

Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals
in den Bereichen Softwareentwicklung,
Internettechnologie und IT-Management aktuell
und kompetent relevantes Fachwissen über
Technologien und Produkte zur Entwicklung
und Anwendung moderner Informationstechnologien.

Wolfgang W. Osterhage

sicher & mobil

Sicherheit in der drahtlosen Kommunikation

 Springer

Dr. Wolfgang W. Osterhage
Finkenweg 5
53343 Wachtberg-Niederbachem
Deutschland
wwost@web.de

ISSN 1439-5428
ISBN 978-3-642-03082-6 e-ISBN 978-3-642-03083-3
DOI 10.1007/978-3-642-03083-3
Springer Heidelberg Dordrecht London New York

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© Springer-Verlag Berlin Heidelberg 2010

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Einbandentwurf: KuenkelLopka GmbH, Heidelberg

Gedruckt auf säurefreiem Papier

Springer ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Inhaltsverzeichnis

1	Einführung	1
2	Grundzüge des WLAN	3
2.1	Kabel oder drahtlos?	3
2.1.1	Mobilität	3
2.1.2	Sicherheit	4
2.2	Funknetze: Grundlagen	5
2.2.1	Das Frequenzspektrum	5
2.2.2	Die Standards: Grundsätzliches	6
2.2.3	Die Symbiose: Computer- und Funktechnologien	6
2.2.4	Senden und Empfangen	8
2.2.5	Geordnete Datenübermittlung	9
2.2.6	Netzwerktopologien	11
2.2.7	Funktechnologien	12
2.3	Sicherheitsaspekte	16
2.3.1	Übergeordnete Sicherheitsaspekte	16
2.3.2	Risiken	17
2.4	Die wichtigsten Standards	19
2.4.1	Überblick	19
2.5	Der IEEE-802.11	22
2.5.1	Allgemeine Entwicklung	22
2.5.2	Die Erweiterungen im Einzelnen	23
2.6	OSI – die Physikalische Schicht im Detail	30
2.6.1	Das FHSS Verfahren	31
2.6.2	Das DSSS Verfahren	31
2.6.3	Die HR/DSSS Variante	32
2.6.4	Die OFDM Methode	33
2.7	OSI – die Medienzugriffsschicht	33
2.7.1	Verpackung	33
2.7.2	Kollision	34

2.7.3	Adressraum	35
2.7.4	SSID	36
2.7.5	Authentifizierung	37
2.7.6	Das Wired Equivalent Privacy – (WEP) Verfahren	38
2.7.7	WEP als Minimalschutz	41
2.7.8	WPA	41
2.7.9	Zertifizierung	42
2.8	WMAN	42
2.9	Rechtliche Aspekte	43
2.9.1	Lizenzfragen	43
3	WLAN Architektur	45
3.1	BSS	45
3.2	Der Ad-hoc-Modus	46
3.2.1	Von BSS zu IBSS	47
3.2.2	Die flexible Natur der Ad-hoc-Netze	47
3.3	Der Infrastruktur-Modus	47
3.3.1	LAN Gateway	48
3.3.2	Distribution Systems	49
3.4	Access Points	50
3.4.1	Dimensionierung	50
3.4.2	SSID	50
3.5	Internetzugang über das WLAN	51
3.5.1	Access Point und Router integriert	51
3.5.2	Die IP-Adresse	52
3.5.3	Unterhaltungsmedien	52
3.6	Hotspots	53
3.6.1	Sicherheit und offene Netze	54
3.7	Netzwechsel	54
4	WLAN Geräte	57
4.1	Übersicht	57
4.2	Adapter	58
4.2.1	Adapter für mobile Endgeräte	58
4.2.2	Adapter für PCs	59
4.3	Access Points	60
4.3.1	WLAN-Access-Point	60
4.3.2	WLAN-Router	60
5	WLAN einrichten und konfigurieren	61
5.1	Treiber	61
5.2	Hardware und Konfiguration	62
5.2.1	WLAN-USB-Adapter	62
5.2.2	WLAN-Cardbus-Adapter	62
5.2.3	PCI-Adapter	62

5.2.4	Access Point	63
5.2.5	Router	63
5.3	Checkliste WLAN	64
6	PDAs	73
6.1	Weitere drahtlose Elemente im Netzwerk	73
6.2	Hardware-Komponenten	73
6.2.1	PDAs	74
6.2.2	BlackBerries	77
6.2.3	Drucker	78
6.3	Standards	79
6.3.1	802.11b	79
6.3.2	802.11g	79
6.4	Konfiguration	80
6.4.1	Access Points	80
6.4.2	PDA Adapter	80
6.4.3	Integrierte WLAN-Funktionalitäten	83
6.5	Sicherheitsaspekte	83
6.5.1	Grundsätzliche Gefährdungspotentiale	84
6.5.2	Strategische Maßnahmen	84
6.5.3	Organisatorische Maßnahmen	85
6.5.4	Konkrete Gefährdungsszenarien	89
6.5.5	Sonderfall BlackBerries	91
6.5.6	PDA Direktive	94
6.6	Checkliste PDA	97
7	Mobilfunkgeräte	103
7.1	Einordnung	103
7.2	Grundlagen	104
7.2.1	Kommunikationsstruktur	104
7.2.2	Gerätearchitektur	105
7.3	Betriebssysteme	107
7.3.1	GSM	107
7.3.2	GPRS	108
7.3.3	UMTS	108
7.4	Dienste	108
7.4.1	SMS/EMS/MMS	109
7.4.2	WAP	110
7.4.3	i-mode	110
7.5	Mobilfunk und WLAN	110
7.5.1	Infrastruktur	110
7.5.2	Endgeräte	111
7.6	Bedrohungen und Schutz	111
7.6.1	Grundsätzliche Gefährdungspotentiale und strategische Gegenmaßnahmen	111

7.6.2	Konkrete Gefährdungsszenarien im Mobilfunkbereich	114
7.6.3	Generelle Vorsichtsmaßnahmen	118
7.7	Sonderfall BlackBerries	119
7.8	Smart Phones	120
7.8.1	iPhone	121
7.8.2	VoIP	123
7.9	Sicherheitscheck	123
7.10	Richtlinie	124
7.11	Checkliste	126
8	Bluetooth	133
8.1	Einleitung	133
8.2	Technische Grundlagen	133
8.2.1	Protokolle	134
8.2.2	Systemtopologie	136
8.3	Konfiguration	137
8.3.1	Optionen	137
8.3.2	Konfiguration	138
8.3.3	Netzwerkverbindungen	139
8.4	Sicherheitsaspekte	139
8.4.1	Instrumente	140
8.4.2	Gefährdungspotentiale	142
8.4.3	Gegenmaßnahmen	144
8.5	Zukunft	145
8.5.1	Weiterentwicklung	145
8.5.2	Nutzungsfelder	145
8.6	Checkliste	146
9	Sicherheitsrichtlinie	149
9.1	Einleitung	149
9.1.1	Sicherheitsanforderungen	149
9.1.2	Risiken	150
9.1.3	Maßnahmen	150
9.2	Geltungsbereiche	150
9.2.1	Normative Verweisungen	151
9.3	Informations- und Kommunikationssicherheit	152
9.3.1	Strategische Einbindung	153
9.3.2	Sicherheitsorganisation	154
9.3.3	Genehmigungsverfahren	154
9.3.4	Vertraulichkeit	155
9.4	Physische Sicherheit	156
9.4.1	Objekte	156
9.4.2	Zutritt	156
9.4.3	Bedrohungen	156
9.4.4	Betriebsmittel	157

9.4.5	Versorgungseinrichtungen	157
9.4.6	Entsorgung	157
9.5	Dokumentation	158
9.5.1	Prozesse	158
9.5.2	Verbindlichkeiten	159
9.6	Drahtlose Sicherheit	160
9.7	Zusammenfassung	161
Bibliographie		163
Sachverzeichnis		165

Abkürzungen

AAI	Authentication Algorithm Identification
ACL	Asynchronous Connectionless Link
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Exchange
AUC	Authentication Center
BDA	Bluetooth Device Address
BDGS	Bundesdatenschutzgesetz
BES	BlackBerry Enterprise Server
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BSC	Base Station Controller
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Basic Service Set
BTS	Base Transceiver Station
CCK	Complementary Code Keying
CD	Compact Disk
CEPT	Conference Europeenne des Postes et Telecommunications
CF	Compact Flash
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DUN	Dialup Network Profile
DVD	Digital Versatile Disc
EAP	Extensive Authentication Protocol

EIR	Equipment Identity Register
EMS	Enhanced Message Service
ESS	Extended Service Set
ETSI	European Telecommunications Standardisation Institution
EU	European Union
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FMC	Fixed Mobile Convergence
FTP	File Transfer Profile
FÜV	Fernmeldeverkehr-Überwachungs-Verordnung
GAP	Generic Access Profile
GFSK	Gaussian Shift Keying
GHz	Gigahertz
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	General User Interface
HID	Human Interface Device Profile
HIPERLAN	High Performance Radio Local Network
HomeRF	Home Radio Frequency
HR/DSSS	High Rate/Direct Sequence Spread Spectrum
HRL	Home Location Register
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HSP	Head Set Profile
IBSS	Independent BSS
ICV	Integrity Check Value
ID	Identifier
IEEE	Institute of Electrical and Electronic Engineers
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISM	Industrial, Scientific, Medical
ISO	International Organisation for Standardisation
IT	Information Technology
ITU	International Telecommunications Union
IuKDG	Informations- und Kommunikationsdienstegesetz
IV	Initialisierungsvektor
Kbit/s	Kilobits per second
kHz	Kilohertz
km	Kilometer
L2CAP	Logical Link Control and Adaption Protocol
LAN	Local Area Network
LLC	Logical Link Control
m	Meter
MAC	Medium Access Control

MAN	Metropolitan Area Network
MBit/s	Megabits per second
MDS	Mobile Data Service
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MMS	Multimedia Message Service
MPDU	MAC Protocol Data Units
MSC	Mobile Switching Center
mW	Milliwatt
NAT	Network Address Translation Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OpenSEA	Open Secure Edge Access
OSI	Open Systems Interconnection Model
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PHY	Physical Layer
PIM	Personal Information Manager
PIN	Personal Identification Number
PPPoE	Point to Point Protocol over Ethernet
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial In User Service
RC4	Rivest Cipher No. 4
RFCOMM	Radio Frequency Communication
RFID	Radio Frequency Identification
RIM	Research In Motion
ROM	Random Access Memory
RSN	Robust Security Network
RTS	Request To Send
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAP	SIM Accessy Profile
SCO	Synchronous Connection Oriented
SDMA	Spatial Division Multiple Access
SDP	Service Discovery Protocol
SIG	Special Interest Group
SigG	Signaturgesetz
SIM	Subscriber Identity Module
SMS	Short Message Service
SPAM	Spiced Pork And Meat
SPIT	SPAM over Internet Telephony
SSID	Server Set Identifier
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	Telephony Control Protocol Specification

TDK	Teledienstegesetz
TDSV	Teledienste-Datenschutzverordnung
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
UMA	Unlicensed Mobil Access
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIMAX	World Wide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Network
WPA	Wi-Fi Protected Access
WPS	Wireless Provisioning Service
XOR	eXclusive OR

Kapitel 1

Einführung

Das vorliegende Buch gibt in komprimierter Form, aber dennoch umfassend, den aktuellen Stand der drahtlosen Kommunikationstechnologie wieder. Besondere Aufmerksamkeit erfahren dabei die Sicherheitsaspekte. Berücksichtigung finden folgende Themenkomplexe:

- WLAN
- PDAs
- Mobiltelefonie und
- Bluetooth.

Keine Berücksichtigung haben zunächst gefunden:

- Infrarot
- Abstrahlung
- VoIP im Detail
- Skype.

Da WLAN das umfassendste und grundlegende Thema ist, sind ihm drei Kapitel gewidmet: Grundlagen, Geräte und Konfiguration. Alle anderen Themen werden in den darauf folgenden Kapiteln jeweils für sich abgehandelt. Es ist nicht unbedingt erforderlich, das ganze Buch zu lesen, wenn man sich beispielsweise für Sicherheitsprobleme beim Mobilfunk interessiert. Die Kapitel sprechen in der Regel für sich.

Nach den technologischen Grundlagen werden die möglichen Bedrohungsszenarien vorgestellt, gefolgt von den organisatorischen und technischen Gegenmaßnahmen. Sowohl Bedrohungsszenarien als auch Gegenmaßnahmen können sich für unterschiedliche Themenkomplexe bzw. Technologien (z. B. PDAs und Mobilfunk) gelegentlich überlappen. Da das Buch nach Technologien und nicht nach Sicherheitsaspekten gegliedert ist, sind mitunter Redundanzen sichtbar. Das ist so gewollt, da die einzelnen Kapitel ja für sich genommen sprechen sollen.

Ähnliches gilt für die umfangreichen Checklisten, die mitgeliefert werden. Vom Grundaufbau her beginnen sie immer mit strategischen Ansätzen, um dann mehr und mehr auf technische Details einzugehen. Die Checklisten sind als zweispaltige Tabellen ausgeführt. In der linken Spalte erscheinen Fragen, die rechts erläutert

werden (warum ist etwas beachtenswert?). Bei sicherheitsrelevanten Fragen, hinter denen ernsthafte Bedrohungen liegen können, erfolgt in der Zeile darunter in kursiv ein erweiterter Hinweis, der auch als Warnung verstanden werden kann. Jeder Technologie ist am Schluss des Kapitels eine solche Checkliste zugeordnet. Die Checkliste für WLAN für alle drei Kapitel erscheint erst am Ende des dritten Kapitels.

Für viele Sicherheitsprobleme werden auch organisatorische Maßnahmen angeboten. Deshalb ist an einigen Stellen auch von Richtlinien die Rede. In den Kapiteln über PDAs und Mobiltelefone werden jeweils einfache Richtlinien als Durchführungsbestimmungen vorgestellt. Im letzten Kapitel wird eine umfassende Richtlinie, die in eine unternehmensstrategische Gesamtdokumentation eingebettet werden kann, strukturell vorgestellt. Die einleitenden Abschnitte können mehr oder weniger wie präsentiert übernommen werden, für die Technologie-spezifischen Teile wird ein Raster vorgegeben, dass sich aus dem inhaltlichen Material der Vor-Kapitel füttern lässt.

Obwohl viele Beispiele und Szenarien aus dem Alltag von Organisationen und Unternehmen stammen, auch etliche organisatorische Lösungsansätze, sind die beschriebenen Sicherheitsprobleme ebenso relevant für die Nutzung von drahtloser Kommunikation im privaten Bereich. Die meisten Fragen in den Checklisten treffen auf die einzelne Station zuhause wie auf große Rechnernetze in Firmen zu. Das gilt gleichermaßen auch für die technischen Gegenmaßnahmen.

Als weitere praktische Hilfe werden Konfigurationsdialoge für WLAN-Geräte, PDAs und Bluetooth-Geräte dokumentiert. Beispielhaft für eine besondere Geräteklasse werden BlackBerries behandelt, die eine eigene Sicherheitsphilosophie mit sich bringen. Ansonsten ist der Versuch unternommen worden, den neuesten Stand der Technologie, soweit sie in den breiten Markt gedrungen ist, zu berücksichtigen. Angesichts der Kurzlebigkeit von Technologien kann das wiederum auch nur eine Momentaufnahme sein, die hoffentlich dennoch einen gewissen Bestand haben wird.

Kapitel 2

Grundzüge des WLAN

Die Vernetzung von Computern und deren Komponenten hat sowohl für Organisationen als auch private Nutzer eine neue Qualität durch den Einsatz von drahtlosen Übertragungen erreicht. Am vorläufigen Ende dieser Entwicklung steht das WLAN mit seinen ihm eigenen Sicherheitsanforderungen, die Gegenstand dieses und der beiden folgenden Kapitel sein sollen. WLAN steht für *Wireless Local Area Network* oder „drahtloses lokales Netzwerk“ oder „drahtloses lokales Funknetz“.

2.1 Kabel oder drahtlos?

Verkabelung bindet Systeme und User an feste Orte, während drahtlose Anwendungen den Anwender von Leitungssystemen befreit. Er wird auch im Hinblick auf seine IT-Systeme mobil. Optisch scheint sich sein Arbeitsplatz von sterilen Büroräumen hin zur Gartenlaube zu wandeln (wenn man entsprechenden Werbespots Glauben schenken will). Und überall auf der Welt kann man sich – ganz so wie mit dem Mobiltelefon – an jedem beliebigen Ort ins Firmennetz einklinken, vorausgesetzt, es sind genügend Hotspots in der Nähe. So ganz ist diese Vision zwar noch nicht realisiert, aber in Teilen ist sie doch schon Wirklichkeit – mit all den Sicherheitsproblemen, die das mit sich bringt.

2.1.1 Mobilität

Neben den Veränderungen in den Arbeitsprozessen, die durch den Einsatz von Mobiltelefonen eingetreten sind, ergeben sich durch die Möglichkeiten einer mobilen Vernetzung weitere Entwicklungsschübe. So gibt es eine Vielzahl von Arbeitsfeldern, die sich für mobile Anwendungen anbieten, bzw. die ohne eine solche heute fast nicht mehr denkbar sind: Großbaustellen, Logistikunternehmen, große Lagerhäuser, Supermärkte, aber auch im Klinikbereich, wo dezentrale medizinische Daten lebensrettend sein können. Ein weiterer Vorteil mobiler Datenkommunikation liegt in der Abwicklung unterbrechungsfreier Prozesse. Man braucht nicht an

seinen Stammarbeitsplatz zurück zu kehren, um Informationen zu suchen, sondern kann sie dort abfragen, wo sie gerade gebraucht werden.

Unabhängig von Performance-Gesichtspunkten (die aber gelöst werden können) unterscheiden sich in der Praxis für den Enduser LAN- und WLAN-Lösungen nicht. Neben Kriterien wie Mobilität gibt es aber noch weitere Gesichtspunkte, bei denen WLAN-Lösungen vorzuziehen sind: Kostenersparnis bei aufwendigen Verkabelungen – insbesondere bei älteren Gebäuden, bei denen bauliche Strukturen den Aufbau eines Backbone unmöglich machen können. Und natürlich als temporäre Lösungen auf Veranstaltungen, Messen oder zeitlich begrenzter Gruppenarbeit im Projekt, in Unternehmen. Funknetze sind flexibel und zeitnah zu realisieren.

Einen ganz besonderen Aufschwung der WLAN-Anwendungen hat es in letzter Zeit insbesondere auch im privaten, häuslichen Bereich gegeben. Da hier häufig eine professionelle Unterstützung fehlt, ist bei diesen Anwendungen mit erhöhten Sicherheitsrisiken zu rechnen.

2.1.2 Sicherheit

Eine drahtlose Vernetzung setzt sich anderen Gefährdungen aus als Festnetzanwendungen. Das liegt an der verwendeten Form der Datenübertragung per Funk. So können Angreifer z. B. vom Auto auf einem Parkplatz mit einem Notebook und unter Umständen auf Basis einer Chips-Dose mit Antenne die Funkkommunikation im Hause abhören.

Solche Aktivitäten nennt man Wardriving. Im Internet kursieren dazu mittlerweile Webseiten, die ungeschützte WLANs in bestimmten Städten und Regionen auflisten. Deshalb besteht eine gewisse Dringlichkeit zur Absicherung der Funkvernetzung, bzw. zur Entwicklung von entsprechenden Schutzmaßnahmen.

2.1.2.1 Öffentliche und private Netze

Es gibt natürlich eine Vielzahl von Netzen, die der Öffentlichkeit frei zugänglich sind: Internet, Bibliotheken, städtische Informationssysteme und so weiter. Diese Netzwerke enthalten keine vertraulichen Informationen, die komplizierte Zugangsverifikationen benötigen. Geht es aber um Netzwerke im privaten Bereich und um Teile der Informationssysteme von Firmen oder Behörden, kommen zu den aus der klassischen LAN-Welt bekannten Sicherheitsproblemen völlig neue Gefährdungen hinzu. Diese Gefährdungen liegen in der Natur des Übertragungsmediums begründet. Radiowellen sind abhörbar und können von außen massiv gestört werden.

2.1.2.2 Die Anfänge der Sicherheit im WLAN

Von Anfang an war das Bewusstsein der zusätzlichen Gefährdung von WLANs bei den Entwicklern der zugehörigen Standards vorhanden. So wurden auch

entsprechende Verfahren mitgeliefert, die dem Rechnung tragen sollten. Das bekannteste frühe Verschlüsselungssystem läuft unter der Bezeichnung WEP. WEP erwies sich aber schon bald als unzureichend. Mittlerweise werden entsprechende Hacking-Tools im Internet angeboten, mit denen man WEP relativ leicht knacken kann.

Verbesserung gab es im Jahre 2004 mit dem Standard 802.11i der IEEE. Das Problem heute ist allerdings, dass noch immer zahlreiche Komponenten im Gebrauch sind, die die angebotenen Lösungen nicht unterstützen. Dazwischen gibt es Lösungen wie zum Beispiel WPA, die eine weite Verbreitung gefunden haben. Dazu weiter unten mehr.

2.2 Funknetze: Grundlagen

WLAN ist die Abkürzung für Wireless Local Area Network. Diese Bezeichnung weist schon darauf hin, dass LAN-Funktionalitäten drahtlos bereitgestellt werden. Drahtlos geht allerdings über den reinen klassischen Funkverkehr hinaus und kann auch zum Beispiel den Infrarotbereich (nicht Gegenstand der aktuellen Ausgabe des vorliegenden Buches) mit einbeziehen.

Häufig findet man in realisierten Konfigurationen die Kopplung von WLAN und LAN, wobei WLAN-Komponenten oft Frontends von größeren Anwendungen sind. Die WLAN-Teile stehen solchen Anwendern zur Verfügung, deren Aufgabenstruktur im Unternehmen eine hohe Mobilität voraussetzt. Der Phantasie bei Netzkopplungen sind keine Grenzen gesetzt bis hin zur Verbindung mehrerer LANs zu MANs (Metropolitan Area Networks).

2.2.1 Das Frequenzspektrum

Die physikalischen Unterscheidungsmerkmale bei der Klassifikation der elektromagnetischen Wellen für eine WLAN-Kommunikation sind Frequenz und Wellenlänge. Aus den insgesamt verfügbaren Frequenzen lassen sich bestimmte Frequenzbereiche bzw. Frequenzbänder differenzieren. Die Medien Radio und Fernsehen arbeiten im Bereich der Lang- bis Ultrakurzwellen, der zwischen 30 kHz und 300 MHz liegt. Funknetze, die hier betrachtet werden, bewegen sich zwischen 300 MHz und 5 GHz.

Das erste für diese Zwecke durch die Federal Communications Commission (FCC) zur Lizenz freien Nutzung freigegebene Frequenzband war das sogenannte ISM-Band. Das war im Jahre 1985. ISM steht für: Industrial, Scientific, Medical. Aus diesem Band bedienen sich die WLANs – und zwar zwischen 2,4 und 5 GHz. Das war der Startschuss für die Entwicklung entsprechender Komponenten durch die Privatindustrie.