ExpertEmo

Verschlüsselung

Ein Teil des WLAN-Standards ist die Wired Equivalent Privacy (**WEP**)-Verschlüsselung. Die darin enthaltene Verschlüsselung mit einem nur 40 Bit (64 Bit genannt) bzw. 104 Bit (128 Bit genannt), bei einigen Herstellern auch 232 Bit (256 Bit genannt) langen statischen Schlüssel reicht jedoch **nicht** aus, das WLAN ausreichend zu sichern.

Durch das Sammeln von Schlüsselpaaren Angriffe möglich. Es gibt Programme, die in der Lage sind das Passwort zu entschlüsseln bzw. zu berechnen.

Der Nachfolger des WEP ist der neue Sicherheitsstandard WPA. Er bietet eine erhöhte Sicherheit durch die Verwendung von TKIP bei WPA bzw. AES bei WPA2 und gilt zur Zeit als nicht zu entschlüsseln, solange keine einfachen Passwörter verwendet werden, die über eine Wörterbuch-Attacke geknackt werden können. Als Empfehlung kann gelten, mit einem Passwortgenerator Passwörter zu erzeugen, die Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sind.