

Per Anhalter durchs Internet

Drahtlos Surfen ist in. WLAN-DSL-Router für wenig Geld oder gar kostenlos vom Internetprovider machen den Schritt zu mehr Bewegungsfreiheit einfach und ersparen das Kabellegen durch das Wohnzimmer.

Doch Komfort und Mobilität haben auch ihre Schattenseiten: Anders als bei kabelgebundener Kommunikation kann jeder in Reichweite eines Access-Points Funkpakete mitlesen – egal ob von der Straße oder der Nachbarwohnung. Natürlich gibt es technische Maßnahmen um das Funknetzwerk vor ungebetenen Gästen zu schützen. Diese sind aber in den WLAN- Routern im allgemeinen standardmäßig nicht aktiviert. Der Benutzer muss sich darum selber kümmern. Was er erfahrungsgemäß aber nicht immer tut. Ein ein zufälliger Test brachte auch in unseren Wohnhäusern einige völlig frei zugängliche Funknetze zutage.

Schwarz-Surfer und Gelegenheits-Cracker kennen diese Schwächen und nutzen solche offenen Funknetze für Ihre Aktivitäten. Durch das WLAN-Schwarzfahren können dem Besitzer des benutzten Routers unter Umständen Kosten entstehen, wenn dieser einen Zeit- oder Volumentarif für seinen Internetzugang gebucht hat. Doch das ist nicht das Schlimmste, noch ärger kommt es, wenn der Router als Ausgangspunkt für kriminelle Aktivitäten missbraucht wird, etwa zum Einspeisen verbotener oder urheberrechtlich geschützter Inhalte. Die Abmahnung der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) flattert dann dem Falschen in den Briefkasten und bei möglichen zivilrechtlichen Klagen ist es für das Opfer schwierig seine Unschuld zu beweisen.

Und nicht zu vergessen Ihr eigenes Netz - die daran angeschlossenen Rechner sind dabei durch einen möglichen unkontrollierten Zugriff auf Ihre Daten ebenso gefährdet.

Um daher eine ähnliche Sicherheit des Datenaustauschs wie beim Kabel zu erreichen, sollten Sie die folgenden vier Konfigurationsschritte an Ihrem WLAN-Router überprüfen und gegebenenfalls ausführen um somit einen Mindestschutz für Ihr Funknetzwerk herzustellen.

Zur Vereinfachung der Konfiguration empfiehlt es sich, eine kabelgebundene Verbindung zu benutzen. Dass zufällige Mitlauschen eines Einbrechers wird damit ebenfalls vermieden.

Routerpasswort setzen

Der WLAN-Router selbst stellt ein lohnendes Ziel da, er enthält schließlich die Provider-Zugangsdaten die zum Missbrauch verlocken.

Ein gutes Router-Passwort ist keinesfalls das vom Hersteller vorgegebene, es besteht aus mindestens 8 Ziffern und Buchstaben in gemischter Groß- und Kleinschreibung. Sonderzeichen und Umlaute sind oft problematisch und sollten nicht benutzt werden. Das Passwort darf nicht in Namenslisten oder Wörterbüchern auftauchen, da die üblichen Cracker-Tools solche Wortlisten zuerst durchprobieren.

Wer sich nicht selbst kreativ genug fühlt, um eine Zufallskombination zu erfinden benutzt einfach einen Passwortgenerator, wie er z.B. unter folgendem Link im Internet zu finden ist: <http://www.anonym-surfen.com/service/passwort-generator/>

Fernkonfiguration ausschalten

Die zweite Lücke die es zu schließen gilt ist die Fernkonfiguration (Remote Management). Wer diese Funktion nicht dringend braucht um z.B. den Router über das Internet zu warten, schaltet sie ab.

WLAN verschlüsseln

Der dritte Schritt ist die Verschlüsselung des Funknetzwerkes zum Schutz vor ungebetenen Mit-Surfern. Zwei Verfahren stehen zur Auswahl: „Wi-Fi Protected Access“ (WPA) sowie das ältere und nicht so sichere „Wired Equivalent Privacy“ (WEP). Wenn alle Stationen im LAN damit zurechtkommen, ist WPA die erste Wahl. Das WPA Passwort, auch WPA-Key genannt, sollte mindestens 20 Zeichen lang sein und aus allen möglichen Zeichen gemischt sein, die das Web-Interface des Routers korrekt überträgt. Als Verschlüsselungsverfahren sollte Advanced Encryption Standard (AES) oder Temporal Key Integrity Protokoll (TKIP) eingestellt werden.

Wer WEP zur Verschlüsselung benutzen muss, und das ist immer noch besser als gar keine

Verschlüsselung, findet einen Generator zur Erzeugung einer entsprechenden hexadezimalen Zufallszahl unter folgendem Link: <http://www.zugerweb.ch/keygen.asp.asp#anker>

802.1x abschalten

Über das Protokoll IEEE 802.1x versorgt der Access-Point die Clients automatisch mit dem WEP- oder WPA-Schlüssel. Diese Funktion ist aber nur in sehr großen Netzwerken sinnvoll einzusetzen. Wenn der Router also eine 802.1x-Einstellung hat (kann auch „Automatic Key Distribution“ heißen) sollten Sie diese als vierten Schritt der Grundsicherung deaktivieren.

Clientseitig müssen Sie die Verschlüsselung ebenfalls aktivieren und den WPA-Key eintragen, unter Windows erledigen Sie dies unter „drahtlose Netzwerkverbindung“ in den Eigenschaften des jeweiligen Netzwerkes. Für WPA empfiehlt sich unter Windows XP ein installiertes Service Pack 2, Mac OS X unterstützt WPA ab Version 10.3.

Die vier grundlegenden Konfigurationsschritte schließen eilige Einbrecher und normale Schnorrer aus dem WLAN aus. Ein mit WPA und einem guten Passwort gesichertes Netz ist nach dem Stand der Technik sogar einbruchsicher.

Wer tiefer in die Sicherung seines Netzes einsteigen will, findet auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) <http://www.bsi.de/literat/doc/wlan/wlan.pdf> ein ausführliches Papier zur WLAN-Sicherheit.

*Jens Ostmann
Moll 8*