

# WLAN – Aber sicher!

Ein Praxisleitfaden für kleine- und mittlere Unternehmen (KMU)



**Mainfränkisches Electronic Commerce**

**Kompetenzzentrum (MECK)**

Sedanstraße 27, 97082 Würzburg

<http://www.meck-online.de>

Gefördert durch das Bundesministerium für Wirtschaft und Technologie (BMWi).

Trägereinrichtungen des MECK:



**Handwerkskammer  
für Unterfranken**

**Autoren:**

**Jaufmann, Oliver**

**Jeschke, Georg**

**Zeidler, Marc**

## Gliederung

<b>1</b>	<b>Netzwerke .....</b>	<b>4</b>
1.1	ISO/OSI-Referenzmodell.....	4
1.2	Lokale Netze .....	5
1.2.1	Ethernet .....	5
1.2.2	Token Ring.....	6
1.3	Weitverkehrsnetze.....	6
<b>2</b>	<b>Übertragungsmedien .....</b>	<b>8</b>
2.1	Kabel .....	8
2.1.1	Kupferkabel.....	8
2.1.1.1	Koaxialkabel .....	9
2.1.1.2	Twisted Pair .....	10
2.1.2	Lichtwellenleiter .....	11
2.2	Funk .....	12
2.2.1	WLAN.....	13
2.2.1.1	IEEE 802. 11x-Standards.....	15
2.2.1.2	Störquellen und Dämpfung .....	17
2.2.1.3	Werkzeuge zur Positionierung und Abstimmung der Access Points.....	19
2.2.2	Bluetooth.....	21
2.2.3	Richtfunk.....	22
2.3	Sicherheitsrelevante Aspekte bei Funknetzen.....	22
<b>3</b>	<b>WLAN Verbindungsgeräte .....</b>	<b>25</b>
3.1	WLAN Adapter.....	25
3.2	Access Points .....	25
3.3	Router.....	25
<b>4</b>	<b>Maßnahmen zur Absicherung von WLANs .....</b>	<b>27</b>
4.1	Planungsphase.....	28
4.2	IP-Management.....	28
4.3	SSID .....	28
4.4	MAC-Filter.....	29
4.5	Verschlüsselung und Authentifizierung.....	29
4.5.1	Wireless Equivalent Privacy (WEP) .....	30
4.5.2	Wi-Fi Protected Access (WPA) .....	30
4.5.3	802.1x.....	31
4.5.4	802.11i.....	31
4.5.5	Virtual Private Network (VPN) im WLAN .....	31
4.5.6	Internet Protocol Security (IPSec) .....	32
4.5.7	Secure Socket Layer (SSL) .....	33
<b>5</b>	<b>Weitere Schwachstellen in Netzwerken und Gegenmaßnahmen .....</b>	<b>34</b>
5.1	Schwachstelle „Mitarbeiter“ .....	34
5.2	Unerlaubte Zugriffe auf Netze von außen.....	35
5.2.1	Firewall .....	35
5.2.2	Monitoring und Intrusion Detection Systeme (IDS).....	36
<b>6</b>	<b>Fazit .....</b>	<b>37</b>
	Quellenverzeichnis.....	38

# 1 Netzwerke

Rechnernetze bestehen aus mehreren, für sich gesehen autonomen Computern, die über eine bestimmte Technologie miteinander verknüpft werden. Die Auffassung, dies müsse unbedingt über die Kabeltechnologie geschehen, ist überholt. Heute werden mehr und mehr Rechnernetze über Funk aufgebaut und bieten so ein hohes Maß an Flexibilität. Auf ihrem „Weg durch die Luft“, sind die Daten aber spezifischen Risiken ausgesetzt. Diese aufzuzeigen und adaptierte Lösungen anzubieten, ist die Idee des vorliegenden Leitfadens. Zuvor wollen wir uns jedoch mit der Technologie der Rechnernetze vertraut machen.

## 1.1 ISO/OSI-Referenzmodell

Die International Organization for Standardization (ISO) hat ein Modell vorgeschlagen, das die Kommunikation offener Systeme abstrakt beschreibt und in sieben Schichten (Layer) unterteilt: Das OSI-Referenzmodell (OSI = Open Systems Interconnection). „Offene Systeme“ sind offen für die Kommunikation mit anderen Systemen [TANE03, S. 54]. Auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik erhält man unter [www.bsi.bund.de/gshb/deutsch/m/m04090.html](http://www.bsi.bund.de/gshb/deutsch/m/m04090.html) einen umfassenden Einblick in den Aufbau und die Funktionsweise dieses Modells. Die sieben Schichten (Abbildung 1) sind hierarchisch aufeinander aufgebaut.

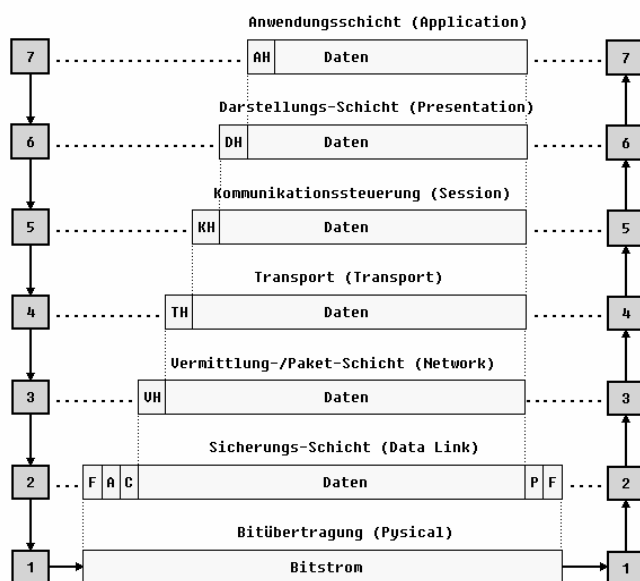


Abbildung 1: Das ISO/OSI-Referenzmodell aus [PLAT04]

Jede erfüllt bei der Kommunikation der Systeme eine spezifische Aufgabe und stellt Dienste zur Verfügung, die von der nächst höheren Schicht benutzt werden. Die Er-

klärung und Bewertung des OSI-Referenzmodells ist nicht Gegenstand dieses Beitrags. Eine ausführliche Abhandlung dazu findet sich auch in [TANE03, S. 54-58]. Bei der Übertragung der reinen Bitdatenströme bewegt man sich auf der untersten Schicht des ISO/OSI-Referenzmodells.

## 1.2 Lokale Netze

Lokale Netze (LANs = Local Area Networks) sind private Netze innerhalb eines Geländes oder eines Gebäudes. Die Reichweite solcher Netzwerke ist begrenzt. Die miteinander verbundenen Computer und Workstations tauschen über das Netzwerk Informationen aus und benutzen gemeinsame Ressourcen wie Drucker, Scanner und andere Peripheriegeräte. LANs lassen sich anhand der Kriterien

- Größe,
- Übertragungstechnik und
- Topologie (Art der Netzbildung)

unterscheiden. Zwei LAN-Typen, die auch häufig in der Praxis Anwendung finden, werden in den folgenden Abschnitten kurz erläutert.

### 1.2.1 Ethernet

Der zurzeit am weitesten verbreitete Standard für LANs ist das Ethernet. Sein Erfinder Bob Metcalfe guckte sich die Idee vom Wissenschaftler Norman Abramson ab, der an der Universität von Hawaii zu Beginn der 70er Jahre des 20. Jahrhunderts Niederlassungen auf benachbarten Inseln mit dem Zentralrechner über das sogenannte „ALOHANET“ verband. Xerox entwickelte damals den Vorläufer des PC, der allerdings als „Standalone“, das heißt als isoliertes Gerät geplant war.

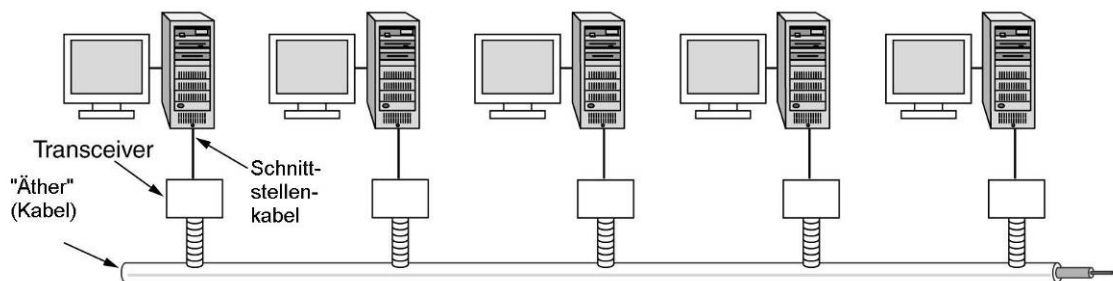


Abbildung 2: Ursprüngliche Architektur des Ethernet [TANE03, S. 85]

Metcalfe übernahm nun die Idee des ALOHANET, um ein kabelgebundenes Netzwerkprotokoll zu entwickeln, das sich in der Folge zum Ethernet weiterentwickelte. Das Übertragungsmedium ist beim ursprünglichen Ethernet ein dickes Koaxialkabel

gewesen, der „Äther“ (siehe Abbildung 2). Die zentrale Idee ist nun, dass jeder Rechner im Ethernet, der Daten an einen anderen Rechner im Netz versenden will, zuerst prüft, ob der Äther bereits zum Datentransfer zwischen anderen Rechnern benutzt wird. Die verantwortliche Einheit, der Transceiver (Abbildung 2) enthält die hierzu notwendige Elektronik. Ist der Äther belegt, verschiebt der Computer sein Vorhaben auf einen späteren Zeitpunkt. Die aktuellen Ethernets folgen immer noch demselben Prinzip. Neue Technologien und Anwendungen (Router, Switch und Hub) ergänzen das bewährte System.

### 1.2.2 Token Ring

Der Token Ring ist eine weitere gängige Technologie, welche den Datenverkehr in einem LAN regelt. Wie der Name schon sagt, geht die Architektur des Token LANs weg von der rein linearen Struktur des Ethernet: Sie ist kreisförmig (Abbildung 3). Ein freies Token (unter Token kann man sich anschaulich ein Staffelholz vorstellen) kreist auf dem Ring. Die Station welche senden möchte, nimmt das Token an sich und ändert es in ein sogenanntes „belegtes Token“ (sie hält nun das Staffelholz in den Händen, das zum Senden berechtigt) und sendet die Nachricht. Unbeteiligte Stationen regenerieren die Signale. Die Zielstation kopiert die Nachricht. Die Quellstation entfernt die Nachricht und generiert ein neues, freies Token. Der Prozess kann von neuem beginnen.

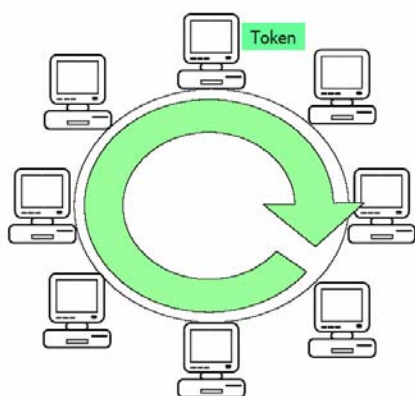


Abbildung 3: Token im Token Ring (eigene Darstellung)

## 1.3 Weitverkehrsnetze

Die Aufgabe der Weitverkehrsnetze oder auch WANs (Wide Area Networks) liegt in der Verbindung der LANs. Nachrichten, die von einem Sender aus dem „LAN A“ zu einem Empfänger in „LAN B“ gelangen sollen, müssen über ein solches WAN gelei-

tet werden. Daher kann ein solches WAN auch als Verbindungsnetz bezeichnet werden (Abbildung 4).

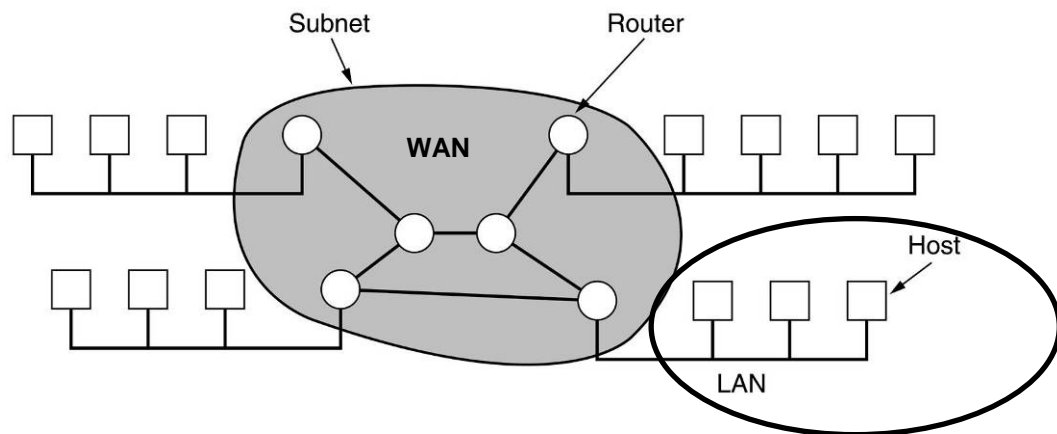


Abbildung 4: WAN als Verbindungsnetz in Anlehnung an [TANE03, S. 35]

Das Verbindungsnetz besteht grob aus zwei Elementen. Den Übertragungsleitungen (Transmission Lines) und den Vermittlungseinheiten (Switching Elements). Die Übertragungsleitungen sind Kupfer- oder Glasfaserkabel, seltener im WAN-Bereich findet man auch Funk oder Richtfunk. Die Vermittlungseinheiten sind spezielle Rechner, die man auch Router nennt, denn sie „routen“ selbstständig eingehende Nachrichten, das heißt sie entscheiden, welchen Weg die Nachricht „gehen“ soll. Das Internet ist wohl das bekannteste WAN. Neben dem Internet gibt es einige andere WANs von Telekommunikationsunternehmen, darunter auch auf Basis von Satellitenkommunikation.

## 2 Übertragungsmedien

Nachdem wir uns jetzt einen groben Überblick darüber verschafft haben, in welcher Weise Computer miteinander verknüpft werden können, widmen wir uns nun im zweiten Abschnitt den zugrunde liegenden Verbindungstechnologien (Abbildung 5):

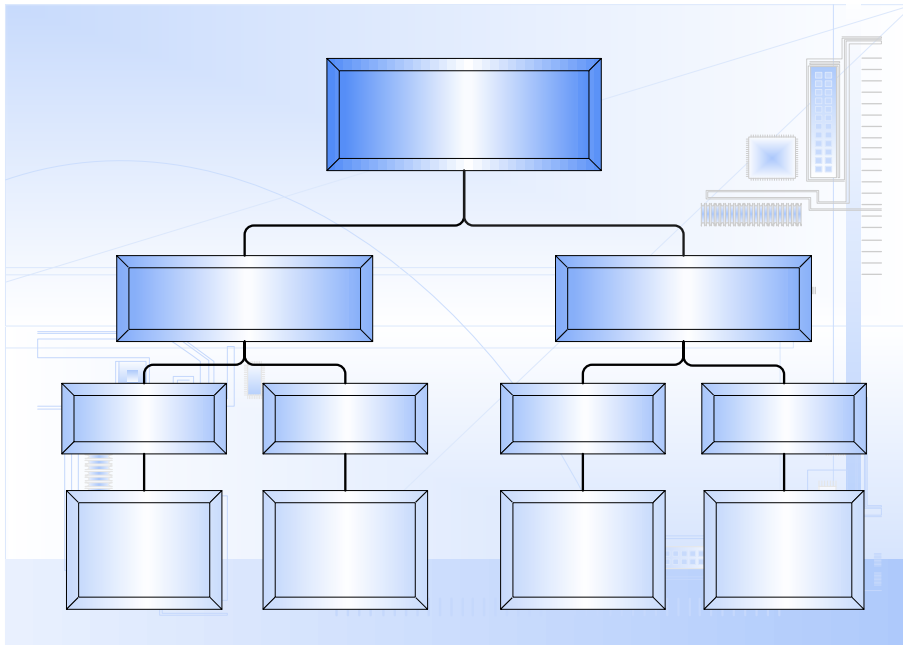


Abbildung 5: Übertragungsmedien (eigene Darstellung)

Übertragungsmedium

### 2.1 Kabel

Die Aufgabe der Verbindungstechnologie ist, die Daten in Form von Bits (ein Bit ist die kleinste denkbare Informationseinheit) über einen Träger zu transportieren. Da der Transport in Form von Impulsen erfolgt, kommen zur Übertragung verschiedene physikalische Medien in Frage. Metallische Leiter (elektrische Impulse), optische Leiter (Lichtimpulse) oder Luft (Funk, Infrarot). In Abschnitt 2.1.1 blicken wir auf metallische Leiter, in Abschnitt 2.1.2 auf Lichtwellenleiter.

#### 2.1.1 Kupferkabel

Als metallischen Leiter findet man in der Regel Kupfer vor. Das liegt an seinem günstigen „Preis-/Leistungsverhältnis“. Gold ist eigentlich ein viel besserer Leiter, aber schlicht zu teuer. Durch Anlegen einer Spannung an den Leiter, erzeugt man elektromagnetische Schwingungen, die aus der Bewegung der Elektronen resultieren und sich über das Kabel ausbreiten. Die unterschiedlichen Frequenzen der Schwingungen werden in Erinnerung an den deutschen Physiker Heinrich Hertz in der Ein-

Kupferkabel

Lichtwellenleiter

gerichtet

Twisted Pair  
Koaxialkabel

Glasfaser

Richtfaser  
„gerichtetes V...

heit Hertz (Hz = Schwingungen pro Sekunde) gemessen. Jeder Kabeltyp unterstützt, je nach seiner Qualität, nur einen begrenzten Umfang an Frequenzen. Den Bereich der Frequenzen die das Kabel unterstützt, nennt man Bandbreite [SIKO03, S. 64]. Der amerikanische Mathematiker und Informatiker Claude E. Shannon (1916-2001) hat eine Formel aufgestellt, mit der man aus der Bandbreite unter Berücksichtigung des so genannten Rauschens (Störgrosse, die durch die thermische Bewegung der Elementarteilchen in der Materie erzeugt wird) die maximale Datenrate eines Kabeltyps berechnen kann: Maximale Datenrate =  $H * \lg(1 + S/N)$ , mit  $H$  = Bandbreite,  $\lg(x)$  = dualer Logarithmus zur Basis 2,  $S$  = Leistung des Nutzsignals,  $N$  = Leistung des Rauschsignals (noise) und  $S/N$  = Signal-Rausch-Abstand (signal-to-noise-ratio), die in Dezibel (dB) gemessen wird. Damit kann ein analoger Telefonkanal mit 3.000 Hz Bandbreite und einem Signal/Rausch-Abstand von 30 dB maximal 30.000 Bit/s übertragen [SIKO03, S. 65]. Die multiplikative Verknüpfung mit der Bandbreite  $H$  ergibt, dass hohe Bandbreiten, auch hohe Datenübertragungskapazitäten bedeuten. Kabel, die hohe Bandbreiten unterstützen, verursachen aber auch höhere Produktionskosten.

#### **2.1.1.1 Koaxialkabel**

Das Koaxialkabel ist verwandt mit dem Twisted-Pair-Kabel (Abschnitt 2.1.1.2), da die zum Bau verwendeten Materialien identisch sind. Jedoch ist der Aufbau anders. Die „Seele“ des Koaxialkabels bildet ein im Kern verlaufender Kupferdraht (Abbildung 6), der mit einem Isoliermantel umgeben ist. Um den Isoliermantel herum spinnt sich das feine Netz des Außenleiters, bestehend aus dünnem Kupferdraht. Dieser ist abgeschirmt durch den äußeren Plastikschutzmantel. Durch diesen Aufbau erreicht man eine gute Kombination von hoher Bandbreite und ausgezeichneter Rauschunempfindlichkeit. Aktuell erreicht das Koaxialkabel Bandbreiten von nahezu 1 GHz. Wegen relativ hoher Produktionskosten und zunehmender Konkurrenz der Twisted Pair Kabel mit ausreichenden Bandbreiten, ist die Verwendung von Koaxialkabeln beschränkt.

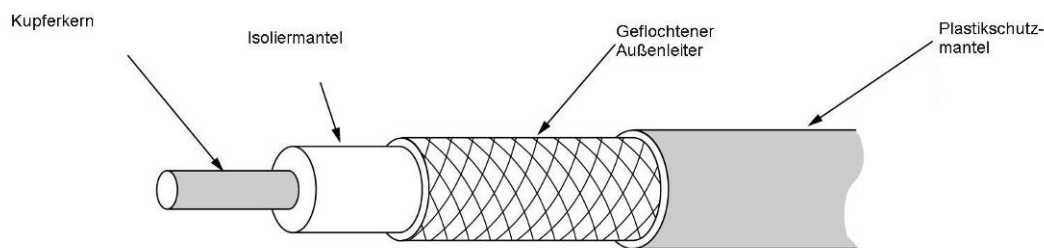


Abbildung 6: Aufbau des Koaxialkabels [TANE03, S. 113]

Bei lokalen Netzwerken mit geringen zu überwindenden Entfernungen dominiert Twisted Pair, während bei größeren Entfernungen vor allem die Glasfaser eingesetzt wird. Im LAN-Bereich kommen auch immer mehr drahtlose Technologien zum Einsatz [PLAT04].

### 2.1.1.2 Twisted Pair

Das Twisted-Pair-Kabel besteht in der Regel aus vier verdrehten Kupferdrahtpaaren. Jeder Draht ist isoliert und 0,5 bis 0,6 mm dick. Die Verdrillung dient zum Schutz vor Ein- und Abstrahlung der Störsignale. Je mehr Verdrillungen pro Zentimeter Kabel, desto besser die Abschirmung. Man unterscheidet fünf verschiedene Qualitätskategorien. Je besser die Abschirmung und je höher die Bandbreite, desto höher die Kategorie. Die Kategorien, kurz CAT-1 bis CAT-5 genannt, besitzen Übertragungsraten von unter einem MBit/s und Bandbreiten von weniger als einem MHz (CAT-1) bis typischerweise 100 MHz Bandbreite und Übertragungsraten von 100 MBit/s (CAT-5). Die Unterschiede beruhen auf der Bauweise (Abbildung 7):

- UTP-Kabel (Unshielded Twisted Pair, nicht abgeschirmte verdrehte Leitungen), früher typischerweise CAT-3, heute CAT-5.
- S/UTP-Kabel (Screened/Unshielded Twisted Pair) haben einen Gesamtschirm aus einem Kupfergeflecht zur Reduktion der äußeren Störeinflüsse.
- S/STP-Kabel (Screened/Shielded Twisted Pair) besitzen eine Abschirmung für jedes Kabelpaar sowie eine Gesamtschirmung [PLAT04]

In der Zwischenzeit gibt es sich weitere Kategorien (CAT-6, CAT-7), die in der Lage sind, Daten in der Dimension von GBit/s zu übertragen [SIKO03, S. 69].

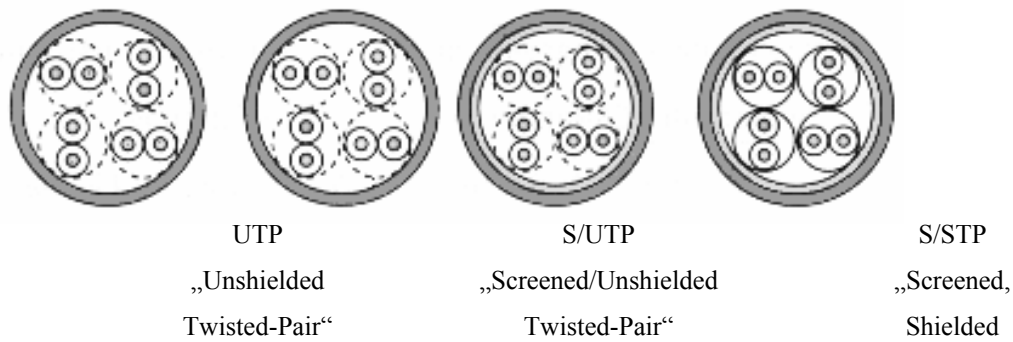


Abbildung 7: Querschnitt durch Twisted Pair Kabeltypen [PLAT04]

### 2.1.2 Lichtwellenleiter

Im optischen Leiter breiten sich keine elektromagnetischen Schwingungen aus, sondern Licht. Als Lichtquellen dienen entweder LEDs (lichtemittierende Dioden) oder Halbleiterlaser [TANE03, S. 117]. Am anderen Ende des Kabels empfängt eine Fotodiode die Lichtsignale. Die Glasfasertechnologie hat zwei entscheidende Vorteile: Einerseits operiert man bei der Übertragung der Daten mit Lichtgeschwindigkeit und andererseits fallen elektromagnetische Störgrößen, wie sie bei der Kupferdrahttechnologie vorliegen, weg. Ein Nachteil ist die Empfindlichkeit des Glaskörpers gegen Biegung und ein weiterer, dass die Umwandlung der Lichtwellenimpulse in elektrische Impulse beim heutigen Stand der Technik noch einen Engpass darstellt. Glasfaserkabel sind in ihrem Aufbau mit dem Koaxialkabel vergleichbar. Jedoch besteht der Kern nicht aus Kupfer, sondern aus einem Quarzglaskern.

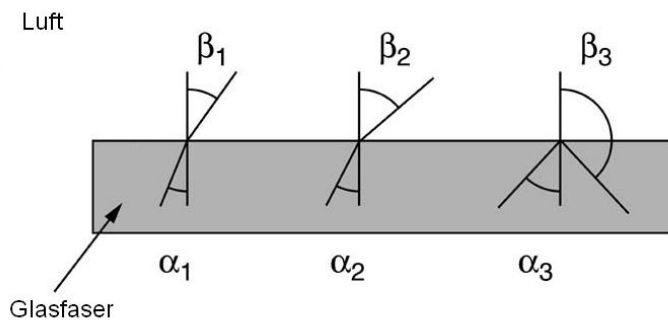


Abbildung 8: Einfallswinkel  $\alpha$  bestimmt Ausfallwinkel  $\beta$ ;  $\alpha_3$  ist kritischer Winkel [TANE03, S. 114]

Darum ist ein weiterer Glasmantel gehüllt und außen befindet sich eine Plastikschicht. Der Mantel hat einen im Verhältnis zum Kern niedrigeren Brechungsindex. Die Folge ist, dass beim Erreichen eines kritischen Einfallswinkels (Abbildung 8) eine Totalreflexion der Lichtstrahlen am Übergang von Kern zu Mantel herbeigeführt und so das Licht im Kern gehalten wird [SIKO03, S. 74f.]. Das Licht breitet sich im Kabel in Abhängigkeit vom Einfallswinkel und der Materialbeschaffenheit auf unter-

schiedlichen Wegen aus. Die Wege, auf denen sich das Licht ausbreitet, nennt man Moden [SIKO03, S. 75]. Die unterschiedlichen Wege der Lichtstrahlen beschreiben auch unterschiedliche Längen. So kommt es zu unterschiedlichen Durchlaufzeiten des Lichtes. Am anderen Ende ist das Ergebnis daher ein „Verschmieren“ des ursprünglichen Signals, was man als Dispersion bezeichnet [SIKO03, S. 75]. Man unterscheidet drei Kabeltypen: Erstens Multimode-Lichtwellenleiter mit Stufenprofil, zweitens Monomode-Lichtwellenleiter mit Stufenprofil und drittens Multimode-Lichtwellenleiter mit Gradientenprofil. Je feiner der Kern, desto geringer fällt die Dispersion aus. Am Ende steht ein Kern, der so fein ist, dass das Licht nur noch auf einem Weg durch das Kabel läuft. Dann spricht man von einem Monomodekabel. Bei einem Gradientenprofil ist die Brechzahl im Faserkern nicht konstant. Das hat zur Konsequenz, dass sich die Lichtstrahlen parabelförmig im Kabel ausbreiten und wellenförmig verlaufen. Damit erhöht sich die Bandbreite bei der Übertragung [SIKO03, S. 76]. In der folgenden Tabelle findet sich eine Übersicht über die verschiedenen Kabeltypen mit ihren Eigenschaften (Tabelle 1):

Tabelle 1: Übersicht über die Kabeltypen und ihre Eigenschaften in Anlehnung an [PLAT04]

Eigenschaften	Dünnes Koaxial	Dickes Koaxial	Twisted-Pair	Lichtwellenleiter
<b>Kosten</b>	billig	teurer	billig	teure Anschlusskomponenten
<b>Max. Kabellänge</b>	185 m	500 m	100 m	2 bis 100 km
<b>Datenraten</b>	10 Mbit/s	10 Mbit/s	4 bis 100 Mbit/s	100 Mbit/s bis 100 Gbit/s
<b>Biagsamkeit</b>	relativ biegsam	weniger biegsam	biegsam	bedingt biegsam
<b>Installation</b>	einfach	einfach	sehr einfach	weniger einfach
<b>Störanfälligkeit</b>	zuverlässig	zuverlässig	anfällig	kaum anfällig
<b>Abhörsicherheit</b>	bedingt sicher, Abhören möglich	bedingt sicher, Abhören schwer möglich	bedingt sicher, Abhören möglich	sicher, Abhören unmöglich

## 2.2 Funk

Um die Teilnahme an einem Local Area Network flexibel, einfach und kabelfrei zu gewährleisten, bieten sich immer mehr Funktechnologien als Übertragungsmedien an. Bluetooth und WLAN sind die Varianten die in letzter Zeit einen großen Boom erfahren haben und auch stark weiterentwickelt wurden.

### 2.2.1 WLAN

WLAN ermöglicht eine mobile Vernetzung von Computern ohne Kabel-Infrastruktur. Mit Hilfe von WLAN-Karten können sowohl PCs als auch Notebooks problemlos vernetzt werden. Hierzu sind einige wenige Hardwarekomponenten notwendig; einen kleinen Überblick gibt Abbildung 9.

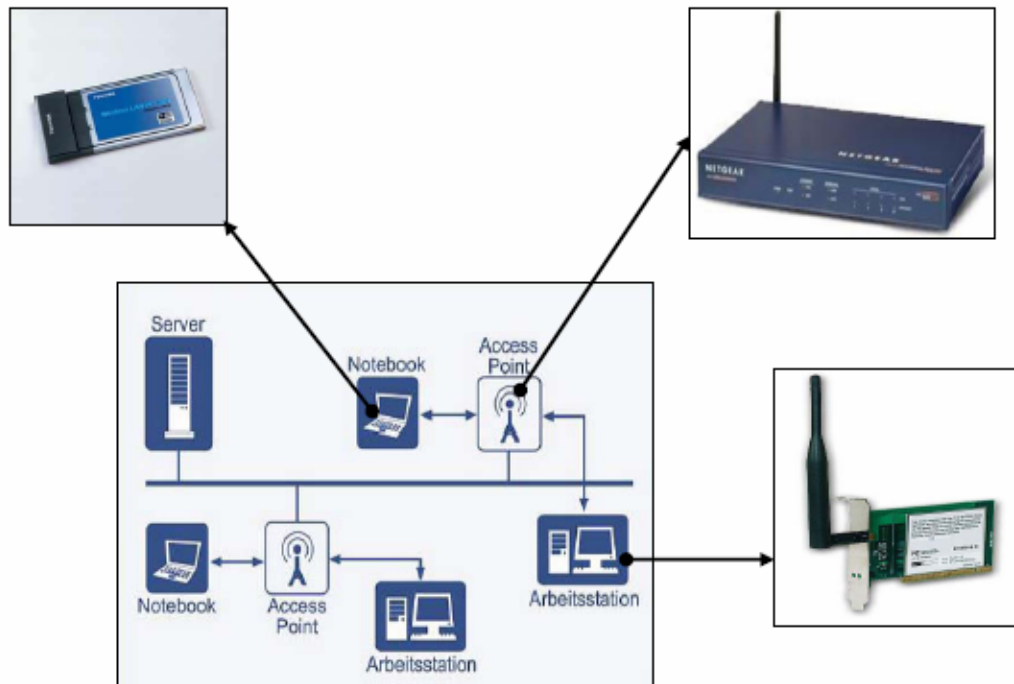


Abbildung 9: WLAN-Kommunikationskomponenten

Grundsätzlich gibt es zwei Konfigurationsmöglichkeiten von WLANs:

1. Bei der unabhängigen Variante sind die einzelnen Rechner, die eine WLAN-Karte besitzen, im Netzwerk gleichberechtigt und können im so genannten Peer-to-Peer Betrieb miteinander kommunizieren.
2. Die weitaus häufiger genutzte Variante ist das Infrastructure-WLAN. Neben den WLAN-Karten in den einzelnen Rechnern gibt es eine weitere Komponente, den Access-Point (AP), der das Rückgrat des WLAN bildet. Die Verbindung der einzelnen WLAN-Clients (PC, Notebook, PDA etc.) erfolgt über den AP, wobei der AP selbst einen kabelgebundenen Netzwerkanschluss besitzt und so mit dem vorhandenen Local Area Network (LAN) verbunden ist. Dadurch können mehrere WLAN-Clients, wie in Abbildung 10 zu sehen, auf alle freigegebenen Ressourcen des Netzwerkes zugreifen.

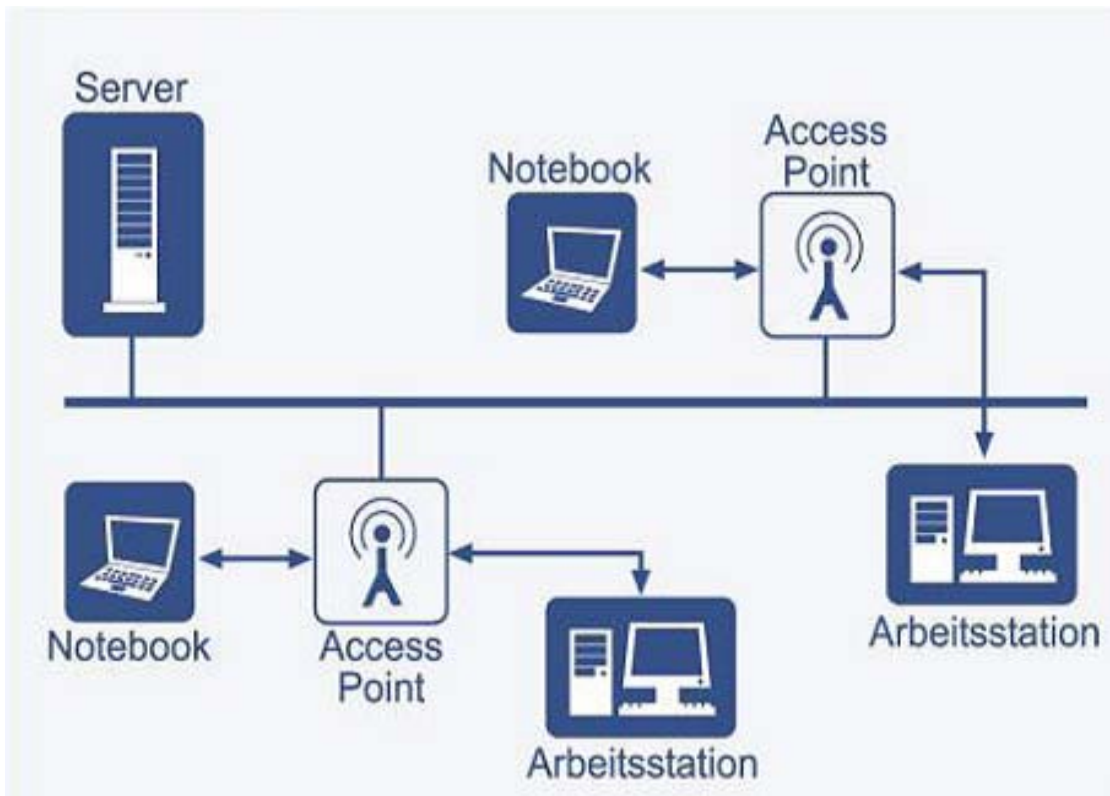


Abbildung 10: WLAN-Aufbau (eigene Darstellung)

Die Funkausleuchtung (Abbildung 11) kann durch das Aufstellen mehrerer APs aus-  
geweitet und verbessert werden, so dass der Bewegungsradius der Clients nicht auf  
eine AP-Funkzelle beschränkt ist.

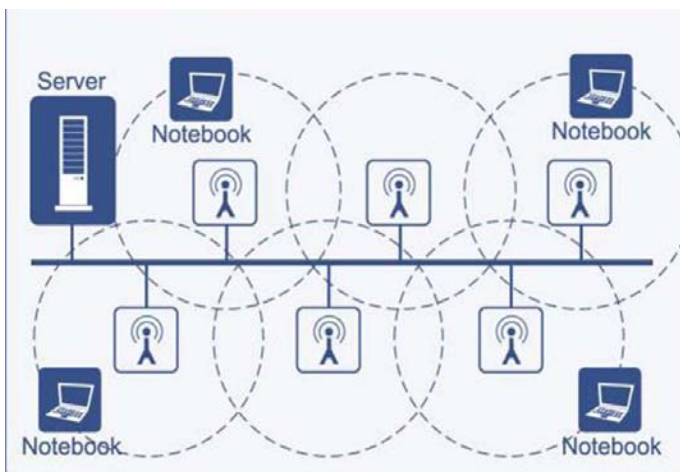


Abbildung 11: Funkzellen-Funktionsweise (eigene Darstellung)

Durch das so genannte Roaming (Abbildung 12) können diese von einer zur anderen  
Funkzelle wechseln. Aus logischer Sicht besitzen die Clients somit immer Zugriff  
zum gesamten LAN.

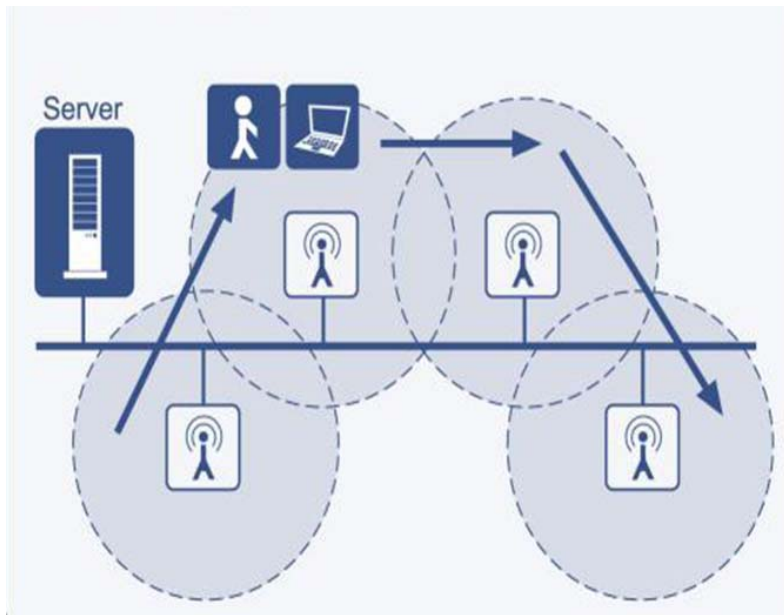


Abbildung 12: Roaming-Funktionsweise (eigene Darstellung)

### 2.2.1.1 IEEE 802.11x-Standards

Bei der Auswahl der WLAN-Hardware-Komponenten ist zu beachten, dass nicht alle Produkte im gleichen Frequenzbereich arbeiten. Grundsätzlich gibt es zwei verschiedene Frequenzen die bei WLANs zum Einsatz kommen. In Europa ist das 2,4-GHz-Band die bevorzugte Übertragungsfrequenz. In Deutschland ist es noch nicht sehr lange her, dass das 5-GHz-Band für private Nutzung frei gegeben wurde. Der momentane Vorteil der 5-GHz-Frequenz ist die geringere Störanfälligkeit, da zurzeit im Gegensatz zur 2,4-GHz die Frequenzbenutzung wesentlich geringer ausfällt. Bluetooth oder auch Küchen-Mikrowellengeräte verwenden ebenfalls das 2,4-GHz-Band und stellen somit zusätzliche Störquellen da. Jedoch ist es nur eine Frage der Zeit bis auch die 5-GHz-Frequenz ein dementsprechendes Nutzungsspektrum aufweist.

Ein weiterer Gesichtspunkt der zu beachten ist, sind die verschiedenen Übertragungsgeschwindigkeiten. 11- und 54-MBit sind die zwei Geschwindigkeiten die sich bis heute durchgesetzt haben. Für die Verabschiedung von praktikablen Standards bei WLAN-Komponenten, setzt sich Berufsverband der Elektrotechnik und Elektronik-Ingenieure (IEEE) ein. Die momentan wichtigsten IEEE-Standards sind:

- 802.11a: 54-MBit-Funknetz im 5-GHz-Band.
- 802.11b: 11-MBit-Funknetz im 2,4-GHz-Band.
- 802.11g: Erhöhung der Geschwindigkeit in 802.11b-Netzen von 11- auf 54-MBit/s.

Um sich beim Kauf zu Recht zu finden und die richtigen Komponenten zu wählen, gibt es das so genannte WIFI-Logo (Wireless Fidelity). Dieses Logo ist auf solchen Produkten aufgebracht die nach den 802.11x-Standards arbeiten und innerhalb ihrer verwendeten Frequenz abwärts kompatibel sind.



Abbildung 13: Wifi-Produktlogo

### **2.3.1.2 Gezielte und flächendeckende Funkausleuchtung**

Damit das WLAN auch effektiv arbeitet und an die vorhandene Umgebung angepasst und eingestellt ist, sollte nach dem Kauf der Komponenten und vor der Inbetriebnahme des Funknetzwerkes die Funkausleuchtung der gewünschten Bereiche ausgiebig getestet und eingestellt werden. Nicht nur damit die kabellosen Clients ohne Funklöcher im Netzwerk arbeiten können sondern auch aus Sicherheitsüberlegungen sollte man sich im Klaren darüber sein wo eine Funkausleuchtung erwünscht ist und wo das Firmennetz auf keinen Fall mehr erreichbar sein darf. Funkwellen halten sich nicht an Grundstücks- oder Gebäudegrenzen und somit sollte es potentiellen Netzwerkeindringlingen nicht ermöglicht werden schon ohne ihr Firmengebäude oder Gelände zu betreten einen Angriff auf das Netzwerk zu starten. Installiert man beispielsweise einen AP an der Innenseite einer Außenwand so wird er in der Regel nicht nur in den Raum funken sondern standardmäßig kommen bei den meisten Access-Points Rundumstrahlantennen zum Einsatz, die horizontal gleichmäßig in alle Richtungen und vertikal meist nur nach oben funken. Um diesem Problem entgegenzuwirken haben die meisten APs einen externen Antennenanschluss um Antennen mit bestimmten Strahlungscharakteren verwenden zu können. Richtantennen, die ihren Abstrahlungsschwerpunkt in bestimmte Richtungen und oder nur in einem bestimmten Abstrahlungswinkel funken, bieten eine Möglichkeit die Funkausleuchtung den Gegebenheiten anzupassen. Um sich die Abstrahlungscharakter plastischer vorstellen zu können, hilft ein Blick auf ein so genanntes Antennenstrahlungsdiagramm:

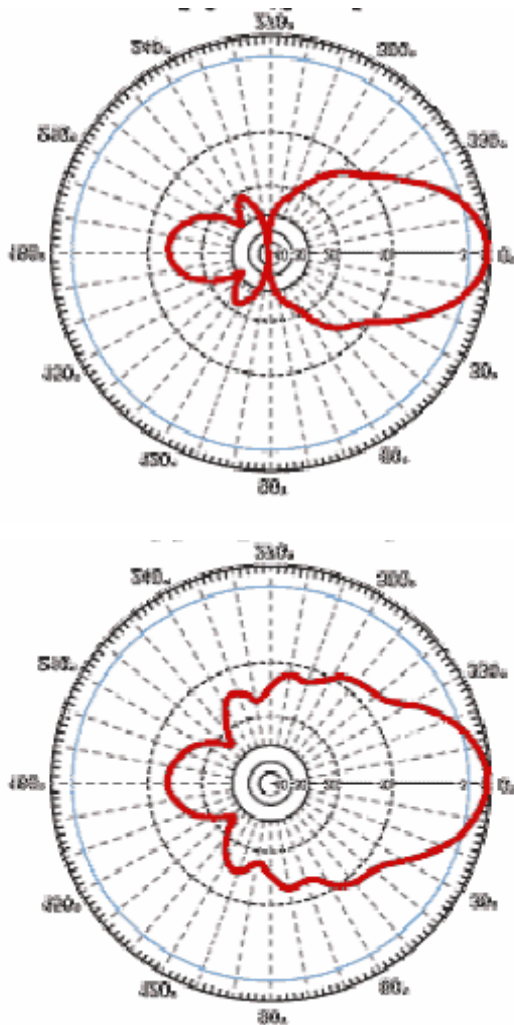


Abbildung 14: Vertikales Abstrahlungsdiagramm (links), Horizontales Abstrahlungsdiagramm (rechts)

Je nach Art der verwendeten Antenne (hier: Yagi-Antenne) spiegeln sich die Strahlungscharaktere in diesen Diagrammen ab und geben Aufschluss über die Funktionalität der verschiedenen Antennen.

### 2.2.1.2 Störquellen und Dämpfung

Neben den sehr theoretischen Strahlungseigenschaften der eingesetzten Antennen spielen für die flächendeckende Ausleuchtung jedoch auch die möglichen Störquellen eine große Rolle. Hierbei ist zu unterscheiden ob das WLAN innerhalb eines Gebäudes, wie zum Beispiel in Büros, in Konferenzräumen, Arbeitshallen, oder auch im freien genutzt werden soll.

Innerhalb von Gebäuden existiert eine Vielzahl an Materialien durch die Funkwellen absorbiert oder reflektiert werden und somit das theoretische Leistungspotential der WLAN-Hardware stark beeinträchtigen. Stahlbetonwände oder Feuerschutztüren sind dabei die schwerwiegendsten Beeinträchtigungen mit den in fast allen Büro- o-

der Firmengebäuden zu rechnen ist. Um den Funkempfang stark einzuschränken genügen allerdings auch schon andere weniger starke Störquellen.

Tabelle 2: Dämpfungsmaterialien-Übersicht (kein Anspruch auf Vollständigkeit)

Material	Beispiele	Dämpfung
Holz	Möbel, Decken, Zwischenwände	Gering
Gips	Zwischenwände ohne Metallgitter	Gering
Glas	Fensterscheiben	Gering
Mauersteine	Wände	Mittel
Wasser	feuchte Materialien, Aquarium	Mittel
Beton	Außenwände	Hoch
Gips	Zwischenwände mit Metallgitter	Hoch
Metall	Aufzugsschächte, Brandschutztüren, Stahlbetonkonstruktionen	Sehr hoch

Generell ist die Decke der beste Platz einen AP anzubringen um die Funkausleuchtung zu maximieren, weil dort in der Regel am wenigstens Störquellen vorhanden sind. Jedoch darf die Position des APs nicht nur aus dem Gesichtspunkt der Störanfälligkeit gewählt werden. Um sensible Daten zu schützen sollte deshalb besser in einen weiteren Access Point investiert werden der die Funkversorgung gewährleistet, aber dafür bewusst in gewünschten geographischen Grenzen gehalten werden kann.

Für den Fall das das Firmen-WLAN auch im Freien genutzt werden soll, muss neben den Dämpfungsmaterialien noch ein weiterer Aspekt beachtet werden. Damit die best mögliche Leistung erzielt werden kann muss Sichtkontakt zwischen den verwendeten Komponenten bestehen und 80% der unteren Fresnel-Zone sollte frei von Bäumen, Masten oder Gebäuden sein, da sonst trotz Sichtkontakt die Verbindung dauerhaft abbrechen kann. Die Fresnel-Zone bezeichnet ein gedachtes Ellipsoid zwischen zwei Funk-Kommunikations-Punkten (Abbildung 15) in der sich die Funkwellen ausbreiten.

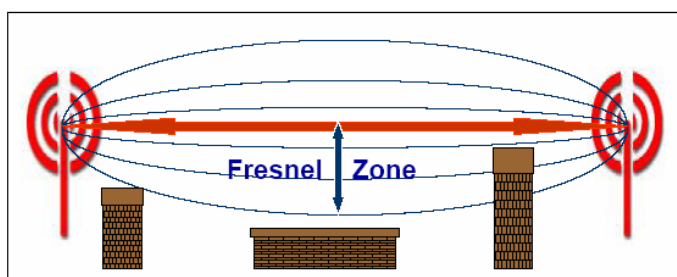


Abbildung 15: Fresnel-Zone (eigene Darstellung)

### 2.2.1.3 Werkzeuge zur Positionierung und Abstimmung der Access-Points

Die einfachste Methode, die Übertragungsraten und die Signalstärke der Verbindungen von Clients zum Access Point zu testen, ist die Benutzung eines Client-Managers. Solche Client-Manager (siehe Abbildung 16 und Abbildung 17) werden bei den meisten WLAN-Karten als Software mit ausgeliefert und auch unter Windows-XP ist bereits ein akzeptabler Client Manager integriert.

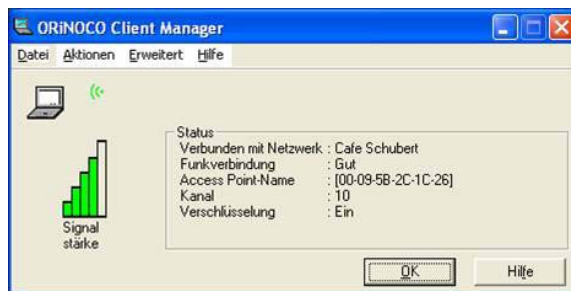


Abbildung 16: Orinoco Client Manager (Screenshot)

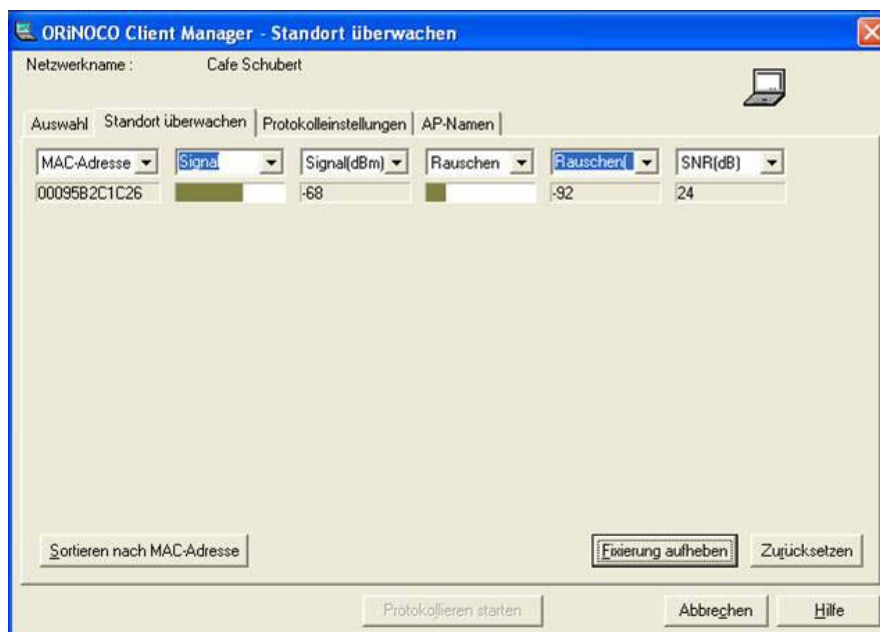


Abbildung 17: Orinoco Client Manager – Standortdaten (Screenshot)

Angezeigt werden die Signalstärke, das Rauschen (entspricht einer Grundstörung) und die effektive Signalstärke (SNR = Differenz von Signal und Rauschen), welche die entscheidende Größe darstellt. Bei einer Datenübertragungsrate von 11 Mbit/s benötigt man einen SNR von ca. 10 dB. Fällt der Wert unter 10 dB wird die Datenrate herabgesetzt, bei weniger als 6 dB bricht die Verbindung ab. Für kleine Büroräume mit nur wenigen Access-Points sind diese Informationen eines Client Managers zwar ausreichend aber bieten nicht genügend Features um einen vernünftigen Ausleuchtungsplan mit einer Übersicht für verschiedene APs zu erstellen.

Weitaus professioneller ist der Netstumbler. Er besitzt eine Aufzeichnungsfunktion, so dass durch Ablaufen der Räumlichkeiten mit einem Laptop ein bestimmter Zeitraum aufgezeichnet werden kann und die Daten später graphisch nachvollzogen werden können. Außerdem zeigt er neben der Graphik auch die verschiedenen APs mit deren Namen, Mac-Adressen, Verschlüsselungsdaten an. Auch ein akustischer Modus ist möglich, der es ermöglicht, ohne ständig auf den Bildschirm zu sehen, einen guten Standort zu ermitteln.

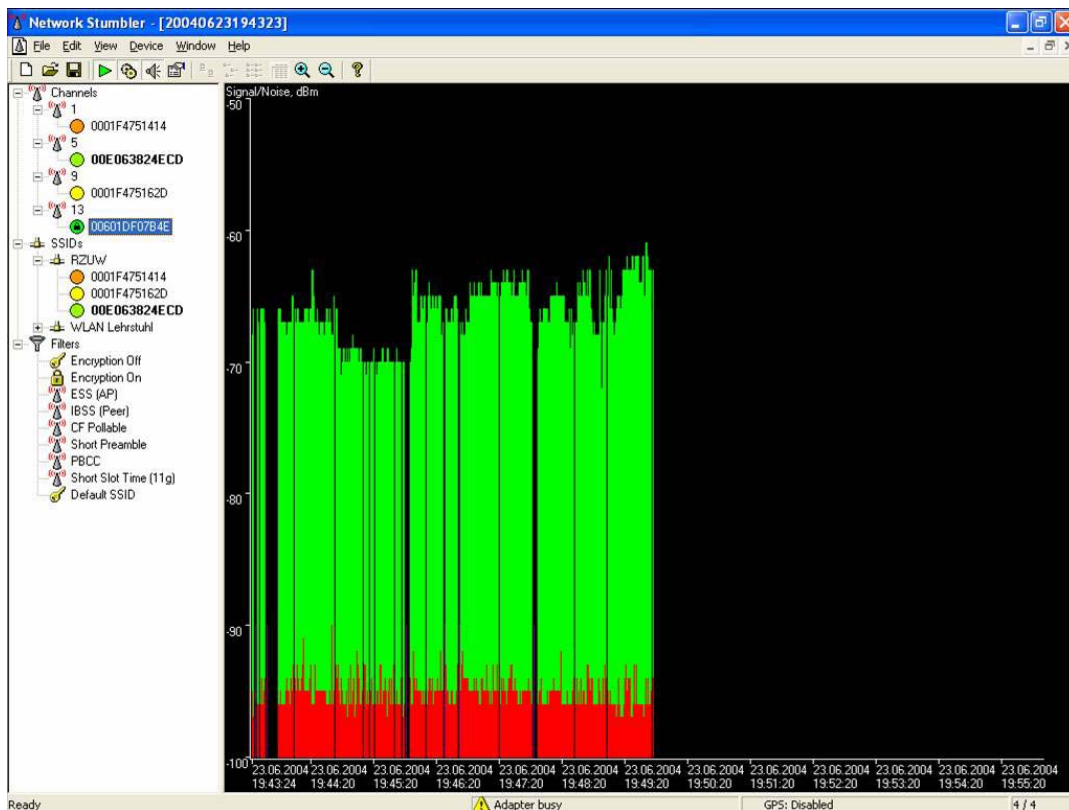


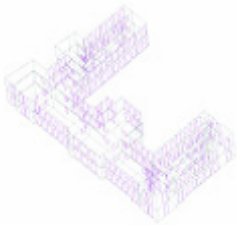
Abbildung 18: Netstumbler – Graphische Darstellung (Screenshot)

Es gibt auch Firmen die durch den Einsatz teurer Messgeräte und Software ganze Gebäudekomplexe vermessen und diese Ergebnisse entsprechend visualisieren (Abbildung 18 und Abbildung 19). Diese Kosten stehen jedoch in den meisten Fällen in keiner rentablen Relation zum Nutzen.

# In Gebäuden

## Datenbanken

### 3D Vektor Daten



Beispiel: Bürogebäude

- Wandform (Polygone)
- Wandposition
- Materialdaten
- Unterteilungen (Türen, Fenster)

## Prognosemodelle

- One Slope
- Motley Keenan
- COST 231 Multi Wall
- 2D Strahlenoptik
- 3D Strahlenoptik (Ray Tracing)

## Prognoseberechnung

### Multi Wall

### 3D Ray Tracing

## Penetration

### Empfangsleistung

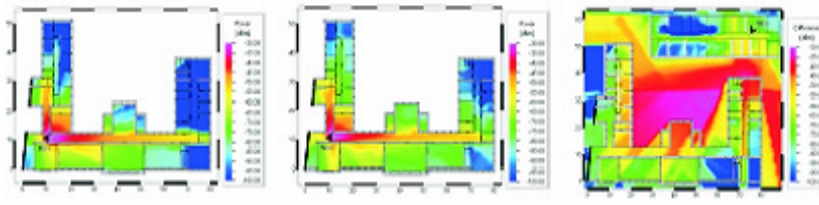


Abbildung 19: Profiauswertung

## 2.2.2 Bluetooth

Die Datenfunkübertragung durch Bluetooth ist gerade im Bereich der Handys und PDAs auf dem Vormarsch. Was zu Beginn des Mobile-Booms noch einzig und allein durch Infrarotschnittstellen möglich war wird immer mehr durch Bluetooth realisiert. Bluetooth-Verbindungen zwischen Mobiltelefonen und PDAs, mit Druckern oder Rechnern, liefern eine zusätzliche, immer häufiger angewandte Datenübertragungsvariante, die das private aber auch das Firmen-LAN ergänzt. Um PDAs und Handys über das LAN an das Internet anzubinden gibt es auch die Möglichkeit Bluetooth-Access-Points einzusetzen. Zwar ist die technische Umsetzung etwas anders als bei WLAN-Access-Points, die Sicherheitsrisiken sind jedoch dieselben. Es sollte ebenfalls darauf geachtet werden, dass die Funkzellen der APs räumlich abgestimmt sind und auch bei Bluetooth sollte auf eine verschlüsselte Datenübertragung nicht verzichtet werden. Theoretisch bestehen bei den Bluetooth-Schlüsseln ähnliche Schwächen und Angriffsmöglichkeiten wie bei WEP für WLAN. Wenn man hingegen bedenkt, dass Bluetooth eigentlich nur für Headsets oder Datenübertragung zu Druckern entwickelt wurde, ist das auch nicht verwunderlich. Für sensible Daten sollte

deshalb beim momentanen Stand der Bluetooth-Sicherheit auf diese Art der Kommunikation verzichtet werden.

### 2.2.3 Richtfunk

Bei der Richtfunktechnologie werden wie der Name schon sagt Funksignale „gerichtet“ gesendet. Es sind Punkt-zu-Punkt- bzw. Multi-Punkt-Verbindungen realisierbar. Ein quasi freies Bewegen innerhalb eines bestimmten Areals, wie man es von ungerichtetem Funk (WLAN, Bluetooth, Mobilfunk) kennt, ist jedoch nicht möglich. Bei Richtfunk unterscheidet man Mikrowellen und Optischen Richtfunk sowie gerichtetes WLAN. Die Richtfunktechnologie wird in der Regel für die Verbindung bestehender Netzwerke verwendet. Die verschiedenen Arten unterscheiden sich nicht nur in der Wellenlänge, sondern auch in der überbrückbaren Reichweite und der möglichen Bandbreite. Beides hängt stark von der Leistungsfähigkeit der verwendeten Geräte ab. So unterliegt beispielsweise ein gerichtetes WLAN prinzipiell den gleichen Bandbreitenbegrenzungen wie ein ungerichtetes, und ein optisches Richtfunksystem kann durchaus eine Reichweite von mehreren Dutzenden Kilometern erreichen. Da Richtfunksysteme grundsätzlich über Sichtverbindungen laufen, sind sie meist auf Gebäuden angebracht und somit schon aufgrund der Höhe schwierig abzuhören. Die Abhörsicherheit liegt auch darin begründet, dass Richtfunk zum Teil nur in einem sehr kleinen Öffnungswinkel abgestrahlt wird (bei Mikrowellenrichtfunk nur 0,5 – 1 Grad). Bei Optischem Richtfunk (Infrarot) sind die Wellen ebenfalls sehr stark gebündelt und außerdem müsste der Strahl, um die Übertragung abzuhören, unterbrochen werden [o.V.01a, S. 3-5]. Weiterhin kommen auch beim Richtfunk Sicherheitsmaßnahmen wie Frequenzwechsel sowie Authentisierungs- und Verschlüsselungsverfahren zum Einsatz.

## 2.3 Sicherheitsrelevante Aspekte bei Funknetzen

Es ist nahe liegend, dass bei Funknetzen das Übertragungsmedium die Achillesferse ist. Denn im Gegensatz zu Kabelnetzen sind Funknetze nicht nur im Bereich der verlegten Kabel bzw. Anschlüsse verfügbar und damit auch angreifbar, sondern im gesamten Abdeckungsgebiet der Funkwellen. Eine Gefahr bei Funknetzen ist, dass es Angreifern mit Hilfe eines einfachen Störsenders möglich ist, das Netz vollkommen lahm zu legen. Ein solcher Störsender kann relativ einfach und kostengünstig hergestellt werden. Prinzipiell können aber auch Sender eines „fremden“ Netzwerkes oder auch Sender wie Mobiltelefone und Mikrowellengeräte als Störsender fungieren. Ei-

ne weitere Möglichkeit, die sich Hackern bietet, um ein Funknetz auszuschalten, ist eine Denial-of-Service Attacke (DoS). Hierbei setzt der Hacker den AP dadurch außer Gefecht, dass er ihn z. B. mit Authentifikationsanfragen überflutet und so blockiert. Bei diesen DoS-Attacken besteht zunächst keine Gefahr für Daten oder die Systeme im Netzwerk, aber allein dadurch, dass das Netz nicht verfügbar ist, entstehen schnell hohe Kosten für den Betreiber. Schafft es ein Angreifer jedoch, sich als autorisierter Benutzer auszugeben oder zumindest die Datenübertragung mitzulesen, kann sehr schnell ein beträchtlicher Schaden durch Datendiebstahl und Datenspionage entstehen. Insbesondere das Mitlesen bzw. „Sniffen“ ist in Funknetzen deutlich einfacher als in Kabelnetzen, da der Angreifer keinen Rechner mit direktem Zugang zum Netz benötigt. Es genügt, wenn er sich mit einem entsprechenden Empfänger im Bereich des Funknetzes aufhält, da die Signale quasi „frei durch die Luft schweben“. Außerdem muss man hierbei bedenken, dass ein Abhören der Signale mit einem entsprechend empfindlichen Empfänger noch weit außerhalb des eigentlichen Wirkungsbereichs möglich ist [BARN02, S. 195; KAUF02, S. 329].

Tabelle: Sicherheitsbedrohungen für WLAN's – Eigene Darstellung in Anlehnung an [o.V.05]

<b>Bedrohung</b>	<b>Beschreibung</b>
Abhören und ändern von übertragenen Daten	Durch Abhören können Angreifer in den Besitz von vertraulichen Daten wie z. B. Anmeldedaten kommen. Ein Eindringling kann außerdem übertragene Daten verändern.
Denial-of-Service (DoS)	WLAN's können von Angreifern auf verschiedene Art und Weise außer Gefecht gesetzt werden.
Freie Internetbenutzung	Verfügt das WLAN über einen Internetzugang, kann ein Angreifer diesen nutzen. Zum einen kann sich dies negativ auf die Verfügbarkeit auswirken, und zum anderen können evtl. illegale Aktionen nur auf den WLAN Betreiber zurückgeführt werden.
Zufällige Sicherheitsbedrohungen	Bei nicht abgesicherten WLAN's könnte sich ein Besucher versehentlich am Netz anmelden und eine Sicherheitsbedrohung darstellen.
Inoffizielle WLAN's	Von Mitarbeitern selbstständig eingerichtete, un-

<b>Bedrohung</b>	<b>Beschreibung</b>
	zureichend abgesicherte WLAN's sind eine Sicherheitslücke.

### **3 WLAN Verbindungsgeräte**

Wichtige Komponenten eines Netzwerks sind die Verbindungsgeräte, sie können je nach Typ verschiedene Aufgaben in Netzen erfüllen. Einfache Geräte dienen z. B. lediglich der Signalverstärkung, während „intelligenter“ Geräte in der Lage sind, unterschiedliche Netzwerkumgebungen zu verbinden. Der Aufbau eines möglichst sicheren Netzwerks beginnt bereits bei der Auswahl der richtigen Hardware und des richtigen Herstellers, denn der Funktionsumfang und die Umsetzung der Standards seitens der Hersteller haben einen wesentlichen Einfluss auf die Sicherheit.

#### **3.1 WLAN Adapter**

Um Clients mit dem WLAN zu verbinden, benötigt man, wie auch bei der Verbindung zu einem kabelbasierten Netz, einen Netzwerkadapter. Für Desktop PCs stehen „PCI-Karten“ zur Verfügung, während bei Laptops meist „PCMCIA-Karten“ oder interne „Mini-PCI-Karten“ zum Einsatz kommen. Außerdem existieren mittlerweile auch „USB WLAN Adapter“, die sowohl für Desktop PC's als auch für Laptops verwendet werden können. Neuere Laptops, die mit einem Centrino Prozessor ausgestattet sind, sind bereits WLAN fähig und benötigen keine zusätzliche Hardware. Mittlerweile sind auch PDAs WLAN fähig, sie besitzen entweder eine interne Lösung oder können mit WLAN-CompactFlash/SD-Cards aufgerüstet werden.

#### **3.2 Access-Points**

Für den Aufbau eines WLAN's benötigt man Access-Points (AP). Ein AP verbindet die WLAN Endgeräte untereinander sowie mit bestehenden, kabelgebundenen Netzen. Weiterhin können AP die Funktionalität von Repeatern übernehmen, indem sie die WLAN Signale verstärken und so die Reichweite des Netzes erhöhen.

#### **3.3 Router**

Eine Stufe intelligenter sind Router, die auf der Netzwerkschicht des ISO/OSI-Modells (siehe 1.1) arbeiten. Die Positionierung auf dieser Schicht ermöglicht es Routern, den Inhalt von Datenpaketen/Frames genauer zu analysieren und entsprechend zu behandeln. Aufgrund dieser Fähigkeit sind Router in der Lage, nicht nur gleiche, sondern auch unterschiedliche Netzwerke zu verbinden (z. B. LAN und WAN). Typischerweise ermöglichen Router neben der AP-Funktionalität zusätzlich

den Zugang zum Internet, z. B. über einen DSL-Anschluss. In diesem Fall wird der Router über Ethernet mit einem DSL-Modem verbunden oder das Modem ist bereits im Router integriert. Routern ist es weiterhin möglich, Firewallfunktionen zu realisieren. Der Router verwendet hierfür die Access Control List (ACL), in der Netzwerksegmente oder Ports, die blockiert werden sollen, hinterlegt werden. Denkbar wären z. B. eingehende HTTP-Verbindungen (Hyper Text Transfer Protocol, Port 80) oder bestimmte Dienste wie FTP (File Transfer Protocol, Port 21), POP3 (Post Office Protocol, Port 110) oder SMTP (Simple Mail Transfer Protocol, Port 25) zu blocken [MEYE03, S. 220].

## 4 Maßnahmen zur Absicherung von WLANs

Wie zuvor gezeigt, bieten WLANs, wie auch kabelbasierte Netzwerke, verschiedene Angriffsmöglichkeiten, die Gegenmaßnahmen unverzichtbar machen. Im Folgenden werden nun die Möglichkeiten aufgezeigt, mit denen man ein WLAN absichern kann.

Der 802.11 Standard sieht zur Absicherung von Netzen drei Verfahren vor:

- Service-Set-Identifizier (SSID),
- MAC-Adressenfilter und
- Wireless Equivalent Privacy (WEP).

### SSID-Broadcast

Dieser Begriff bedeutet, dass ein AP in regelmäßigen Abständen die SSID an in Reichweite befindliche Clients sendet um seine Existenz bekannt zu machen und, dass die SSID auch auf Anfrage jedem Client bekannt gegeben wird [BLUM03, S. 6].

Die drei zuvor genannten Verfahren haben einige Schwachstellen bezüglich Administrationsaufwand (z. B. Änderungen des SSID und des WEP-Schlüssels müssen händisch am AP und jedem Client vorgenommen werden) und weisen gravierende Sicherheitsmängel auf. Um die Sicherheit in WLANs zu erhöhen,

wurden mit 802.1x, Wi-Fi Protected Access (WPA) sowie 802.11i weitere Sicherheitsstandards entwickelt [BARN02, S. 147].

Die vorgestellten Verfahren zur Absicherung eines WLAN bieten alle einen mehr oder weniger guten Schutz gegen unberechtigte Nutzung und potentielle Angriffe. Es muss jedoch klar sein, dass der Nutzen sehr stark von der jeweiligen Implementierung seitens der Hardware-Hersteller sowie der Nutzer abhängt. Einige Hersteller bieten z. B. nicht die Möglichkeit, das SSID-Broadcast zu deaktivieren. Auch die Wahl des SSID oder auch der kryptographischen Schlüssel seitens der Nutzer haben einen wesentlichen Einfluss auf die Qualität der Sicherungsmaßnahmen. Die Änderung des Standardpassworts für die Routerkonfiguration in ein eigenes komplexes Passwort ist absolut notwendig für eine sichere Konfiguration eines WLANs.

Außerdem gilt: Selbst schwache Schutzmaßnahmen sind besser als gar kein Schutz!

Tabelle: Sicherheitsmaßnahmen für WLANs – Eigene Darstellung in Anlehnung an [o.V.05].

## 4.1 Planungsphase

Bereits in der Planungsphase sind erste Sicherheitstechnische Überlegungen absolut notwendig, und das Erstellen eines Sicherheitsregelwerks sinnvoll. Bereits zuvor wurde beschrieben, dass die Positionierung und die Funkausleuchtung Einfluss auf die Sicherheit eines WLANs haben. Es ist jedoch schon in dieser Phase sinnvoll, sich auch über sonstige notwendige Sicherungsmaßnahmen bewusst zu sein, denn bei der Auswahl der Hardware ist darauf zu achten, dass diese alle relevanten Sicherheitsfunktionen unterstützt. Weiterhin ist es empfehlenswert, sich bereits frühzeitig bewusst zu machen, wie groß das Netz sein wird, wie es in die bereits bestehende Infrastruktur eingebunden wird, an welchen Stellen sich sinnvoller Weise Firewalls befinden sollen usw.

## 4.2 IP-Management

Die Hersteller von AP und Routern vergeben standardmäßig IP-Adressen. Diese können von jedermann in Benutzerhandbüchern nachgelesen werden und sollten deshalb geändert werden. Ist das Dynamic Host Control Protocol (DHCP) aktiviert, wird es einem Angreifer zudem erleichtert, Zugang zum WLAN zu erlangen. Sofern es der Administrationsaufwand zulässt, sollte also DHCP deaktiviert werden, und stattdessen die IP-Konfiguration der Clients manuell erfolgen.

### DHCP

DHCP ermöglicht mit Hilfe eines entsprechenden Servers, die dynamische Zuweisung von IP-Adressen und weiteren Konfigurationsparametern an Computer in einem Netzwerk (z. B. Internet oder LAN).

## 4.3 SSID

Das erste Verfahren zur Authentifizierung der Netzteilnehmer ist der Service-Set-Identifizierer (SSID), der auch als Netzwerkname bezeichnet wird. Der SSID ist eine Art einfaches „Passwort“, mit dem sich jedes Endgerät an einem Access Point anmelden muss. Dieses „Passwort“ wird von allen Clients verwendet. Die von den Hardwareherstellern voreingestellten Standard-SSIDs müssen auf jeden Fall geändert werden, da auch diese von jedem potentiellen Angreifer leicht über Handbücher und zahllose Internetseiten herausgefunden werden können. Dabei ist darauf zu achten, dass die gewählte SSID nicht direkt auf das Unternehmen, die Abteilung oder allgemein den Betreiber des WLANs schließen lässt.

Das Deaktivieren des SSID-Broadcast als Sicherheitsmassnahme zu bezeichnen, ist sicher übertrieben, denn für ambitionierte Angreifer stellt es kein Problem dar, sich die SSID, die im Klartext übertragen wird, zu beschaffen. Trotzdem sollte dies aber auf jeden Fall gemacht werden, denn zumindest „Gelegenheitshacker“ kann man auf diese Weise abhalten, sich am Netz anzumelden.

#### **4.4 MAC-Filter**

Der MAC-Adressenfilter ist ebenfalls eine Methode, um den Zugang zu AP's zu kontrollieren und nur autorisierte Endgeräte zuzulassen. Hierfür muss im AP eine Liste der MAC-Adressen (feste, hexadezimale 48-Bit-Hardwareadresse) aller Endgeräte angelegt werden, die auf den AP zugreifen dürfen.

Genau wie die SSID werden auch die MAC-Adressen im Klartext übertragen und können auch ohne weiteres gefälscht werden. Somit bietet also auch der MAC-Filter keinen Schutz vor ernst zu nehmenden Hackern. In kleineren Netzen, in denen der damit verbundene Administrationsaufwand (Pflege der Adresslisten) nicht zu groß wird, sollte der MAC-Filter aber durchaus als Schutz gegen „Gelegenheitshacker“ genutzt werden.

#### **4.5 Verschlüsselung und Authentifizierung**

Die bisher beschriebenen Möglichkeiten, SSID und MAC-Filter, bieten also keinen zufrieden stellenden Schutz gegen Angreifer. Ein versierter Angreifer wird immer einen Weg finden, sich Zugang zur Datenübertragung zu verschaffen. Deshalb ist es notwendig, die Daten auch während der Übertragung zu schützen, d. h. die Vertraulichkeit, Authentizität der Teilnehmer und der Nachricht sowie die Anonymität müssen bei der Datenübertragung gewährleistet sein [SCHW02, S. 6]. Hierfür werden die Daten verschlüsselt. Im Folgenden werden daher einige Verschlüsselungs- und Authentifizierungsverfahren vorgestellt:

### 4.5.1 Wireless Equivalent Privacy (WEP)

Wireless Equivalent Privacy (WEP) ist Bestandteil der 802.11a/b/g Spezifikationen und ist ein symmetrisches Verschlüsselungsverfahren, das zum einen die Daten während der Übertragung zwischen Client und AP schützen und zum anderen ebenfalls der Authentifizierung dienen soll. Allerdings wurden bereits Schwachstellen in diesem Verschlüsselungsverfahren nachgewiesen, die es Angreifern relativ einfach machen, an die verwendeten Schlüssel zu gelangen. Falls also ein ausreichender Schutz auch gegen gewieftere Angreifer erreicht werden soll, kann von der Verwendung von WEP nur abgeraten werden. Sollte WEP trotzdem zum Einsatz kommen, ist unbedingt auf die Verwendung von Schlüsseln mit der maximalen, von der Hardware gerade noch unterstützten, Länge zu achten. Außerdem sollte der Schlüssel regelmäßig geändert werden, was allerdings wiederum zu einem erhöhten Administrationsaufwand führt. Weitere Informationen zu der Funktionsweise und den Schwächen von WEP findet man in [BLOM03, S. 3-4 und S. 8-9].

### 4.5.2 Wi-Fi Protected Access (WPA)

WPA wurde von der Wi-Fi Alliance als Antwort auf die Schwächen von WEP entwickelt und basiert auf dem neuen Standard 802.11i. WPA hat den Vorteil, dass keine Investitionen in spezielle Hardware nötig sind, aber trotzdem gegenüber den herkömmlichen Verfahren ein deutlich höheres Sicherheitsniveau erreicht wird. Die höhere Sicherheit wird dadurch realisiert, dass im Gegensatz zu WEP dynamische Schlüssel verwendet werden. Mittels Temporal Key Integrity Protocol (TKIP) werden von einem Initialisierungsschlüssel ausgehend regelmäßig neue Schlüssel be-

#### **Symmetrische Verschlüsselung**

Bei der symmetrischen Verschlüsselung wird nur ein gemeinsamer Schlüssel für die Ver- und Entschlüsselung verwendet. Die Kommunikationspartner müssen sich zuvor auf diesen einigen.

rechnet, was einen Angriff deutlich erschwert. Konkret bedeutet das, dass ein Angreifer zwar auch hier den Schlüssel ausspionieren und sich somit auch am AP anmelden kann, aber ein Abhören des Verkehrs der andern Teilnehmer ist nicht möglich.

Außerdem ist das Ausspionieren des Schlüssels nicht so einfach wie bei WEP, da dieser nur bei der Anmeldung eines Teilnehmers am Netz übertragen wird. Aber: Auch hier ist es wichtig, dass die Schlüssel mit Bedacht, d. h. ausreichend lang und komplex, gewählt werden. Neben dem PSK (Pre Shared Key) Authentifizierungsver-

fahren erlaubt WPA auch die Authentifizierung nach dem 802.1x Standard [o.V.02, S. 1]. Die vor kurzem veröffentlichte neue Version von WPA nennt sich WPA2 und verwendet wie 802.11i bereits AES (Advanced Encryption Standard) als Verschlüsselungsverfahren. Weitere Informationen zu WPA und WPA2 finden sie auf der Wi-Fi Alliance Webseite: [www.wi-fi.org](http://www.wi-fi.org).

#### **4.5.3 802.1x**

Um die Sicherheitslücken im Authentifizierungsprozess zu schließen, wurde der Standard 802.1x entwickelt. Hierbei kommen dynamische Schlüssel sowie ein Authentifizierungsserver zum Einsatz, der das Extensive Authentication Protocol (EAP) unterstützt (z. B. Remote Authentication Dial In User Service <RADIUS> oder Kerberos). Bei diesem Verfahren verifiziert der Server die Clients, die sich am AP anmelden möchten, und legt die Schlüssel für eine gesicherte Übertragung fest. Der Einsatz des Authentifizierungsservers verbessert die Sicherheit des WLAN's dadurch, dass der gesamte Authentifizierungsvorgang verschlüsselt abläuft und außerdem benutzerindividuell über eine auf dem Server abgelegten Benutzerdatenbank erfolgt, und sich nicht alle Nutzer nur durch einen gemeinsam genutzten Schlüssel authentifizieren. Es ist an dieser Stelle jedoch anzumerken, dass die erhöhte Sicherheit mit der Konfiguration des Authentifizierungsservers und der Pflege der Benutzerdatenbank auch einen gewissen Administrationsaufwand mit sich bringt [SCHÄ03, S. 190; o.V.03c, S. 5].

#### **4.5.4 802.11i**

Der im Sommer 2004 von der IEEE verabschiedete Standard 802.11i beinhaltet die Verbesserungen die bereits durch WPA und 802.1x umgesetzt waren. Die wichtigsten Neuerungen sind zum einen, dass anstelle des bisher verwendeten Verschlüsselungsprotokolls RC4 nun das bessere AES (Advanced Encryption Standard) Verfahren Verwendung findet und zum anderen Verbesserungen der Sicherheit im Ad-hoc-Modus. Nachteil des neuen Standards ist, dass er nicht mehr zu bestehender Hardware abwärtskompatibel ist.

#### **4.5.5 Virtual Private Network (VPN) im WLAN**

Ein VPN ermöglicht eine sichere Datenübertragung über unsichere Netzwerke. Die Sicherheit wird dadurch gewährleistet, dass eine verschlüsselte Punkt-zu-Punkt Verbindung aufgebaut wird. Diese Punkt-zu-Punkt Verbindung hat für Unternehmen ne-

ben dem Sicherheitsaspekt außerdem den Vorteil, dass sie bei Verbindungen zwischen Netzwerken an verschiedenen Orten auf teure Standleitungen verzichten können und stattdessen einen „Tunnel“ über das Internet aufbauen. Bei der Verschlüsselung kommen beispielsweise die Protokolle IPSec und SSL zum Einsatz, die im Folgenden noch näher vorgestellt werden. Aufgrund der verwendeten Verschlüsselungsverfahren gilt VPN als eine sichere Übertragungstechnologie. Um die VPN-Technologie nutzen zu können, benötigt man ein VPN-Gateway (auch VPN-Concentrator genannt) und einen entsprechenden VPN-Client auf den Endgeräten. Derzeit befinden sich zahlreiche kostenpflichtige aber auch kostenfreie VPN-Lösungen auf dem Markt, bzw. sind zum Teil auch schon in Betriebssystemen integriert. VPNs werden bereits häufig in Unternehmen genutzt, was den Vorteil hat, dass die erforderlichen Systeme bereits vorhanden sind, und die User sich nicht an eine neue Technologie gewöhnen müssen. Für den Einsatz von VPN in einer WLAN Umgebung stehen mittlerweile auch spezielle Wireless Firewall Gateways zur Verfügung. Um die Sicherheit noch weiter zu erhöhen, bietet es sich an, anstelle von Username und Passwort Token- oder Smart-Cards zu verwenden. In diesem Fall besteht nicht die Gefahr, dass Benutzer unsichere Passwörter wählen oder diese an unberechtigte Dritte weitergeben. Außerdem können beliebig lange und komplexe Passwörter gewählt werden.

#### **4.5.6 Internet Protocol Security (IPSec)**

IPSec wurde von der Internet Engineering Task Force (IETF) erarbeitet und in einer Sammlung von Request for Comment-Dokumenten (RFC) veröffentlicht, in denen u. a. die kryptographischen Algorithmen und das Schlüsselmanagement beschrieben werden. IPSec ist eine Erweiterung des Internet Protocol und ist damit auf der Vermittlungsschicht des ISO/OSI-Modells angesiedelt. Ein IPSec-Paket besteht aus einem Authentication Header (AH), der mittels einer Hashfunktion die Integrität der IP-Pakete sicherstellt sowie aus Encapsulation Security Payload (ESP), das die Vertraulichkeit und Integrität der übertragenen Daten gewährleisten soll. Weiterhin unterscheidet man in Transport- und Tunnel-Mode. Im erstgenannten Fall wird lediglich die „Nutzlast“ des Pakets verschlüsselt, während im zweiten Fall das eigentliche Paket in ein neues verpackt und somit komplett geschützt übertragen wird. Das Schlüsselmanagement bei IPSec wird derzeit mit dem Internet Key Exchange Protocol (IKE) realisiert. Da dieses jedoch zu langsam, zu kompliziert und anfällig für DoS-Attacken ist, wird derzeit an einem Nachfolger gearbeitet, der diese Probleme

beseitigen soll. Eine typische Anwendung von IPSec ist die Virtual Private Network (VPN) Technologie. Für Unternehmen haben VPNs den Vorteil, dass sie auf teure Standleitungen zwischen Netzwerken an verschiedenen Orten verzichten können, da sie eine exklusive Punkt-zu-Punkt Verbindung (Tunnel) über das Internet aufbauen [SCHW02, S. 116; SCHM98, S. 269].

#### **4.5.7 Secure Socket Layer (SSL)**

Die Firma Netscape entwickelte 1994 das kryptographische Protokoll „SSL“, das mittlerweile in der Version 3.0 vorliegt und es geschafft hat, zum erfolgreichsten Internet-Sicherheitsstandard zu werden. SSL baut darauf auf, dass oberhalb der TCP-Schicht, also zwischen Transport- und Anwendungsschicht des OSI-Modells, eine zusätzliche „Sicherheitsschicht“ eingefügt wird. Im Wesentlichen wird SSL für die Verschlüsselung von Hypertext Transfer Protocol (HTTP) verwendet. Aufgrund der Tatsache, dass SSL unterhalb der Anwendungsschicht ansetzt, sind prinzipiell jedoch auch andere Anwendungen möglich. Auf der zusätzlichen, auch Record Layer genannten, Schicht wird die Verschlüsselung und Authentisierung realisiert, bevor die Daten über das Transportprotokoll TCP übertragen werden. SSL zeichnet sich dadurch aus, dass die kryptographischen Parameter mit Hilfe des Handshake-Protokolls automatisiert zwischen Client und Server ausgehandelt werden. SSL gilt als ein sicheres kryptographisches Verfahren. Schwachstellen wurden mit dem Wechsel von Version 2.0 auf 3.0 beseitigt, und bisher bekannt gewordene Angriffe wurden nur durch fehlerhafte Implementierungen des Standards ermöglicht [SCHW02, S. 87; SCHM98, S. 229].

## 5 Weitere Schwachstellen in Netzwerken und Gegenmaßnahmen

In den vorangegangenen Kapiteln wurde bereits eine Vielzahl von Schwachstellen von Funknetzen dargestellt. Im Folgenden wird auf weitere Schwachstellen hingewiesen und entsprechende Gegenmaßnahmen vorgestellt. Bei der Umsetzung von Gegenmaßnahmen bzw. der Konzeption eines Sicherheitsmodells kommt es darauf an, dass die eigentliche Nutzung der Netze nicht unnötig eingeschränkt wird und möglichst benutzerfreundlich bleibt. Bei allen Schutzmaßnahmen ist zu überlegen, in wie weit die entstehenden Kosten und Einschränkungen mit der Wichtigkeit vereinbar sind.

### 5.1 Schwachstelle „Mitarbeiter“

„Der Mensch ist fast immer das schwächste Glied in der langen Kette der Sicherheitsmaßnahmen. Die meisten Sicherheitsvorfälle im Unternehmen gehen von Mitarbeitern aus, nicht von externen Hackern“ [MEYE03, S. 55]. Typische Beispiele für von Mitarbeitern verursachte Sicherheitsvorfälle sind z. B. das unvorsichtige Öffnen von mit Viren, Würmern oder Trojanern verseuchten eMails oder die Missachtung von Sicherheitsvorschriften (z. B. die Nutzung und regelmäßige Aktualisierung von Sicherheitssoftware wie Personal Firewall oder Virens Scanner oder auch der Aufbau eigener Internetverbindungen). Hiergegen hilft nur eine gründliche Schulung der Mitarbeiter sowie eine möglichst effektive Verhinderung durch ein geeignetes Berechtigungsmanagement, automatisiertes Update der Sicherheitssoftware und Patchmanagement auf allen Systemen, Wechseldatenträger nur falls nötig usw. Laut einer Studie des Computer Security Institute aus dem Jahr 2000 haben 71 Prozent der Befragten unautorisierte Zugriffe von Insidern entdeckt. Dies zeigt, dass auch die Gefahr aktiver Angriffe durch Mitarbeiter

#### Passwort Policy

Die Passwort Policy enthält Regeln, die ein Passwort erfüllen muss, um „schwache“ Passwörter zu vermeiden. Beispielsweise sollte eine Mindestlänge und Verwendung von Zahlen und Sonderzeichen vorgeschrieben werden.

nicht zu unterschätzen ist [ANON01, S. 746]. Verwunderlich ist dies allerdings kaum, schließlich kennt der Mitarbeiter z. B. die Systeme und hat keine Firewall zu überwinden. Aus der von Mitarbeitern ausgehenden Gefahr folgt auch

die Notwendigkeit einer effektiven Zugriffskontrollverwaltung. Hierbei wird geregelt, wer wie und worauf zugreifen darf. Es versteht sich von selbst, dass jeder die Zugriffsrechte haben muss, die er für seine spezifischen Aufgaben benötigt, aber gleichzeitig mehr Berechtigungen auch mehr Risiko darstellen [MEYE02, S. 86]. Aufgrund der Gefahr, die von Mitarbeitern ausgeht ist es unerlässlich, diese dafür zu sensibilisieren und dazu zu bringen, sich an Sicherheitsrichtlinien zu halten, bzw. mit einer erzwungenen Passwort Policy überhaupt keine „schwachen“ Passwörter zuzulassen. Auch sicherheitskritische Softwareupdates (z. B. Virendefinitionen und Patches) sollten zentral ausgeführt und überwacht werden, damit die Sicherheit nicht von der Fahrlässigkeit einzelner Mitarbeiter untergraben wird. Es ist weiterhin darauf zu achten, dass Mitarbeiter keine eigenen, also illegalen APs (Rogue Device) betreiben, die mit unzureichenden Sicherheitseinstellungen zu einer Bedrohung der bestehenden Netzwerkinfrastruktur werden.

## **5.2 Unerlaubte Zugriffe auf Netze von außen**

Heutzutage verfügt in der Regel jedes Netzwerk über eine Verbindung zum Internet. Die damit verbundenen Vorteile implizieren zwangsläufig auch den großen Nachteil, dass Angreifer von jedem beliebigen Ort der Welt jedes beliebige Netzwerk attackieren können. Alles was sie dazu benötigen, ist ein Internetzugang.

### **5.2.1 Firewall**

Genau dieses Problem, dass Hacker von überall Daten stehlen, fälschen und löschen sowie ganze IT-Systeme lahm legen können, in den Griff zu bekommen, ist die Aufgabe von Firewalls. Sie bilden die Schnittstelle zwischen einem zu schützenden und einem unsicheren öffentlichen Netz wie dem Internet. Die Firewall soll regeln, welche Datenpakete vom unsicheren Netz in das gesicherte Netz gelangen dürfen [POHL03, S. 43]. Die Unterscheidung zwischen zulässigem und unzulässigem Datenverkehr bewerkstelligt eine Firewall mit Hilfe eines Regelwerks. In diesem Regelwerk wird z. B. festgelegt, zu welchen Adressen Verbindungen aufgebaut werden dürfen, welche Protokolle zugelassen sind und über welche Ports die Kommunikation laufen darf [POHL03, S. 185]. Damit dieses Konzept mit der Firewall als „Common Point of Trust“ (d. h. sie ist der einzige Weg aus dem gesicherten in das ungesicherte Netz) auch funktioniert, ist es unabdingbar, dass keine weiteren Verbindungen nach außen, sog. „Backdoors“, existieren. Wie bereits in 5.1 erwähnt, kann eine Firewall auch keinen Schutz gegen Angreifer bieten, die sich „hinter“ ihr, also im ge-

geschützten Netz, befinden. Als Instrument gegen Angriffe von Insidern bietet es sich an, auf internen Systemen Personal Firewalls zu installieren [POHL03, S. 354]. Dies ist insbesondere bei WLAN-Clients anzuraten, da diese angreifbarer sind als Endgeräte in einem kabelgebundenen Netz.

### **5.2.2 Monitoring und Intrusion Detection Systeme (IDS)**

Es wurden alle wesentlichen Schritte gezeigt, die notwendig sind, um ein möglichst gut geschütztes WLAN aufzubauen. Ein wesentlicher Sicherheitsaspekt ist die kontinuierliche Überwachung während des Betriebs. Ziel dieser Überwachung muss es sein, Konfigurationsfehler und Rogue Devices ausfindig zu machen und zu beseitigen. Es sollte außerdem versucht werden, bösartigen Datenverkehr frühzeitig zu entdecken. Während Firewalls lediglich zwischen zulässigem und unzulässigem „Traffic“ unterscheiden, kann der Einsatz eines IDS eine sinnvolle Ergänzung zur aktiven Erkennung von Angriffen sein. Intrusion Detection ist das „Erkennen unerlaubter Handlungen seitens eines Unbefugten (etwa eines feindlich gesonnenen Nutzers oder eines Einbrechers) zum Zwecke des Zugriffs auf ein System“ [ANON01, S. 290]. Diese so genannten IDS oder Monitoring Systeme sind z. B. in der Lage, anhand von Regelwerken Denial-of-Service Attacken, nicht autorisierte Geräte (Rogue Devices) oder auch Tools, die von Hackern verwendet werden (wie z. B. Netstumbler), aufzuspüren und den Netzwerkadministrator zu informieren. Weiter Informationen zu Monitoring Systemen finden Sie in [o.V.04, S. 26-36].

## 6 Fazit

<b>Leitfaden – Checkliste</b>	<b>ToDo's</b>	<b>Verant- wortlich</b>	<b>In Arbeit</b>	<b>Erledigt</b>
<b>Schritt 1: Planung</b>				
- Festlegung der Größe				
- Festlegung des Layouts				
- Erstellen eines Sicherheitsregel- werks				
- Auswahl der Hardware				
<b>Schritt 2: Absicherung des Access Point</b>				
- Ausrichtung / Funkausleuchtung				
- Standardpasswort ändern				
- Standard SSID ändern und Broad- cast deaktivieren				
- Mac-Filter einrichten				
- Standard IP-Bereich ändern und DHCP deaktivieren				
<b>Schritt 3 : Verschlüsselung und Authentifizierung</b>				
- WEP (nicht empfehlenswert)				
- WPA – PSK				
- WPA – 802.1x Authentifizierung				
- WPA2 – PSK				
- WPA2 – 802.1x Authentifizierung				
- 802.11i – PSK				
- 802.11i – 802.1x Authentifizierung				
- VPN				
<b>Schritt 4: Überwachung</b>				
- Intrusion Detection System (IDS)				
- Erkennen von inoffiziellen AP und Clients				
- Einhaltung der Sicherheitsregeln				

## Quellenverzeichnis

- [ANON01] Anonymuos: Der neue Hacker's Guide. Sicherheit im Internet und im Lokalen Netz. Markt und Technik Verlag, München 2001.
- [BARN02] Barnes Christian et al.: Die Hacker-Bibel für Wireless LANs. mitp-Verlag. Bonn 2002.
- [BLUM03] Blumenthal Bruno: Wireless LAN (IEEE 802.11) Security Glossar. In: [http://www.computec.ch/dokumente/unsortiert/wireless\\_lan\\_security\\_glossar.pdf](http://www.computec.ch/dokumente/unsortiert/wireless_lan_security_glossar.pdf), Erstellungsdatum vom 15.10.03.
- [KAUF02] Kauffels Franz-Joachim: Wireless LANs. mitp-Verlag, Bonn 2002.
- [MEYE03] Meyers Mike, Harris Shon: CISSP. Certified Information Systems Professional. mitp-Verlag, Bonn 2003.
- [o.V.01] Ohne Verfasser: 10 Wahrheiten über Richtfunk. In: [http://www.cbl.de/downloads/pdf/10\\_wahrheiten\\_or.pdf](http://www.cbl.de/downloads/pdf/10_wahrheiten_or.pdf), Erstellungsdatum vom 29.02.2001.
- [o.V.02] Ohne Verfasser: Wi-Fi Protected Access. Wi-Fi-Alliance. In: [http://www.wifi.org/OpenSection/pdf/Wi-Fi\\_Protected\\_Access\\_Overview.pdf](http://www.wifi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf), Erstellungsdatum vom 31.10.2002.
- [o.V.03c] Ohne Verfasser: Securing Wi-Fi Wireless Networks with Today's Technologies. Wi-Fi-Alliance. In: [http://www.wifi.org/OpenSection/pdf/Whitepaper\\_Wi-Fi\\_Networks2-6-03.pdf](http://www.wifi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Networks2-6-03.pdf), Erstellungsdatum vom 06.02.2003.
- [o.V.04] Ohne Verfasser: Flugüberwachung, WLAN-Monitoring-Systeme. In: Network Computing 8-9 (2004), S. 26.
- [o.V.05] Ohne Verfasser: Sichern von WLANs mit PEAP und Kennwörtern, Einführung: Festlegen einer Strategie für die WLAN-Sicherheit. In: <http://www.microsoft.com/germany/ms/security/guidance/modules/peap/int.mspx>, Informationsabfrage vom 15.01.05.
- [POHL03] Pohlmann Dr. Norbert: Firewall-Systeme. mitp-Verlag, Bonn 2003.
- [SCHÄ03] Schäfer Günter: Netzsicherheit. Algorithmische Grundlagen und Protokolle. Dpunkt-Verlag, Heidelberg 2003.
- [SCHM98] Safer Net: Kryptografie im Internet und Intranet. Dpunkt-Verlag, Heidelberg 1998.
- [SCHW02] Schwenk Jörg: Sicherheit und Kryptographie im Internet. Von sicherer eMail bis zu IP-Verschlüsselung. Vieweg-Verlag, Braunschweig 2002.