



WLAN

WLAN ist eine Abkürzung für Wireless Local Area Network (drahtloses lokales Netzwerk), also ein lokales Funknetzwerk, mit dem zwei oder mehr Endgeräte miteinander verbunden werden. Die Anbindung an das Internet erfolgt über eine Kabelverbindung oder über Mobilfunk.

WLAN beruht auf einem Funkstandard, der vom Institute of Electrical and Electronical Engineers (kurz IEEE) festgelegt wurde. Das Institut ist ein weltweiter Verband von Ingenieur:innen mit Sitz in den USA, der neben der Herausgabe von Fachzeitschriften auch Gremien zur Standardisierung verschiedener Techniken bildet.

Die dafür nützlichen Frequenzen werden in Österreich von der Rundfunk und Telekom Regulierungs-GmbH (RTR) vergeben, die als Geschäftsstelle der Kommunikationsbehörde Austria und der Telekom-Control-Kommission arbeitet.

Wi-Fi wird häufig gleichbedeutend für WLAN verwendet. Wi-Fi bezeichnet im engeren Sinn aber die Zertifizierung von Produkten durch die Wi-Fi Alliance. Damit soll gewährleistet werden, dass verschiedene Wireless-Geräte miteinander funktionieren.

Technik

Ein WLAN besteht meistens aus mehreren Endgeräten, die sich per Funk mit einem Access Point bzw. einem WLAN-Router verbinden. Mit handelsüblichen Geräten lässt sich dabei auf freier Fläche eine Reichweite von 30 bis 100 Meter erzielen. In Gebäuden hängt die Reichweite stark von den räumlichen Gegebenheiten ab. Wände, Decken oder Fenster können je nach verwendetem Material die Reichweite verringern oder, falls die Materialien als Reflektoren wirken, auch erhöhen.

Der Datenaustausch zwischen den Endgeräten erfolgt über den Access Point. Dieser stellt das Zentrum des WLAN dar und übernimmt wichtige Verwaltungsaufgaben wie z.B. die Wahl des

Frequenzbandes, des Funkkanals, der Bitrate und Sicherheitseinstellungen. Ein aktueller WLAN-Standard ist 802.11ax. Hier sind theoretisch Bitraten bis zu 9,6 Gbits/s möglich. Dafür stehen die beiden lizenzfreien Frequenzbänder 2,4 GHz und 5 GHz zur Verfügung. Jedes dieser Frequenzbänder ist in mehrere Kanäle unterteilt. Durch die Lizenzfreiheit und die starke Verbreitung von WLANs sind diese Kanäle z.B. in vielen Mehrfamilienhäusern aber schon stark überlastet.

Für den Austausch von Daten werden von den einzelnen Geräten sogenannte Datenpakete gebildet. Diese bestehen aus den Daten im engeren Sinn, einem Header und einer Prüfsumme. Jeder Funkkanal kann zu einem bestimmten Zeitpunkt immer nur von einem Gerät verwendet werden, um ein Datenpaket zu senden oder zu empfangen. Je mehr Geräte auf einen Kanal zugreifen, umso weniger Datendurchsatz bleibt für jedes einzelne Gerät. Kommt es zu Kollisionen, müssen bereits gesendete Pakete erneut verschickt werden. Access Points lassen sich so einstellen, dass sie automatisch den am wenigsten benutzten Kanal wählen. Allerdings können Funkkanäle auch durch andere Geräte wie z.B. Bluetooth-Geräte oder Mikrowellenherde genützt bzw. blockiert werden.

Die Anbindung an das Internet erfolgt in der Regel mit einem Modem, welches die digitalen Signale für eine analoge Leitung (z.B. Telefonnetz oder Kabel-TV) verarbeitet. Im privaten Bereich werden dafür häufig Geräte verwendet, die die Funktion des Routers und des Modems vereinen und von Telekommunikationsanbietern zur Verfügung gestellt werden.

Gesellschaftliche Bedeutung

Die Verbreitung drahtloser Netze geht Hand in Hand mit dem Trend zu mehr Mobilität und flexibleren Arbeitsbedingungen. Bereits 2005 wurden in der EU mehr Notebooks verkauft als Desktop-Rechner, die meisten davon mit eingebauten WLAN-Chips. Viele andere Geräte sind



mittlerweile so klein, dass sie keinen Anschluss für Netzkabel mehr haben. Zudem ist der Aufbau von Funknetzen im Vergleich zu verkabelten Netzwerkan schlüssen mit weniger Aufwand und Kosten verbunden, zumal wenn größere Bereiche abgedeckt werden. WLAN bietet also einen mobilen Internetzugang für eine Vielzahl von Geräten: Smartphone, Tablet, Laptop, TV, Receiver, Spielkonsolen etc. Und das sowohl in heimischen Wohnzimmern als auch in Hotels oder an öffentlichen Plätzen. Auch bei Musikanlagen kommt WLAN zum Einsatz, da es bei der Übertragung großer Datenmengen bzw. bei größeren Distanzen leistungsstärker als Bluetooth ist. Zunehmend wird WLAN auch zur Lokalisierung der Nutzer verwendet.

Sicherheit

Da sich im WLAN übertragene Daten frei im Raum ausbreiten, können sie theoretisch von jedem, der sich im Empfangsbereich befindet, abgefangen werden. Um das zu verhindern, werden die WLAN-Pakete verschlüsselt. Jedes Gerät verwendet dafür einen eigenen, mit dem Access Point ausgehandelten Schlüssel. Am sichersten ist dafür derzeit das Verschlüsselungsverfahren WPA3 (Wifi Protected Access). Darüber hinaus verfügt ein nicht-öffentliches WLAN in der Regel über einen Passwortschutz. Nur wer das Passwort kennt, kann sich anmelden.

Öffentliche drahtlose Internetzugänge, sogenannte Hot-Spots, sind in diesem Punkt gefährlich: Sie haben meist keinen Passwortschutz und die Daten werden unverschlüsselt gesendet. Dadurch können Daten relativ leicht mitgelesen werden.

Deshalb wird empfohlen, in öffentlichen Netzen keine Online-Überweisungen durchzuführen oder andere sensible Daten zu übertragen. Auch für Software Updates ist es besser, keine Hotspots zu verwenden. Generell sollte das automatische Einwählen in ein WLAN am Smartphone deaktiviert werden.

Quellen und Links

www.rtr.at
(2024-07-24)

<https://academy.technikum-wien.at/ratgeber/wie-funktioniert-wlan>
(2024-07-24)

https://de.wikipedia.org/wiki/Wireless_Local_Area_Network
(2024-07-24)

www.sueddeutsche.de/wissen/sicher-im-wlan-unterwegs-in-fremden-netzen-7-hotspot-sicherheitsregeln-dpa.urn-newsml-dpa-com-20090101-240129-99-797867
(2024-07-24)

www.sueddeutsche.de/digital/kampf-gegen-stoererhaftung-so-schuetzen-sie-sich-in-oeffentlichen-wlan-netzen-1.2726524
(2024-07-24)

www.chip.de/artikel/WPA3-Neue-WLAN-Verschlüsselung-optimal-nutzen_148220425.html
(2024-07-24)

Anmerkungen
