Innerhalb der verschiedenen WLAN-Standards stehen einheitliche Sicherheitssysteme zur Verfügung, die nach dem Kauf aktiviert und gegebenenfalls konfiguriert werden müssen. Damit Datenlangfinger keine Chance haben, reichen einzelne Sicherungsmechanismen nicht aus, sinnvoll ist ein ganzes Maßnahmen-Paket.

Tipps:

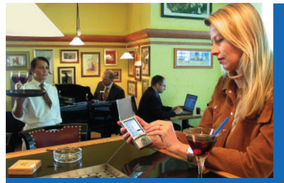
- Voreingestellte Passwörter ändern.
- Netzwerknamen (SSID) ändern und SSID Broadcasting deaktivieren, damit Unbefugte nicht von außen das eigene Netzwerk identifizieren können.
- MAC-Filterung aktivieren, um Nutzerinnen und Nutzer gezielt für das Netz freizuschalten oder zu blocken.
- WEP-Verschlüsselung einschalten, dabei möglichst hohen Verschlüsselungscode von 128 Bit, besser 256 Bit, verwenden.
- WPA-Verschlüsselung (soweit vorhanden) einschalten; Dieses Verfahren ist der WEP-Verschlüsselung vorzuziehen.
- Firewall konfigurieren und verwenden, um unbefugten Zugriff über das Internet zu verhindern.

Generell gilt: Alle Daten, Briefe, Passwörter sind sensibel. Daher sollten die Tipps unbedingt beherzigt werden. Im Zweifelsfall sollten Fachleute die Sicherheitseinstellungen analysieren.

Zum Weiterlesen: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet kostenlos eine ausführliche Information zum Thema „Sicherheit im Funk-LAN“:
http://www.bsi.de/literat/doc/wlan/wlan.pdf

Mit HotSpots online

Ein HotSpot ist ein funkbasierter öffentlicher Internetanschluss, um mit einem Laptop, Webpad oder PDA mit WLAN Karte (WiFi-Standard) im Internet zu surfen, E-Mails abzurufen oder eine VPN-Verbindung zu seinem Firmennetzwerk aufzubauen.



Der HotSpot wird entweder an ein kabelgebundenes Local Area Network (LAN) oder an ein X DSL-Modem angeschlossen. Öffentliche, drahtlose Datennetze existieren z.B. an Flughäfen und Bahnhöfen, in Hotels und Restaurants sowie in Konferenz- und Einkaufszentren.

Die Nutzung des World Wide Web, das Abrufen und Versenden von E-Mails bzw. die Einwahl ins Unternehmensnetz (Voraussetzung hier ist, dass das Endgerät des Nutzers sowie die Firmen-EDV entsprechend vorkonfiguriert wurden) sind in der Regel kostenpflichtig. Teilweise können Stadtinformationen, Informationen zu Flughäfen und Mietwagenverleih kostenlos abgerufen werden.

Der Internetzugang per HotSpot funktioniert mit jedem Betriebssystem, sofern kompatible internetfähige Browser (z.B. Internet Explorer oder Netscape Navigator) installiert sind. Die WLAN-Karten erkennen den HotSpot in der Regel automatisch, wenn er in Reichweite ist. Beim Starten des Internetbrowsers wird automatisch die Anmeldeseite des jeweiligen HotSpot-Betreibers angezeigt. Beim Anmeldevorgang wählt man Preise und Art der Abrechnung aus, bzw. gibt – wenn man schon angemeldet ist – seine Zugangsdaten (Benutzername und Kennwort) ein. Hilfestellung beim Auffinden der HotSpots sowie Informationen zu Provider, Kosten und Abrechnungsoptionen geben u.a. folgende Adressen:

- http://www.portel.de/hotspot_portel
- http://wlan.lycos.de
- http://intel.jiwire.com
- http://mobileaccess.de
- http://www.hotspot-locations.com
- http://www.wifinder.com
- http://www.wi-fihotspotlist.com

Es stehen folgende Zahlungsmöglichkeiten zur Verfügung:

- Prepaidkarte (Voucher), die ein gewisses Zeitguthaben fürs Surfen bereitstellt
- Kreditkarten
- Postpaid; Abrechnung erfolgt mit der Handy- oder Telefonrechnung

Weitergehende Informationen

- http://www.munlv.nrw.de
- http://www.isis.de
- http://www.bsi.de/literat/doc/wlan/wlan.pdf

Glossar

Bluetooth	Funktechnologie für den Nahbereich (bis 10m)
IEEE	Institute of Electrical and Electronic Engineers (Standardisierungsinstitut in den USA)
MAC-Filter	Media Access Control (gewährt nur bestimmten MAC-Adressen Zugang zum WLAN)
PCMCIA	Personal Computer Memory Card International Association
PCI	Peripheral Component Interconnect Bus (Standard für Erweiterungssteckplätze im Computer)
SSID	Service Set Identifier (eindeutige Kennzeichnung für Datenpakete über WLAN)
UMTS	Universal Mobile Telecommunications System (Mobilfunktechnik der 3. Generation zur Übertragung von Sprache und Daten)
UWB	Ultra Wide Band (Funktechnologie mit sehr hoher Geschwindigkeit)
VPN	Virtual Private Network (private Verbindung über das öffentliche Internet)
WEP	Wired Equivalent Privacy (Verschlüsselungsverfahren)
WPA	WiFi Protected Access (Verschlüsselungsverfahren)
WLAN	Wireless Local Area Network (kabelloses lokales Netzwerk)
WiFi	Wireless Fidelity (Zertifikat für WLAN-Karten)

Diese Broschüre ist im Rahmen des **Aktionsprogramms Umwelt und Gesundheit Nordrhein-Westfalen** (APUG NRW) in Kooperation mit der Verbraucherzentrale Nordrhein-Westfalen und der Firma ISIS Multimedia Net GmbH & Co. KG, Düsseldorf entstanden. Weitere Informationen zum Aktionsprogramm Umwelt und Gesundheit NRW finden Sie im Internet unter: **www.apug.nrw.de**

Umwelt Naturschutz Landwirtschaft Verbraucherschutz Eine Welt

Herausgeber Ministerium für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen
Abteilung Immissionsschutz

Fotos ISIS Multimedia Net GmbH & Co. KG

Gestaltung DIALOGIK GmbH, Aachen

Druck RITTERBACH Medien GmbH, Frechen

Stand September 2004

Gedruckt auf 100% Recyclingpapier mit Umweltzeichen

Funknetztechnik WLAN

Tipps und Informationen

NRW.

Ministerium für **Umwelt** und **Naturschutz, Landwirtschaft** und **Verbraucherschutz** des Landes Nordrhein-Westfalen

Mobile Kommunikation mit WLAN

Die Zukunft der Informationstechnik liegt in der mobilen, drahtlosen Kommunikation. Weit verbreitet ist inzwischen das Telefonieren mit dem Handy. Die drahtlose Vernetzung zwischen Computern oder zum Internet mit der Funknetztechnik WLAN nimmt an Bedeutung zu. WLAN steht für Wireless Local Area Network, zu deutsch: Ein kabelloses, lokales Netzwerk.

Die Einsatzbereiche für WLAN sind vielfältig:

In **Privathaushalten** kann WLAN beispielsweise genutzt werden, um in verschiedenen Räumen kabellos einen Zugang zum Internet einzurichten. WLAN ermöglicht auch die gemeinsame Nutzung von Ressourcen wie z.B. Drucker oder Speicher bis hin zur kompletten Vernetzung der gesamten Hauselektronik.

An besonders belebten und stark frequentierten **öffentlichen Einrichtungen** und Plätzen wie z.B. Messen, Flughäfen, Bahnhöfen, Hotels, Restaurants

oder Einkaufszentren kann man mit WLAN über sogenannte HotSpots online gehen.

In **Unternehmen** wird immer häufiger WLAN eingesetzt, um mobile Arbeitsplätze an das Firmennetzwerk anzuschließen. Auch im Rahmen der Prozess- und Maschinenüberwachung zeichnen sich Anwendungsmöglichkeiten ab.

Universitäten, **Schulen** und Bildungseinrichtungen nutzen WLAN, um durch die Installation eines Funknetzwerkes z.B. eine begrenzte Zahl von Laptops flexibel in den Unterricht einzubringen.

WLAN-Technik

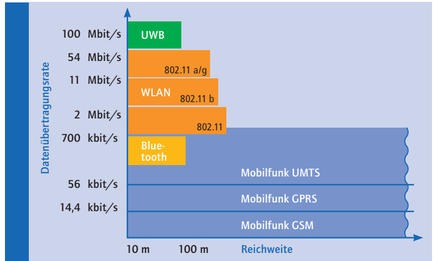
Funknetzwerke werden – je nach Einsatzzweck – auf zwei Arten betrieben:

Im Ad-hoc-Modus kommunizieren die Endgeräte direkt per Funk über kürzere Entfernungen miteinander. Im Infrastruktur-Modus dagegen werden die mobilen Rechner über feste Basisstationen (Access Points) miteinander verbunden, um größere Abstände zwischen den verschiedenen Geräten zu überbrücken. Zugleich werden über den Access Point die drahtlosen Verbindungen zu und zwischen den mobilen Rechnern organisiert und können als Schnittstelle zum Festnetz und damit auch zum Internet genutzt werden.

Neuere PCs oder Laptops sind häufig bereits beim Kauf WLAN-tauglich. Um ältere Geräte für WLAN zu nutzen, muss man diese mit einem Netzwerk-Adapter ausrüsten. Eine Nachrüstung erfolgt meist über den Einbau einer PCMCIA-Karte oder PCI-Karte in den Rechner. Ein externer Anschluss des Adapters ist z.B. über die USB-Schnittstelle möglich.

Die meisten auf dem Markt befindlichen WLAN-Systeme arbeiten nach dem Standard IEEE 802.11. Nach IEEE 802.11 erfolgt die Funkübertragung im lizenzfreien 2,4 bzw. 5,0 GHz-Frequenzband. An dem Buchstaben, der hinter der Nummer 802.11 steht, erkennt man wie schnell die Daten übertragen werden. 802.11 b ist beispielsweise der Standard, der WLAN bekannt gemacht hat und der weltweit zur Zeit am meisten verbreitet ist. Die maximale Datenrate beträgt hier 11 Mbit/s. Der IEEE 802.11-Standard wurde so konzipiert, dass er durch andere Funkquellen nicht gestört wird.

Geräte mit dem sogenannten WiFi-Logo gewährleisten die Kompatibilität von Geräten verschiedener Hersteller. Im 2,4-GHz-Band darf die Strahlungsleistung des Senders maximal 100 Milliwatt betragen. Damit lassen sich - je nach räumlicher und baulicher Situation - Reichweiten von etwa 30 Metern in Gebäuden und 300 Metern außerhalb von Gebäuden erreichen. Durch den Einbau von Zusatzantennen können verschiedene Ausbreitungsrichtungen und Reichweiten realisiert werden.



Brutto-Datenübertragung und Reichweiten drahtloser Kommunikations- und Datendienste

Die WLAN-Technik unterscheidet sich von anderen Funktechnologien wie UMTS, Bluetooth oder UWB darin, dass sie in einem anderen Frequenzbereich arbeitet. Zudem sind Reichweiten und Übertragungsraten unterschiedlich. Während z.B. der Mobilfunk auf die Versorgung der Fläche ausgelegt ist, bleibt der Datenverkehr bei WLAN auf lokale Funkinseln beschränkt.

Für die Einrichtung eines WLANs ist keine Genehmigung erforderlich.

Gesundheit

Mit der Verbreitung von schnurlosen DECT-Telefonen, Bluetooth, WLAN & Co nimmt die Belastung durch elektromagnetische Felder in Privathaushalten und an Arbeitsplätzen insgesamt zu. Deshalb sollte man auf Möglichkeiten zur Minimierung der Belastung achten.

Zum Schutz vor den gesundheitlichen Auswirkungen durch elektromagnetische Felder wurden vom Gesetzgeber Grenzwerte festgelegt, die den menschlichen Körper vor zu starker Erwärmung schützen. Ob darüber hinaus aber mit weiteren Gesundheitsrisiken zu rechnen ist, konnte bisher nicht ausreichend geklärt werden.

Die Sendeleistung bei WLAN ist mit 100 Milliwatt vergleichsweise gering, so dass die Strahlenbelastung in typischen Gebrauchsabständen zu WLAN-Komponenten deutlich unterhalb der eines Handys oder eines DECT-Telefons liegt.

WLAN-Systeme halten die derzeitigen Personenschutzgrenzwerte ein. Solange in der Wissenschaft bei der Bewertung der gesundheitlichen Auswirkungen noch Unsicherheiten bestehen, sollte auch bei WLAN Vorsorge getroffen werden. Um vermeidbaren Risiken vorzubeugen, sollten die WLAN-Systeme so aufgebaut und betrieben werden, dass Personen, die sich in der Nähe des Netzwerkes befinden, möglichst wenig hochfrequenter Strahlung ausgesetzt sind.

Geräte/ Anlage	Frequenz in Giga Hertz	Abstand in Meter	Leistungsflussdichte in Watt pro Quadratmeter
WLAN-Netzwerkkarte	2,4	0,5	0,005 - 0,1
WLAN-Access Point	2,4	2,0	0,0005 - 0,01
DECT-Basisstation	1,9	1,0	0,007 - 0,02
GSM-Handy	0,9	0,1	12,5 - 42,5
GSM-Mobilfunkbasisstation	0,9	verschieden	0,00001 - 0,1

Vergleich der Immissionen von WLAN mit anderen Funktechnologien (typ. Messwerte)

Tipps:

- Strahlungsarme Geräte kaufen (hierzu Testergebnisse vergleichen)
- Access Point nicht in Schlaf- oder Kinderzimmer installieren
- Access Point im Abstand von ca. 2 Metern von Daueraufenthaltsbereichen installieren (z.B. im Flur)
- Access Point bei Nichtgebrauch ausschalten
- Während der Nutzung möglichst großen Abstand zum WLAN-Endgerät (z.B. PC) einhalten
- WLAN-Endgeräte ausschalten, wenn sie nicht benutzt werden (z.B. bei WLAN-Karten in PCs: Einschalten der Stromsparfunktion)
- WLAN-Karte deaktivieren oder aus dem Gerät entfernen, wenn die WLAN-Funktion nicht benötigt wird

Datensicherheit

Da Funkwellen nicht an der Hauswand oder der Grundstücksgrenze halt machen, besteht bei WLAN die Gefahr, dass Unberechtigte auf private, betriebliche oder behördliche Daten zugreifen oder Internetverbindungen auf fremde Kosten mitnutzen.

WLAN-Experten fordern angesichts der Missbrauchsgefahr mehr Sensibilität im Umgang mit der neuen Technik: Wo sicherheitsrelevante Daten ausgetauscht werden, muss das WLAN gut geplant und installiert sein. Die Datenverschlüsselung ist ein absolutes Muss!