



Medientyp:	Tageszeitung	Gedr. Auflage:	154380
Erscheinungsdatum:	06.10.2008	Verk. Auflage:	111234
Seite:	40-41	Verbr. Auflage:	111883
		Reichweite:	270000

So machen Sie Ihr WLAN sicher

Wo die Gefahren lauern – und wie Sie Eindringlinge einfach aussperren

HAMBURG
Strippen ziehen war gestern – schon neun Millionen deutsche Haushalte gehen über ein WLAN-Funknetzwerk ins Internet. Das ist bequem, aber auch riskant. Denn: Die Funkwellen des WLAN haben eine hohe Reichweite und dringen mühelos durch Mauern. So können Hacker sich mit einem Laptop Zugang zum Netzwerk verschaffen und sensible Daten rauben. Die MOPO zeigt, wie sie ihr WLAN gegen Eindringlinge absichern.

► Die Gefahren

Bei vielen WLAN-Routern sind die Sicherheitseinstellungen standardmäßig deaktiviert. So geht die Installation des Netzwerkes zwar schnell, in der Folge kann sich aber jeder in Funk-Reichweite an Ihrem Netzwerk vergreifen. Achtung: Fremde Nutzer könnten Ihr Netzwerk nutzen, um etwa Kinderpornografie zu downloaden. „Wenn jemand über Ihren Internet-

zugang strafbewehrte Inhalte herunterlädt, gelten Sie erstmal als Verdächtiger“, mahnt Matthias Gärtner vom Bundesamt für Sicherheit in der Informatik.

► Daten verschlüsseln

Um das Netzwerk zu schützen, müssen die gesendeten Daten verschlüsselt werden. Die meisten WLAN-Netzwerke lassen

sich mit einer „WEP“-Verschlüsselung sichern: Im WLAN-Konfigurationsprogramm finden sich unter dem Menüpunkt „Encryption“ oder „Security“ die Verschlüsselungseinstellungen. Dort muss das WEP-Passwort aktiviert werden. Gibt man dieses Kennwort bei den Netzwerk-PCs ein (unter Start/Systemsteuerung/ Netzwerkverbindung/Drahtlosnetzwerkinstallation), ist das WLAN gegen die meisten Angriffe gesichert. Deutlich besser als WEP ist aber eine WPA-Codierung. Deshalb: Schon beim Kauf des Routers fragen, ob das Gerät eine WPA- oder WPA2-Verschlüsselung unterstützt.

► Zusätzlicher Schutz

Da auch die Verschlüsselung keine absolute Sicherheit bietet, sollten WLAN-Surfer zusätz-

lich eine Firewall besitzen. Dafür empfiehlt sich das Programm „ZoneAlarm“ (Download: www.chip.de). Aber auch ein Sicherheitspaket wie „Kaspersky Internet Security 2008“ (Ca. 40 Euro) bietet effektiven Schutz.

► Hotspots

Durch WLAN-Hotspots ist auch unterwegs kabelloses surfen möglich. Die öffentlichen Netzwerke sind aber in der Regel kaum geschützt – und ein beliebtes Jagdrevier von Datendieben. An Hotspots gilt: Unbedingt die

„Daten- und Druckerfreigabe“ in Windows abschalten, und persönliche Daten nur auf verschlüsselten Websites eingeben. Ob eine Seite sicher ist, erkennen Sie an der Adresse: Steht dort nicht „http://“, sondern „https://“, werden die abgerufenen Daten verschlüsselt. Auch das Mail-Programm „Microsoft Outlook“ bietet Schutz, der ist allerdings gut versteckt: Erst wenn Sie unter Extras/Konten/E-Mail/Eigenschaften/Erweitert das Kästchen „SSL“ anklicken, sind Ihre Mails vor Hackern sicher. **CHRISTOPH HEINEMANN**

Urteil zu WLAN

Ein unverschlüsseltes WLAN-Netzwerk kann auch **rechtliche Folgen** haben. Ermöglicht man es Webganoven durch ein ungeschütztes Netzwerk, **Straftaten im Internet** zu begehen, kann man für die dadurch entstehenden Schäden **mit haftbar gemacht werden**. Das hat das Landgericht Hamburg entschieden (Az.: 308 O 407 / 06). „Wenn zum Beispiel Rechtsanwälte oder Ärzte die ihnen anvertrauten Daten nur mangelhaft schützen, ist **Missbrauch Tür und Tor geöffnet**“, erklärt Michael Kittlitz, Geschäftsführer des Computer-Service „PC-Feuerwehr“. Deshalb sollte ein **Fachmann die Einrichtung** des WLAN-Netztes vornehmen.

Vorsicht, Hacker-Gefahr!

So machen Sie

Ein Laptop benötigt WLAN-Netzwerke sind oft kaum gesichert – so können sich Hacker leicht Zugang verschaffen. Die Vorwärtiger bekommen oft gar nicht mit, dass sie beim surfen manipuliert werden (.).

Ihr WLAN sicher