


Rheinische Post – Ersch.-Ort: Düsseldorf – Deutschland

Medientyp:	Tageszeitung	Gedr. Auflage:	435434
Erscheinungsdatum:	31.10.2006	Verk. Auflage:	390746
Seite:	12	Verbr. Auflage:	407538
		Reichweite:	1156000

Sicher drahtlos ins Internet

Ohne lästige **Kabel** von überall im Internet unterwegs. Heute die angenehmste Art, im Web zu surfen. Doch viele **verschlüsseln** ihren Zugang nicht. Wie sich PC-Anwender schützen und gegen **Mit-Surfer** wappnen können.

VON SILKE FREDRICH

DÜSSELDORF So gut wie kein Internet-Provider verzichtet mehr darauf: Kunden, die einen DSL-Anschluss beantragen, bekommen meist kostenlos einen WLAN-Access Point oder WLAN-Router dazu, um drahtlos ins Internet gehen zu können. Praktisch ist das schon, bequem vom Sofa aus online gehen zu können. Doch wer seinen PC per Kabel mit dem Internet verbindet, hat es zumindest in einem Punkt besser: Kein Nachbar oder Fremder kann sich hier einfach so einklinken und mitsurfen – das würde einfach auffallen, wenn hier plötzlich ein Kabel mehr eingesteckt wäre.

Beim drahtlosen Internet, WLAN, sieht das anders aus. Zwar kann man so überall in der Wohnung bequem ins Netz. Auch mehrere Leute gleichzeitig. Aber: Die Funkwellen der WLAN-Zentrale machen nicht Halt an Haustür oder Wohnungsgrenzen. Und das ist durchaus ein ernstzunehmendes Sicherheitsrisiko. Denn natürlich können nicht nur die eigenen Familienmitglieder sich in das WLAN-Netz einklinken, sondern jeder, der einen Computer mit WLAN hat und sich in Reichweite des Funksignals aufhält. Denn WLAN kann bis zu 100 Meter weit funken.

Erreicht also problemlos auch die Nachbarwohnungen. Selbst auf der Straße kann das Funksignal empfangen werden. Mit speziellen Schnüffelprogrammen können findige Betrüger bequem herausfinden, ob es in der näheren Umgebung ein offenes WLAN-Netz gibt. Der WLAN-Test des Computernotdienstes PC-Feuerwehr hat ergeben, das jeder vierte Zugang in Deutschland ungeschützt ist. Das sei zwar weniger als im vergangenen Jahr, dennoch sei die Quote laut PC-Feuerwehr immer noch viel zu hoch. Dabei kann ein ungeschütztes Netzwerk sogar rechtli-

che Folgen haben. Nach einem Urteil des Landgerichts Hamburg (AZ 308 O 407/06) können Anwender mithaftbar gemacht werden, wenn Dritte ein ungeschütztes WLAN missbrauchen. Hintergrund ist die so genannte Störerhaftung.

Und die Schnüffelprogramme haben es in sich: Das Programm zeigt die Funkqualität des Netzwerks an. Das Problem: Klinken sich Fremde ins WLAN-Netz ein, bemerken Anwender das nicht unbedingt und die böse Überraschung kommt mit der nächsten Internet-Rechnung. Denn wer keinen Internet-Pauschaltarif hat, muss natürlich die Internetsitzungen der Einbrecher mitbezahlen. Außerdem können die Einbrecher sogar auf die Festplatte zugreifen, falls die nicht ausreichend geschützt ist. Mit folgenden Tipps wird das Funk-Netzwerk sicher:

Tipp 1 Diskretion Der WLAN-Sender muss unbedingt zur Diskretion verpflichtet werden. Normalerweise sendet dieser unentwegt eine Art Erkennungssignal. So kann jeder Computer mit WLAN bequem Kontakt herstellen. Ein unnötiges Sicherheitsrisiko, denn Anwender wissen ja, wie das WLAN-Netz heißt. Deshalb sollte der SSID genannten Sendecode im WLAN-Sender abschalten. Das geht ganz bequem mit Hilfe der Kontrollmenüs im WLAN-Sender.

Tipp 2 Verschlüsselung Computer und WLAN-Sender unterhalten sich rege per Funk miteinander. Die Daten flitzen dabei normalerweise in Klartext durch die Luft. Jeder kann mit lesen. Deshalb sollte der Funk unbedingt verschlüsselt werden. Computer und WLAN-Station tauschen die Daten dann mit einem Geheimcode aus. Webseiten und E-Mails bleiben vertraulich. Fremde können nicht mehr einfach alles mitlesen. Dazu in den Menüs des WLAN-Senders die Verschlüsse-

lung ausdrücklich einschalten. WEP oder WPA genannt. Danach ein geheimes Kennwort eintragen, das erzeugt den Schlüssel – fertig. Danach muss noch in jedem Computer, der drahtlos Kontakt herstellen will, exakt dieser Schlüssel eingetippt werden. Auch wichtig: Jeder WLAN-Sender ist durch ein Passwort geschützt. Die meisten PC-Benutzer behalten das vom Hersteller eingestellte Passwort bei oder schalten es sogar ab. Das ist schlecht. Denn so kann jeder Hacker ganz bequem Ihren WLAN-Zugang manipulieren. Deshalb unbedingt das Passwort im Gerät ändern.

Tipp 3 Pings ignorieren Grundsätzlich sollten Internetanwender vorsichtig und eher misstrauisch eingestellt sein. So sollte man zum Beispiel nicht auf so genannte Pings antworten. Bei Pings handelt es sich um Rechneranfragen nach Datenpaketsendungen. Wenn der eigene Rechner solche Anfragen beantwortet und Datenpakete weitersendet, können leicht Daten herausgefunden werden wie zum Beispiel welcher Router sich hinter der IP-Adresse versteckt. Dies lässt sich leicht vermeiden, indem Nutzer auf solche Pings einfach nicht antworten.

INFO

Wireless LAN

Das kabellose lokale Netzwerk bezeichnet ein „drahtloses“ lokales Funknetz. Das Kürzel „Wi-Fi“ wird oft fälschlich mit WLAN gleichgesetzt. Im Gegensatz zum Wireless Personal Area Network (WPAN) haben WLANs größere **Sendeleistungen** und Reichweiten und bieten im Allgemeinen höhere Datenübertragungsraten. Die Antennen handelsüblicher Endgeräte lassen 30 bis 100 Meter Reichweite auf freier Fläche erwarten. Mit neuester Technik sind sogar 80 Meter in geschlossenen Räumen möglich.



Wer zu Hause über WLAN ins Internet geht, braucht keine **lästigen Kabel** mehr. Da wird das Arbeiten viel entspannter.

FOTO: T-MOBILE