

# Kabellose Netze sind in Sekunden geknackt

Nur bei den wenigsten WLANs ist die Verschlüsselung aktiviert.

Daniel Schröder



| let's warchalk...! |                                  |
|--------------------|----------------------------------|
| KEY                | SYMBOL                           |
| OPEN NODE          | ssid<br>bandwidth                |
| CLOSED NODE        | ssid                             |
| WEP NODE           | ssid access contact<br>bandwidth |

Mit diesen Zeichen markieren Hacker Gehwege oder Straßen, wenn sie ein Netzwerk gefunden haben. Sie sagen aus, wie stark das Netzwerk geschützt ist – durch eine MAC-Adressen-Sperre, eine WEP-Verschlüsselung oder überhaupt nicht.

Bei einer Autofahrt mit einem Notebook durch Münchens Vororte zeigt das Programm Netstumbler nach etwa einer Stunde bereits 20 gefundene kabellose Netzwerke. Etwa die Hälfte dieser Netze ist vollkommen ungeschützt. Ein großer Teil der ungeschützten WLANs wird von Privatleuten betrieben, die das Sicherheitsrisiko unterschätzen („Es ist mir egal, wenn jemand in mein Netz eindringt. Erstens wird es schon niemand tun und zweitens entstehen mir keine Kosten: Ich habe eine Flatrate“). Doch der Anwender wiegt sich in trügerischer Sicherheit. Nicht nur ins Internet zieht es die so genannten WLAN-Hijacker: Freigegebene Ordner und Dateien können interessant sein, bei T-Online-Kunden können die Hacker sogar ohne zusätzliches Kennwort E-Mails abfragen und persönliche Daten einsehen (siehe Seite 38). An noch schlimmere Folgen denkt dabei niemand: Ein Hacker könnte problemlos per Funk einen fremden Internet-Zugang nutzen, um illegale Geschäfte im Netz zu treiben. Die Schuld fällt dann auf den ahnungslosen Anschlussinhaber zurück.

## 75 Prozent zu langsam

Doppelt so schnell wie früher sollen neue Wireless-LAN-Geräte von U. S. Robotics, D-Link und SMC Daten durch die Luft funken. Zumindest auf den Verpackungen sieht das so aus, die wirkliche Datenrate liegt nicht ansatzweise bei der Hälfte dessen, was aufgedruckt ist. 802.11b+, eine Weiterentwicklung des verbreiteten IEEE 802.11b, ist kein anerkannter Standard. Chipsatzhersteller Texas Instruments wollte zwar, dass 802.11b+ anerkannt wird, IEEE lehnte den Antrag aber ab. Der Vorteil dieser Geräte ist übrigens die Abwärtskompatibilität zu alten Geräten. Größter Nachteil ist, dass es diese 22-MBit-Norm nicht gibt: Das kann zu Inkompatibilitäten führen. Bei unseren Tests funktionierten die Geräte mit Karten und Access-Points anderer Hersteller allerdings problemlos.

Tatsächlich neu ist 802.11a. Die von diesen Geräten genutzten Frequenzen wurden im November von der Regulierungsbehörde für Telekommunikation und Post freigegeben. 54 MBit erreichen Geräte dieser Norm in der Theorie, sie sind allerdings zu den

anderen Standards nicht kompatibel. In Deutschland wird der A-Standard aufgrund der großen Verbreitung von B wohl kaum erhältlich sein. Der zweite Grund, der gegen den Verkauf von A-Geräten spricht, ist der G-Standard: Er funkt ebenfalls mit 54 MBit, nutzt allerdings das 2,4-GHz-Band und ist deswegen mit Geräten nach IEEE 802.11b kompatibel.

## Sicherheit ist gleich schlecht

Während die Datenübertragungsraten fast vervinfacht wurden, blieb die Entwicklung bei der Sicherheit auf der Strecke. Bei verkabelten Netzwerken muss man sich kaum sorgen, dass Eindringlinge physikalischen Zugriff auf das Netzwerk bekommen. Beim Wireless LAN ist das ein größeres Problem: Die Funkwellen verbreiten sich ja auch außerhalb von Büro, Wohnung oder Haus. So kann jeder mit einem Notebook und Wireless-LAN-Karte in unmittelbarer Nähe eines

Access-Points direkt auf das gesamte Netzwerk zugreifen. Dazu zählen Internet-Gateways wie DSL-Router, Dateifreigaben, NAS-Dienste und andere Server sowie PCs. Einen einfachen Schutz kann man in fast jedem Access-Point aktivieren: Nur kabellose Netzwerkkarten, deren MAC-Adressen explizit in einer Erlaubnisliste eingetragen wurden, lässt der Access-Point dann zu. Übertragene Daten kann trotzdem jeder Netzwerkniffer sichtbar machen. Außerdem ist es mit einem Rechner, auf dem das Betriebssystem Linux läuft, innerhalb von wenigen Sekunden möglich, trotz des Schutzes einzudringen. Mit nur einem `ifconfig`-Aufruf kann der Anwender die MAC-Adresse nämlich auf einen beliebigen anderen Wert ändern.

## Verschlüsselung mit Sicherheitsloch

Um den Datenverkehr gegen Schnüffler abzusichern und um das Eindringen in das Netzwerk zu erschwe-

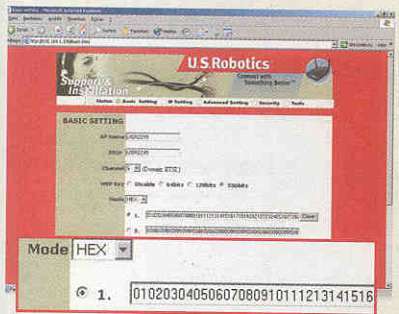
## So machen Sie Ihr Netz sicher

### 1. AP-Software installieren



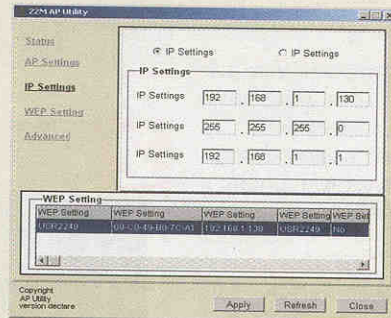
Wenn kein DHCP-Server im Netzwerk läuft, müssen Sie in der Regel die mitgelieferte Software installieren, um den Access-Point konfigurieren zu können. Besondere Einstellungen sind bei der Installation normalerweise nicht nötig, je nach Hersteller kann die Software aber stark unterschiedlich aussehen. Im Idealfall läuft sie ohne Installation direkt von CD.

### 4. WEP-Key festlegen



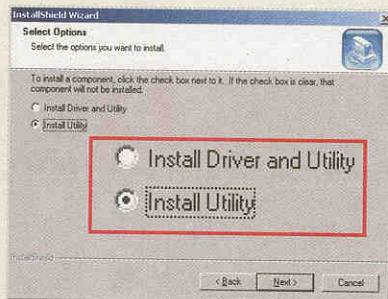
Suchen Sie nun die Optionsseite Ihres Access-Points, auf der Sie den WEP-Key einstellen können. Er wird normalerweise hexadezimal eingegeben, es dürfen also nur Zahlen von 0 bis 9 sowie die Buchstaben von A bis F verwendet werden. Man sollte immer die größtmögliche Verschlüsselung auswählen, bei aktuellen Geräten in der Regel 256 Bit.

### 2. IP-Adresse zuweisen



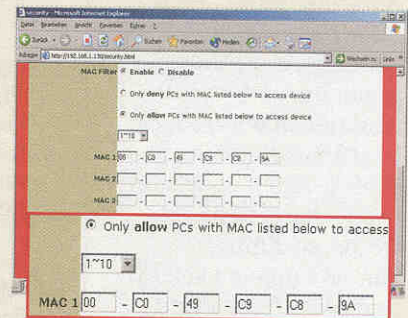
Nach dem Start der Software erscheint der Access-Point in einer Liste. Legen Sie eine IP-Adresse fest, die Ihrem Netzwerk entspricht – etwa 192.168.1.130, wenn Ihr Computer 192.168.1.129 hat. Die Netzmaske in dem Fall ist 255.255.255.0. Öffnen Sie dann einen Browser und geben Sie die IP-Adresse in die Adresszeile ein.

### 5. NIC-Software installieren



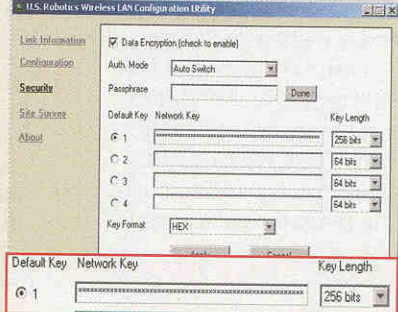
Auch wenn Funknetzkarten unter Windows ohne die mitgelieferte Software grundsätzlich funktionieren, sollten Sie unbedingt die mitgelieferten Utilities installieren. Zum einen haben Sie dann Zusatzfeatures, beispielsweise können Sie Energiesparoptionen einstellen. Zum anderen können Sie in der Software die Verschlüsselung aktivieren.

### 3. MAC-Adressen sperren



Das Kennwort im Auslieferungszustand steht im Handbuch und muss unbedingt geändert werden. Es wird in der Regel abgefragt, wenn Sie Ihren Browser zum AP verbinden. Suchen Sie dann den Menüpunkt, in dem Sie die MAC-Sperre aktivieren können. Die MAC-Adressen Ihrer Karten sehen Sie mit dem Befehl `ipconfig /all` bzw. mit `wiwinpcfg` bei Windows 9x und ME.

### 6. WEP-Key lokal eingeben



Die meisten Access-Points verlangen einen Reboot, wenn ein WEP-Schlüssel eingestellt wurde. Nach dem Neustart bekommt Ihr Computer keine Verbindung mit dem Netz mehr, da er den Schlüssel nicht kennt. Geben Sie nun denselben WEP-Key im Konfigurationstool Ihrer Netzwerkkarte ein. Davor müssen Sie gegebenenfalls auch die Schlüssellänge anpassen.

ren, gibt es die WEP-Verschlüsselung: Wired Equivalent Privacy. Bei der Auslieferung von kabellosem Netzwerkzubehör ist die Verschlüsselung allerdings grundsätzlich abgeschaltet, damit die Geräte direkt nach dem Einstecken funktionieren. Außerdem ist die Konfiguration der Verschlüsselung häufig nicht komfortabel: Einen Schlüssel muss der Anwender meistens von Hand im HEX-Format eingeben.

Perfekt ist die WEP-Verschlüsselung auch nicht: Lediglich ein statischer Schlüssel soll die Daten schützen. Außerdem müssen Hacker aufgrund einer zusätzlichen Sicherheitslücke nur etwa 800 MByte transferierte Daten mitlesen. Dann kann eine spezielle Software den WEP-Schlüssel berechnen und der Hacker ist im Netz. Für private Netzwerke reicht der WEP-Schutz in der Regel aber aus, wenn keine allzu geheimen Daten in freigegebenen Ordnern liegen.

## Sicherer Schutz ist kompliziert

Der Hersteller Cisco übertrifft in puncto Sicherheit den Wifi-Standard. Bei der Wireless-LAN-Serie Aironet

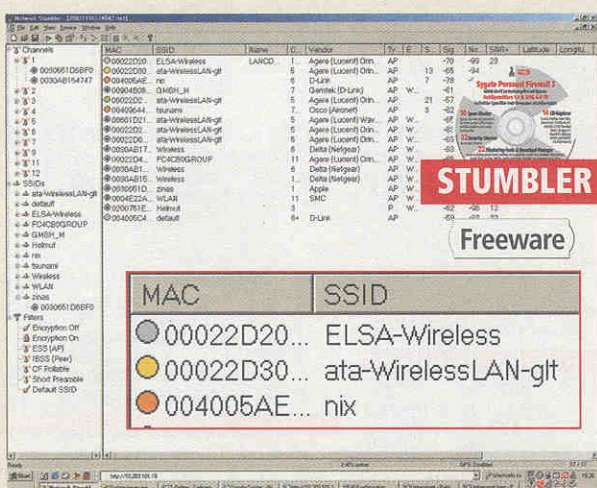
gibt es zwar auch eine WEP-Verschlüsselung mit einem festen Key. Allerdings ist die statische Verschlüsselung nicht so unsicher wie nach Wifi, da keine schwachen Initialisierungsvektoren verwendet werden.

Noch professioneller, aber einen Cisco-Sicherheitsserver erfordernd, ist das so genannte Dynamic WEP. Es wechselt den Schlüssel in bestimmten Zeitabständen: Ein geknackter Code wäre also nutzlos, sofern sich überhaupt genügend Daten mit demselben Schlüssel auffangen ließen.

Auch ohne spezielle Hardware, aber dann deutlich komplizierter, ist mehr Sicherheit möglich. Virtual Private Networks (VPN) sind zwar gedacht, um zwei Netzwerke über einen verschlüsselten Datentunnel im Internet zu verbinden, bieten aber auch bei kabellosen Netzwerken einen vergleichsweise sicheren Schutz – richtige Konfiguration natürlich vorausgesetzt.

Der Nachfolger der WEP-Verschlüsselung, WPA, macht bereits vor seiner Einführung Schlagzeilen:

## Netstumbler findet jedes WLAN



Das kostenlose Programm Netstumbler ist das bekannteste Tool für Windows um Funknetzwerke aufzufinden. Netstumbler führt eine aktive Suche nach Access-Points durch. Er veranlasst die Netzwerkkarte so genannte Probesignale zu versenden. Access-Points antworten auf diese Anfragen. Sobald der Stumbler eine Antwort von einem bislang unbekannten Zugangspunkt empfängt, zeigt er einen neuen Eintrag im Programmfenster an. Auf den ersten Blick erkennen Hijacker, also Leute, die auf der Suche nach Wireless LANs sind, ob es sich dabei um ein verschlüsseltes oder unverschlüsseltes Netz handelt. Außerdem wird die Signalstärke in Ampelfarben dargestellt: Ein grüner Punkt steht für besten Empfang.

Anhand der MAC-Adresse und einer Herstellerdatenbank ist Netstumbler auch in der Lage, nach einem empfangenen Signal den Hersteller der Netzwerkhardware zu ermitteln. Das ist sehr interessant, denn bei Geräten aus dem Hause Cisco ist das Eindringen ins Netzwerk beispielsweise deutlich schwieriger als bei günstigeren Produkten.

Die aktive Suche nach offenen Netzwerken hat allerdings auch Nachteile: Besonders in Unternehmen mit sensiblen Daten gibt es häufig AID-Dienste: Active Intrusion Detection. Sobald Signale von Netstumbler auftauchen, ist bekannt, dass ein Angriff auf das Netzwerk stattfindet, und das System kann entsprechend reagieren: Eine rabiate Möglichkeit ist, das Funknetz vollständig abzuschalten.

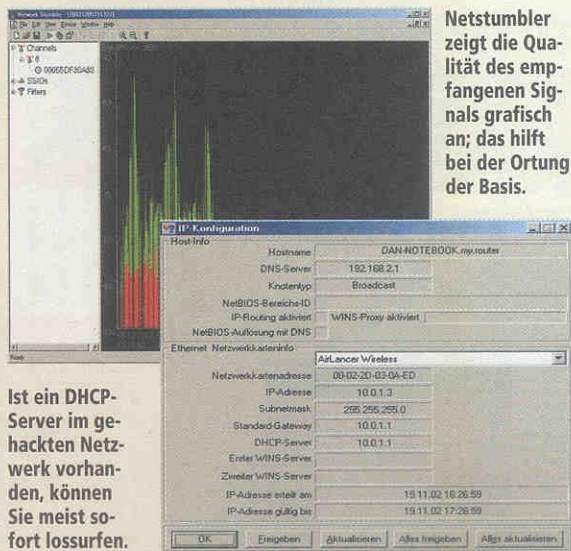
[www.stumbler.net](http://www.stumbler.net)

## Netstumbler stellt die Empfangsqualität grafisch dar

Das Schnüffel-Tool ist sogar in der Lage, empfangene Daten grafisch auszuwerten. Dabei wird die Signalqualität, die auf der Hauptseite in einem farbigen Kreis angezeigt wird, in ein Liniendiagramm eingezeichnet. Je rauschfreier die Verbindung ist, umso höher steigt die Linie an. Ein Doppelklick auf einen Eintrag auf der linken Seite unter Channels öffnet den Graphen für einen bestimmten Kanal. Alternativ kann man auch unter SSID einen bestimmten Access-Point durch einen Doppelklick auswählen und die Qualität der Verbindung zu diesem Zugangspunkt grafisch darstellen lassen.

## DHCP-Server in Netzwerken heißen Hacker willkommen

Sie vergeben automatisch eine IP-Adresse an jeden neuen Client und legen Gateway sowie DNS-Server fest. Das Aktualisieren der IP-Adresse erfolgt bei Windows 95, 98 und ME über das Programm *winnpcfg*. Bei Windows NT, 2000 und XP muss der Befehl *ipconfig/renew* eingegeben werden, damit der Rechner eine neue IP-Adresse anfordert. Die Windows-Versionen 95, 98 und ME eignen sich weniger, um in Netzwerke einzudringen: Wenn der Anwender die IP-Adresse manuell ändert, weil beispielsweise kein DHCP-Server aktiv ist, ist ein Neustart fällig.



Ist ein DHCP-Server im gehackten Netzwerk vorhanden, können Sie meist sofort lossurfen.

Netstumbler zeigt die Qualität der empfangenen Signale grafisch an; das hilft bei der Ortung der Basis.

Die Entwickler scheinen es zu gut gemeint zu haben. Bereits einfache DOS-Attacken (Denial of Service) lösen einen übertriebenen Schutzmechanismus aus: Das gesamte Netzwerk wird für eine Minute gesperrt und keine Daten werden mehr übertragen. Sicher ist das zwar, denn zumindest in dieser Sperrzeit ist ein Eindringen unmöglich – ebenso jedoch Arbeiten oder Surfen.

## Netzwerke aktiv und passiv suchen

Access-Points schicken ununterbrochen Signale, so genannte Beacons. Das zeigt kabellos verbundenen Geräten, dass die Verbindung noch steht, und ermöglicht es anderen Geräten, das Netzwerk zu finden – natürlich auch ungewollten Gästen.

Beim so genannten passiven Scannen ist eine Linux-Software zur Suche Voraussetzung. Die drei bekanntesten Programme sind Aircrack, Kismet und Wellenreiter. Sobald die Netzwerkkarte ein Beacon-Signal empfängt, informiert sie den Benutzer über Signalstärke, Netzwerknamen, MAC-Adresse und

Weiteres. Der Hacker kann sich dann auf die Suche nach einem Ort machen, an dem er eine gute Verbindung hat. Meist reicht es, das Auto ein paar Meter vor- oder zurückzufahren. Es wurden aber auch schon Menschen mit Notebooks kniend auf der Straße gesehen, die einen Zugangspunkt gefunden hatten. Beim passiven Suchen benötigt man eine zweite Netzwerkkarte, um sich mit dem Netz zu verbinden, da die meisten Kartentreiber unter Linux bei aktiviertem Monitor-Modus nicht gleichzeitig senden können.

Mittlerweile gibt es auch für Windows eine Software, die nach kabellosen Netzen sucht. Sie sucht allerdings aktiv, sendet also selbst Signale, um eventuelle Access-Points auf sich aufmerksam zu machen. Keine gute Idee wäre es, mit so einer Software in gut bewachte Netzwerke einzudringen: AID-Systeme (Active Intrusion Detection) sind in der Lage, die Pakete der Software zu entlarven. Der Vorteil dieser Suchmethode ist, dass sich die Wireless-LAN-Karte sofort in ein gefundenes Netz einbucht.

## WLAN-Suche mit Pocket-PC

### Ministumbler für Pocket-PCs

Sozusagen für das schnelle Hijacking zwischendurch gibt es auf der Stumbler-Webseite auch den kleinen Bruder von Netstumbler: den Ministumbler. Er kann auf Pocket-PC-PDAs eingesetzt werden. Selbstverständlich ist eine Funknetzkarte Voraussetzung, wie sie in einigen PDAs bereits eingebaut ist. Zum Nachrüsten gibt es Wireless-LAN-Karten für den Compactflash-Einschub.



## Access-Points mit GPS wiederfinden

Besonders TV-Medien berichteten in letzter Zeit auch über das so genannte Warchalking. Dabei markieren Hacker gefundene Netzwerke mit Kreidezeichnungen an Häuserwänden, Zäunen oder auf der Straße, damit sie wieder gefunden und auch von anderen genutzt werden können. In Deutschland kommen solche Kreidezeichnungen bislang aber kaum vor.

Die moderne Alternative zu den Kreidezeichnungen gibt es in höheren Autoklassen: GPS. Zwar benötigt man kein Navigationssystem, um nach Netzwerken Ausschau zu halten. Doch ein GPS-Empfänger auf dem Autodach ist zumindest in der Lage, die genaue Position zu ermitteln. Fast jedes Schnüffelprogramm kann mittlerweile GPS-Empfänger für USB und die serielle Schnittstelle ansteuern und trägt die Koordinaten neben weiteren Informationen in eine Tabelle ein.

## Das bedeuten MAC, SSID & Co.

**MAC** Weltweit einmalige Seriennummer eines Netzwerkadapters.

**SSID** Service Set Identifier: Der Name eines Funknetzes.

**Name** Zusätzlicher Netzwerkname, in der Regel leer.

**Chan** Der Kanal, auf dem Daten empfangen wurden.

**Vendor** Hersteller der Netzwerkhardware, wird anhand der MAC-Adresse ermittelt.

**Type** Zeigt an, ob es sich um einen Access-Point oder um eine Netzwerkkarte handelt.

**Encryption** Ist die Verschlüsselung des Netzes aktiv, steht hier WEP.

**SNR** Signal to Noise Ratio ist das Verhältnis zwischen Signalqualität und Umgebungsrauschen.

**Signal+ / Noise-** Signalstärke.

**SNR+** Verhältnis zwischen Signalqualität und Umgebungsrauschen.

**Latitude** Breitengrad, wird aus optionalem GPS-Empfänger ermittelt.

**Longitude** Längengrad, wird aus optionalem GPS-Empfänger ermittelt.

**First seen** Datum und Uhrzeit, wann das jeweilige Netzwerk zuerst entdeckt wurde.

**Last seen** Datum und Uhrzeit, wann das jeweilige Netzwerk zuletzt empfangen wurde.

**Flags** Dieses Feld zeigt die Netzwerkstruktur. 0001 bedeutet Infrastructure, 0002 steht für Ad-hoc-Betrieb ohne Access-Point.

**Beacon Interval** Der Wert gibt an, wie häufig ein Access-Point seine Beacon-Signale versendet.

## Eindringlinge sind willkommen

Manchmal haben Hacker aber auch einfach nur Glück. Direkt nachdem Netstumbler ein Netz gefunden hat, bucht sich das Notebook in selbiges ein – dann ist zumindest kein MAC-Adress-Schutz eingestellt. Ein verschlüsseltes Netz markiert Netstumbler mit einem kleinen Schloss.

Besonders in Privatnetzen erhalten die Eindringlinge häufig vom DSL-Router oder Access-Point gleich eine IP-Adresse per DHCP und können sofort im Internet surfen. Läuft kein DHCP-Server, ist für viele Eindringlinge erst mal Schluss. Dann heißt es, übliche IP-Adressen durchzuprobieren. In Privat- und Firmennetzen finden häufig die IP-Adressen 192.168.0.X, 192.168.1.X, 10.0.0.X, 10.0.1.X sowie 172.30.0.X und 172.30.1.X Verwendung. Der Hacker probiert lediglich diese Bereiche durch, indem er seinem Notebook etwa die Adresse 192.168.0.222 gibt, also eine Adresse, die wahrscheinlich noch nicht belegt ist. Dann startet er einen Scan, ob irgendeine andere IP-Adresse in diesem Bereich aktiv ist – wenn ja, ist er im Netz.

# T-Online macht es Hackern leicht

**W**er einen T-Online-Zugang nutzt, gilt für den marktführenden DSL-Provider immer als Vertragsinhaber. Dabei kann der Provider Mitnutzer, die über denselben Zugang zur gleichen Zeit online gehen, nicht unterscheiden. Sie haben dieselben Rechte wie der Anschlussinhaber, sie dürfen also ohne weitere Kennwortabfrage E-Mails abrufen, auf das Homepage-Verzeichnis zugreifen, persönliche Vertragsdaten einsehen und sogar Vertragsbedingungen, wie etwa den gewünschten Tarif, ändern. Dies gilt auch für ungewollte Mitnutzer, die sich per Wireless LAN in das Netzwerk einklinken und denselben Zugang nutzen.

Netzwerk-Hijacker haben vollen Zugriff auf das Portal <http://service.t-online.de>, da die Verbindung mit der Kennung des T-Online-Kunden aufgebaut wurde. Ein Klick auf *Tarif wechseln* reicht beispiels-

weise aus, um den vollen Namen des Anschlussinhabers inklusive Adresse herauszufinden. Auch ein Tarifwechsel wäre durchführbar, ebenso kann man die Inhaberadresse ändern. Auf dieser Seite gibt es außerdem Premium-Rate-Dienste, wie das kostenpflichtige Versenden von SMS. Auf den Kosten bliebe dann der echte Anschlussinhaber sitzen, doch immerhin gibt es hier einen Kennwortschutz. Bedeutend schlimmer ist die Tatsache, dass das Abfragen der E-Mails ohne Kennwort erfolgt. Auf der Serviceseite von T-Online heißt es: „Outlook Express verlangt die Eingabe von Kontoname und Kennwort. (T-Online wertet diese Angaben jedoch nicht aus, da die Identifikation bereits bei der Einwahl mit Ihren T-Online Zugangsdaten erfolgt.)“ Ein gefundenes Fressen also, denn um E-Mails des Opfers abzufragen, müssen WLAN-Hijacker nur den Server [pop.t-online.de](http://pop.t-online.de) abrufen.

## Rechtsanwalt Christian Czirnich im Interview

### 1. Darf man passiv (mit einer Linux-Software, die nicht selbstständig sendet und nur empfangene Datenpakete sichtbar macht) nach Wireless LANs suchen?

Derzeit grundsätzlich ja. Es ist weder verboten, Wireless LAN im Notebook an beliebigen Orten zu verwenden, noch wird man aktiv tätig um fremde Netze zu nutzen. Der eingesetzte Wireless-LAN-Empfänger zeigt nur an, dass er sich im Bereich eines Netzwerkes befindet. Verboten ist jedoch jegliche weitere Nutzung des fremden Netzwerks oder die Mitteilung an Dritte, dass sich an einer bestimmten Stelle ein Funk-LAN befindet. Markierungen, die anderen mitteilen, dass man hier ungestört auf Kosten anderer surfen kann, sind damit verboten.

### 2. Darf man aktiv (mit Windows-Software, die Probesignale sendet, um Access-Points ausfindig zu machen) nach kabellosen Netzwerken suchen?

Auch dies ist derzeit zulässig. Mit Inkrafttreten der Cybercrime Convention und ihrer Umsetzung in deutsches Recht soll jedoch jegliches Abhören oder Ausspionieren von Funknetzen verboten werden.

### 3. Ist es verboten, kabellos übertragenen, vollständig unverschlüsselten Netzwerkverkehr mitzulesen?

Nach § 202a Strafgesetzbuch nicht, denn die Daten sind nicht besonders vor dem Zugriff von außen geschützt. Sofern ein Wireless LAN aber unter das Telekommunikationsgesetz fällt, kann ein Verstoß gegen das Abhörverbot (§ 86 TKG) vorliegen, womit eine Strafe von bis zu zwei Jahren drohen kann. Hiernach ist der Empfang von Nachrichten, die nicht für einen selbst bestimmt sind, worunter auch Datenverkehr zu verstehen ist, unzulässig.

### 4. Mache ich mich strafbar, wenn sich mein Windows-Notebook ohne mein Wissen oder

### mit meinem Wissen in ein ungeschütztes, fremdes Wireless LAN einbuucht?

Bucht man sich unbeabsichtigt in ein fremdes Wireless LAN ein, macht man sich hiermit noch nicht strafbar. Dringt man hingegen absichtlich ein, auch in ein nur mittels der üblichen Technik geschütztes Netzwerk, liegt ein Verstoß gegen § 202a Strafgesetzbuch und eventuell auch § 86 Telekommunikationsgesetz vor. Zwar ist das Eindringen an sich nicht strafbar, jedoch sind sämtliche Daten, auch die Verzeichnisstruktur oder Dateinamen des fremden Netzwerks, vor Zugriff besonders geschützt. Sobald man von diesen Kenntnis erlangt, liegt daher ein Ausspähen von Daten im Sinne des Strafgesetzbuchs vor.

### 5. Darf ich in geschützte Funknetzwerke eindringen?

Nein. In dem Moment, in dem man die Verzeichnisstruktur des fremden Netzwerks angezeigt bekommt, liegt ein Verstoß gegen § 202a Strafgesetzbuch vor. Das Bundesjustizministerium vertritt die Ansicht, dass bereits die im Wireless LAN implementierte Verschlüsselung ausreicht, um die Daten als vor Zugriff besonders geschützt anzusehen. Dies kann mit bis zu drei Jahren Haft geahndet werden.

### 6. Darf ich aus einem fremden Netzwerk Dateien aus freigegebenen Ordnern laden?

Nein. Damit liegt definitiv ein Verstoß gegen § 202a Strafgesetzbuch vor.

### 7. Darf ich fremde Gateways nutzen, um im Internet zu surfen?

Nein. Hierdurch wird dem Betreiber des Wireless LANs finanzieller Schaden zugefügt, während man selbst Aufwendungen spart. Man macht sich hiermit nach § 263a Strafgesetzbuch strafbar und gleichzeitig auch Schadensersatzpflichtig.

| Ihre Kundendaten    |                     |
|---------------------|---------------------|
| T-Online Nr.        | 000000000000-0001   |
| T-Online Tarif      |                     |
| Vorname Name        | Wilhelm Mustermann  |
| Straße und Hausnr.* | Beispielstraße 19   |
| PLZ, Ort*           | 01011   Musterstadt |

Unter <http://service.t-online.de> haben Hacker ungeschützten Zugriff auf persönliche Daten des Anschlussinhabers. Der Screenshot wurde in einem Vorort von München gemacht. Der Betreiber des privaten Heimnetzwerkes war sich der Sicherheitslücke nicht bewusst. Aus Gründen der Diskretion haben wir die Daten ausgetauscht.

| let's warchalk..!              |                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| KEY                            | SYMBOL                                                                                                                    |
| OPEN NODE                      | ssid<br><br>bandwidth                |
| CLOSED NODE                    | ssid<br><br>bandwidth                |
| WEP NODE                       | ssid access contact<br><br>bandwidth |
| blackbeltjones.com/warchalking |                                                                                                                           |

Erfahrene WLAN-Hijacker verlassen ihr Haus niemals ohne Tafel- oder Straßenkreide und obige Karte. Findet ein Hacker ein Netzwerk, markiert er die Stelle mit Kreide auf der Straße oder auf dem Gehweg. Die Symbole (von oben nach unten) zeigen ein ungeschütztes Netzwerk, ein Netz mit MAC-Adress-Schutz sowie ein verschlüsseltes WLAN.