Straftaten huckepack: Zehn Prozent der Speyerer Haushalte haben ihr Internet nur unzureichend geschützt

DRUCK

In immer mehr Haushalten wird das Internet genutzt. Laut statistischem Bundesamt waren 2012 etwa 77 Prozent der Deutschen ein- oder mehrmals täglich im weltweiten Datennetz unterwegs. Meist findet der Computer mittels WLAN, das ist eine Funkverbindung, über einen so genannten "Router" seinen Weg ins Internet. Diese Funkverbindung kann aber auch eine Sicherheitsschwachstelle sein, wenn der Datenaustausch nicht ausreichend verschlüsselt ist.

Wir wollten wissen, wie es in Speyer mit der Internetsicherheit bestellt ist. Am Rosenmontag durchstreiften wir gemeinsam mit den Internet-Spezialisten von "Colab", einem gemeinnützigen Unternehmen, das sich der beruflichen Qualifizierung von Jugendlichen verschrieben hat, mit dem Auto das Stadtgebiet von Speyer. Ein Computer mit Spezialsoftware erfasste zwischen 9:00 Uhr und 11:30 Uhr 2.263 WLAN-Verbindungen stichprobenartig sowohl in Bereichen mit Blockbebauung als auch Einfamilienbebauung.

Das besorgniserregende Ergebnis war, dass etwa zehn Prozent der gemessenen Anschlüsse nicht ausreichend gesichert waren. So hatten 3,27 Prozent (74) gänzlich ungeschützte Funknetze, 7,07 Prozent (160) solche mit ungenügender Verschlüsselung.

Besonders schlecht war die Sicherung der Netze in Speyer Nord auf der Höhe Weißdornweg und in Speyer West im Bereich um die Straße im Erlich. Die restlichen Stadtteile lagen alle gut im Schnitt. Nur das Neubaugebiet auf dem Dupré-Gelände ragt heraus, denn es hält den Positiv-Rekord mit vorbildlicher Verschlüsselung an allen gemessenen WLAN Anschlüssen.

Diejenigen mit nicht ausreichend geschützten WLAN-Verbindungen gehen ein hohes Risiko ein, denn es können sich Straftäter über solche Anschlüsse sozusagen huckepack anonym ins Internet einloggen und beispielsweise Musik oder Filme illegal herunterladen, was eine Urheberrechtsverletzung darstellt, die mit hohen Strafen geahndet wird. Auch Pädophile können solch einen Anschluss für ihre schmutzigen Machenschaften nutzen, ohne dass sie erkannt werden. Wer sich heimlich Zugang verschafft, der nutzt die Internetkennungen des Anschlussbesitzers. So wird dieser auch bei Straftaten über seinen Anschluss erst einmal zur Rechenschaft gezogen, wenn er nicht beweisen kann, dass er zur Zeit der Straftat beispielsweise in Urlaub war.

In einem Urteil machte der Bundesgerichtshof im Mai 2010 unmissverständlich klar: "Auch Privatpersonen, die einen WLAN-Anschluss in Betrieb nehmen, ist es zuzumuten zu prüfen, ob dieser Anschluss durch angemessene Sicherungsmaßnahmen hinreichend dagegen geschützt ist, von außenstehenden Dritten für die Begehung von Rechtsverletzungen missbraucht zu werden. Der Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses ist adäquat kausal für Urheberrechtsverletzungen, die unbekannte Dritte unter Einsatz dieses Anschlusses begehen."

Hintergrund

Der Hintergrund dieser Aktion ist es, die Wahrnehmung der Gefahren und Verantwortungen im heimischen WLAN-Netz zu schärfen. Denn längst ist es nicht mehr so einfach zu sagen: „Wer mein WLAN nutzt, begeht eine Straftat." Wer sein Netz nicht mit Hilfe eines Passwortes oder einer anderen Authentifikation schützt, muss damit rechnen, als Störer für etwaige von anderen im eigenen Netz begangenen Straftaten haftbar gemacht zu werden. Auch ist die Zumutbarkeit eines passenden Schutzes des WLAN im Privatbereich im stetigen Wandel, somit wird man als Endnutzer immer mehr in die Pflicht genommen, für seine Funknetze weitere Verantwortung zu übernehmen.

Hierbei kann getrost die Verschlüsselung "WPA2" empfohlen werden, die derzeit als ausreichend sicher gilt und von jedem gängigen aktuellen Gerät unterstützt wird.

Wichtig ist jedoch, dass eine WEP Verschlüsselung keine Sicherheit mehr bieten kann. Sollten sich noch Geräte im Haushalt befinden, welche nur eine WEP Verschlüsselung unterstützen, ist dringend die Anschaffung einer zeitgemäßen Netzwerkkarte zu empfehlen. Diese gibt es beim Fachhändler bereits zu einem Preis von etwa 20 Euro.

Besonderes Augenmerk sollte man auch auf die Wahl eines sicheren Passwortes legen. In diesem sollten keine Wörter aus dem Wörterbuch vorkommen, es sollte Zahlen, Buchstaben (Klein- und Großschreibung) und bestenfalls Sonderzeichen enthalten. Auch sollten keine persönlichen Daten im Passwort enthalten sein.

Sollten sich Anwender nun nicht sicher sein, ob bei ihrem Netzwerk Handlungsbedarf besteht, so sollten sie sich fachlichen Rat beispielsweise bei "Colab" holen.

Wired Equivalent Privacy (WEP, engl. „Verdrahteten (Systemen) entsprechende Privatsphäre") ist das ehemalige Standard-Verschlüsselungsprotokoll für WLAN. Es sollte sowohl den Zugang zum Netz regeln als auch die Vertraulichkeit und Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen gilt das Verfahren als unsicher. Die Berechnung des Schlüssels aus einigen Minuten an aufgezeichneten Daten dauert normalerweise nur wenige Sekunden. Daher sollten WLAN-Installationen die sicherere WPA2-Verschlüsselung verwenden. (ks/spa)

Info: www.colab.de