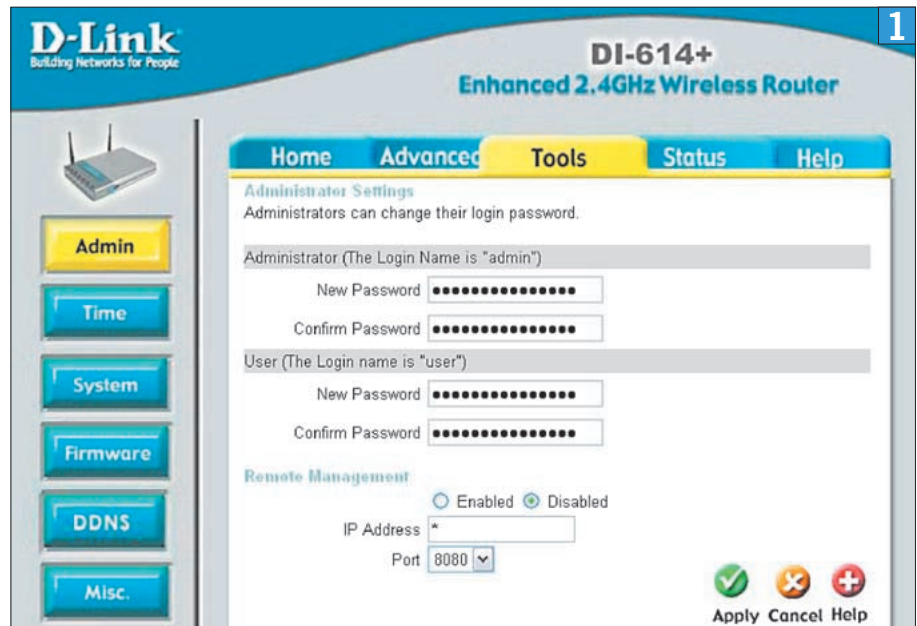
FACHCHINESISCH

MAC-Adresse

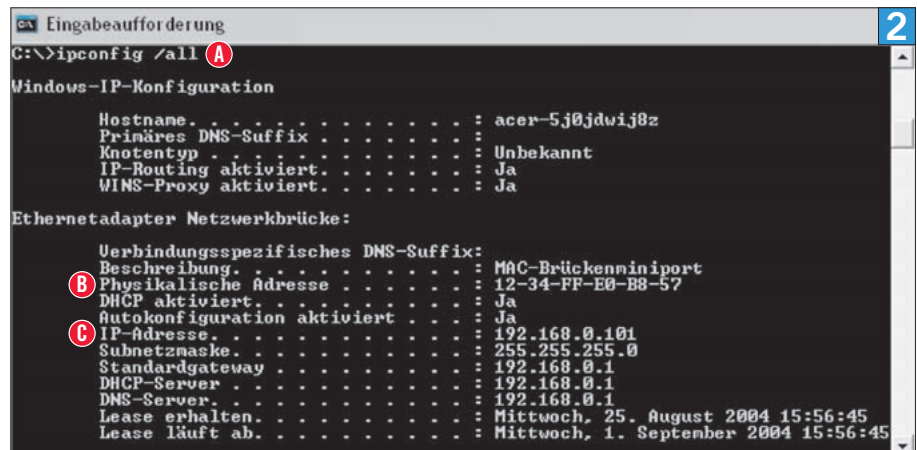
Media Access Control: Dieser zwölfstellige Code, der in der Form FF-FF-FF-FF-FF-FF geschrieben wird, ist der Netzwerkkarte in Ihrem PC zugeteilt und dient als eindeutige Hardware-Identifikation. Die MAC-Adresse verändert sich nicht bei jeder Einwahl neu, wie das bei der IP-Adresse möglich ist.

IP-Adresse

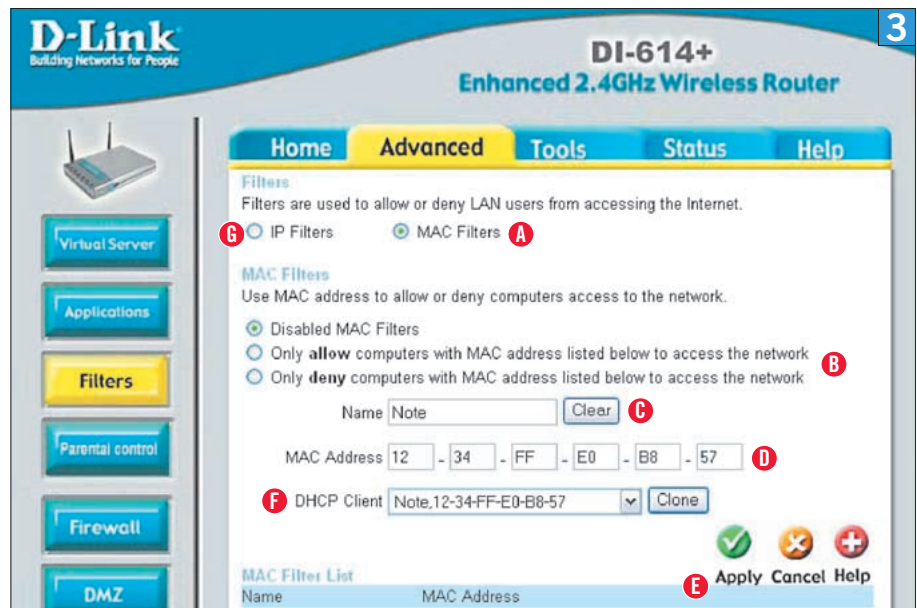
Mit der Internet-Protokoll-Adresse identifiziert sich ein Computer im Internet oder in einem anderen Netzwerk, z. B. WLAN. Die Adresse besteht aus vier maximal dreistelligen Zahlen, die durch einen Punkt getrennt sind und deren Werte zwischen 0 und 255 liegen.



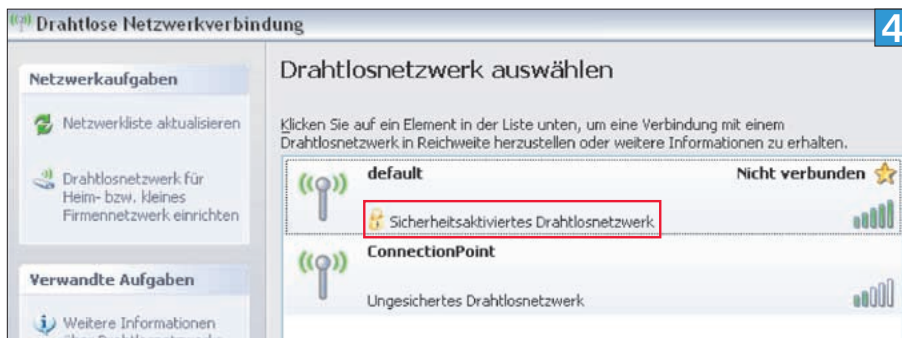
Kontrollieren Sie den Zugang zum Access Point mit einem Passwort



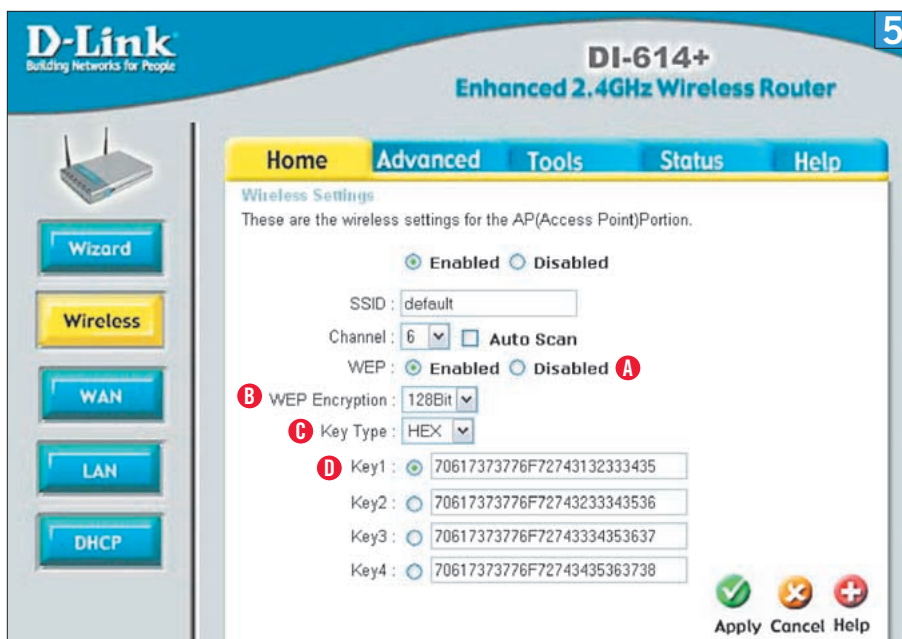
Hier erkennen Sie IP- und MAC-Adresse Ihres PCs



Definieren Sie, wer Zugang zum WLAN hat



Das Schlosssymbol garantiert eine sichere Verbindung



Bereiten Sie die Verschlüsselung im Access Point vor

HINTERGRUND

WLAN auf einen Blick

Als WLAN (Wireless Local Area Network, drahtloses lokales Netzwerk) bezeichnet man ein Funknetzwerk für Computer.

Übertragungsstandards: Zwei Standards sind für Anwender relevant:

802.11b: Mit einer Datenübertragung von 11 Mbit/s (= ca. 1,3 MB pro Sekunde) ist dieser Standard schon etwas veraltet. Mit zusätzlichen Antennen beträgt die Reichweite maximal 300 Meter.

802.11g: Mit 54 Mbit/s (ca. 6,4 MB) ist dies der aktuelle Standard. Er ist abwärtskompatibel und kommuniziert problemlos mit 802.11b-Geräten. Die tatsächliche Übermittlungsrate liegt etwas tiefer und kann bei verschlüsselter Übertragung auf 50 Prozent des theoretischen Wertes sinken.

Hardware: Wer die drahtlose Kommunikation nutzen möchte, muss sicher sein, dass sein Notebook (oder der Desktop-PC) mit dieser Technologie ausgerüstet ist. Dies ist immer der Fall, wenn das Notebook mit Intels **Centrino-Technologie** ausgerüstet ist. Das erkennen Sie am Centrino-Logo.



An diesem Logo erkennen Sie ein Notebook mit Centrino-Technologie

Ansonsten kann fast jedes Notebook mit einer Karte für den PC-Card-Slot nachgerüstet werden. Desktop-PCs statten Sie mit einer Steckkarte für einen PCI-Slot aus. Das zweite wichtige Element ist der **Access Point** (Zugangspunkt). Hier gibt es zwei Möglichkeiten: Sie kaufen einen Access Point, den Sie mit Ihrem Internetzugang (Kabel- oder ADSL-Modem) verbinden, oder Sie kaufen ein Modem mit bereits integrierter WLAN-Funktionalität. Manche Geräte bieten zusätzliche Schnittstellen für ein Kabelnetzwerk (LAN). In diesem Fall spricht man von einem WLAN-Router. Weitere Informationen zum Einrichten eines WLANs finden Sie im Artikel «Drahtlos glücklich», PCTipp 5/2003, S. 46, oder [WEBCODE pdf030546](#).

Sicherheitstipp Filtern von IP-Adressen: In Netzwerken mit fixen IP-Adressen definiert der Administrator, welche Computer auf das drahtlose Netzwerk zugreifen dürfen. In den Voreinstellungen auf Heim-PCs ist jedoch meist DHCP aktiviert, das die IP-Adressen automatisch zuweist. In diesem Fall funktioniert der Tipp nicht. Diese Einstellung sollten Sie nur verändern, wenn Sie etwas vom Umgang mit Computer-Netzwerken verstehen.

Vorgehen: Zuerst müssen Sie den Computern, die auf das WLAN-Netzwerk Zugriff haben sollen, fixe IP-Adressen zuweisen. Für die Einstellung im Access Point markieren Sie anschließend «IP Filters», [Screen 3 6](#). Die Vorgehensweise ist ähnlich wie bei der MAC-Adresse, nur dass Sie jetzt die IP-Adressen eintragen, die Sie zuvor mit dem Befehl `ipconfig /all` gefunden haben. Sie können einzelne IP-Adressen freigeben oder ein ganzes Spektrum, zum Beispiel die Adressen 192.168.0.2 bis 192.168.0.10.

Grenzen: Ein Computer mit einer IP-Adresse, die im Access Point freigegeben ist, kann auf das WLAN zugreifen. Es ist aber nicht ganz einfach, eine solche Adresse herauszufinden. Der Trick funktioniert zudem nicht, wenn DHCP aktiviert ist, was normalerweise die Standardeinstellung ist.

Daten verschlüsseln

Die größte Gefahr bei der Anwendung von WLAN ist, dass Hacker Ihren Datenverkehr abfangen. Sie lesen sämtliche Daten, die via WLAN übermittelt werden: unverschlüsselte Passwörter oder den gesamten Mailverkehr. Dem beugen Sie vor, indem Sie die Daten verschlüsseln. Ob ein Netzwerk verschlüsselte oder unverschlüsselte Daten übermittelt, erkennen Sie am Schlosssymbol, [Screen 4](#), im Fenster «Drahtlose Netzwerkverbindung», das Sie mit einem Doppelklick auf das Symbol der drahtlosen Netzwerkverbindung in Windows öffnen.

Sicherheitstipp Verschlüsselung: Verschlüsseln Sie Ihre Daten. Hacker sehen dann nur noch einen Zeichensalat.

Vorgehen: Klicken Sie im Konfigurationsmenü des Access Points auf WIRELESS. Hier haben Sie die Möglichkeit, die WEP-Verschlüsselung zu aktivieren (WEP = Wired Equivalent Privacy). Klicken Sie hierfür neben dem Eintrag WEP, [Screen 5 A](#), auf ENABLED. Wählen Sie die 128-Bit-Verschlüsselung [B](#) und «Key Type» HEX [C](#). Nun müssen Sie die Schlüssel (Key1 bis Key4) generieren. Surfen Sie dazu im Internet auf die Seite www.warewolfabs.com/portfolio/programming/wepskg/wepskg.html. Hier finden Sie ein Programm zum Generieren solcher Schlüssel.

So funktioniert: Erstellen Sie neben «Custom Phrase» ein 13-stelliges Passwort, [Screen 6 A](#). Schreiben Sie dieses Passwort auf, da Sie es später noch brauchen! Klicken Sie anschließend auf GENERATE 128-BIT KEY [B](#), und schon sehen Sie neben «HEX» den fertigen Schlüssel [C](#). Den tragen Sie bei «Key1», [Screen 5 D](#), ein. Wiederholen Sie den Vorgang mit anderen Passwörtern für die Keys 2 bis 4. Am Schluss wählen Sie APPLY.

Aktivieren Sie jetzt in [Screen 5](#) «Key1». Beim ersten Einwählen ins WLAN werden Sie nach dem

Passwort gefragt, [Screen 7](#). Geben Sie jenes an, das Sie für Key1 gewählt haben.

Grenzen: WEP-Verschlüsselung gilt als relativ leicht knackbar. In ganz neuen Geräten ist eine verbesserte Verschlüsselung (WPA) integriert.

Ordner schützen

Zusätzlichen Schutz verschaffen Sie sich so auf Ihrem PC oder Notebook: In Windows XP ist zum Beispiel der Ordner «Gemeinsame Dokumente» automatisch freigegeben. Der enthält zwar keine Daten, die Sie nicht explizit darin abgelegt haben, trotzdem sollten Sie ihn nicht unbedingt zur Schau stellen.

Sicherheitstipp Ordner-Freigabe: Deaktivieren Sie die Freigabe des Ordners. Gleichzeitig verschwindet Ihr Computer aus der Ansicht START/NETZWERKUMGEBUNG der anderen Computer im Netzwerk: Sie sind unsichtbar.

Vorgehen: Klicken Sie auf START und öffnen Sie den ARBEITSPLATZ. Klicken Sie mit der rechten Maustaste auf den Ordner «Gemeinsame Dokumente» und wählen Sie EIGENSCHAFTEN. Wechseln Sie ins Register FREIGABE. Deaktivieren Sie das Häkchen vor «Diesen Ordner im Netzwerk freigeben», [Screen 8](#), und klicken Sie auf Ok.

Grenzen: Sie machen Ihren Computer unsichtbar, nicht aber den Access Point. Der ist immer noch für alle Nachbarn sichtbar.

Fazit

Jeder einzelne Sicherheitstipp hat seine Grenzen. Wer über WLAN kommuniziert, setzt sich in jedem Fall einem Sicherheitsrisiko aus. Doch bleiben wir realistisch: Der Aufwand, ein WLAN zu hacken, ist gross. Ein Angreifer muss zahlreiche Möglichkeiten durchspielen. Die Mühe lohnt sich deshalb für private Netzwerke oder Netzwerke kleiner Firmen kaum. Ein – wie vorgängig beschrieben – geschütztes Netzwerk gilt deshalb als sicher.

WEP STRONG KEY GENERATOR v2.1 by Warewolf Labs & Kraix

6

To generate a **random WEP key**, select the bit key length to generate and press the corresponding button; the ASCII or HEX key can then be copied to your clipboard manually or via the copy to clipboard button to the right of the generated key text field.

You can also generate a **custom WEP key** based on your own pass phrase or other input -- thanks to [Kraix](#) for providing the idea and original code for this feature, as well as needed updates to the documentation and implementation of this script.

A good primer on WEP key setup and terms is located [here](#).

NOTES:

- If your product vendor requests 40-bit keys, use the 64-bit key
- If your product vendor requests 104-bit keys, use the 128-bit key
- Apple users can enter HEX keys into their AirPort setup by prefixing the generated string with a "\$" symbol (i.e. if the generated HEX code is **6b5e454532** then you would enter **\$6b5e454532** into your configuration)

Random WEP Key

64	generate 64-bit key
128	generate 128-bit key B
152	generate 152-bit key
256	generate 256-bit key

Custom WEP Key

NOTE: 5/13/16/29 characters are needed for 64/128/152/256-bit WEP

A Custom Phrase
 Character Count

Generated Key

ASCII
 HEX **C**

Hier generieren Sie die Schlüssel

Mit dem drahtlosen Netzwerk verbinden

7

Die folgenden Netzwerke sind verfügbar. Wählen Sie ein Netzwerk aus der Liste, und klicken Sie auf "Verbinden", um auf ein Netzwerk zuzugreifen.

Verfügbare Netzwerke:

Für dieses Netzwerk muss ein Netzwerkschlüssel (WEP) eingegeben werden. Geben Sie den Schlüssel ein, und klicken Sie auf "Verbinden", um auf dieses Netzwerk zuzugreifen.

Netzwerk-schlüssel:

Klicken Sie auf "Erweitert", wenn die Verbindung mit dem Netzwerk nicht hergestellt wird.

Netz gefunden, jetzt müssen Sie nur noch das Passwort eingeben

Eigenschaften von Gemeinsame Dokumente

8

Allgemein **Freigabe**

Lokale Freigabe und Sicherheit

 Klicken Sie auf diesen Ordner, und ziehen Sie ihn in den Ordner [Gemeinsame Dokumente](#), um ihn nur für Benutzer dieses Computers freizugeben.

Aktivieren Sie folgendes Kontrollkästchen, um den Ordner und untergeordnete Ordner nicht freizugeben.

☐ Diesen Ordner nicht freigeben

Netzwerkfreigabe und -sicherheit

 Aktivieren Sie das erste Kontrollkästchen, und geben Sie einen Freigabename ein, um diesen Ordner für andere Benutzer dieses Computers und im Netzwerk freizugeben.

☐ Diesen Ordner im Netzwerk freigeben

Freigabename:

☐ Netzwerkbenutzer dürfen Dateien verändern

Verstecken Sie Ihren Computer im Netzwerk