

Schotten dicht im Funknetzwerk

Wie man Drahtlos-Systeme vor Eindringlingen schützt

Von Till Wortmann

Ein drahtloses Funknetz ist ein ideales Ziel für Hacker – wenn es schlecht konfiguriert und nicht verschlüsselt ist. Wir geben Tipps, wie sich der PC-Nutzer gegen Spione und Trittbrett-Surfer wappnen kann.

Im Funknetz, unter Insidern WLAN (siehe Wortweiser) genannt, flutschen die Daten ohne lästige Kabel von Raum zu Raum. Eigentlich eine tolle Sache. Doch ein Funknetz birgt auch enorme Risiken, über die sich viele Anwender nicht im Klaren sind. Denn die Signale machen nun mal nicht an der Hauswand Halt. Für Datenspione ist die Verlockung groß, offene Netze anzuzapfen und auf fremden Festplatten herumzustöbern.

Höchste Zeit also, Hackern einen Riegel vorzuschieben. Dies geschieht mit Hilfe eines Schlüssels, der aus einer Kombination von Zahlen und Buchstaben besteht. So ein Passwort schottet das Netz nach außen hin vor Unbefugten ab. Doch gerade hier hapert es: Der „WLAN Test 2006“ des Computer-Notdienstes PC-Feuerwehr (www.pc-feuerwehr.de) in Hamburg deckt auf, dass etwa jedes vierte WLAN in Deutschland völlig ungeschützt ist.

Was die wenigsten Anwender wissen: Ein unverschlüsseltes WLAN lädt nicht nur Hacker zur Datenspionage an, sondern kann für den Anwender auch ein rechtliches Nachspiel haben. Nach einem Urteil vom 26. Juli 2006 des Landgerichts Hamburg (Aktenzeichen 308 O 407/06) können Anwender zumindest als Störer mithaftbar gemacht werden, wenn

WORTWEISER

WLAN

Als WLAN (Wireless Local Area Network) bezeichnet man ein drahtloses Netzwerk. Dabei werden der Hauptrechner (Server) mit einer kleinen Funkstation (Wireless Access Point) ausgerüstet und die Zugriffsrechner mit WLAN-Karten. Bei einigen Modellen, den WLAN-Routern, ist sogar noch ein DSL-Modem integriert. Router fungieren als eine Art „Lotse“ im WLAN. Voraussetzung ist, dass PC und/oder Notebook WLAN-fähig sind. Sie las-

sen sich aber einfach mit einem WLAN-Adapter nachrüsten. In Gebäuden werden mit dieser Funktechnik Reichweiten von 40 bis 50 Metern erreicht, im Freien 100 bis 400 Meter. Dritte ein ungeschütztes WLAN missbrauchen (Details unter www.lampmannbehn.de/wlan.html). Insbesondere die Musikindustrie zeigt ein großes Interesse daran, Rechtsverletzungen in PC-Netzen abzumahnern.

Vielen Leuten ist laut Kittlitz offenbar gar nicht bewusst, dass sie ein offenes WLAN betreiben. Der Rat des Experten: „Laien sollten gerade bei moderner Funktechnik immer einen Fachmann mit der Installation beauftragen.“ Aber auch Anwender, die anscheinend alles richtig gemacht haben, sollten sich nicht in falscher Sicherheit wiegen. Die meisten von ihnen nutzen nämlich die als völlig unzureichend geltende WEP-Codierung (siehe eigenen Bericht). Kittlitz warnt: „Das veraltete WEP ist zwar besser als kein Schutz, jedoch keine wirkliche Barriere gegen böswillige Angriffe mehr.“ Der Grund: Mit Hilfe im Internet frei verfügbarer Software wie das eigentlich für Systemadministratoren gedachte Aircrack (www.aircrack-ng.org) ist es selbst für Laien innerhalb weniger Sekunden möglich, in ein mit WEP verschlüsseltes Netz einzubrechen.

Wer auf Nummer sicher gehen will, sollte eine Codierung nach dem aktuellen WPA-Standard oder – noch besser – dem brandneuen WPA2 wählen. Die Anbieter von WLAN Produkten kommen dem PC-Anwender dabei entgegen: „Wir liefern unsere Geräte mit vorinstalliertem WPA aus“, bestätigt Jan Schöllhammer, Produktmanager bei AVM, einem Hersteller von Hard- und Software für DSL und WLAN. Die Codierung haben die Berliner auf die Unterseite ihrer Router namens „Fritz!BOX“ aufgedruckt. Sie lässt sich nachträglich jederzeit ändern.

Neben der Codierung mit WPA kursieren in Fachzeitschriften und Internet-Foren eine Reihe von weiteren Tipps, wie der Anwender sein WLAN optimal vor Hackern schützen kann – wie zum Beispiel mit dem MAC-Accessfilter. Doch Vorsicht: Wer im Konfigurationsmenü seines WLAN-Routers und in den Netzwerkeinstellungen von Windows herumdoktert, kann sich leicht verheddern. Schnell tippt man was Falsches ein und der Zugang

ins Netz ist gesperrt. Da hilft dann nur noch ein teurer Anruf bei der Hotline des Internet-Providers.

So viel Aufwand beim Sichern eines WLANs ist aber zum Glück gar nicht nötig. Schöllhammers Rat: „Letztlich reicht die Ver-

schlüsselung mit WPA2 vollkommen aus.“ Als Schlüssel empfiehlt der Profi kein natürliches Wort zu verwenden, sondern eine nicht zu erratende Kombination aus Ziffern und Buchstaben.



Der zehn Gramm schwere USB-Stick von AVM verschlüsselt Daten nach dem sicheren WPA2-Standard. Preis: rund 50 Euro.



An immer mehr öffentlichen Plätzen, aber auch in vielen Privathaushalten gibt es WLANs. Viele sind ungeschützt. Bilder: Archiv