Wolfgang W. Osterhage

Sicherheitskonzepte in der mobilen Kommunikation

Drahtlose Kommunikation – Protokolle und Gefahren

Springer Vieweg

Sicherheitskonzepte in der mobilen Kommunikation

Wolfgang W. Osterhage

Sicherheitskonzepte in der mobilen Kommunikation

Drahtlose Kommunikation – Protokolle und Gefahren

Springer Vieweg

Wolfgang W. Osterhage
Wachtberg-Niederbachem
Deutschland

ISBN 978-3-662-57902-2 ISBN 978-3-662-57903-9 (eBook)
https://doi.org/10.1007/978-3-662-57903-9

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

Springer Vieweg

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Die Verlinkung von Computern und deren Komponenten hat mit den Möglichkeiten der drahtlosen Kommunikation eine neue Qualität erreicht – sowohl für private Nutzer als auch für Organisationen. Diese Entwicklung führt zu neuen Herausforderungen für die IT-Sicherheit. Darum geht es in diesem Buch. Die gesamte Bandbreite der drahtlosen Kommunikation wird abgedeckt (WLAN, Bluetooth, Mobiltelefonie u. a.) mit detaillierten Beschreibungen der Technologie, der Standards, Verschlüsselung und Konfiguration. Aber das ist nicht alles.

Um einen Komplettcheck seiner drahtlosen Anwendungen zu gewährleisten, benötigt der IT-Sicherheitsverantwortliche den Überblick über eine Vielzahl kritischer Bereiche. Er muss sicher stellen, dass ein Eindringling keinen Zugriff auf interne Daten oder Systemfunktionalitäten erhält. Um diese Aufgabe zu unterstützen, werden ihm umfassende Checklisten an die Hand gegeben. Hierdurch werden alle wesentlichen Aspekte drahtloser Sicherheit abgedeckt.

Mein Dank gilt Herrn Martin Börger und Frau Sophia Leonhard und dem Team von Springer Vieweg, die mich beim Verfassen des Buches professionell begleitet haben.

Wachtberg, den 25. Juli 2018

Inhaltsverzeichnis

1 Einführung 1

2 Vorteile drahtloser Kommunikation 3
- 2.1 Kabel oder drahtlos? 3
  - 2.1.1 Mobilität 3
- 2.2 Grundsätzliche Sicherheitsaspekte 4
  - 2.2.1 Öffentliche und private Netze 4
- 2.3 Übergeordnete Sicherheitsaspekte 5
  - 2.3.1 Netzverfügbarkeit 5
  - 2.3.2 Problem der Datenintegrität 5
  - 2.3.3 Wechselseitige Authentizität 5
  - 2.3.4 Anforderungen an die Vertraulichkeit 5
- 2.4 Risiken 6
  - 2.4.1 Angreifer und ihre Motive 6

3 WLAN 7
- 3.1 Funknetze: Grundlagen 7
  - 3.1.1 Das Frequenzspektrum 7
  - 3.1.2 Die Standards: Grundsätzliches 8
- 3.2 Die Symbiose: Computer- und Funktechnologien 8
  - 3.2.1 Vorteile von ISM 8
  - 3.2.2 WLAN-Komponenten 9
  - 3.2.3 Access Points 9
- 3.3 Senden und Empfangen 10
  - 3.3.1 Typen 10
  - 3.3.2 Leistung 10
  - 3.3.3 Interferenzen 10
- 3.4 Geordnete Datenübermittlung 11
  - 3.4.1 Einsatz von Routern 11
  - 3.4.2 Nachrichtenpakete 11
- 3.5 Netzwerktopologien 13

3.6 Funktechnologien . . . 14
3.6.1 Das Modulationsverfahren . . . 15
3.6.2 Bandbreite . . . 16
3.6.3 Reichweite von Funksignalen . . . 16
3.6.4 Kanalverteilung . . . 17
3.6.5 Trennung von Kanälen . . . 17
3.7 Die wichtigsten Standards . . . 18
3.7.1 Überblick . . . 18
3.8 Der IEEE-802.11 . . . 21
3.8.1 Allgemeine Entwicklung . . . 21
3.8.2 Die Erweiterungen im Einzelnen . . . 22
3.9 WLAN Architektur . . . 26
3.9.1 BSS . . . 27
3.9.2 Der Ad-hoc-Modus . . . 27
3.9.3 Der Infrastruktur-Modus . . . 28
3.9.4 Access Points . . . 31
3.9.5 Internetzugang über das WLAN . . . 32
3.9.6 Hot Spots . . . 33
3.9.7 Netzwechsel . . . 36
3.10 Sicherheitsaspekte bei WLANs . . . 36
3.10.1 Verschlüsselung knacken . . . 37
3.10.2 Authentifizierung . . . 37
3.11 Checkliste – WLAN . . . 42

4 Mobilfunk . . . 53
4.1 Mobilfunkgeräte . . . 53
4.1.1 Einordnung . . . 53
4.1.2 Grundlagen . . . 53
4.2 Kommunikationsprotokolle . . . 64
4.2.1 GSM . . . 64
4.2.2 HSCSD . . . 65
4.2.3 GPRS . . . 65
4.2.4 UMTS . . . 65
4.2.5 HSDPA . . . 66
4.2.6 LTE . . . 66
4.2.7 5G . . . 66
4.2.8 Dienste . . . 66
4.3 Sicherheitsaspekte beim Mobilfunk . . . 68
4.3.1 Allgemeine organisatorische Maßnahmen . . . 69
4.3.2 Allgemeine technische Maßnahmen . . . 70
4.3.3 Konkrete Gefährdungsszenarien im Mobilfunkbereich . . . 70
4.3.4 Generelle Vorsichtsmaßnahmen . . . 75
4.4 Checkliste – Mobiltelefone . . . 76

5 Bluetooth 85
5.1 Einleitung 85
5.2 Technische Grundlagen 85
5.2.1 Protokolle 85
5.2.2 Systemtopologie 89
5.3 Version 5.0 91
5.4 Sicherheitsaspekte bei Bluetooth 92
5.4.1 Instrumente 92
5.4.2 Gefährdungspotenziale 95
5.4.3 Gegenmaßnahmen 97
5.4.4 Bezahltransaktionsproblematik 98
5.5 Checkliste – Bluetooth 98

6 Infrarot 103
6.1 Hintergrund 103
6.2 IrDA 103
6.2.1 Allgemeines 104
6.2.2 Protokoll 105
6.3 Anwendungen 106
6.3.1 Endgeräte 107
6.3.2 Voraussetzungen 107
6.3.3 Kommunizieren 107
6.4 Sicherheitsaspekte bei IrDA 109
6.5 Checkliste – Infrarot 110

7 Near Field Communication 111
7.1 Einleitung 111
7.2 Technologie allgemein 111
7.2.1 Geschichte 111
7.3 Spezifikationen 112
7.3.1 Protokoll 112
7.3.2 Technologien im Einzelnen 113
7.3.3 NFC Forum Spezifizierungen 114
7.4 Sicherheitsaspekte 115
7.4.1 Bezahlkartenproblematik 116

8 Internet of Things 117
8.1 Einleitung 117
8.2 Informationslogistik 117
8.2.1 Kritische Informationen am Beispiel ERP 118
8.3 Kanban 119
8.4 Von der Ubiquität zum Internet der Dinge 120
8.5 Die Praxis 122
8.6 Sicherheitsaspekte 123

9 Sicherheitsrichtlinie 125
9.1 Einleitung 125
9.1.1 Sicherheitsanforderungen 125
9.1.2 Risiken 126
9.1.3 Maßnahmen 126
9.2 Geltungsbereiche 126
9.2.1 Normative Verweisungen 127
9.3 Informations- und Kommunikationssicherheit 128
9.3.1 Strategische Einbindung 129
9.3.2 Sicherheitsorganisation 130
9.3.3 Genehmigungsverfahren 131
9.3.4 Vertraulichkeit 132
9.4 Physische Sicherheit 132
9.4.1 Objekte 132
9.4.2 Zutritt 133
9.4.3 Bedrohungen 133
9.4.4 Betriebsmittel 133
9.4.5 Versorgungseinrichtungen 134
9.4.6 Entsorgung 134
9.5 Dokumentation 134
9.5.1 Prozesse 135
9.5.2 Verbindlichkeiten 135
9.6 Drahtlose Sicherheit 136
9.7 Zusammenfassung 137

10 Telematik 139
10.1 Definition 139
10.2 Einleitung 139
10.3 Big Data 140
10.4 Einsatzbereiche 141
10.5 Wearables und Technologien 141
10.6 Telematik in den Kfz-Versicherungen 143
10.7 Telematik in der Krankenversicherung 145
10.8 Telematik im Energiesektor 147
10.9 Bezahlterminals 148
10.10 Telematik in der Verbrechensbekämpfung: Pre-Crime–Analytics 148
10.11 Internet-Spione 149
10.12 FutureICT 150
10.13 Fazit 151

11 Rechtliche Aspekte 153
11.1 Gesetzliche Vorschriften 153
11.2 Rechtliche Probleme beim Test von Malware 153

11.2.1 Gesetzestext 154
11.2.2 Malware 155
11.2.3 Sicherheitsprüfungen 155
11.2.4 Dual-Use 156
11.2.5 Beispiele. 156
11.2.6 Risiken 156
11.2.7 Auswirkungen 157
11.3 Störerhaftung 157
11.4 DSGVO 158

Stichwortverzeichnis 159

Einführung

1

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
- Mobiltelefonie
- Bluetooth
- Infrarot und
- NFC

Keine Berücksichtigung haben gefunden:

- VoIP im Detail
- Skype.

Die einzelnen Kommunikationsprotokolle werden in jeweils einzelnen Kapiteln abgehandelt. Zum Verständnis ist es 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 jeweiligen 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 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.

W. W. Osterhage, *Sicherheitskonzepte in der mobilen Kommunikation*,
https://doi.org/10.1007/978-3-662-57903-9_1

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.

Für viele Sicherheitsprobleme werden auch organisatorische Maßnahmen angeboten. Deshalb ist an einigen Stellen auch von Richtlinien die Rede. In einem gesonderten Kapitel wird eine umfassende Richtlinie, die in unternehmensstrategische Gesamtdokumentation eingebettet werden kann, strukturell vorgestellt. Die einleitenden Abschnitte können mehr oder weniger wie präsentiert übernommen werden, für die technologiespezifischen 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 Rechnerverbünde in Firmen zu. Das gilt gleichermaßen auch für die technischen Gegenmaßnahmen.

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.

Vorteile drahtloser Kommunikation

2

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 Hot Spots 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 sie mit sich bringt.

Andererseits lässt sich die Frage „Kabel oder drahtlos?“ in der Praxis meistens nicht mit ja oder nein beantworten. Komplexe Anwendungen verlange heute beides in Kombination. Feste installierte Netze mit zentralen Anwendungen verfügen über Gateways über die von außen drahtlos zugegriffen werden kann.

2.1.1 Mobilität

Neben den Veränderungen in den Arbeitsprozessen, die durch den Einsatz von Mobiltelefonen oder Tablets 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.

W. W. Osterhage, *Sicherheitskonzepte in der mobilen Kommunikation*,
https://doi.org/10.1007/978-3-662-57903-9_2

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.

2.2 Grundsätzliche Sicherheitsaspekte

Eine drahtlose Vernetzung setzt sich anderen Gefährdungen aus als Festnetzanwendungen. Das liegt an der verwendeten Form der Datenübertragung per Funk. In den Anfangsphasen des WLAN konnten 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. Durch die WLAN-Fähigkeiten von Smartphones lassen sich bei einem Spaziergang z. B. durch ein Wohnviertel jede Menge WLAN-Zugänge aufspüren, die sich durch Aussenden der Beacon Frames bemerkbar machen.

2.2.1 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 Netzte enthalten keine vertraulichen Informationen, die komplizierte Zugangsverifikationen benötigen. Geht es aber um Netzte 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.

Öffentliche Netze sind für jedermann frei verfügbar, sobald Zugangsbedingungen und Kosten geklärt sind. Auf jeden Fall sind die Informationen nicht durch Vertraulichkeitsregelungen geschützt. Deshalb spielen die üblichen Sicherheitsverfahren wie Verschlüsselung auch beim Zugriff über Hot Spots keine Rolle. Aus Gründen der Einfachheit wird dann in der Regel für die SSID der Jokername „Any“ verwendet.

2.3 Übergeordnete Sicherheitsaspekte

2.3.1 Netzverfügbarkeit

Störungen bei Funknetzen sind ein grundsätzliches Problem. Hierbei geht es nicht um zufällige Störungen durch Geräte, die denselben Frequenzbereich nutzen.. Es gibt Störungen, die bewusst von Angreifern hervorgerufen werden, um den Funkverkehr zu sabotieren.

Zur Disposition steht dabei eines der wesentlichen Ziele beim Betrieb von IT-Anlagen: die Verfügbarkeit. Zunächst wird diese sichergestellt durch die konkrete Netztopologie selbst, d. h. die geografische Fixierung der Netzelemente. Von Bedeutung ist auch eine optimale Konfiguration unter Berücksichtigung des Betriebsmodus, der Frequenzbereiche und der Übertragungsgeschwindigkeit. Wegen der Störanfälligkeit ist eine kontinuierliche Beobachtung des Netzbetriebs erforderlich. Bei Störungen sollte die Ursache möglichst zeitnah gefunden werden.

2.3.2 Problem der Datenintegrität

In Funknetzen wie auch in drahtgebundener Umgebung muss sichergestellt werden, dass alle Daten ihren Adressaten vollständig und unverändert erreichen. Falls die Daten unterwegs manipuliert worden sind, muss der Empfänger diesen Umstand wahrnehmen können, um auf eine solche Manipulation reagieren zu können. Vom Ergebnis her ist es unerheblich, ob eine solche Störung durch bewusste Manipulation oder durch technisch bedingte Übertragungsfehler hervorgerufen wird.

2.3.3 Wechselseitige Authentizität

Eine wesentliche Rolle bei der drahtlosen Kommunikation spielt die Authentizität. Jede Station muss sich der Authentizität, d. h. auch der Berechtigung, des gegenüberliegenden Kommunikationspartners sicher sein. Das gilt für Sender und Empfänger und genauso umgekehrt. Es muss sichergestellt sein, dass niemand unbefugt ins Netz eindringen kann, dadurch dass er sich als gültiges Mitglied der Netzteilnehmer verstellt. Selbstverständlich gilt diese Anforderung besonders dann, wenn sensible Daten ausgetauscht werden, die für den Geschäftsverkehr und die Unternehmenssicherheit von Bedeutung sind.

2.3.4 Anforderungen an die Vertraulichkeit

Gegenüber der Kommunikation in offenen Netzen, die gerade auf die allgemeine Teilhabe an allen zugänglichen Informationen ausgelegt sind, spielt die Vertraulichkeit des

Informationsaustausches in privaten drahtlosen Netzen aus Sicht des Datenschutzes eine ganz andere Rolle. Hier müssen entsprechende Geheimhaltungsstufen tatsächlich zum Tragen kommen. Da Funksignale prinzipiell mitgehört werden können, geht dieser Weg nur über eine Verschlüsselung. Eine Verschlüsselung erfüllt dabei zwei Aufgaben:

- Sie sollte die übermittelten Informationen und
- die zugehörigen Verbindungsdaten schützen.

2.4 Risiken

Aus der Tatsache, dass bei der Funkübertragung gewissermaßen der freie Raum als Übertragungsmedium genutzt wird, ist das Abhören einfacher als bei drahtgebundenen Anwendungen. Entsprechend drastisch ändern sich die Anforderungen durch die spezifische Sicherheitslage gegenüber verkabelten LANs. LANs sind zudem geografisch fixiert. Deren Anwender sind bekannt. Bei WLANs gibt es weder Gebäudegrenzen noch ist sichtbar, welche Personen gerade zugreifen.

2.4.1 Angreifer und ihre Motive

Hier die wichtigsten Angriffsmotive und -formen:

- technische Herausforderung: spielerische Hacker, die ausprobieren wollen, ob sie irgendwo Zugang gewinnen können, ohne bewusst Schaden anrichten zu wollen; dazu gehört auch die Intention, andere ohne deren Wissen zu belauschen und in deren Privatsphäre einzudringen. Die Tools dazu sind meist aus dem Internet bezogen.
- kriminelle Zielsetzungen: die Absicht ist, anderen Personen oder Unternehmen Schaden zuzufügen, oder sich zu bereichern.
- unbefugte Mitbenutzung des Internetzugangs; hierbei besteht die Möglichkeit, den Account für Downloads von vertraulichen Daten oder für kriminelle Kontakte zu missbrauchen.
- sich direkte materielle Vorteile verschaffen: alle Arten des unbefugten Zugriffs sind möglich; ohne dass der Betroffene zunächst oder auch über einen längeren Zeitraum etwas davon merkt.
- einschleusen von Daten oder Software: unbefugte Stationen in ein Netz einschmuggeln, um dort gezielt Daten abzusetzen, indem dem System eine autorisierte Identität vorgetäuscht wird; Beispiele: Implantierung von Spyware, um Kreditkartendaten auszuspionieren, Attacken mit trojanischen Pferden, die wichtige Datenbestände eines Unternehmens stehlen, Viren, die Daten zerstören können.

WLAN

3

3.1 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 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).

3.1.1 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.

W. W. Osterhage, *Sicherheitskonzepte in der mobilen Kommunikation*,
https://doi.org/10.1007/978-3-662-57903-9_3