

Diese Meldung kann unter <http://www.presseportal.de/pm/31385/1609822/sicheres-wlan-drahtloses-netzwerk-nur-bei-bedarf-aktivieren-tuev-rheinland-ungeschuetztes-netz> abgerufen werden.

TÜV Rheinland AG

Sicheres WLAN: Drahtloses Netzwerk nur bei Bedarf aktivieren

TÜV Rheinland: Ungeschütztes Netz birgt Sicherheitsrisiken
Routerpasswort ändern
Netzwerk ausreichend verschlüsseln

07.05.2010 - 10:00 Uhr, TÜV Rheinland AG

Köln (ots) - Ob am Küchentisch, auf dem Balkon oder im Garten - rund 40 Prozent aller deutschen Haushalte mit Internetanschluss nutzen WLAN (Wireless Local Area Network) für den drahtlosen Zugang ins Netz. Das ergab eine Umfrage des Bundesverbandes Bitkom. Was aber viele Nutzer nicht wissen: Eine unverschlüsselte WLAN-Verbindung birgt ein erhebliches Sicherheitsrisiko. "Jeder, der sich in der Reichweite eines ungesicherten drahtlosen Funknetzes befindet, kann leicht dieses Netzwerk missbrauchen. So kann ein Eindringling etwa urheberrechtlich geschütztes Material aus dem Internet laden oder auch strafrechtlich relevante Inhalte", warnt Klaus Rodewig, IT-Sicherheitsexperte von TÜV Rheinland. "Und das kann für den WLAN-Betreiber nicht nur teuer werden, sondern er riskiert unter Umständen sogar eine Strafanzeige, Hausdurchsuchung und die Beschlagnahme seiner Computer."

Doch mit wenigen Handgriffen können Nutzer diesen Sicherheitsrisiken entgegenwirken. WLAN-Nutzer sollten beim Einrichten ihres drahtlosen Netzwerks auf jeden Fall das Routerpasswort ändern. "Sonst haben Hacker beim Datenzugriff leichtes Spiel, etwa so, als würde man Einbrecher direkt durch die offene Haustür lassen", warnt der Experte. Denn: Einige Hersteller vergeben bei den Werkseinstellungen der Router die gleichen Standardpasswörter für mehrere Geräte - was auch den Hackern bekannt ist. Zudem muss der Nutzer bei der Einrichtung den Namen des drahtlosen Netzwerks, die sogenannte SSID (Service Set Identifier), vergeben. Hier gilt, wie auch bei den anderen Passwörtern: keine kurzen oder bekannten Namen wie etwa "WLAN" oder "Zuhause" wählen, um dem potenziellen Angreifer das Knacken der Verschlüsselung zu erschweren. Denn je nach Verschlüsselungsart des WLANs dient die SSID als ein Baustein der Verschlüsselung. So können Außenstehende nicht gleich Rückschlüsse auf den Betreiber ziehen.

Weiterhin sollten Verbraucher bei der Konfiguration des WLAN-Routers die richtige Verschlüsselung wählen. "Am besten eignet sich hierfür die Verschlüsselungsart WPA2", rät Rodewig. "Sie lässt sich zurzeit nicht knacken." Doch eine Schwachstelle gibt es: das einmalig zu vergebende Passwort, den so genannten Preshared key (PSK). Nur wenn er sich schwer knacken lässt, gewährleistet WPA2 genügend Sicherheit. "Das Passwort sollte aus zufälligen Kombinationen von Buchstaben und Zahlen bestehen und möglichst lang sein", erklärt der IT-Experte. "Je länger, desto besser." Bei Nichtgebrauch sollten WLAN-Nutzer überdies stets das Funknetzwerk abschalten, oder - wenn kein Schalter vorhanden - den Stecker ziehen. Denn ohne Verbindung kein Datenklau!

Ihr Ansprechpartner für redaktionelle Fragen:

Jörg Meyer zu Altenschildesche, Presse, Tel.: 0221/806-2255
Die aktuellen Presseinformationen erhalten Sie auch per E-Mail über presse@de.tuv.com sowie im Internet: www.tuv.com/presse

Originaltext:

TÜV Rheinland AG

Pressemappe:

<http://www.presseportal.de/pm/31385/tuev-rheinland-ag>

Pressemappe als RSS:

http://presseportal.de/rss/pm_31385.rss2