IT+Technik

Vorsicht **Funkwellen**

Sicheres W-LAN? Auch per **Knopfdruck**? Im Gegensatz zum kabelgebundenen Netzwerk lassen sich die Teilnehmer eines drahtlosen Netzwerks nicht im Vorhinein beschränken. Deshalb sollte man hier besondere Vorsicht walten lassen.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Das unsichtbare Netzwerk umgibt uns regelmäßig mit seinen Wellen und ist – ausreichende Ausleuchtung durch den Router vorausgesetzt – auch unser treuer Begleiter auf dem Weg durch die eigenen vier Wände. Da jedoch unter anderem die Frage der Störerhaftung bei W-LANs die deutschen Gerichte beschäftigt, sollten Sie Ihr W-LAN immer gut absichern.

Alte Standards wie WEP („Wired Equivalent Privacy“) und WPA („Wi-Fi Protected Access“), die oftmals noch in aktuellen Geräten unterstützt werden, sind nicht mehr sicher. Einzig die ohne größeren Aufwand zu realisierende Absicherung mittels Passwort unter Verwendung der **WPA2-Verschlüsselung** gilt als sicher.

802.11 a/b/g/n/ac

802.11 a/b/g/n/ac – Der Standardreihe des amerikanischen Instituts IEEE („Institute of Electrical and Electronics Engineers“) sind schon mehrere Fassungen entsprungen, die vorgenannten sind die für den Heimgebrauch geläufigen. Der derzeit häufig in Werbeprospekten anzutreffende Standard 802.11ac schafft derzeit ca. 1.300 Mbit/s, also mehr als das Doppelte dessen, was der Vorgänger 802.11n maximal leisten kann (600 Mbit/s). Die regelmäßigen Leistungssteigerungen werden durch unterschiedliche Ansätze ermöglicht – Nutzung von Frequenzbändern mit weniger Störquellen (Stichwort: „5-GHz Band“), größere Kanalbandbreiten und der Einsatz von mehreren Sende- und Empfangseinrichtungen (MIMO – Multiple Input Multiple Output). Aber auch hier gilt: Die Aufstellung des Gerätes sowie die Ausrichtung der Antennen kann wesentlich für die Geschwindigkeit sein – und nicht zuletzt die Wahl des Kanals, auf dem gefunkt wird.

Hierbei empfiehlt es sich, vorkonfigurierte Passwörter (erst recht solche wie „admin“, „1234“) zu ändern. Ein **starkes Passwort** mit 12 Zeichen oder mehr, nicht aus einem Wörterbuch, angereichert mit Zahlen und Sonderzeichen ist angemessen und muss ja in der Regel nicht täglich eingegeben werden. Für die Konfigurationsoberfläche des Routers ist oftmals auch eine Passworteingabe erforderlich oder zumindest möglich – diese sollten sie auf jeden Fall aktivieren und hierfür nicht dasselbe Kennwort wie für Ihr W-LAN verwenden.

Die Aufnahme weiterer Kommunikationspartner per Knopfdruck (WPS – Wi-Fi Protected Setup) sollten Sie mit Vorsicht genießen. Sofern Sie den Dienst dauerhaft aktiviert haben und für die Bestätigung nur ein 4-stelliger Code eingegeben werden muss, kann sich ein Angreifer per einfachem Ausprobieren („Brute-Force“ – englisch für Rohe Gewalt) relativ leicht in Ihrem Netzwerk anmelden. Um den Zugang zum Netzwerk stärker zu reglementieren, kann man in manchen Geräten das Aufnehmen neuer Endgeräte aktiv unterbinden – aber **Vorsicht**, das gilt auch für Ihre neueste technische Anschaffung wie Fernseher oder Tablet und gerät schon mal schnell in Vergessenheit.

Für den professionellen Einsatz gedacht ist die Authentifizierung von Clients gegen einen sogenannten RADIUS-Server, bei dem mittels **Zertifikat** geprüft werden kann, ob die Verbindung hergestellt oder unterbunden wird. Für die Arztpraxis und hier insbesondere für Netze mit Patientendaten sind **physikalische Netzwerkverbindungen**, also das klassische LAN, vorzuziehen. Denn die physische Barriere in Form von Türen und Wänden erschwert den ersten Schritt zum Zugriff schon erheblich.

Foto: iStockphoto