

Im Internet surfen - ohne ewig lange Strippen zwischen Computer und Telefondose ziehen zu müssen. Mit WLAN ist das kein Problem: Die Daten werden zwischen Computer und einem Empfänger hin und her gefunkt. Und die meisten der zurzeit verkauften Computer haben die dafür nötige Karte schon drin. Aber: Viele Computernutzer sichern ihr Funknetzwerk nicht. Und so ein unverschlüsseltes WLAN ist eine Einladung für Mitbenutzer und für Hacker.

Auf fremden Wellen mitsurfen

Bis zu 300 Metern weit reicht ein WLAN-Netzwerk – in diesem Umkreis können sich andere Computernutzer einklinken und mitsurfen. An sich kein Problem: Dadurch werden nur große Dateien etwas langsamer runter geladen als sonst.

Für Taten anderer bestraft?

Problematisch wird es, wenn über den eigenen Anschluss Kinderpornographie oder Nazipropaganda hoch geladen oder SPAM-Mails verschickt werden. Oder wenn der unbekannte Mitbenutzer massenhaft Musik aus illegalen Tauschbörsen saugt. Dann drohen Schadenersatzklagen oder sogar ein Strafverfahren. Hier muss man erst mal beweisen können, dass man damit nichts zu tun hatte. Das ist extrem ärgerlich und aufwändig. Und es gibt auch Gerichte die ahnungslose WLAN-Besitzer trotzdem dafür haftbar gemacht haben.

Außerdem können Hacker mit wenig Aufwand E-Mails und verschickte Textdateien mitlesen und sehen, welche Webseiten man besucht, wenn man das eigene W-LAN nicht sichert. Bei Passwörtern fürs Online-Banking, für Internetauktionen oder Online-Shopping geht das nicht – noch nicht. Die werden schon vom eigenen Computer aus verschlüsselt gesendet. Das erkennt man am „https“ in der Adresszeile des Browsers.

Eintritt nur mit Schlüssel

Derzeit verkaufte WLAN-Empfänger kommen mit der nötigen Software für die Verschlüsselung. Die muss man nur einrichten. Dabei sollte man drauf achten, dass das so genannte WPA-Verfahren fürs Sichern benutzt wird. Und nicht das ältere WEP-Verfahren - das können Hacker in wenigen Minuten knacken. Der eigene Computer oder die vom Mitbewohner bekommen dann einen Datenschlüssel. Nur mit diesem Schlüssel kann man sich dann ins WLAN einklinken.

„A358Z57OP7Z“ statt „Passwort“

Auch wichtig: Das für den Schlüssel verwendete Passwort sollte möglichst ungewöhnlich oder gleich eine Zahlen-Buchstaben-Kombination sein. Hacker kommen sonst mit einem so genannten Wörterbuchangriff ins WLAN rein – dabei probiert die Hacker-Software alle Wörter aus dem Duden oder auch Namen durch.

MAC-Liste – Nichts zum Essen

Passwörter können Hacker mit etwas Glück herausbekommen. Deshalb ist es sicherer, wenn man das WLAN zusätzlich über die so genannte Access Control Lists – kurz ACL – absichert. Diese Liste nutzt die so genannten MAC-Adressen. Jede Netzwerkkarte – die man fürs WLAN im Computer hat – besitzt eine eigene MAC-Adresse.

Ein Computer kann also über diese Adresse eindeutig identifiziert werden. Damit kommen nur Rechner ins Funknetz, die man vorher mit deren MAC-Adresse in die Adressliste des WLANs eingetragen hat. Hacker können zwar auch eine

WLAN sicher machen – warum muss ich das?

2008

Hardware-Adresse einer Netzwerkkarte fälschen – da gehört aber schon ein gehöriger Aufwand dazu.

Für Laien

Wem das alles zu kompliziert ist, für den bieten Hersteller wie AVM mit der Fritzbox oder auch Linksys oder Buffalo WLAN-Empfänger, die ab Werk mit Verschlüsselung arbeiten.

Für Täter

Das machen viele: Im Urlaub oder unterwegs, sich mal schnell in ein offenes Netzwerk einklinken und ein bisschen surfen (wohlgemerkt: es geht nicht um Hotspots). Hier sollte man wissen: In dem Moment, in dem man sich in das fremde Netz einklinkt – ohne das Wissen des Besitzers – begeht man eine Straftat. Laut Gesetz erfüllt das den Tatbestand des Ausspähens von Daten. Es ist verboten, ein erkanntes Netzwerk zu besuchen, es sei denn der Inhaber hat es ausdrücklich erlaubt.