Ilmenauer Beiträge zur Wirtschaftsinformatik

Herausgegeben von U. Bankhofer; P. Gmilkowsky;
V. Nissen und D. Stelzer

Daniel Fischer, Dirk Stelzer, Danny Kreyßel

Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen – eine empirische Untersuchung unter deutschen Unternehmen und Behörden

Arbeitsbericht Nr. 2006-03, Juni 2006

Technische Universität Ilmenau
Fakultät für Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik

Autor: Daniel Fischer, Dirk Stelzer, Danny Kreyßel

Titel: Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen – eine empirische Untersuchung unter deutschen Unternehmen und Behörden

Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2006-03,
Technische Universität Ilmenau, 2006

ISSN 1861-9223

ISBN 3-938940-07-7

Anschrift: Technische Universität Ilmenau, Fakultät für Wirtschaftswissenschaften, Institut für Wirtschaftsinformatik, PF 100565, D-98684 Ilmenau.
http://www.tu-ilmenau.de/fakww/Ilmenauer_Beitraege.1546.0.html

Gliederung

Gliederung ii

Abbildungsverzeichnis iii

Tabellenverzeichnis v

Abkürzungsverzeichnis vi

1 Einführung 1

1.1 Problemstellung 1

1.2 Zielstellung 2

1.3 Vorgehensweise und Aufbau 2

2 Wireless LAN-Infrastrukturen 3

2.1 IEEE 802.11-Standardfamilie 3

2.2 Architekturen 6

2.3 Sicherheitsspezifikationen der IEEE 802.11-Standardfamilie 7

2.3.1 Grundlegende Sicherheitsmaßnahmen nach IEEE 802.11 7

2.3.2 Sicherheitsmaßnahmen nach WPA 9

2.3.3 Sicherheitsmaßnahmen nach IEEE 802.11i 10

3 WLAN-spezifische Sicherheitsmaßnahmen 10

3.1 Begriffsbestimmungen 10

3.2 Klassifikation von Sicherheitsmaßnahmen 13

3.3 Katalog WLAN-spezifischer Sicherheitsmaßnahmen 14

3.3.1 Organisatorische Maßnahmen vor der Inbetriebnahme 16

3.3.2 Organisatorische Maßnahmen während des Betriebs 21

3.3.3 Hardware-technische Maßnahmen 23

3.3.4 Software-technische Maßnahmen 24

4 Empirische Untersuchung 31
4.1 Ziel der Untersuchung und Hypothesenformulierung 31
4.2 Vorbereitung und Durchführung 32
4.3 Beschreibung und Auswertung der Ergebnisse 34
4.3.1 Rücklaufquote und Beschreibung der Befragungsteilnehmer 34
4.3.2 Verbreitung von WLAN-Infrastrukturen 37
4.3.3 Verbreitung bestimmter Formen von WLAN-Infrastrukturen 40
4.3.4 Einsatz von Sicherheitsmaßnahmen in WLAN-Infrastrukturen 44
4.3.5 Zusammenhänge zwischen unternehmensspezifischen Merkmalen und WLAN-Sicherheitsmaßnahmen 53
5 Zusammenfassung und Ausblick 62
Literaturverzeichnis 65
Anhang – Fragenbogen 74

Abbildungsverzeichnis

Abb. 1-1: Gesicherte und ungesicherte WLAN-Infrastrukturen in Großstädten [RSA05, 7] 1
Abb. 2-1: Überblick Standardfamilie IEEE 802.11 [BSI05a, 16] 6
Abb. 2-2: Ad-hoc-WLAN [BSI03a, 4] 6
Abb. 2-3: Infrastruktur-WLAN ohne (links) und mit (rechts) LAN-Anbindung [BSI03a, 5] 7
Abb. 3-1: Kausalmodell der Sicherheit der Informationsverarbeitung nach [Stel93, 29] 11
Abb. 3-2: Auswirkungen verursachter Schäden auf die Sicherheitsziele [Stel93, 37] 12
Abb. 3-3: Antennenbeispiele und deren Funkzellenformungen 19
Abb. 3-4: Beispiel einer überlappungsfreien Kanalbelegung 19

Abb. 4-1: Auszug aus dem Fragebogen 33

Abb. 4-2: Branchenzugehörigkeit der Befragungsteilnehmer 35

Abb. 4-3: Größe der befragten Unternehmen und Behörden 35

Abb. 4-4: Gründungsjahr der befragten Unternehmen und Behörden 36

Abb. 4-5: Tätigkeiten/Position der befragten Personen 36

Abb. 4-6: Entwicklung der Verbreitung von WLAN-Infrastrukturen 37

Abb. 4-7: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Existenzdauer der befragten Unternehmen und Behörden 38

Abb. 4-8: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Branche der befragten Unternehmen 39

Abb. 4-9: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Größe der Unternehmen und Behörden 40

Abb. 4-10: Anwendungszwecke von WLAN-Infrastrukturen 41

Abb. 4-11: Anbindung von WLAN-Infrastruktren an andere drahtgebundene Netze 42

Abb. 4-12: Verbreitung von WLAN-Standards 43

Abb. 4-13: Einsatz von Infrastruktur- vs. Ad-hoc-Modus 43

Abb. 4-14: Sicherheitsrelevanz der über WLAN-Infrastrukturen übertragenen Daten 44

Abb. 4-15: Anteil der den Befragungsteilnehmern unbekannten WLAN-Sicherheitsmaßnahmen 48

Abb. 4-16: Bekanntheitsgrade ausgewählter software-technischer WLAN-Sicherheitsmaßnahmen 49

Abb. 4-17: Bekanntheitsgrade und Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen 50

Abb. 4-18: Bekanntheitsgrade und Einsatzhäufigkeiten am Beispiel von Authentifizierungsverfahren 50

Abb. 4-19: Gründe für die Nichteinsatz von WLAN-Sicherheitsmaßnahmen 51

Abb. 4-20: Hoher Implementierungs- / Betriebsaufwand als häufigster Grund für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen 52

Abb. 4-21: Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Branche 54

Abb. 4-22: Einsatzhäufigkeiten von Authentifizierungsverfahren in Abhängigkeit von der Branche 54

Abb. 4-23: Einsatzhäufigkeiten von Verschlüsselungsverfahren in Abhängigkeit von der Branche 55

Abb. 4-24: Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Existenz eines IT-Security-Managements 56

Abb. 4-25: Einsatzhäufigkeiten von organisatorischen Sicherheitsmaßnahmen in Abhängigkeit von der Existenz eines IT-Security-Managements 57

Abb. 4-26: Bekanntheitsgrade und Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Größe der Institutionen 58

Abb. 4-27: WLAN-Sicherheitsmaßnahmen, deren Einsatz stark mit der Größe der Unternehmen und Behörden variiert 58

Abb. 4-28: Dauer der Nutzung von WLAN-Infrastrukturen 59

Abb. 4-29: Einsatz von Sicherheitsmaßnahmen in Abhängigkeit von der Dauer des WLAN-Betriebs 60

Abb. 4-30: WLAN-Sicherheitsmaßnahmen, die häufiger in WLAN-Infrastrukturen mit längerer Nutzungsdauer eingesetzt werden 61

Abb. 4-31: Einsatz von Sicherheitsmaßnahmen in Abhängigkeit von Unternehmensbereichen 62

Tabellenverzeichnis

Tab. 2-1: Kenngrößen der wichtigsten IEEE 802.11-Standards [Grot04, 39] 5

Tab. 3-1: Katalog WLAN-spezifischer Sicherheitsmaßnahmen 16

Tab. 4-1: Hypothesen zur empirischen Untersuchung 32

Tab. 4-2: Top-10-Liste der eingesetzten WLAN-Sicherheitsmaßnahmen 46

Tab. 4-3: Weitere von den Befragungsteilnehmern angegebene WLAN-Sicherheitsmaßnahmen 47

Tab. 4-4: Weitere von den Befragungsteilnehmern angegebenen Gründe für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen 53

Abkürzungsverzeichnis

ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Basic Service Set
CRC32	Cyclical Redundancy Check 32
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DECT	Digital European Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ESS	Extended Service Set
ESSID	Extended Service Set Identify
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
GSM	General System for Mobile Communication
IEEE	Institute of Electrical and Electronic Engineers
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IrDA	Infrared Data Association
IT	Information Technology

IuK	Informations- und Kommunikationstechnologie
IV	Informationsverarbeitung
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Media Access Control
MIC	Message Integrity Check
n_A	Anzahl der gesamten Befragungsteilnehmer, n_A=290
n_B	Anzahl der Befragungsteilnehmer mit WLAN-Infrastrukturen, n_B=75
n_C	Anzahl der Befragungsteilnehmer mit WLAN-Infrastrukturen und komplett ausgefüllten Fragebögen, n_C=36
OFDM	Orthogonal Frequency Division Multiplexing
PC	Personal Computer
PSK	Pre-Shared-Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Cipher 4
RTS/CTS	Request to Send / Clear to Send
SSID	Service Set Identify
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications Systems
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WIP	Wirtschafts- und Innovationsportal Thüringen
WLAN	Wireless Local Area Network
WNT	Wirtschaftsnetz Thüringen
WPA	Wi-Fi Protected Access

Zusammenfassung: Die Studie beschreibt Durchführung und Ergebnisse einer empirischen Untersuchung zur Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen (WLAN) in deutschen Unternehmen und Behörden. Es werden Erkenntnisse über die Verbreitung der WLAN-Technologie, den Einsatz von WLAN-Sicherheitsmaßnahmen, die Gründe des Nichteinsatzes von Sicherheitsmaßnahmen sowie Zusammenhänge zwischen unternehmensspezifischen Merkmalen und dem Einsatz von Sicherheitsmaßnahmen ermittelt. Ausgangspunkt der Untersuchung ist ein von uns entwickelter Katalog WLAN-spezifischer Sicherheitsmaßnahmen, der in einen Fragebogen für eine Internet-Befragung überführt wird. Die Befragung wurde von November 2005 bis Januar 2006 in Kooperation mit der NetSys.IT Information & Communication, dem Wirtschaftsnetz Thüringen, dem Wirtschafts- und Innovationsportal Thüringen, dem TeleTrusT Deutschland e.V. durchgeführt. Von 1.164 eingeladenen Unternehmen und Behörden nahmen 290 an der Untersuchung teil. Das entspricht einer Rücklaufquote von 24,9%. 75 der Befragungsteilnehmer nutzen WLAN-Infrastrukturen. Dies ergibt eine WLAN-Verbreitung von 25,9%. Von der Gruppe der WLAN-nutzenden Befragungsteilnehmer beantworteten 36 den Fragebogenteil zum Einsatz von WLAN-Sicherheitsmaßnahmen vollständig. Unsere Auswertungen ergaben folgende zentrale Ergebnisse:

- *Bei den Befragungsteilnehmern ist seit 2002 eine kontinuierliche Zunahme der Verbreitung von WLAN-Infrastrukturen zu beobachten. Dieser Trend wird auch 2006 fortgesetzt. Im Jahr 2005 betrug die Wachstumsrate der WLAN-Nutzung 33,9%.*
- *Hauptsächlich große Unternehmen und Behörden setzen WLAN-Infrastrukturen ein. Jedoch planen insbesondere kleinere und mittlere Institutionen in naher Zukunft in zunehmendem Maße den Einsatz von WLAN-Infrastrukturen.*
- *Nachdem in den vergangenen Jahren der Standard IEEE 802.11b in WLAN-Infrastrukturen dominierte, setzt heute die Mehrheit (50,7%) der Befragungsteilnehmer mit WLAN-Infrastrukturen den neueren Standard IEEE 802.11g ein.*
- *Die Befragungsteilnehmer setzen zum Schutz ihrer WLAN-Infrastrukturen mehr organisatorische (53,4%) als technische Sicherheitsmaßnahmen (35,6%) ein.*
- *43,7% der im Fragebogen genannten WLAN-Sicherheitsmaßnahmen sind den Befragungsteilnehmern nicht bekannt.*
- *Im Durchschnitt setzen die Befragungsteilnehmer nur 77,7% der ihnen bekannten Sicherheitsmaßnahmen ein, 22% bleiben ungenutzt. Insbesondere bei den Authentifizierungsverfahren liegen die Einsatzhäufigkeiten weit unter den Bekanntheitsgraden.*
- *Als Gründe für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen nennen die Befragungsteilnehmer eine zu geringe Praktikabilität (22,7%), einen zu hohen Implementierungs-/ Betriebsaufwand (9,6%) sowie eine zu geringe Wirkung (7,6%) der Maßnahmen.*
- *Befragungsteilnehmer aus der IuK-Branche setzen mehr Sicherheitsmaßnahmen (55,1%) ein als Befragungsteilnehmer aus anderen Branchen (Dienstleistungen: 46,9%; Industrie: 38,3%) und Behörden (24,7%). Darüber hinaus ist bei Befragungsteilnehmern der IuK-Branche zu beobachten, dass sie im Vergleich zu Befra-*

gungsteilnehmern aus anderen Branchen und Behörden stärkere Verschlüsselungsverfahren (WPA/WPA2) nutzen.

- *Bei Befragungsteilnehmern, die ein IT-Security-Management betreiben, ist der Einsatz von Sicherheitsmaßnahmen wesentlich höher (50,6%) als bei Befragungsteilnehmern ohne IT-Security-Management (25,0%). Insbesondere der Einsatz organisatorischer Maßnahmen ist von der Existenz eines IT-Security-Management stark abhängig.*
- *In punkto Bekanntheitsgrad und Einsatzhäufigkeit von Sicherheitsmaßnahmen stehen kleinere Unternehmen und Behörden den größeren in nichts nach.*
- *Befragungsteilnehmer, die längere Erfahrung mit WLAN-Infrastrukturen haben, setzen nicht mehr Sicherheitsmaßnahmen ein (38,1%) als Befragungsteilnehmer mit weniger Erfahrung (51,9%).*

Schlüsselworte: Wireless LAN-Infrastrukturen, Verbreitung, Sicherheitsmaßnahmen, Einsatzhäufigkeit, Bekanntheitsgrad

1 Einführung

1.1 Problemstellung

Sowohl in Unternehmen und Behörden als auch im Home Office Bereich ist die Vernetzung von Rechnersystemen unverzichtbar für ein effizientes und erfolgreiches Arbeiten. In den vergangenen Jahren hat sich hierbei der Einsatz mobiler Technologien stetig verstärkt [BSI03c, 140; BüGö03, 4 ff.; Dete03, 5 ff.; StLe04, 15]. Eine zentrale Technologie in diesem Bereich sind funkbasierte Netze, so genannte Wireless Local Area Networks (WLAN).[1] Sie ermöglichen eine flexiblere Nutzung und Vernetzung von Rechnersystemen. Diese ist aber oft mit einer mangelhaften Sicherheit in diesen WLAN-Infrastrukturen verbunden. Eine Studie von RSA-Security belegt beispielsweise, dass rund 34% aller WLANs von Unternehmen in den Großstädten London, New York, San Francisco und Frankfurt ungesichert sind.

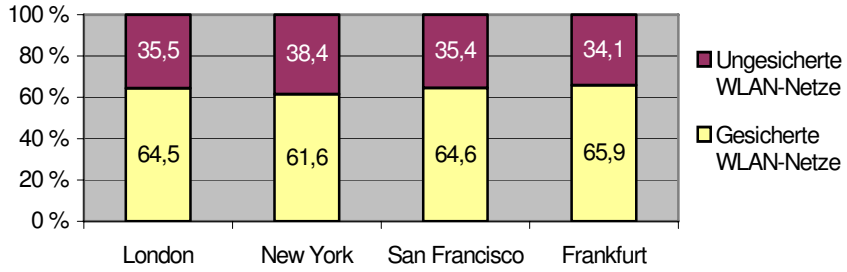

Abb. 1-1: Gesicherte und ungesicherte WLAN-Infrastrukturen in Großstädten [RSA05, 7]

Als Ursachen für diese Sicherheitsdefizite werden unterschiedlichste Gründe genannt [BüGö03; Delb03; RSA04; RSA05]. Dazu zählen insbesondere der zu sorglose Umgang mit der WLAN-Technologie, die Unkenntnis von Anwendern bzw. Betreibern über potentielle Bedrohungen und Sicherheitsmaßnahmen, der hohe Aufwand für Einrichtung und Betrieb von Sicherheitsmaßnahmen, die fehlende Berücksichtigung der WLAN-Infrastrukturen im Sicherheitsmanagement, aber auch die geringe Berücksichtigung von Sicherheitsaspekten bei der Entwicklung der WLAN-Standards. Obwohl es eine Vielzahl von Sicherheitsmaßnahmen für WLAN-Infrastrukturen gibt, werden diese oftmals nicht bzw. nicht angemessen eingesetzt. Potentielle Angreifer sind unter diesen Umständen in

[1] In dieser Arbeit betrachten wir ausschließlich Funknetze der weit verbreiteten IEEE 802.11-Protokollfamilie.

der Lage, sich mit geringem Aufwand Zugang zu sicherheitskritischen Daten zu verschaffen. Bisherige Untersuchungen, welche den Einsatz von WLAN-Sicherheitsmaßnahmen analysieren, beschränken sich meist auf wenige ausgewählte Maßnahmen [BüGö03; Delb03; RSA05]. Weiterhin ist unklar, ob Zusammenhänge zwischen unternehmensspezifischen Merkmalen und dem Einsatz von Sicherheitsmaßnahmen existieren.

1.2 Zielstellung

Ziel dieser Studie ist die Untersuchung der Verbreitung und der Sicherheit von WLAN-Infrastrukturen in deutschen Unternehmen und Behörden. Dabei sollen insbesondere folgende Fragen beantworten werden:

- Wie verbreitet ist die WLAN-Technologie in Unternehmen und Behörden?
- Wie häufig kommen welche Sicherheitsmaßnahmen zum Schutz der WLAN-Infrastrukturen zum Einsatz?
- Warum werden einige Sicherheitsmaßnahmen eingesetzt, andere nicht?
- Gibt es Zusammenhänge zwischen unternehmensspezifischen Merkmalen und der Verwendung einzelner Sicherheitsmaßnahmen?

1.3 Vorgehensweise und Aufbau

Um die Verbreitung von WLAN-Infrastrukturen sowie die Einsatzhäufigkeit WLAN-Sicherheitsmaßnahmen zu untersuchen, führen wir eine empirische Untersuchung durch. Mit Hilfe der Analyse der Standardspezifikationen der IEEE-802.11-Familie[2] ermitteln wir in einem ersten Schritt mögliche Differenzierungsmerkmale für WLAN-Infrastrukturen. Dies ermöglicht es uns, WLAN-Infrastrukturen genauer zu beschreiben sowie die Verbreitung bestimmter Formen detaillierter zu untersuchen. In einem zweiten Schritt entwickeln wir durch umfangreiche Literaturanalysen, Experteninterviews sowie persönliche Einschätzungen und Tests einen Katalog WLAN-spezifischer Sicherheitsmaßnahmen. Auf Basis dieser Vorarbeiten folgt im dritten Schritt die Durchführung einer Umfrage. Dazu leiten wir aus den Fragen der Zielstellung konkretere Hypothesen ab. Zur Untersuchung dieser Hypothesen entwickeln wir einen Fragebogen, der nach Vortests einer ausgewählten Stichprobe von Unternehmen und Behörenden zugesendet wird. Mit Hilfe einer Datenanalyse werten wir die Antworten aus und beschreiben die ermittelten Ergebnisse.

---

[2] Vgl. dazu Abschnitt 2.1

Die vorliegende Studie hat folgenden Aufbau: Im zweiten Abschnitt erläutern wir Grundlagen sowie mögliche Merkmale zur Unterscheidung von WLAN-Infrastrukturen. Es werden unterschiedliche WLAN-Architekturen, WLAN-Standards sowie Sicherheitsspezifikationen, die in den jeweiligen WLAN-Standards verankert sind, beschrieben. Abschnitt 3 dient der Entwicklung unseres Kataloges WLAN-spezifischer Sicherheitsmaßnahmen. Es werden dazu eingangs wichtige Begriffe der IT-Sicherheit definiert sowie Klassifikationsansätze für Sicherheitsmaßnahmen erläutert. Anschließend stellen wir unseren Katalog WLAN-spezifischer Sicherheitsmaßnahmen vor und beschreiben die darin enthaltenen Maßnahmen. Abschnitt 4 ist der Hauptteil dieser Studie. Nach der Ableitung von Hypothesen beschreiben wir die Auswahl der Untersuchungsform und der Befragungsteilnehmer sowie die genaue Vorgehensweise bei der Befragung. Anschließend dokumentieren und aggregieren wir die Untersuchungsergebnisse und diskutieren die aufgestellten Hypothesen. Im letzten Abschnitt fassen wir die wesentlichen Ergebnisse nochmals zusammen, unterziehen diese einer kritischen Würdigung und geben einen Ausblick auf zukünftige Forschungsaufgaben.

2 Wireless LAN-Infrastrukturen

Drahtlose Netzwerke können auf Basis unterschiedlichster Standards (IrDA, Bluetooth, DECT, GPRS, GSM oder UMTS) aufgebaut werden. Die vom Institute of Electrical and Eletronic Engineers (IEEE) herausgegebene Standardfamilie IEEE 802.11* gehört mit ihren Erweiterungen 802.11a, 802.11b und 802.11g zu den am weitest verbreiteten Spezifikationen für drahtlose Netzwerke. Die Standards der IEEE 802.11*-Familie schaffen eine gemeinsame „Plattform“, die es ermöglicht, herstellerübergreifend kompatible WLAN-Lösungen zu entwickeln. Die Kompatibilität wird durch die Vergabe des WiFi-Zertifikats durch die Herstellervereinigung WiFi-Alliance[3] gewährleistet [BSI03b, 7].

2.1 IEEE 802.11-Standardfamilie

IEEE 802.11 bezeichnet einerseits die gesamte Protokollfamilie 802.11* und wird andererseits für den ersten Standard 802.11, der durch das IEEE für drahtlose Netzwerke 1997 herausgegeben wurde, verwendet [IEEE03a, IV]. Dieser Standard bildete die Grundlage

[3] Herstellervereinigung von WLAN-Komponenten nach IEEE 802.11 (früher WECA)

für weitere Folgestandards. 802.11 definiert zur Datenübertragung die Verwendung des lizenzfreien 2,4 GHz Frequenzbandes [IEEE03a, 173]. Mit Hilfe der spezifizierten Bandspreizverfahren FHSS (Frequency Hopping Spread Spectrum) bzw. DSSS (Direct Sequence Spread Spectrum) können maximale Übertragungsraten von bis zu 2 MBit/s erreicht werden.

1999 wurde der Standard **IEEE 802.11a** als Erweiterung verabschiedet. Er nutzt das 5 GHz Frequenzband und verwendet als Übertragungsverfahren OFDM (Orthogonal Frequency Division Multiplexing). Dies ermöglicht Übertragungsraten von bis zu 54 MBit/s [IEEE03b, 19]. Da das 5 GHz Frequenzband jedoch bis 2003 nicht frei nutzbar war, konnte sich dieser Standard in Deutschland nicht durchsetzen. Erst seit der Freigabe 2003 gibt es einige Hersteller, die Geräte für den Standard 802.11a anbieten [Kopp04, 6].

Der ebenfalls 1999 herausgegebene Standard **IEEE 802.11b** nutzt das erweiterte DSSS-Verfahren zur physikalischen Übertragung und erreicht Übertragungsraten von bis zu 11 MBit/s [IEEE03c, 11]. So wurde erstmals die Übertragung von multimedialen Daten in Echtzeit möglich [Kopp04, 4]. Neben einer verbesserten Bandbreite enthält der Standard erweiterte Verfahren zur Netzwerksicherheit sowie eine Funktion zur adaptiven Anpassung der Bandbreite an die Übertragungsentfernung [Davi04, 6]. Da 802.11b für das lizenzfreie 2,4 GHz Frequenzband ausgelegt ist, besteht zu 802.11a keinerlei Kompatibilität [Kopp04, 6].

Die Zunahme der Nutzung der WLAN-Technologie ließ das aufkommende Datenvolumen stetig wachsen und die Forderung nach höheren Übertragungsraten immer größer werden. Da sich bei der Freigabe des von dem Standard 802.11a genutzten 5 GHz Frequenzbandes lange keine Einigung abzeichnete, wurde 2003 ein weiterer Standard verabschiedet, die Erweiterung **IEEE 802.11g**. Er ermöglicht mit 54 MBit/s die gleiche Übertragungsrate wie IEEE 802.11a, nutzt aber das lizenzfreie 2,4 GHz Frequenzband und OFDM als Übertragungsverfahren [IEEE03f, 24]. Ein weiterer Vorteil dieses Standards ist die frequenzbedingte Abwärtskompatibilität zu 802.11b. Als nachteilig erwies sich jedoch die geringe Bruttodatenrate, die aus der immer stärkeren Auslastung des genutzten Frequenzbereiches resultierte [PeKa04].

Ein neuer, noch in der Entwicklung befindlicher Standard ist die Erweiterung **IEEE 802.11n**. Er soll Datenraten von bis zu 600 MBit/s unter Nutzung des 2,4 oder 5 GHz Frequenzbandes ermöglichen. Die Verabschiedung von 802.11n ist für Ende 2006 geplant [Heis05].

Tab. 2-1 gibt einen Überblick über die wesentlichen Merkmale der wichtigsten Standards der IEEE 802.11-Familie.

	802.11	802.11a	802.11b	802.11g	802.11n
maximale Daten-übertragungsrate	2 MBit/s	54 MBit/s	11 MBit/s	54 MBit/s	600 MBit/s
Frequenzbereich	2400,0 - 2483,5 MHz	5150,0 - 5350,0 und 5470,0 - 5725,0 MHz	2400,0 - 2483,5 MHz	2400,0 - 2483,5 MHz	Im 2,4 und 5 GHz-Bereich
Gleichzeitig nutzbare Kanäle	3 Kanäle	8 Kanäle	3 Kanäle	3 Kanäle	k.A.
Reichweite (indoor/outdoor)	40/500 m	25/150 m	40/500 m	40/500 m	k. A.
Sendeleistung	100 mW	30 mW	100 mW	100 mW	k. A.
Übertragungsverfahren	FHSS & DSSS	OFDM	DSSS	OFDM	MIMO
IEEE-Ratifizierung	1997	1999	1999	2003	k. A.

Tab. 2-1: Kenngrößen der wichtigsten IEEE 802.11-Standards [Grot04, 39]

Neben den zuvor beschriebenen Standards der IEEE 802.11-Familie existiert noch eine Reihe von weiteren Erweiterungen mit speziellen Funktionen:[4]

- **IEEE 802.11d**: Anpassung an spezifische Bestimmungen verschiedener Länder
- **IEEE 802.11e:** Zuweisung von Bandbreite für Audio- und Video-Applikationen, Quality of Service (noch nicht ratifiziert)
- **IEEE 802.11f:** Interoperabilität zwischen Basisstationen (Roaming)
- **IEEE 802.11h**: Automatische Anpassung der Sendeleistung an die Reichweite
- **IEEE 802.11i**: Erweiterung bezüglich Sicherheit und Authentifizierung

Abb. 2-1 zeigt die aktuell existierenden Standards der IEEE 802.11-Familie als Übersicht.

[4] Für detaillierte Beschreibung der Standards vgl. [IEEE03d; IEEE03e; IEEE03g] sowie zu IEEE 802.11i Abschnitt 2.3.3.

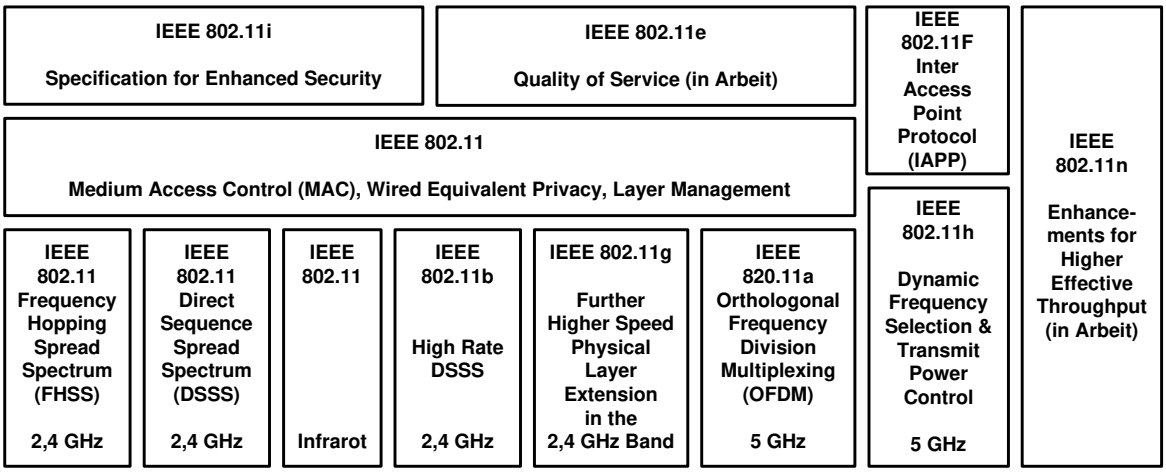

Abb. 2-1: Überblick Standardfamilie IEEE 802.11 [BSI05a, 16]

2.2 Architekturen

Ein WLAN kann in zwei Modi betrieben werden: im Infrastruktur-Modus oder im Ad-hoc-Modus [IEEE03a, 10 ff.].

Die einfachste Form ist der so genannte **Independent-** oder **Ad-hoc-Modus**. In diesem Modus kommunizieren zwei oder mehrere WLAN-Endgeräte direkt miteinander. Eine zentrale Verwaltungsinstanz, die z. B. Sicherheitsmaßnahmen unterstützt, fehlt bei dieser Architektur. Solche Peer-to-Peer-Verbindungen werden in der Standardfamilie 802.11* auch als Independent Basic Service Set (IBSS) bezeichnet [IEEE03a, 24].

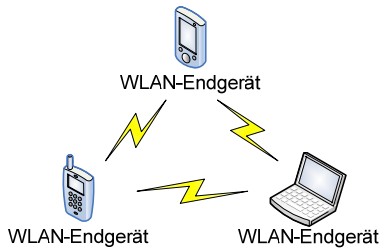

Abb. 2-2: Ad-hoc-WLAN [BSI03a, 4]

In den meisten Fällen werden WLANs im **Infrastruktur-Modus** betrieben [BSI03b, 8]. Der gesamte Netzwerkverkehr wird hier über eine zentrale Infrastruktur, den so genannten Access Point (AP), abgewickelt [LeSt02, 40]. Auch die Anbindung an kabelgebundene Local Area Networks (LANs) erfolgt in der Regel über den zentralen AP. Abb. 2-3 zeigt ein derartiges Infrastruktur-WLAN mit und ohne LAN-Anbindung.

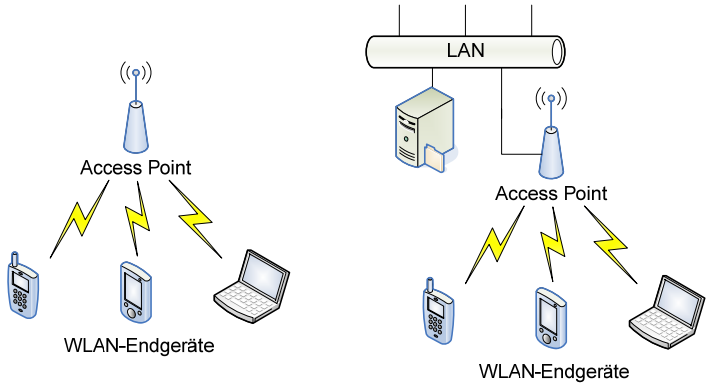

Abb. 2-3: Infrastruktur-WLAN ohne (links) und mit (rechts) LAN-Anbindung [BSI03a, 5]

Die einfachste Form eines Infrastruktur-WLAN besteht aus einem AP und mehreren über Funk angeschlossenen WLAN-Endgeräte, welche als Basic Service Set (BSS) bezeichnet werden [BSI03b, 8]. Durch die Kopplung mehrerer BSS ist es möglich, größere Bereiche flächendeckend per Funk zu vernetzen, die außerhalb der Reichweite einer einzelnen Funkzelle liegen. Solche gekoppelten BSS sind im Standard als Extended Service Set (ESS) definiert. Eine möglichst dicht überlappende Struktur solcher Funkzellen ermöglicht den Anwendern das Wandern von einer Funkzelle zur nächsten, ohne dass die Verbindung abbricht. Das wird als Roaming bezeichnet [Ecol04, 12]. Der Austausch der dafür notwendigen Informationen zwischen den APs, die in ihrer Gesamtheit als Distribution System (DS) bezeichnet werden, findet in der Regel über drahtgebundene Verbindungen statt.

2.3 Sicherheitsspezifikationen der IEEE 802.11-Standardfamilie

2.3.1 Grundlegende Sicherheitsmaßnahmen nach IEEE 802.11

Der Standard 802.11 definiert verschiedene Basis-Sicherheitsmaßnahmen, die ausschließlich der Sicherung der Funkstrecke zwischen zwei Kommunikationspartnern dienen sollen. Diese Sicherheitsmaßnahmen werden im Folgenden kurz beschrieben [BSI03b, 6].

Bei jedem Wireless LAN besteht die Möglichkeit, einen **Netzwerknamen** zu vergeben. Dieser wird als (Extended) Service Set Identity (ESSID bzw. SSID) bezeichnet. Dieser Netzwerkname kann auf zwei unterschiedliche Weisen verwendet werden. Wird die Kennung „any“ als Netzwerkname vergeben, werden alle WLAN-Endgeräte ohne Prüfung zur Kommunikation akzeptiert [Radm04, 32]. Wird ein anderer Netzwerkname als „any“ verwendet, erfolgt vor der Kommunikation eine Überprüfung und es werden nur WLAN-

Endgeräte mit der gleichen SSID zur Kommunikation zugelassen. Des Weiteren wird die SSID genutzt, um beim Verlassen einer Funkzelle den AP der nächsten benachbarten Funkzelle zu finden. Da die SSID im Klartext gesendet wird, kann ein Angreifer sie mit relativ einfachen Mitteln in Erfahrung bringen. Einige APs bieten die Möglichkeit, die Verbreitung der SSID via Broadcast zu unterbinden. Allerdings ist dies nicht standardkonform [BSI03a, 7].

Der Nutzung eines AP kann mit Hilfe eines **MAC-Adressenfilters** bzw. einer **Access Control List (ACL)** eingeschränkt werden [Lanc04b]. Da jede Netzwerkkarte über eine eindeutige Hardwareadresse verfügt, die so genannte MAC-Adresse, ist es möglich, Adressen zu definieren, denen der Zugang zum WLAN erlaubt bzw. nicht erlaubt ist [Köhr04, 242]. Die Verwaltung der ACL auf den APs ist allerdings mit einem hohen Aufwand verbunden, da die Adresslisten „von Hand“ gepflegt werden müssen. Mit zunehmender Zahl der zugangsberechtigten WLAN-Endgeräte steigt der Pflegeaufwand [Poll04, 12]. Der Einsatz von MAC-Adressenfiltern ist deshalb häufig nicht realisierbar.

Um Sicherheitsziele wie Vertraulichkeit, Integrität und Authentizität zu gewährleisten, kann in WLAN-Infrastrukturen die **Wired Equilent Privacy-Verschlüsselung (WEP)** eingesetzt werden. WEP ist im 802.11-Standard als optionale Komponente beschrieben. Es handelt sich um eine auf dem RC4-Algorithmus basierende Stromverschlüsselung, die den Datenaustausch zwischen einem WLAN-Engerät und dem AP absichern soll. Der zur Verschlüsselung notwendige Schlüssel ist eine Zeichenkette von 40 oder 104 Bits und muss allen Teilnehmern der Kommunikation einschließlich der APs bekannt sein [BSI03b, 10]. Bevor ein WLAN-Endgerät mit einem AP verschlüsselt Daten austauschen kann, muss es verschiedene Phasen der Authentifizierung durchlaufen:

- Phase 1: Endgerät ist nicht authentifiziert und nicht angemeldet. Es sendet einen „Authentication Request“ und wird vom AP authentifiziert.
- Phase 2: Endgerät ist authentifiziert und nicht angemeldet. Es sendet einen „Association Request“ und meldet sich am AP an.
- Phase 3: Endgerät ist authentifiziert und angemeldet. Es kann jetzt Daten verschlüsselt übertragen.

Die Authentifizierung von WEP greift in Phase 1 ein, in welcher der AP entscheiden muss, ob er das Endgerät authentifiziert oder nicht. Es werden zwei Modi der Authentifizierung unterschieden: **Open-System**- und **Shared-Key-Authentifizierung**. Bei der Open-

System-Authentifizierung findet eigentlich keine Authentifizierung statt, sondern lediglich die Identifizierung des WLAN-Endgerätes mit Hilfe der MAC-Adresse [Davi04, 14]. Dagegen wird bei der Shared-Key-Authentifizierung ein „Challenge-Response"-Dialog zusammen mit einer geheimen Passphrase (engl. shared secret) zur Authentifizierung verwendet. Zu Beginn sendet der AP dazu eine Zufallszahl unverschlüsselt an das WLAN-Endgerät (Challenge). Das Endgerät schickt das empfangene Datenpaket verschlüsselt zum AP zurück (Response). Der Access Point entschlüsselt die Response und prüft, ob diese mit der vorher gestellten Challenge übereinstimmt. Bei Übereinstimmung ist das WLAN-Endgerät authentifiziert. Eine Authentifizierung des AP findet nicht statt [Radm04, 33].

2.3.2 Sicherheitsmaßnahmen nach WPA

Der Einsatz der bisher beschriebenen Sicherheitsmaßnahmen ermöglicht keine ausreichende Sicherheit in WLAN-Infrastrukturen. Insbesondere nach dem relativ schnellen Bekanntwerden von Sicherheitsschwächen in WEP arbeitete die IEEE und die Herstellervereinigung WiFi-Alliance an der Erweiterung der Sicherheitsmaßnahmen. Nach einigen kurzfristigen Übergangslösungen wie WEPplus [Lanc04c, 4] und Fast Packet Keying [Heis01] wurde Ende 2002 vom IEEE-Komitee **Wi-Fi Protected Access (WPA)** als neuer Sicherheitsstandard verabschiedet. Er soll durch erweiterte Sicherheitsmaßnahmen die Schwachstellen der Authentifizierung, Integritätsprüfung und Verschlüsselung beim Einsatz von WEP beseitigen [Wifi03].

Es werden anhand des Authentifizierungs-Modus zwei WPA-Varianten unterschieden [Wifi03, 5 ff.]. Die einfache Variante, speziell für Heim-Anwender, nennt sich **WPA-PSK (Pre-Shared Key)**. Um WPA-PSK zu nutzen, benötigt man ein WPA-taugliches Endgerät und einen WPA-tauglichen Access Point [Jöck04, 147]. Der zweite Modus nennt sich **WPA-Enterprise**. WPA-Enterprise benötigt neben WPA-tauglichen Endgeräten und Access Points noch eine Reihe von Hilfsprotokollen und Standards für die Authentifizierung. Basierend auf den Entwürfen von IEEE 802.11i werden das **Temporal Key Integrity Protocol (TKIP)** oder **IEEE 802.1X** unterstützt. Mit Hilfe von TKIP werden zwei Hauptprobleme von WEP eliminiert. Zum einen wird der statische WEP-Schlüssel durch einen dynamischen ersetzt, zum anderen wird die leicht umgehbare Integritätssicherung des in WEP verwendeten CRC-Algorithmus durch den **Message Integrity Check (MIC)** ausgetauscht [GeSc04, 6]. IEEE 802.1X, was ursprünglich nicht speziell für WLANs entwickelt wurde, sieht eine eindeutige Identifikation der Anwender mit Hilfe eines RADIUS-Server

vor. Das heißt, die eigentliche Authentifizierung wird nicht vom Access Point durchgeführt, sondern von einem RADIUS-Server [Micr05, 10]. Dieser kann verschiedene Varianten des Extensible Authentication Protocols (EAP), wie beispielsweise EAP-TLS für die Authentifizierung einsetzen [Lanc04a, 2]. Aufgrund der Abwärtskompatibilität wird jedoch bei allen WPA-Varianten weiterhin der schwache RC4-Stromchiffrieralgorithmus zur Verschlüsselung genutzt.

2.3.3 Sicherheitsmaßnahmen nach IEEE 802.11i

Der 2004 ratifizierte Standard 802.11i, der auch als WPA2 bezeichnet wird, umfasst alle oben beschriebenen Fähigkeiten von WPA.[5] Die vollständige Umsetzung der Standardspezifikation 802.11i schreibt zur Verschlüsselung den Algorithmus des **Advanced Encryption Standards (AES)** vor. Dieses neue Verschlüsselungsverfahren ersetzt den unsicheren RC4-Stromchiffrieralgorithmus. Stattdessen kommt ein starkes Blockverschlüsselungsverfahren zum Einsatz, bei dem die Daten in 16 Byte Blöcken verschlüsselt werden [IEEE04]. Während bei der Umstellung der WLAN-Geräte von WEP auf WPA oft nur ein Firmware-Update der WLAN-Geräte benötigt wird, ist bei der Umsetzung von 802.11i neue Hardware zur Ver- und Entschlüsselung erforderlich. Grund dafür sind die durch den neuen Verschlüsselungsalgorithmus gestiegenen Hardwareanforderungen. Ältere WLAN-Endgeräte und APs erfüllen diese Anforderungen nicht mehr und müssen ausgetauscht werden [Heis04].

3 WLAN-spezifische Sicherheitsmaßnahmen

3.1 Begriffsbestimmungen

Viele Begriffe aus dem Bereich IT-Sicherheit sind in der Literatur unterschiedlich definiert oder werden nicht immer einheitlich verwendet. Aus diesem Grund werden wir im Folgenden die wichtigsten Begriffe kurz definieren.

[5] Aus diesem Grund wird WPA auch als eine zu IEEE 802.11i aufwärtskompatible Zwischenlösung bezeichnet.

Sicherheit allgemein ist der Zustand der Abwesenheit von Gefahren bzw. Bedrohungen für ein definiertes System.[6] Stelzer definiert den Begriff der **Sicherheit in der Informationsverarbeitung** als Zustand, in dem alle sicherungswürdigen Sachverhalte vor Beeinträchtigungen, die im Zusammenhang mit der IV entstehen können, bewahrt sind [Stel93, 20ff.]. „Sicherheit in der Informationstechnik bedeutet im Sinne des BSI-Errichtungsgesetzes die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen betreffen." [BSI04, Anhang F; DBCr01, 15 ff.] Unter einer **Gefahr oder Bedrohung** wird jedes potenzielle negative Ereignis auf ein System verstanden, das zu einem Schaden führen kann [PiRi94, 149]. Gefahren gehen von verschiedenen Gefahrenquellen aus [Stel93, 30 ff.]. Die **Gefahrenquellen** lassen sich nach Mensch (beabsichtigt oder zufällig), Technik, Natur bzw. Höhere Gewalt oder sonstige Umfeldeinflüsse unterscheiden. Ein **negatives bzw. sicherheitsgefährdendes Ereignis** beschreibt das Einwirken einer Gefahr auf eine **Schwachstelle** eines sicherheitsrelevanten Objekts[7]. Dies kann zu einer Schädigung des sicherheitsrelevanten Objekts führen.

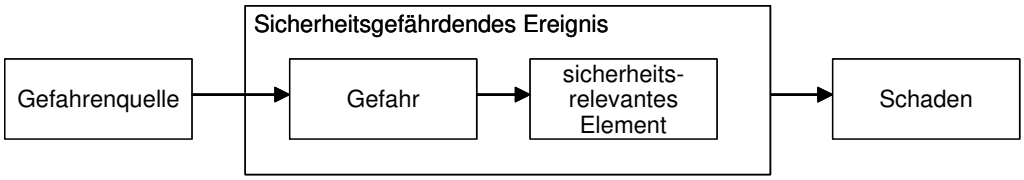

Abb. 3-1: Kausalmodell der Sicherheit der Informationsverarbeitung nach [Stel93, 29]

Sicherheitsziele sind Eigenschaften, die ein IT-System bereitstellen muss, um den Sicherheitsanforderungen seiner Anwender zu entsprechen. Das Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) unterscheidet die folgenden Sicherheitsziele [BSI03c, 58]:[8]

- ***Vertraulichkeit:*** Zu sichernde Objekte sind nur für Befugte zugänglich bzw. nutzbar. Unbefugte dürfen keinen Zugriff erhalten. Bei WLAN bedeutet dies z. B. Schutz vor dem Abhören von Nachrichten oder das Verhindern einer unberechtigten Nutzung einer WLAN-Infrastruktur.

---

6 Ein System ist die Gesamtheit von Elementen, die miteinander in Beziehung stehen und einen bestimmten Zweck erfüllen [KFGr99, 21].

7 Angriffe auf IT können sich richten gegen: Infrastrukturen, Anwender, Anwendungen, Systeme und Netze sowie Daten und Informationen [Hump04, 7; Stel93, 32 f.].

8 Für weitere Klassifizierungen von Sicherheitszielen vgl. [FePf00; PSWW00; RPMü97]

- ***Integrität:*** Unberechtigte Manipulationen von zu sichernden Objekten durch Fälschung oder Veränderung können ausgeschlossen werden. Der Empfänger kann die Echtheit einer über ein WLAN versendeten Nachricht überprüfen.
- ***Verfügbarkeit:*** Ein zu sicherndes Objekt steht dem Anwender in vollem Umfang stets zur Verfügung. Ein WLAN-Endgerät kann zum benötigten Zeitpunkt auf einen AP zugreifen.
- ***Authentizität:*** Die Kommunikationspartner können zweifelsfrei feststellen, dass die Verbindung tatsächlich mit dem gewünschten Partner aufgebaut wurde. Es findet zwischen Sender und Empfänger eine gegenseitige Identifikation statt. Im Gegensatz zur Authentizität schützt die Anonymität eine Person davor, ihre Identität, z. B. aus Gründen des Datenschutzes preiszugeben.
- ***Nichtabstreitbarkeit:*** Die Ausführung von bestimmten Aktionen soll nicht abgestritten werden können. So soll beispielsweise der Sender einer Nachricht einer dritten Partei gegenüber das Senden der Daten - und umgekehrt auch der Empfänger einer Nachricht einer dritten Partei gegenüber - den Nachrichtenempfang beweisen können.

Sicherheitsziele werden durch sicherheitsgefährdende Ereignisse beeinträchtigt (siehe Abb. 3-2).

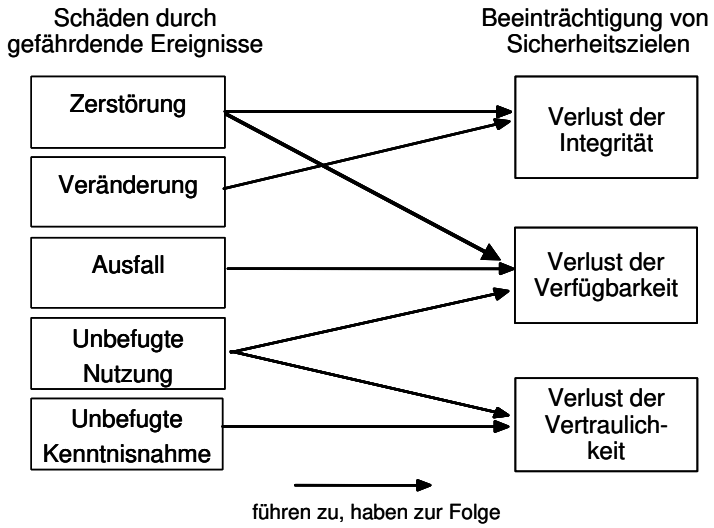

Abb. 3-2: Auswirkungen verursachter Schäden auf die Sicherheitsziele [Stel93, 37]

Unter einer **Sicherheitsmaßnahme** wird jede mögliche Maßnahme verstanden, die zur Erhöhung der Sicherheit in einem System - hier: in einer WLAN-Infrastruktur - führen kann [Stel93, S. 40]. Es können präventive Maßnahmen (Schutz und Erkennung) und reaktive

Maßnahmen (Reaktion) unterschieden werden [Hump04, 15; Schn01, 269 f.]. Sicherheitsmaßnahmen wirken gegen Schwachstellen und verhindern dadurch sicherheitsgefährdende Ereignisse. Jedes Systemelement hat spezifische Maßnahmen, um die Entstehung von Schäden zu vermindern. Auch für WLAN-Infrastrukturen gibt es eine Vielzahl von unterschiedlichen Sicherheitsmaßnahmen.

3.2 Klassifikation von Sicherheitsmaßnahmen

Zur Vorbereitung der empirischen Untersuchung werden WLAN-Sicherheitsmaßnahmen klassifiziert. In der Literatur gibt es unterschiedliche Ansätze zur Klassifikation[9] von Sicherheitsmaßnahmen. Neben eher allgemeinen Klassifikationen, wie z. B. im IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[10], dem Ebenenmodell der Sicherheit der Informationsverarbeitung von Stelzer[11] oder der Recommendation X.800 der International Telecommunication Union (ITU)[12], existieren auch Klassifikationen für WLAN-spezifische Sicherheitsmaßnahmen. Das BSI strukturiert beispielsweise in einer ersten Informationsschrift zu WLAN-Infrastrukturen Sicherheitsmaßnahmen in die Klassen *Konfiguration und Administration der Funkkomponenten*, *zusätzliche technische Maßnahmen* und *organisatorische Maßnahmen* [BSI03b]. Martin verwendet für seine Klassifikation im WLAN-Umfeld neben der Unterscheidung von *organisatorischen* und *technischen* Sicherheitsmaßnahmen zusätzlich das Merkmal der Umsetzungshäufigkeit und differenziert zusätzlich in *einmalige* und *wiederkehrende* Maßnahmen [Mart04, S. 2, 6]. Darüber hinaus gibt es weitere Klassifikationsansätze und Auflistungen, insbesondere ist hier die „Technische Richtlinie sicheres WLAN“ des BSI [BSI05a] zu nennen. Es fällt auf, dass in den meisten Klassifikationen organisatorische und technische Sicherheitsmaßnahmen unterschieden werden. Außerdem werden häufig die Merkmale Einsatzzeitpunkt und -häufigkeit zur Klassenbildung verwendet.

---

9 Klassifikationen sind Ordnungsvorhaben mit dem Ziel, Untersuchungsgegenstände mit gleichen Merkmalen durch Bildung von Klassen übersichtlich zu gruppieren [DIN32705, S. 7 ff.]. Durch die gebildeten Klassen kann die Analyse von Zusammenhängen auf typische Vertreter einer Klasse beschränkt werden.

10 Das IT-Grundschutzhandbuch des BSI unterscheidet Maßnahmen für die Bereiche *Infrastruktur*, *Organisation*, *Personal*, *Hardware/Software*, *Kommunikation* und *Notfallvorsorge* [BSI04, S. 13].

11 Im Ebenenmodell der Sicherheit der Informationsverarbeitung unterscheidet Stelzer in Anlehnung an [Mart73] *physische*, *logische*, *organisatorisch-soziale* sowie *rechtlich-wirtschaftliche* Maßnahmen [Stel93, S. 26 ff.].

12 In Bezug auf das OSI-Referenzmodell erfolgt in der Recommendation X.800 International Telecommunication Union (ITU) eine Unterscheidung der Sicherheitsmaßnahmen in Maßnahmen für die *gegenseitige Authentifizierung*, für die *Zugriffskontrolle*, für die *Vertraulichkeit der Daten*, für die *Datenintegrität* und für die *Datenannahme* (Non-Repudiation) [ITU91].

Wir ordnen die WLAN-spezifischen Sicherheitsmaßnahmen mit Hilfe folgender Klassen:

- Organisatorische Maßnahmen vor der Inbetriebnahme
- Organisatorische Maßnahmen während des Betriebs
- Hardware-technische Maßnahmen
- Software-technische Maßnahmen

3.3 Katalog WLAN-spezifischer Sicherheitsmaßnahmen

Für die Zusammenstellung relevanter Sicherheitsmaßnahmen für WLAN-Infrastrukturen haben wir folgende Quellen ausgewertet: Informationen des BSI zur WLAN-Sicherheit [BSI03c], Sicherheitsspezifikationen der Standardfamilie IEEE 802.11 für WLANs [IEEE06], die Standards ISO/IEC 17799:2005 [ISO05a] und ISO/IEC 27001:2005 [ISO05b] sowie weitere Dokumentationen, Rahmenwerke und Publikationen, wie z. B. [FMSh01; Kopp04]. Unsere Analyse ergab eine erste sehr umfangreiche Zusammenstellung. Diese haben wir in einem zweiten Schritt in Expertendiskussionen weiterentwickelt. Auf Basis persönlicher Einschätzungen und dem Test einzelner Maßnahmen nahmen wir eine nochmalige Auswahl vor. Dabei entstand ein Exzerpt von 46 Sicherheitsmaßnahmen. Die ausgewählten Maßnahmen ordneten wir abschließend in die von uns entwickelte Klassifikation[13] ein. Tab. 3-1 zeigt unseren Katalog WLAN-spezifischer Sicherheitsmaßnahmen[14].

ID	Klasse	Maßnahme/Beschreibung
...	**Organisatorische Maßnahmen vor der Inbetriebnahme**	
...	Sicherheitskonzept für WLAN-Infrastruktur erstellen	
1		Notwendigkeit, Ziele und Anwendungszweck der WLAN-Infrastruktur begründen
2		Anforderungen an Sicherheitsziele festlegen
3		Schutzbedarfsfeststellung und Risikoanalyse durchführen
4		WLAN-Policy erstellen
…	Inbetriebnahme (Rollout) planen	
5		Einsatzorte/Einsatzbereich exakt festlegen und abgrenzen
6		Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)
7		Messplanung durchführen (Ermittlung der Signalstärke)
8		Antennentyp und Aufstellort der Access Points so wählen, dass eine maximale Ausleuchtung gewährleistet ist

[13] Vgl. Abschnitt 3.2

[14] Der Maßnahmenkatalog steht zum Download unter [Wlan06] zur Verfügung.

9			Überlappungsfreie Kanalbelegung (maximal 3 parallele Kanäle bei 802.11b, g und maximal 8 parallele Kanäle bei 802.11a)
10			Kontrolle und Überprüfung des WLAN durch abschließenden Netzwerkscan und Auswertung der Logdatei
...		Weitere organisatorische Maßnahmen vor einer WLAN-Installation	
11			Testläufe im Vorfeld durchführen
12			Notfallstrategien für den Ausfall entwickeln
13			Administration der Access Points nicht über WLAN-Schnittstelle vollziehen
14			Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen
15			Sensibilisierung bzw. Schulung der Anwender
…	**Organisatorische Maßnahmen während des Betriebs**		
16			Einhaltung der Datenschutzbestimmungen überprüfen
17			Regelmäßige Kontrolle und Überwachung des WLAN durch Netzwerkscans und Auswertung von Logdateien
18			Physischer Zugriff zu Access Points nur autorisiertem Personal ermöglichen
19			Überprüfung der WLAN-Policy
20			Physische Überprüfung der installierten Access Points auf Zugänglichkeit und Beschädigungen, um Netzausfälle und missbräuchliche Verwendungen zu verhindern
21			Regelmäßige Kontrolle und Wartung der Einstellungen der WLAN-Endgeräte, wie Firewall- und Betriebssystem-Konfiguration an den Endgeräten
…	**Hardware-technische Maßnahmen**		
22			Geeignete WLAN-Geräte (Signaltechnik: z. B. OFDM/DSSS) und Standard (IEEE 802.11g, etc.) wählen
23			WLAN-Geräte und -Services nur bei Gebrauch einschalten bzw. zeitgesteuerten Zugriff aktivieren
24			WLAN-Tapete zur Abschirmung nutzen
25			Registrierte WLAN-Karten über eine Ausleihe ausgeben und regelmäßig austauschen
...	**Software-technische Maßnahmen**		
...		Konfiguration und Administration der WLAN-Geräte	
26			Werkseitige Grundeinstellungen an WLAN-Geräten ändern
27			Ad-hoc-Vernetzung deaktivieren
28			Eigenen Netzwerknamen vergeben (kryptische SSID)
29			SSID im Broadcast abschalten
30			Beacon Intervall maximieren
31			DHCP am Access Point abschalten
32			Verbindung zwischen RADIUS-Server und Access Point absichern
33			Einen WLAN-Standard, anstatt mehrerer parallel nutzen (z. B. 'G-only' oder 'B-only')
34			Block-Intra-BSS-Traffic in öffentlichen Bereichen verwenden
...		Authentifizierungsverfahren anwenden	
35			Authentifizierung über MAC-Adresse
36			Pre-Shared-Key-Authentifizierung

37			Open-System- der Shared-Key-Authentifizierung vorziehen, um Kompromittierung des WEP-Schlüssels zu unterbinden
38			Authentifizierung mit WLAN Smartcard
39			Authentifizierung nach IEEE 802.1x über RADIUS-Server
...		Verschlüsselungstechniken benutzen	
40			WEP-Verschlüsselung
41			Verschlüsselung nach WPA-Standard
42			Verschlüsselung nach WPA2 bzw. 802.11i
...		Weitere softwaretechnische Maßnahmen	
43			Netzwerktechnische Trennung zwischen WLAN und drahtgebundenem Netz (z. B. über Paketfilter, VPN oder VLAN)
44			Installation einer Personal Firewall auf den mobilen Endgeräten
45			Verwendung eines Intrusion Detection Systems zur Überwachung des WLANs
46			Datei- und Ressourcenfreigabe auf allen Endgeräten sowie Geräten, die vom WLAN aus erreichbar sind, restriktiv einschränken

Tab. 3-1: Katalog WLAN-spezifischer Sicherheitsmaßnahmen

3.3.1 Organisatorische Maßnahmen vor der Inbetriebnahme

Sicherheitskonzept für WLAN-Infrastruktur erstellen

1: Notwendigkeit, Ziele und Anwendungszweck der WLAN-Infrastruktur begründen

Vor Beginn der Installation einer WLAN-Infrastruktur ist eine Zieldefinition vorzunehmen. In ihr sind Begründung und Abgrenzung des WLAN-Projektes enthalten. Auch sollten IT- und Sicherheitsverantwortliche mit den Vertretern des Fachbereichs prüfen, ob die Notwendigkeit einer WLAN-Infrastruktur besteht oder ob die Zielerreichung auch mit herkömmlichen LAN-Strukturen erreichbar ist.

2: Anforderungen an Sicherheitsziele festlegen

Die Anforderungen an die WLAN-Infrastruktur sowie die Sicherheitsziele müssen vor der Installation klar formuliert werden. Abhängig vom Grad der Vertraulichkeit der Daten, der Art der Anbindung der WLAN-Infrastruktur an das LAN sowie der Art der Anwender der WLAN-Infrastruktur sollten konkrete Sicherheitsziele und Sicherheitsmaßnahmen zu deren Erreichung festgelegt werden.

3: Schutzbedarfsfeststellung und Risikoanalyse durchführen

Vor der Umsetzung eines WLAN-Projektes ist der Schutzbedarf der entsprechenden Umgebung zu bestimmen. Dazu müssen unter anderem die Daten, die mit Hilfe der WLAN-

Infrastruktur gesendet werden, überprüft werden. Dies sollte der Betreiber mit Vertretern der Fachbereiche durchführen. Wird ein kritischer Schutzbedarf überschritten, ist eine Risikoanalyse durchzuführen. Im Anschluss daran ist zu entscheiden, ob das Projekt wie geplant umgesetzt wird. Sind trotz Umsetzung von Sicherheitsmaßnahmen die Restrisiken zu hoch oder können die Sicherheitsanforderungen nicht wie gewünscht erfüllt werden, sollte von der Inbetriebnahme der WLAN-Infrastruktur abgeraten werden.

4: WLAN-Policy erstellen

Sicherheitsaspekte der WLAN-Infrastruktur sind entweder in der Netzwerkpolicy ausführlich in einem eigenen Kapitel oder in einer eigenen WLAN-Policy zu behandeln. Ziel ist dabei die Integration der Besonderheit der WLAN-Infrastruktur in das bestehende Sicherheitskonzept. Die WLAN-Policy sollten mindestens folgende Inhalte besitzen: Definition des WLAN-Anwenderkreises und Bedingungen für deren Zugang, Definition der Sicherheitsziele, Richtlinien zur Sicherung der Access Points, Richtlinien für das Schlüsselmanagement und die Authentifizierung, Richtlinien zur Sicherung der WLAN-Endgeräte, Richtlinien zum Reporting und Logging.

Inbetriebnahme (Rollout) planen

5: Einsatzorte/Einsatzbereich exakt festlegen und abgrenzen

Der Aufbau einer WLAN-Infrastruktur bedarf einer detaillierten Planung der Einsatzbereiche. Der Betreiber definiert, ob es sich um eine Indoor- oder Outdoor-Installation handelt, ob Roaming-Funktionalitäten benötigt werden, ob kleine Räume oder Großflächen zu versorgen sind und mit wie vielen Anwendern und welchem Datendurchsatz zu rechnen ist. Hierbei sind so genannte Mapping-Tools hilfreich. Mit Hilfe dieser Tools können Gebäude- und Umgebungspläne eingelesen und die Verteilung der APs entsprechend geplant werden.[15]

6: Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)

Nachdem der Einsatzbereich definiert ist, gilt es, die Umgebungsfaktoren zu untersuchen. Hierzu sind Fragen über bauliche Gegebenheiten, verwendete Baustoffe und mögliche, ungewollte Reflexionen durch große Glas- und Metallflächen zu klären. Außerdem muss festgestellt werden, ob benachbarte WLAN-Infrastrukturen oder andere elektromagneti-

[15] Hierfür eignet sich beispielsweise die „Ekahau Site Survey Software ESS 2.1“. Eine Testversion und weitere Informationen gibt es auf: http://www.psiber-data.de

sche Störquellen, wie Schweißroboter, Umspannwerke oder Klimaanlagen vorhanden sind. Die Installationsorte für die APs müssen darauf hin neu abgestimmt werden. Hierbei sind feuerschutzpolizeiliche Vorschriften, evtl. bauliche Vorgaben des Architekten und eine mögliche Verkabelung des AP (Anschluss an das LAN und Stromnetz - evtl. kann die Stromversorgung über die vorhandene Verkabelung mittels Power over Ethernet (PoE) erfolgen.) zu beachten. Die Planungsdaten können in den entsprechenden Tools dokumentiert werden.[15]

7: Messplanung durchführen (Ermittlung der Signalstärke)

Um die Konfiguration der Sendeleistung und den Aufstellort der APs optimal zu gestalten, ist eine Messplanung durchzuführen. Die Sendeleistung der APs ist so zu wählen, dass sie einerseits das geforderte Einsatzgebiet abdeckt, andererseits aber nicht großräumig darüber hinaus „strahlt“. Mit Funk-Analyse-Software können Signalstärke, Rauschen und Signal-Rausch-Abstand der WLAN-Endgeräte und APs gemessen werden. Zudem werden vorhandene WLAN-Installationen und dadurch belegte Kanäle ermittelt. Mögliche Frequenzüberlagerungen sind festzustellen und zu dokumentieren. Ein mögliches Messtool ist die „Mobile Suite“ von AirMagnet[16]. Die Messergebnisse können anschließend in ein Planungstool[15] eingelesen und dort in einer Karte dargestellt werden. Somit lassen sich schlecht ausgeleuchtete Bereiche auffinden.

8: Antennentyp und Aufstellort der Access Points so wählen, dass eine maximale Ausleuchtung gewährleistet ist

Ziel ist es, mit möglichst wenigen APs eine maximale Abdeckung zu gewährleisten. Damit verbundene Vorteile sind verminderte Hardware-Kosten, weniger Wartungsaufwand sowie geringere Kanal-Konflikte. Kriterien für die Antennenauswahl sind Montagesituation, Funkqualität und Wirtschaftlichkeit [Höch03]. Mit Hilfe einer entsprechenden Antennenauswahl lässt sich für den jeweiligen Einsatz eine optimale Funkzellenformung erreichen. Abb. 3-3 zeigt einige Antennenbeispiele und damit realisierbare Funkzellenformungen.

[16] Weitere Informationen gibt es auf der Homepage des Herstellers: http://www.airmagnet.com

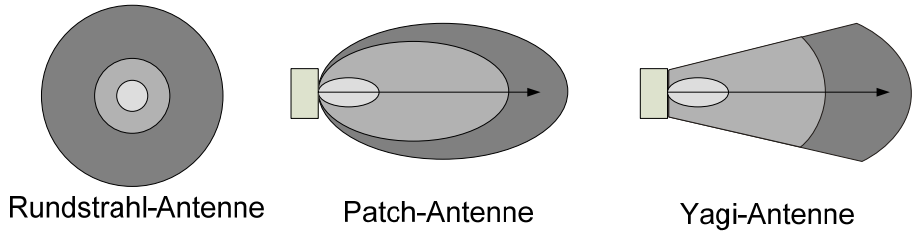

Abb. 3-3: Antennenbeispiele und deren Funkzellenformungen

Als weitere Möglichkeit zur Eingrenzung der Funkbereiche bieten einige Access-Points die Einschränkung ihrer Sendeleistung an. Hierbei ist aber zu beachten, dass eine Mindestsendeleistung innerhalb eines WLAN benötigt wird. Auch ist bei der Planung einer ESS-Infrastruktur zu beachten, dass sich zur Realiserung eines lückenlosen Roamings die Reichweiten von benachbarten APs überschneiden sollten [Miro04].

9: Überlappungsfreie Kanalbelegung (maximal 3 parallele Kanäle bei 802.11b, g und maximal 8 parallele Kanäle bei 802.11a)

Beim Aufbau einer ESS-Infrastruktur sind die verwendeten Kanäle der einzelnen APs überlappungsfrei zu konfigurieren. In Deutschland werden für 802.11b/g zwar 13 Kanäle freigegeben. Lediglich drei Kanäle sind jedoch ohne gegenseitige Interferenzen nutzbar. Die Kanalplanung sollte bei benachbarten APs mit gleicher Frequenz mindestens den doppelten Abstand der Reichweite betragen. Abb. 3-4 zeigt ein Beispiel für eine überschneidungsfreie Kanalbelegung.

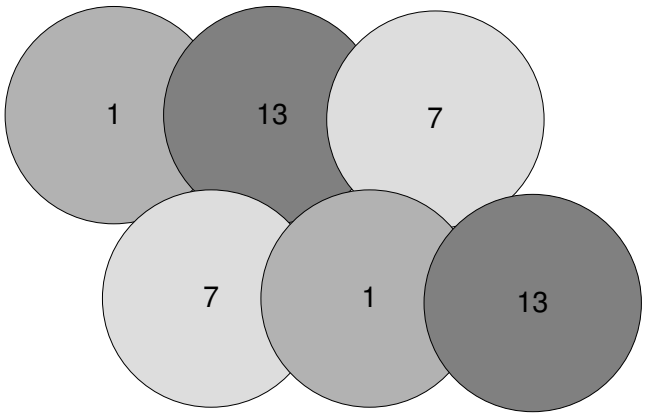

Abb. 3-4: Beispiel einer überlappungsfreien Kanalbelegung

Wird die WLAN-Infrastruktur z. B. in einem Bürogebäude auf mehreren Etagen betrieben, ist das Kanalbelegungsmuster in darüber bzw. darunter liegende Stockwerke entsprechend zu verschieben. Hierbei sollte die Verschiebung der Kanäle mindestens 5-Channels betragen.

10: Kontrolle und Überprüfung des WLAN durch abschließenden Netzwerkscan und Auswertung der Logdatei

Abschließend ist vor der Inbetriebnahme eine Überprüfung aller Einstellungen der WLAN-Endgeräte und APs hinsichtlich der erstellten Vorgaben durchzuführen. Dabei ist zu beachten, dass WLAN-Infrastrukturen dynamische Verbunde sind. Deshalb sind nicht nur eine, sondern mehrfache Netzwerkscans auf allen Kanälen, Frequenzbereichen und Endgeräten zu unterschiedlichen Tagen und Zeiten ratsam. Die Verwundbarkeit und Erreichbarkeit der WLAN-Infrastruktur ist durch Penetrationstests zu kontrollieren. Hier eignen sich Tools, wie z. B. die „Mobile Suite“[16]. Darüber hinaus können Tools genutzt werden, die auch in Hackerkreisen zum Einsatz kommen.[17] Des Weiteren sind vor der Inbetriebnahme die Protokolldateien und Ereignisanzeigen der WLAN-Endgeräte und APs während und nach den Tests regelmäßig auszuwerten.

Weitere organisatorische Maßnahmen vor einer WLAN-Installation

11: Testläufe im Vorfeld durchführen

Die gesamte WLAN-Infrastruktur ist vor der Inbetriebnahme unter realen Bedingungen zu testen. Insbesondere sind dabei die Sicherheitsanforderungen zu überprüfen. Hierzu werden z. B. Datenpakete zu Testzwecken abgefangen und es wird versucht, diese zu entschlüsseln bzw. zu verfälschen. Spätestens bei den Testläufen sollten mögliche Abweichungen und Probleme erkannt und beseitigt werden.

12: Notfallstrategien für den Ausfall entwickeln

Für kritische Anwendungen sind aufgrund der nicht 100%-igen Gewährleistung der Verfügbarkeit einer WLAN-Infrastruktur Notfall- bzw. Backupstrategien zu entwickeln. Durch diese Maßnahmen soll erreicht werden, dass trotz Ausfall der WLAN-Infrastruktur die Arbeit fortgesetzt werden kann.

13: Administration der Access Points nicht über WLAN-Schnittstelle vollziehen

Die meisten APs können komfortabel und plattformunabhängig über die WLAN-Schnittstelle mit Hilfe eines Web-Browsers konfiguriert werden [Arte04]. Um eine mögliche „Man-in-the-middle-Attacke“ zu verhindern, ist die Administration und Konfiguration eines AP kabelgebunden über sichere Kanäle, z. B. über TSL/SSL oder SNMPv3 mit Au-

[17] Z. B. NetStumbler, http://www.netstumbler.com.

thentifizierung, vorzunehmen. Ratsam ist es, den Zugang zu den APs von einem anderen Netzsegment durchzuführen. Auf dieses Netzwerksegment sollten die WLAN-Anwender keinen Zugriff erhalten. Des Weiteren ist die Defaulteinstellung des Zugangspassworts für die AP-Konfiguration zu ändern. Hierbei muss ein starkes Passwort gewählt werden. Die Funktionalitäten der Remote-Administration und Remote-Firmware-Update sind zu deaktivieren. In kleinen WLAN-Infrastrukturen kann die AP-Administration auch direkt über eine serielle, USB- oder Ethernet-Schnittstelle erfolgen. Bei größeren WLAN-Infrastrukturen ist eine manuelle Einzelkonfiguration der AP nicht machbar [Comc03]. Hier können sämtliche APs z. B. an spezielle WLAN-Switches angeschlossen werden, welche die Konfiguration aller angeschlossenen APs übernehmen.[18]

14: Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen

Bei einigen Authentifizierungsverfahren ist es möglich, das Passwort abzuhören und durch Dictionary- oder Brute-Force-Attacken herauszufinden. Daher sind die Zugangsdaten des WLAN unabhängig von denen des herkömmlichen LAN festzulegen.

15: Sensibilisierung bzw. Schulung der Anwender

Die Anwender eines WLANs müssen hinsichtlich der Besonderheiten und Gefährdungen einer WLAN-Infrastruktur sensibilisiert werden. Ihnen sind insbesondere die Inhalte der Sicherheitsrichtlinien zu vermitteln. Ziel ist es, dass die Anwender wissen, was sie tun dürfen, worauf sie achten müssen und wann und wo sie Gefahren ausgesetzt sind. Darüber hinaus sollten sie auch in die Bedienung der zum Einsatz kommenden Technik eingeführt werden (Firewall, VPN).

3.3.2 Organisatorische Maßnahmen während des Betriebs

16: Einhaltung der Datenschutzbestimmungen überprüfen

Der Schutz personenbezogener Daten muss stets gewährleistet sein. Betreiber müssen dem datenschutzkonformen Umgang mit Daten vertraglich zustimmen. Somit soll verhindert werden, dass Bewegungsprofile erstellt oder die Vertraulichkeit von Anwenderdaten nicht gewährleistet wird. Die regelmäßige Überprüfung in Bezug auf die Einhaltung der Datenschutzbestimmungen in den WLAN-Infrastrukturen ist organisatorisch sicherzustellen.

---

[18] Die Firmen „Cranite“ und „Trapeze“ bieten hierzu spezielle Lösungen an.

17: Regelmäßige Kontrolle und Überwachung des WLAN durch Netzwerkscans und Auswertung von Logdateien

Während des Betriebes der WLAN-Infrastruktur sind regelmäßige Überprüfungen der WLAN-Endgeräte und APs hinsichtlich der erstellen Vorgaben durchzuführen. Dabei ist zu beachten, dass WLAN-Infrastrukturen dynamische Verbunde sind. Netzwerkscans auf allen Kanälen, Frequenzbereichen und Endgeräten sind aus diesem Grund zu unterschiedlichen Tagen und Zeiten ratsam. Die Verwundbarkeit und Erreichbarkeit der WLAN-Infrastruktur ist durch Penetrationstests zu kontrollieren. Hier eignen sich Tools, wie z. B. die „Mobile Suite“[16]. Darüber hinaus können Tools genutzt werden, die auch in Hackerkreisen zum Einsatz kommen.[19] Des Weiteren sind die Protokolldateien und Ereignisanzeigen der WLAN-Endgeräte und APs regelmäßig auszuwerten.

18: Physischer Zugriff zu Access Points nur autorisiertem Personal ermöglichen

Der physische Zugriff auf einen Access Point ist nur autorisierten Personen zu ermöglichen. Eine entsprechende Montage der APs ist vorzusehen. Speziell sei auf den „Reset“-Button hingewiesen, den einige Access Points besitzen, um die Defaulteinstellung wieder herzustellen. Unter Umständen kann so ein Unberechtigter Zugang zum AP und damit zur WLAN-Infrastruktur erhalten.

19: Überprüfung der WLAN-Policy

In regelmäßigen Abständen ist die WLAN-Policy hinsichtlich neuer Anforderungen oder neuer Technik zu überprüfen. Die WLAN-Policy sollten mindestens folgende Inhalte umfassen: Definition des WLAN-Anwenderkreises und Bedingungen für deren Zugang, Definition der Sicherheitsziele, Richtlinien zur Sicherung der Access Points, Richtlinien für das Schlüsselmanagement und die Authentifizierung, Richtlinien zur Sicherung der WLAN-Endgeräte, Richtlinien zum Reporting und Logging.

20: Physische Überprüfung der installierten Access Points auf Zugänglichkeit und Beschädigungen, um Netzausfälle und missbräuchliche Verwendungen zu verhindern

Um Netzausfällen vorzubeugen, sind in vorgeschriebenen Zeitabständen die installierten APs regelmäßig zu kontrollieren. Unregelmäßigkeiten sind umgehend abzustellen.

---

19 Z. B. NetStumbler, http://www.netstumbler.com.

21: Regelmäßige Kontrolle und Wartung der Einstellungen der WLAN-Endgeräte, wie Firewall- und Betriebssystem-Konfiguration an den Endgeräten

Die Einstellungen aller WLAN-Endgeräte und APs müssen regelmäßig kontrolliert und gewartet werden. Dazu zählen insbesondere Firewall-Konfigurationen oder betriebssystemabhängige Änderungen.

3.3.3 Hardware-technische Maßnahmen

22: Geeignete WLAN-Technik (Signaltechnik: z. B. OFDM/DSSS) und Standard (IEEE 802.11g, etc.) wählen

Die eingesetzten WLAN-Geräte müssen die gestellten Anforderungen und Sicherheitsziele erfüllen. In Frage kommende Hardwarelösungen sind entsprechend zu prüfen.[20] Sie müssen ggf. spezielle Eigenschaften, wie WEP, WPA oder WPA2, portbasierte 802.1X-Authentifizierung oder ein dynamisches Schlüsselmanagement (TKIP) unterstützen. Wichtig sind auch Erweiterbarkeit (Firmwareupdates) und schnelle Austauschbarkeit. Hier sollte man vor allem auf Kompatibilität achten und ggf. auf Hardware verschiedener Hersteller verzichten. Mit der Auswahl der richtigen WLAN-Technik können auch Interferenzen vermieden und eine höhere Dienstgüte erreicht werden. OFDM basierte Signaltechnik der Standards 802.11a und 802.11g bietet z. B. Vorteile gegenüber dem DSSS-Verfahren des Standards 802.11b, da diese auch bei 60% Signalauslöschung noch saubere Daten übertragen. Somit ist eine höhere Verfügbarkeit der WLAN-Infrastruktur möglich.

23: WLAN-Geräte und -Services nur bei Gebrauch einschalten bzw. zeitgesteuerten Zugriff aktivieren

Wird die WLAN-Infrastruktur nicht benötigt, sind die WLAN-Geräte auszuschalten bzw. deren WLAN-Funktionen zu deaktivieren. An den WLAN-Endgeräten muss der Anwender selbst die WLAN-Funktion deaktivieren. Am AP ist der Betreiber für die Abschaltung verantwortlich. Bei größeren WLAN-Infrastrukturen (ESS) ist ein regelmäßiges, manuelles Deaktivieren nicht realisierbar. Einige APs und Router ermöglichen jedoch eine zeitgesteuerte Zugriffskontrolle und können so z. B. den Zugriff auf eine WLAN-Infrastruktur außerhalb der Geschäftszeiten komplett unterbinden. Somit wird das Risiko, dass ein An-

[20] Zur Validierung von WLAN-Komponenten hat das BSI einen Kritierienkatalog entwickelt, vgl. [BSI05b, 9-32].

griff außerhalb der Geschäftszeiten auf die WLAN-Infrastruktur stattfindet, ausgeschlossen.

24: WLAN-Tapete zur Abschirmung nutzen

Zur Abschirmung von Räumen und Gebäuden sind spezielle Beläge auf die Wände aufzubringen. Diese Wandbeläge (Tapeten) absorbieren Signale in den 2,4 und 5 GHz-Bereichen. Somit kann die Ausbreitung der Funkwellen besser kontrolliert werden. Andere drahtlose Übertragungen, wie der Mobilfunk, sollen aber weiterhin möglich sein. Bei diesem Wandbelag gibt es zwei Varianten: eine aktivierbare, bei der einzelne Bereiche zugeschaltet werden können, und eine permanente Tapete, die einen ständigen „Schutzschild" bildet. Eine Umsetzung dieser Sicherheitsmaßnahme schränkt jedoch einen flächendeckenden WLAN-Einsatz stark ein. Durch den Einsatz dieser Tapete ist eine WLAN-Infrastruktur unanfällig gegen Angriffe, die von außerhalb des abgegrenzten Bereiches kommen. Auch das Interferenzrisiko mit außerhalb liegenden WLAN-Infrastrukturen wird beseitigt. Gegen Angreifer, die sich innerhalb des abgegrenzten Bereiches aufhalten, ist diese Sicherheitsmaßnahme jedoch wirkungslos.

25: Registrierte WLAN-Karten über eine Ausleihe ausgeben und regelmäßig austauschen

Möchte ein Anwender die WLAN-Infrastruktur nutzen, muss er sich bei einer entsprechenden Stelle eine legitime WLAN-Karte mit Begründung des Einsatzes ausleihen. Die Ausleihe wird dokumentiert. Diese Sicherheitsmaßnahme eignet sich nur für kleinere WLAN-Infrastrukturen und ist mit hohem Aufwand und Kosten verbunden. Hierbei wird eine Access-Control-List (ACL), welche die MAC-Adressen der legitimen WLAN-Karten enthält, gepflegt.

3.3.4 Software-technische Maßnahmen

Konfiguration und Administration der WLAN-Geräte

26: Werkseitige Grundeinstellungen an WLAN-Geräten ändern

Beim Kauf von WLAN-Geräten sind ursprünglich keine oder nur unzureichende Sicherheitsmechanismen aktiviert. Deshalb sind diese Grundeinstellungen zu Beginn einer Installation einer WLAN-Infrastruktur zu ändern und ggf. zusätzliche Sicherheitsmaßnahmen (z. B. WEP-Verschlüsselung aktivieren) zu konfigurieren [Müll02]. Einige Hersteller von WLAN-Geräten vergeben Defaulteinstellungen für die SSID, die Konfigurationspasswör-

ter und die Kanalbelegung. Im Internet existieren Listen für einige APs für diese Standardeinstellungen.[21] Die Einstellungen müssen umgehend geändert werden. Wird stattdessen z. B. der Default-WEP-Key beibehalten, könnte ein Angreifer die gesendeten Datenpakete leicht abfangen und entschlüsseln oder ein unberechtigtes WLAN-Endgerät am WLAN teilnehmen.

27: Ad-hoc-Vernetzung deaktivieren

Aktivierte WLAN-Geräte ermöglichen eine Ad-hoc-Vernetzung[22]. Wird diese Funktionalität nicht benötigt, ist die Ad-hoc-Vernetzung zu deaktivieren. So können ungewollte Verbindungen mit anderen, eventuell unbekannten WLAN-Endgeräten unterbunden werden. Bei Bedarf einer Ad-hoc-Vernetzung kann die Funktionalität temporär aktiviert werden.

28: Eigenen Netzwerknamen vergeben (kryptische SSID)

Jede WLAN-Infrastruktur besitzt einen Netzwerknamen (SSID).[23] Die SSID sollte so gewählt werden, dass keine Rückschlüsse auf den Access Point seinen Hersteller sowie den Betreiber gezogen werden können. Die SSID „any“, bei der jeder Zugriff auf die WLAN-Infrastruktur erhält, ist nicht zu verwenden.

29: SSID im Broadcast abschalten

Ein AP sendet in regelmäßigen Abständen ein „Beacon-Frame“[24] mit seiner SSID und anderen Management Informationen an alle WLAN-Endgeräte, um so seine Existenz bekannt zu geben [Blum03]. Diesen „Rundruf“ des AP nennt man „Broadcast“.[25] Er kann von allen WLAN-Endgeräten, die sich in der Reichweite des AP befinden, empfangen werden. So kann die SSID auch von unerwünschten WLAN-Endgeräten empfangen werden. Mit der gleichen Broadcast-Nachricht antwortet ein AP, wenn ein WLAN-Endgerät einen „Probe Request“[26] an einen AP sendet. Einige APs bieten die Möglichkeit, das Senden der SSID über die Broadcast-Nachricht zu unterdrücken. In diesem Fall können sich nur noch WLAN-Endgeräte, welche die SSID kennen, in die WLAN-Infrastruktur einwählen. Für alle anderen, welche die SSID nicht kennen, ist die WLAN-Infrastruktur nicht „sichtbar“.

---

21 Siehe z. B. http://www.doc-x.de/cgi-bin/wiki.pl?action=browse&id=DefaultSSID&revision=1

22 Vgl. Abschnitt 2.2

23 Vgl. Abschnitt 2.3.1

24 Das Beacon-Frame ist ein Management-Frame, welches Informationen über das Netzsegment enthält.

25 Ein Broadcast ist ein Rundruf innerhalb eines Netzwerkes, wobei von einem Punkt aus Datenpakete gleichzeitig an alle Teilnehmer des Netzes übertragen werden.

26 Hierbei sendet ein WLAN-Endgerät ein Paket mit leerer SSID an alle, die ihn empfangen können. Alle APs antworten hierauf mit ihrer SSID und weiteren Informationen.

Man spricht hierbei vom „Closed-“ bzw. „Secure-Mode“. Diese Sicherheitsmaßnahme bietet einen Schutz gegen einige frei verfügbare Hackertools, wie z. B. gegen NetStumbler, und ist deshalb einzusetzen [BSI03a]. Ein passiver Scanner kann jedoch immer noch die SSID ermitteln. Dies geschieht, in dem er die Anmeldung eines legitimen WLAN-Endgerätes mitliest, der dabei die SSID bekannt gibt [Blum03]. Hierzu sind jedoch erweiterte Kenntnisse des Angreifers notwendig.

30: Beacon Intervall maximieren

Kann das Versenden der SSID im Broadcast nicht deaktiviert werden, ist das Beacon-Frame-Intervall[24] zu maximieren. Durch die Umsetzung der Sicherheitsmaßnahme wird das Risiko minimiert, dass Unberechtigte die WLAN-Infrastruktur nutzen. Allerdings ist die Schutzwirkung dadurch relativ gering.

31: DHCP am Access Point abschalten

Mit Hilfe eines Dynamic Host Configuration Protocol (DHCP) Servers auf dem AP erhalten WLAN-Endgeräte automatisiert eine IP-Adresse zugewiesen. Dieser Dienst ist abzuschalten. Stattdessen ist ein möglichst kleiner IP-Adressraum mit statischen IP-Adressen freizugeben [BSI03a]. Somit können berechtigte WLAN-Endgeräte sich anhand ihrer IP-Adresse gegenüber dem AP authentisieren. Diese Sicherheitsmaßnahme wirkt nur bedingt, da ein Angreifer die IP-Adressen während eines Kommunikationsvorgangs zwischen einem legitimen WLAN-Endgerät und AP abhören kann. Des Weiteren führt das Abschalten des DHCP-Dienstes bei größeren WLAN-Infrastrukturen oder in großen Unternehmen und Behörden zu Problemen, da Anwender ihre WLAN-Endgeräte z. B. an verschiedenen Standorten einsetzen wollen, ohne dabei manuell ihre IP-Adresse umkonfigurieren zu wollen.

32: Verbindung zwischen RADIUS-Server und Access Point absichern

Wird ein RADIUS-Server zur Authentifizierung angewandt, muss die Verbindung zwischen RADIUS-Server und Access Point abgesichert werden (z. B. mit TLS oder SSL). Voraussetzung hierfür ist jedoch ein Zugriff zum internen Netzwerk, an dem der AP angeschlossen ist. Mit der Absicherung der Verbindung zwischen RADIUS-Server und Access Point wird das Risiko einer Dictionary-Attacke zur Ermittlung des Sitzungsschlüssels minimiert.

33: Einen WLAN-Standard, anstatt mehrerer parallel nutzen (z. B. 'G-only' oder 'B-only')

Wird an einem Access Point ein Mischbetrieb mehrerer WLAN-Standards ermöglicht (802.11g und 802.11b mit unterschiedlichen Datenraten 11 Mbit/s bzw. 54 Mbit/s), tritt ein unangenehmer Nebeneffekt auf: Die Performance aller WLAN-Endgeräte wird auf den Level der 11 Mbit/s-Technologie reduziert. Dies kann z. B. auch durch den Empfang von Signalen benachbarter WLAN-Infrastrukturen ausgelöst werden. Durch Nutzung der Funktionen „G-only“ oder „B-only“ wird das WLAN auf einen Standard fest eingestellt. Damit können die Verfügbarkeit des Netzes erhöht sowie Störungen benachbarter WLAN-Infrastrukturen vermieden werden.

34: Block-Intra-BSS-Traffic in öffentlichen Bereichen verwenden

Block-Intra-BSS-Traffic ermöglicht, dass sich die WLAN-Endgeräte in derselben WLAN-Infrastruktur nicht „sehen“ können. Somit besteht keine Möglichkeit, den benachbarten Datenverkehr „einzusehen“ [Stud06].

Authentifizierungsverfahren anwenden

Zur Authentifizierung der WLAN-Endgeräte existieren unterschiedliche Möglichkeiten.[27] Je nachdem, welche der folgenden Authentifizierungsverfahren bzw. welche WLAN-Standards die eingesetzten WLAN-Geräte unterstützen, sind folgende Authentifizierungen einzusetzen.

35: Authentifizierung über MAC-Adresse

Zur Authentifizierung der WLAN-Endgeräte ist die Media-Access-Control-Adresse (MAC-Adresse) verwendbar.[28] Dazu müssen in den APs von Hand Access-Control-Lists (ACL) gepflegt werden. Insbesondere bei großen WLAN-Infrastrukturen ist diese Sicherheitsmaßnahme sehr aufwändig. Bei Diebstahl einer zugelassenen WLAN-Karte bzw. des Laptops inklusive WLAN-Karte müssen die ACL sofort aktualisiert und die betroffene MAC-Adresse gesperrt werden. Ein weiterer Nachteil besteht in der Möglichkeit des MAC-Spoofing. Hierbei hört ein Angreifer zunächst den Datenfluss einer WLAN-Infrastruktur ab und ermittelt dabei zugelassene MAC-Adressen, die im Klartext über das Übertragungsmedium versendet werden. Anschließend nutzt der Angreifer eine ermittelte

---

27 Vgl. dazu die Ausführungen in Abschnitt 2.3.

28 Vgl. Abschnitt 2.3.1.

MAC-Adresse und meldet sich mit dieser an der WLAN-Infrastruktur an. Hierfür gibt es frei verfügbare MAC-Spoofing Tools[29].

36: Pre-Shared-Key-Authentifizierung

Unterstützen die eingesetzten WLAN-Geräte WPA, ist die Pre-Shared-Key-Authentifizierung als Sicherheitsmaßnahme einsetzbar. Der Pre-Shared-Key muss auf den APs und jedem WLAN-Endgerät eingetragen werden.[30] Beim Authentifizierungsvorgang wird in einem „Challenge-Response"-Dialog geprüft, ob das WLAN-Endgerät über den entsprechenden Pre-Shared-Key verfügt [Davi04, 23]. Die Kommunikation zwischen WLAN-Endgeräte und AP ist nur möglich, wenn der „Challenge-Response"-Dialog erfolgreich ist.

37: Open-System- der Shared-Key-Authentifizierung vorziehen, um Kompromittierung des WEP-Schlüssels zu unterbinden

Laut IEEE 802.11 können bei WEP zwei unterschiedliche Authentifizierungsverfahren eingesetzt werden. Während des „Challenge-Response"-Dialoges zwischen WLAN-Endgerät und AP kann ein Angreifer den unverschlüsselten Challenge-Text sowie das verschlüsselte Ergebnis abhören. Mit Hilfe dieser Daten kann der Angreifer relativ einfach den WEP-Key berechnen. Gelingt ihm das, kann er den gesamten Datenverkehr entschlüsseln und/oder unberechtigt die WLAN-Infrastruktur nutzen. Aufgrund dieser Schwäche sollte in Verbindung mit der WEP-Verschlüsselung die Open-System-Authentizierung zum Einsatz kommen.

38: Authentifizierung mit WLAN Smartcard

Im April 2004 wurden vom „WLAN Smart Card Consortium"[31] die Spezifikationen für eine Authentifizierung im WLAN mit Hilfe von Smartcards verabschiedet. Zur Authentifizierung via Smart Card im WLAN werden die Standards 802.1X und EAP sowie das WPA-Schlüsselmanagement benutzt. Hierzu ist eine entsprechende Smartcard mit Lesegerät oder ein USB-Key an einem USB-Port notwendig.

---

29 Z. B. SMAC, http://www.klcconsulting.net/smac.

30 Vgl. Abschnitt 2.3.1.

31 Weiterführende Informationen über das WLAN Smart Card Consortium sowie zu den Spezifikationen unter http://wlansmartcard.org.

39: Authentifizierung nach IEEE 802.1x über RADIUS-Server

Für eine unternehmensweit einheitliche Authentifizierung der Endgeräte im LAN und WLAN ist das 802.1x-Authentifizierungsprotokoll einzusetzen.[32] Voraussetzung dafür ist das Vorhandensein der entsprechenden WPA-Funktionalitäten auf den Endgeräten bzw. Betriebssystemen. Darüber hinaus ist ein Authentifizierungsserver notwendig (RADIUS-Server). Das verwendete Protokoll zur Authentifizierung zwischen Endgerät und AP ist EAP. EAP unterstützt wiederum unterschiedliche Authentifizierungsvarianten, die sich in Komplexität und Funktionalität unterscheiden: EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS, PEAP.[33] Diese müssen im Voraus vereinbart und von den entsprechenden Endgeräten unterstützt werden. 802.1X ist ausschließlich ein Verfahren zur Authentifizierung und ggf. zur Schlüsselverteilung. 802.1X ist ohne passende Verschlüsselung und Integritätssicherung sogar als unsicher anzusehen [BSI03a].

Verschlüsselungstechniken benutzen

Zur Verschlüsselung der Datenübertragung in WLAN-Infrastrukturen gibt es unterschiedliche Möglichkeiten.[34] Je nachdem, welche der folgenden Verschlüsselungstechniken bzw. welche WLAN-Standards die eingesetzten WLAN-Geräte unterstützen, sind entsprechende Verschlüsselungen einzusetzen.

40: WEP-Verschlüsselung

Als Basis-Verschlüsselung ist WEP einzusetzen. WEP basiert auf dem RC4-Datenstromchiffreverfahren. Hierbei werden Klardaten paketweise mit einem Schlüssel und einem Initialisierungsvektor (IV) verschlüsselt. Der Schlüssel muss innerhalb einer WLAN-Infrastruktur überall gleich sein. Dazu muss er vorab auf allen APs und WLAN-Endgeräten manuell eingetragen werden. Diese Verteilung des Schlüssels führt häufig dazu, dass Schlüssel selten oder gar nicht gewechselt werden. Ist innerhalb der WLAN-Infrastruktur der Schlüssel einmal kompromittiert, muss er durch physischen Zugriff auf allen WLAN-Geräten manuell ausgetauscht werden. Darüber hinaus sind weitere WEP-Schwachstellen bekannt.[35]

---

32 Vgl. Abschnitt 2.3.2

33 Zum Aufbau und zur Funktionsweise der verschiedenen EAP-Varianten vgl. [Micr05, 7 ff.; SMBa04, 158-192]

34 Vgl. dazu die Ausführung in Abschnitt 2.3

35 Für eine ausführliche Darstellung der WEP-Schwachstellen vgl. [BGWa01].

41: Verschlüsselung nach WPA-Standard

Für eine starke Verschlüsselung ist WPA einzusetzen. Die Verschlüsselung ist gegenüber WEP zu bevorzugen, da einige Schwächen von WEP beseitigt sind.[36]

42: Verschlüsselung nach WPA2 bzw. 802.11i

Unterstützen die eingesetzten WLAN-Geräte bereits den Standard IEEE 802.11i/WPA2, ist die auf dem Advance Encryption Standard basierende Verschlüsselung einzusetzen.[37]

Weitere softwaretechnische Maßnahmen

43: Netzwerktechnische Trennung zwischen WLAN und drahtgebundenem Netz (z. B. über Paketfilter, VPN oder VLAN)

Die Verbindung zwischen einer WLAN-Infrastruktur und einem kabelgebundenen LAN muss besonders gesichert werden. Firewalls/Paketfilter, Virtual Privat Networks (VPN) und/oder Virtuelle LANs können dabei eingesetzt werden. Dies ermöglicht eine bessere Kontrolle des Datenverkehrs in und zwischen den Netzsegmenten sowie eine zusätzliche Absicherung des LANs vor Angreifern aus dem WLAN.

44: Installation einer Personal Firewall auf den mobilen Endgeräten

Auf den WLAN-Endgeräten ist eine Personal Firewall zu installieren. Diese Sicherheitsmaßnahme kann zwar auch in drahtgebundenen LANs eingesetzt werden, jedoch spielt sie bei WLAN-Endgeräten eine besondere Rolle, da WLAN-Endgeräte oft auch öffentliche APs kontaktieren (z. B. in Flughäfen, Bahnhöfen oder Cafes). Da man in diesen Fällen über den AP sowie evtl. weitere Anwender der öffentlichen WLAN-Infrastruktur in der Regel kaum Kenntnisse besitzt, ist der Schutz des eigenen WLAN-Endgerätes sehr wichtig.

45: Verwendung eines Intrusion Detection Systems zur Überwachung des WLANs

Zur Erkennung von Unregelmäßigkeiten während des Betriebes ist ein Intrusion Detection Systems (IDS) zu verwenden. IDS gibt es für drahtgebundene sowie funkbasierte LANs. Funkbasierte IDS überwachen mit Funksensoren die Funkspektren der WLAN-Infrastruktur. Treten Anomalien auf, werden diese erkannt und gemeldet.

---

[36] Vgl. dazu die Ausführungen in Abschnitt 2.3.2

[37] Vgl. dazu die Ausführungen in Abschnitt 2.3.3

46: Datei- und Ressourcenfreigabe auf allen Endgeräten sowie Geräten, die vom WLAN aus erreichbar sind, restriktiv einschränken

Die Freigaben von Dateien und weiteren Ressourcen (Drucker, Scanner, DFÜ-Verbindungen, etc.) muss in WLAN-Infrastrukturen sehr restriktiv erfolgen. Unter diesen Aspekt fällt auch die regelmäßige Überprüfung der Laufwerke nach Freigaben. Diese Maßnahme ist besonders bei öffentlichen APs und bei Ad-hoc-Verbindungen wichtig, da nicht zugriffsgeschützte Dateien für jeden WLAN-Anwender über die Luftschnittstelle zugänglich sind.

4 Empirische Untersuchung

4.1 Ziel der Untersuchung und Hypothesenformulierung

Ziel der empirischen Untersuchung ist es, die zu Beginn gestellten Fragen[38] zur Verbreitung und Sicherheit von WLAN-Infrastrukturen in deutschen Unternehmen und Behörden zu beantworten. Darüber hinaus haben wir zur Konkretisierung dieser Fragen 15 weitere Hypothesen[39] formuliert[40], die mit Hilfe der Untersuchung bestätigt oder widerlegt werden sollen [Krom02, 346].

Verbreitung von WLAN-Infrastrukturen	
Hypothese 1	Der Betrieb von WLAN-Infrastrukturen in Unternehmen und Behörden hat im Vergleich zu vergangenen Jahren stark zugenommen.
Hypothese 2	Neu gegründete Unternehmen und Behörden sowie Unternehmen der IuK-Branche setzen im Vergleich zu älteren Unternehmen und Behörden oder zu Unternehmen anderer Branchen häufiger WLAN-Infrastrukturen ein.
Hypothese 3	Hauptsächlich große Unternehmen und Behörden mit einem entsprechenden IT-Know-How setzen WLAN-Infrastrukturen ein.
Verbreitung bestimmter Formen von WLAN-Infrastrukturen	
Hypothese 4	WLAN-Infrastrukturen werden vor allem als mobiler Internetzugang bzw. als mobiler Zugang zu Unternehmensanwendungen genutzt und sie sind meist an ein anderes LAN im Unternehmen angeschlossen.
Hypothese 5	Zurzeit werden die meisten WLAN-Infrastrukturen mit dem Standard IEEE 802.11g und im Infrastruktur-Modus betrieben.

38 Vgl. Abschnitt 1.2

39 Hypothesen sind auf Annahmen basierte Aussagen über einen Tatbestand [Krom02, 40].

40 Die Herleitung der Hypothesen sowie der Zusammenhang zwischen den Fragen, Hypothesen und Fragestellungen im Fragebogen werden im Abschnitt 4.3 erörtert. Für die Hypothesenbildung haben wir insbesondere folgende Quellen verwendet: [Bach04; BSI03c; BüGö03; Dete03; RSA05; Saut04; Sili05; StLe04; Wick04]

Hypothese 6	Die Sicherheitsrelevanz der Nutzdaten, die über WLAN-Infrastrukturen übertragen werden, ist vergleichbar mit denen, welche über drahtgebundene LANs übertragen werden,.
Einsatz von Sicherheitsmaßnahmen in WLAN-Infrastrukturen	
Hypothese 7	Unternehmen und Behörden setzen mehr technische als organisatorische Sicherheitsmaßnahmen ein.
Hypothese 8	Über ein Drittel der im Fragebogen genannten Sicherheitsmaßnahmen sind den Befragungsteilnehmern nicht bekannt.
Hypothese 9	Obwohl die Befragungsteilnehmer viele Sicherheitsmaßnahmen kennen, setzen sie über 20 Prozent der ihnen bekannten Maßnahmen nicht ein.
Hypothese 10	Wenn bekannte Sicherheitsmaßnahmen nicht eingesetzt werden, ist der am häufigsten genannte Grund dafür ein zu hoher Implementierungs- oder Betriebsaufwand.
Zusammenhänge zwischen unternehmensspezifischen Merkmalen und WLAN-Sicherheitsmaßnahmen	
Hypothese 11	Unternehmen aus der IuK-Branche setzen im Vergleich zu Unternehmen aus anderen Branchen und Behörden mehr Sicherheitsmaßnahmen ein.
Hypothese 12	In Unternehmen und Behörden, die ein IT-Security-Management besitzen, ist der Einsatz von Sicherheitsmaßnahmen wesentlich höher als in Unternehmen und Behörden ohne IT-Security-Management.
Hypothese 13	Größere Unternehmen und Behörden setzen im Vergleich zu kleineren Unternehmen und Behörden mehr Sicherheitsmaßnahmen in ihren WLAN-Infrastrukturen ein.
Hypothese 14	Unternehmen und Behörden, die eine WLAN-Infrastruktur bereits seit mehr als einem Jahr betreiben und damit über längere Erfahrungen verfügen, setzen mehr Sicherheitsmaßnahmen ein als Unternehmen und Behörden, die ihre WLAN-Infrastruktur erst seit einem Jahr betreiben.
Hypothese 15	Setzen Unternehmen und Behörden WLAN-Infrastrukturen in sicherheitskritischen Bereichen, wie Geschäftsführung, Entwicklung, Personal- oder Finanzbereich ein, sind mehr Sicherheitsmaßnahmen realisiert als bei Unternehmen und Behörden, die WLAN-Infrastrukturen nicht in diesen Bereichen einsetzen.

Tab. 4-1: Hypothesen zur empirischen Untersuchung

4.2 Vorbereitung und Durchführung

Für die Durchführung empirischer Untersuchungen gibt es unterschiedliche Erhebungsmethoden.[41] Eine der am häufigsten genutzten Methoden ist die Befragung [SHEs99, 299]. Sie kann beispielsweise als mündliche Befragung, schriftliche Befragung, Telefoninterview oder auch als Online-Befragung durchgeführt werden. Wir haben uns für eine Internetbasierte Befragung (Online-Befragung) entschieden. Mit deren Hilfe können im Vergleich zu anderen Befragungsformen Daten von einer großen Teilnehmerzahl relativ zeitnah und mit überschaubarem Aufwand aufgenommen werden. Des Weiteren wird die Auswertung

[41] Für eine Übersicht empirischer Untersuchungsformen vgl. z. B. [BoDö03; Krom02; SHEs99]

der Befragungsdaten erleichtert und beschleunigt, da die erhobenen Daten direkt nach der Durchführung elektronisch zur Verfügung stehen.

Für die Befragung haben wir einen Fragebogen[42] entwickelt [Krom02, S. 346]. Dieser besteht aus 33 Fragen und gliedert sich in drei Teile. Im ersten Teil werden Informationen zu den teilnehmenden Unternehmen und Behörden sowie der Stellenwert und die organisatorische Verankerung ihres IT-Sicherheitsmanagements ermittelt. Der zweite Teil enthält Fragen zu den WLAN-Infrastrukturen. Im letzten und umfangreichsten Teil werden die Befragungsteilnehmer nach den Sicherheitsmaßnahmen gefragt. Dieser Teil basiert auf unserem Katalog WLAN-spezifischer Sicherheitsmaßnahmen[43]. Abb. 4-1 zeigt einen Auszug aus diesem letzten Fragebogenteil.

Sicherheitsmaßnahme	**Welche der Maßnahmen sind Ihnen bekannt?**	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit**	**keine Angabe**
WEP-Verschlüsselung	☐	☐		☐
Verschlüsselung nach WPA-Standard	☐	☐		☐
Verschlüsselung nach WPA2 bzw. 802.11i	☐	☐		☐

Abb. 4-1: Auszug aus dem Fragebogen

Für jede Sicherheitsmaßnahme wurde erfragt, ob sie dem Befragungsteilnehmer bekannt ist und ob sie im Unternehmen bzw. der Behörde eingesetzt wird. Für den Fall, dass die Sicherheitsmaßnahme bekannt aber nicht eingesetzt ist, wurde nach den Gründen dafür gefragt. Zur Entwicklung des Fragebogens sowie zur Durchführung der Online-Befragung haben wir das Internet-basierte Werkzeug „eQuestionnaire“[44] verwendet. Den Befragungsteilnehmern wurde außerdem angeboten, eine Offline-Version des Fragebogens auszufüllen.

[42] Der vollständige Fragebogen befindet sich im Anhang 1.
[43] Vgl. Abschnitt 3.3 und zur Übersicht Tab. 3-1.
[44] Weitere Informationen zu diesem Werkzeug findet man unter http://www.equestionnaire.de.

Die Befragung wurde in Kooperation mit dem IT-Dienstleister NetSys.IT Information & Communication[45], dem Wirtschaftsnetz Thüringen (WNT)[46], dem Wirtschafts- und Innovationsportal Thüringen (WIP)[47] und dem TeleTrusT Deutschland e.V.[48] durchgeführt. Nach ausführlichen Pretests des Fragebogens in Zusammenarbeit mit Experten unserer Kooperationspartner fand die Untersuchung im Zeitraum von November 2005 bis Januar 2006 statt. Zur Grundgesamtheit zählen wir alle Unternehmen und Behörden in Deutschland, die WLAN-Infrastrukturen einsetzen. Gesicherte Erkenntnisse über die Anzahl dieser Unternehmen und Behörden liegen uns allerdings nicht vor. Aus diesem Grund wählten wir eine Stichprobe aus, die einerseits eine relativ hohe Anzahl von WLAN-Installationen erwarten ließ und andererseits auch Interesse für Sicherheitsfragen in diesem Umfeld hat. Bei der Auswahl von potentiellen Teilnehmern konzentrierten wir uns auf die Mitglieder unserer Partner WIP[49] und TeleTrusT[50]. Insgesamt versendeten wir an 1.164 Unternehmen und Behörden per E-Mail Einladungen zur Teilnahme an der Befragung.

4.3 Beschreibung und Auswertung der Ergebnisse

4.3.1 Rücklaufquote und Beschreibung der Befragungsteilnehmer

290 der insgesamt 1.164 angeschriebenen Unternehmen und Behörden nahmen bis zum 31.01.2006 an der Befragung teil (n_A=290). Dies ergibt eine Rücklaufquote von 24,9%.

Abb. 4-2 zeigt, dass 92,1% der Befragungsteilnehmer Unternehmen und 5,1% Behörden sind.[51] Der größte Teil der Unternehmen verteilt sich auf die Branchen Dienstleistungen (42,1%), Industrie (35,5%) und Information und Kommunikation (12,1%). Demgegenüber sind aus den Branchen Handel (1,7%), Verkehr (0,3%) und Tourismus (0,3%) nur verhältnismäßig wenige Unternehmen vertreten.

45 Weitere Informationen unter http://www.netsys-it.de
46 Weitere Informationen unter http://www.wn-thueringen.de
47 Weitere Informationen unter http://www.wip-thueringen.de
48 Weitere Informationen unter http://www.teletrust.de
49 Die Mitglieder des WIP sind Unternehmen und Behörden, die in Thüringen tätig sind.
50 Die Mitglieder des TeleTrusT e.V. sind Unternehmen und Behörden aus ganz Deutschland, die gemeinsam die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik fördern.
51 Die Befragungsteilnehmer konnten Antworten offen lassen. Aus diesem Grund ergeben die Summierungen der einzelnen Prozentsätze nicht immer 100%.

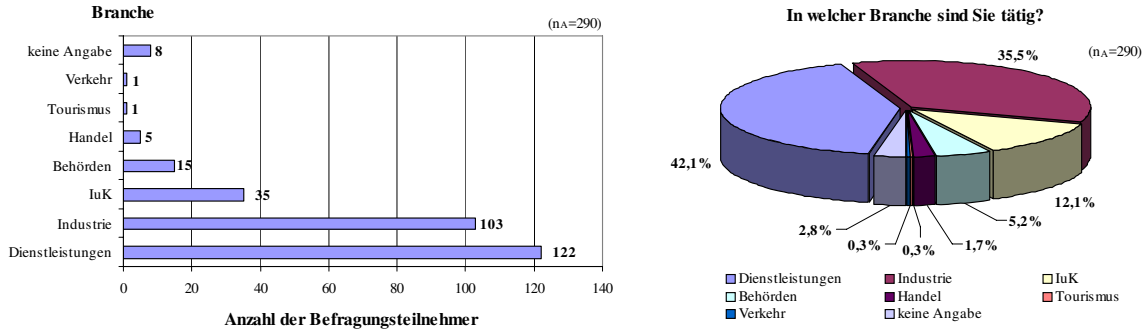

Abb. 4-2: Branchenzugehörigkeit der Befragungsteilnehmer

Hinsichtlich der Größe der Unternehmen und Behörden ist festzustellen, dass 40,0% Kleinstinstitutionen (<10 Mitarbeiter), 29,7% kleine Institutionen (10-50 Mitarbeiter), 18,6% mittlere Institutionen (51-250 Mitarbeiter) und 10% große Institutionen (>250 Mitarbeiter) sind.[52]

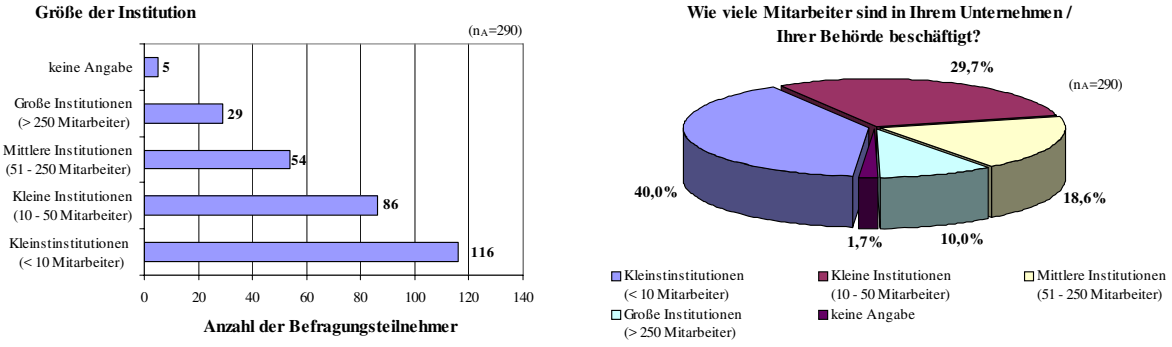

Abb. 4-3: Größe der befragten Unternehmen und Behörden

Des Weiteren haben wir die Befragungsteilnehmer nach dem Gründungsjahr ihrer Institution befragt. Abb. 4-4 zeigt, dass 65,2% der teilnehmenden Unternehmen und Behörden im Zeitraum zwischen 1990 und 1999 gegründet wurden. Weitere 17,9% der Institutionen existieren erst seit dem Jahr 2000 oder sind noch jünger, 11,7% wurden vor dem Jahr 1990 gegründet.

52 Die vorgenommene Größenunterscheidung orientiert sich an den Empfehlungen der Europäischen Union [EU03].

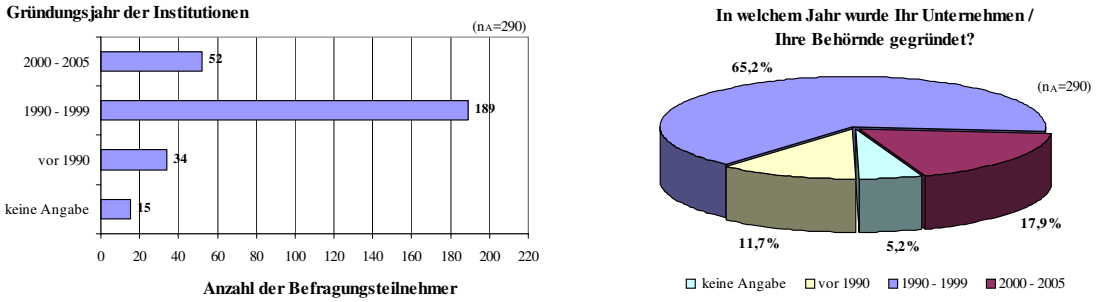

Abb. 4-4: Gründungsjahr der befragten Unternehmen und Behörden

Aufgrund der Stichprobenauswahl[53] kommen 84,1% der Befragungsteilnehmer aus Thüringen, 3,4% aus Nordrhein-Westfalen und 2,8% aus Baden-Württemberg. Die restlichen 6,6% der Befragungsteilnehmer verteilen sich auf die Bundesländer Bayern, Berlin, Bremen, Hessen, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt und Schleswig-Holstein.

Abb. 4-5 zeigt, dass mehr als die Hälfte der Fragebögen (55,2%) von Mitgliedern der Geschäftsführung ausgefüllt wurden. Dies ist mit dem hohen Anteil der Kleinst- und Kleinunternehmen zu erklären. In derartigen Unternehmen ist der Geschäftsführer oft auch der IT- und/oder Sicherheitsverantwortliche. Neben einem Anteil von 17,9% IT-Fachleuten füllten auch Mitarbeiter aus nicht IT-spezifischen Fachbereichen (20,7%) den Fragebogen aus. Insgesamt ist also ein breites Spektrum verschiedener Rollen innerhalb des Unternehmens vertreten, wobei der Anteil der Personen aus der Geschäftsführung dominiert.

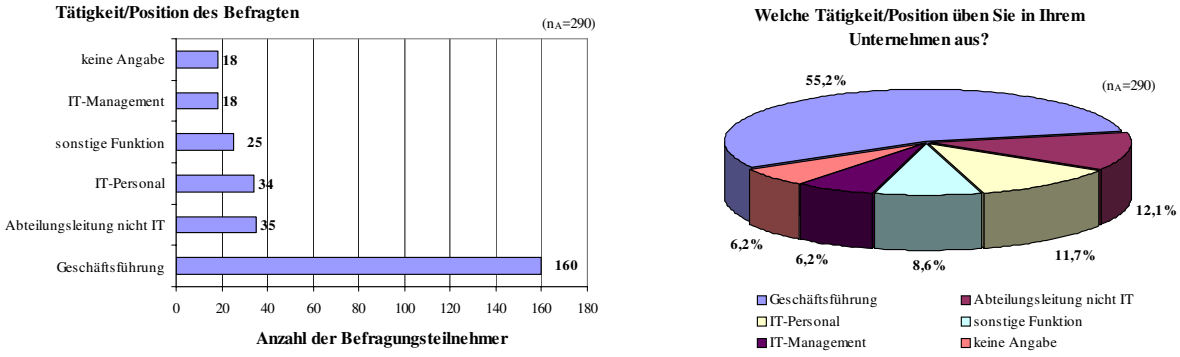

Abb. 4-5: Tätigkeiten/Position der befragten Personen

53 Zur Beschreibung der Stichprobenauswahl vgl. Abschnitt 4.2

4.3.2 Verbreitung von WLAN-Infrastrukturen

75 der 290 befragten Unternehmen und Behörden gaben an, dass sie eine WLAN-Infrastruktur betreiben. Dies ergibt unter den Befragungsteilnehmern eine WLAN-Verbreitung von 25,9%. Die folgenden Auswertungen basieren auf den Antworten aller Befragungsteilnehmer (n_A=290).[54]

Hypothese 1: Der Betrieb von WLAN-Infrastrukturen in Unternehmen und Behörden hat im Vergleich zu vergangenen Jahren stark zugenommen.

Verschiedene Publikationen [BSI03b; BSI03c, 140; BüGö03, 4 ff.; Dete03, 5 ff.; Dete04; StLe04, 15] berichten über einen zunehmenden Einsatz von WLAN-Infrastrukturen und begründen die Behauptung über die Zunahme der WLAN-Nutzung. Zur Bestätigung dieser Hypothese erfragten wir nicht nur ob, sondern auch seit wann die 290 Unternehmen und Behörden ihre WLAN-Infrastrukturen betreiben.

Abb. 4-6 zeigt, dass seit 2002 eine stetige Zunahme der Verbreitung von WLAN-Infrastrukturen zu beobachten ist. Zwar hat sich in den letzten Jahren das Wachstum verlangsamt, dennoch ist weiterhin eine kontinuierliche Zunahme der Verbreitung feststellbar. Die Wachstumsrate der WLAN-Nutzung im Jahr 2005 war mit 33,9% immer noch sehr hoch. Dieser Trend wird auch 2006 anhalten, da 20 Befragungsteilnehmer für dieses Jahr den Einsatz von WLAN-Infrastrukturen planten. Damit ist Hypothese 1 bestätigt.

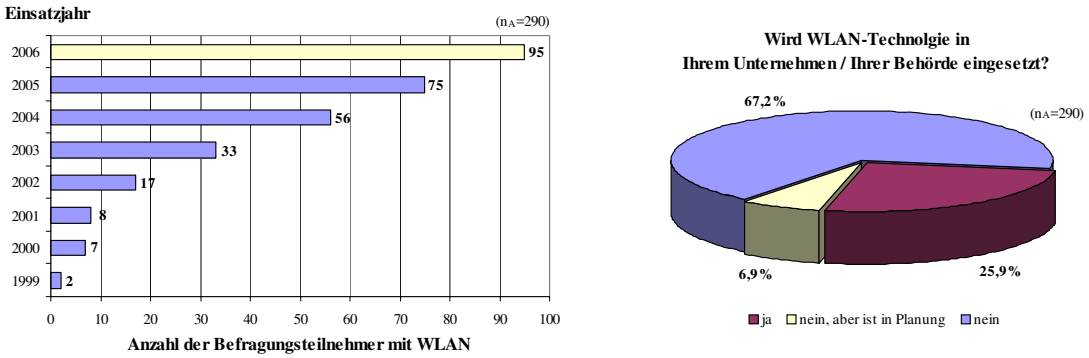

Abb. 4-6: Entwicklung der Verbreitung von WLAN-Infrastrukturen

54 Zur Beschreibung der Gruppe aller Befragungsteilnehmer vgl. Abschnitt 4.3.1.

Hypothese 2: Neu gegründete Unternehmen und Behörden sowie Unternehmen der IuK-Branche setzen im Vergleich zu älteren Unternehmen und Behörden oder zu Unternehmen anderer Branchen häufiger WLAN-Infrastrukturen ein.

Jüngeren Unternehmen und Behörden sowie Unternehmen aus der IuK-Branche wird oft eine größere Aufgeschlossenheit gegenüber neuen IT-Technologien zugeschrieben. Aus diesem Grund nahmen wir für diese im Vergleich zu älteren Unternehmen und Behörden oder Unternehmen anderer Branchen eine intensivere Nutzung von WLAN-Infrastrukturen an.

Abb. 4-7 zeigt, dass 40,4% der befragten Unternehmen und Behörden, die zwischen dem Jahr 2000 und heute gegründet wurden, WLAN-Infrastrukturen einsetzen. Dagegen ist bei Unternehmen und Behörden, die bereits vor dem Jahr 2000 existierten und somit wesentlich älter sind, die Verbreitung von WLAN-Infrastrukturen mit 22,4% wesentlich geringer.

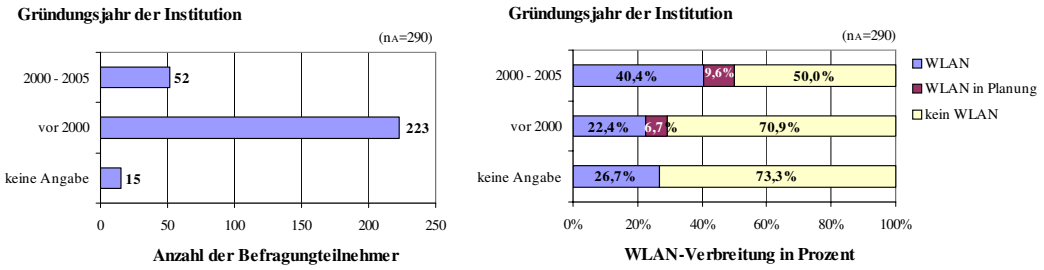

Abb. 4-7: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Existenzdauer der befragten Unternehmen und Behörden

Doch nicht nur die jüngeren Unternehmen und Behörden setzen verstärkt WLAN-Infrastrukturen ein, sondern auch Unternehmen aus der IuK-Branche. Bei ihnen ist die WLAN-Verbreitung mit 45,7% sehr hoch. Dagegen liegt der WLAN-Anteil bei Unternehmen der Branchen Industrie und Dienstleistungen weit unter der durchschnittlichen Verbreitung von 25,9%.[55] Damit ist Hypothese 2 bestätigt. Behörden erreichen mit 46,7% den Spitzenwert der WLAN-Verbreitung.

[55] Aufgrund der geringen Anzahl von Befragungsteilnehmern aus den Branchen Handel, Verkehr und Tourismus werden diese hier nicht berücksichtigt. Vgl. Abschnitt 4.3.1

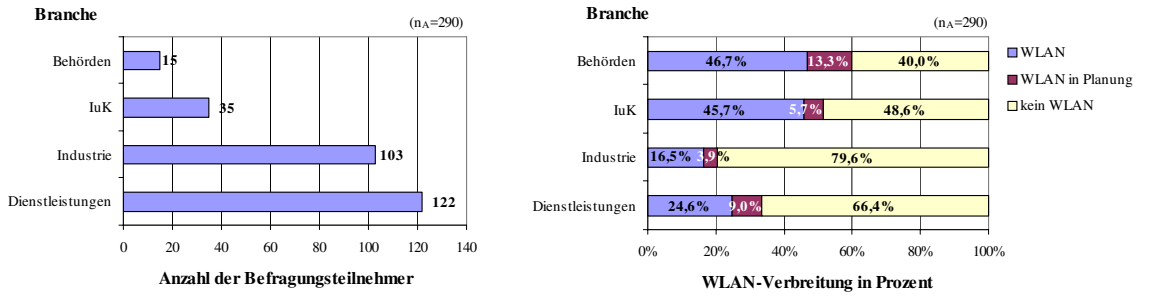

Abb. 4-8: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Branche der befragten Unternehmen[55]

Hypothese 3: Hauptsächlich große Unternehmen und Behörden mit einem entsprechenden IT-Know-How setzen WLAN-Infrastrukturen ein.

In dieser Hypothese formulieren wir eine direkte Abhängigkeit zwischen der Größe[56] eines Unternehmens bzw. einer Behörde und dem Einsatz von WLAN-Infrastrukturen. Wir nahmen an, dass größere Unternehmen und Behörden über ein umfangreicheres IT-Know-How verfügen und aus diesem Grund häufiger WLAN-Infrastrukturen einsetzen als kleinere Institutionen.

Die Analyse der beantworteten Fragebögen bestätigte unsere Vermutung, da 37,9% der Unternehmen und Behörden mit über 250 Mitarbeitern WLAN-Infrastrukturen einsetzen. Das liegt weit über der durchschnittlichen Verbreitung von 25,9%. Auch in mittelgroßen Unternehmen/Behörden ist der Anteil der WLAN Nutzenden mit 31,5% noch hoch. Dagegen setzen nur 15,1% der kleinen Unternehmen und Behörden mit 10 bis 50 Mitarbeitern sowie 29,3% der Kleinstunternehmen mit weniger als 10 Mitarbeitern WLAN-Infrastrukturen ein. Abb. 4-9 zeigt jedoch auch, dass zukünftig wohl insbesondere bei den kleineren Institutionen die Verbreitung zunehmen wird.

56 Die Größe eines Unternehmens bzw. einer Behörde wird durch die Mitarbeiterzahl beschrieben.

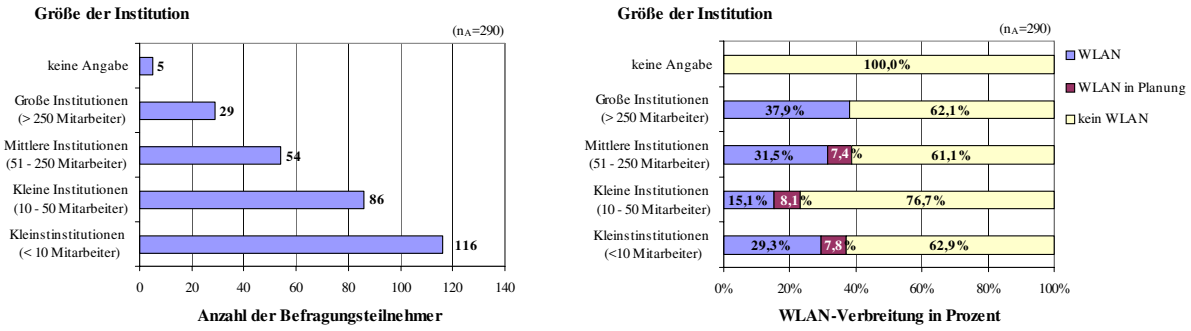

Abb. 4-9: Verbreitung von WLAN-Infrastrukturen in Abhängigkeit von der Größe der Unternehmen und Behörden

4.3.3 Verbreitung bestimmter Formen von WLAN-Infrastrukturen

Die Diskussion der folgenden Hypothesen basiert auf den Antworten der 75 Unternehmen und Behörden, die zum Zeitpunkt der Befragung WLAN-Infrastrukturen einsetzten (n_B=75). 90,7% der Befragungsteilnehmer dieser Gruppe sind Unternehmen, 9,3% Behörden. Die Mehrheit der beteiligten Unternehmen gehört den Branchen Dienstleistungen (40,0%), Industrie (22,7%) und Information und Kommunikation (21,3%) an. Demgegenüber sind die Branchen Handel (4,0%) und Tourismus (1,3%) unterrepräsentiert sowie Unternehmen der Branche Verkehr nicht vertreten. 45,3% der WLAN-nutzenden Unternehmen und Behörden sind Kleinstinstitutionen (<10 Mitarbeiter), 17,3% kleine Institutionen (10-50 Mitarbeiter), 22,7% mittlere Institutionen (51-250 Mitarbeiter) und 14,7% große Institutionen (>250 Mitarbeiter).[57] Die Auswertung der Gründungsjahre der Institutionen ergab, dass 46,7% der Unternehmen und Behörden dieser Gruppe (n_B=75) im Zeitraum zwischen 1990 und 1999, 28,0% zwischen 2000 und 2005 sowie 20,0% vor dem Jahr 1990 gegründet wurden. 80,0% der Befragungsteilnehmer mit WLAN-Infrastrukturen kommen aus Thüringen, 5,3% aus Nordrhein-Westfalen und je 2,7% aus Baden-Württemberg und Berlin. Die restlichen 4,0% verteilen sich auf die Bundesländer Bayern, Niedersachsen und Rheinland-Pfalz. Aus Sicht der Tätigkeiten/Positionen der Befragungsteilnehmer ist im Vergleich zu der Gruppe aller Befragungsteilnehmer (n_A=277)[58] festzustellen, dass der Anteil des IT-Fachpersonals (26,7%) höher und der Anteil der Teilnehmer aus der Geschäftsführung (44,0%) geringer ist. Beim Nicht-IT-Personal ist mit 20,0% keine signifikante Abweichung erkennbar.

---

57 Die vorgenommene Größenunterscheidung orientiert sich an den Empfehlungen der Europäischen Union [EU03].

58 Vgl. Abschnitt 4.3.1, insbesondere Abb. 4-5

Hypothese 4: WLAN-Infrastrukturen werden vor allem als mobiler Internetzugang bzw. als mobiler Zugang zu Unternehmensanwendungen genutzt und sie sind meist an ein anderes LAN im Unternehmen angeschlossen.

In verschiedenen Studien [BüGö03, 4 ff.; Ecol04; StLe04, 15] wurden als Hauptanwendungszwecke von WLAN-Infrastrukturen der Zugang zum Internet sowie der Zugang zu Anwendungen des Unternehmens ermittelt. Zur Überprüfung dieser Ergebnisse fragten wir nach den Anwendungszwecken der eingesetzten WLAN-Infrastrukturen. Die Befragungsteilnehmer konnten aus vorgegebenen Anwendungszwecken wählen bzw. eigene ergänzen (Mehrfachnennungen waren möglich).

Abb. 4-10 zeigt, dass 66,7% der Unternehmen und Behörden ihre WLAN-Infrastruktur für den Zugang zum Internet verwenden. Des Weiteren gaben 45,3% der Befragungsteilnehmer an, die WLAN-Infrastruktur als Zugang zu ihren Unternehmensanwendungen zu nutzen.

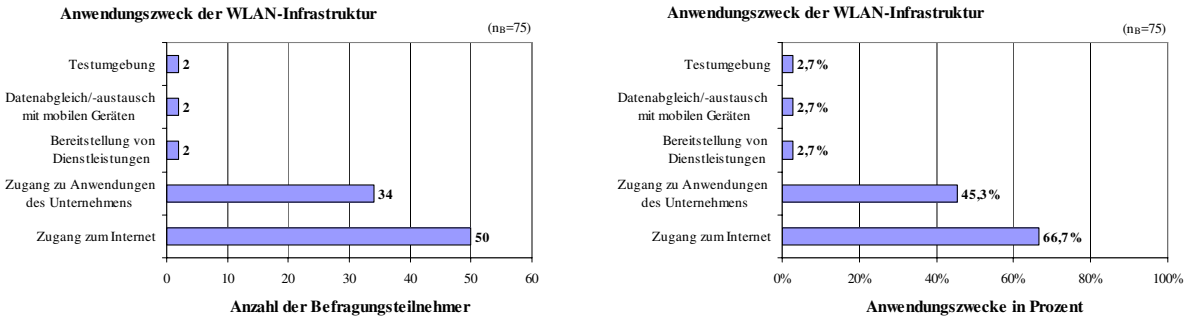

Abb. 4-10: Anwendungszwecke von WLAN-Infrastrukturen[59]

Insbesondere für den Zugang zu Unternehmensanwendungen sind WLAN-Infrastrukturen mit kabelgebundenen Netzen zu verbinden [BüGö03, 8]. Wir ermittelten, dass 60% der Befragungsteilnehmer diese Verbindung realisiert haben und 22,7% keine Anbindung der WLAN-Infrastruktur an ein anderes drahtgebundenes Netz besitzen. Damit ist Hypothese 4 bestätigt.

59 Mehrfachnennungen waren möglich.

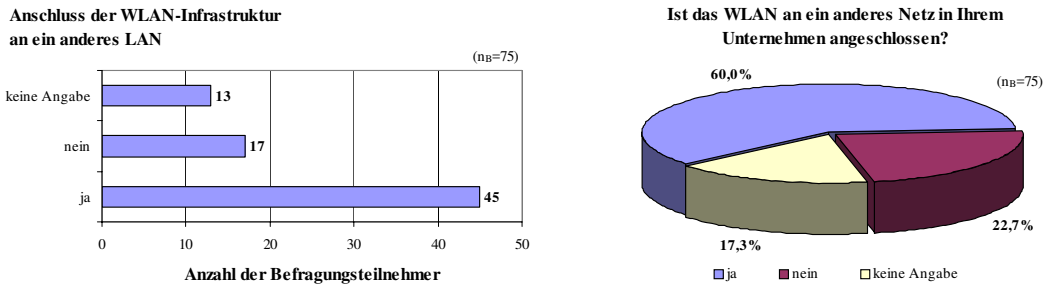

Abb. 4-11: Anbindung von WLAN-Infrastruktren an andere drahtgebundene Netze

Hypothese 5: Zurzeit werden die meisten WLAN-Infrastrukturen mit dem Standard IEEE 802.11g und im Infrastruktur-Modus betrieben.

Wie in Abschnitt 2.1 beschrieben, definiert das IEEE mit der Standardfamilie 802.11* für WLAN-Infrastrukturen verschiedene Standards. Diese unterscheiden sich neben den genutzten Frequenzbereichen vor allem durch die Übertragungsverfahren und die damit verbundenen Datenübertragungsraten. Verschiedene Untersuchungen ermittelten die Verbreitung einzelner WLAN-Standards [BSI03c, 155; BüGö03, 7; StLe04, S. 27]. Eine Studie von Ernst & Young im Jahr 2004 ergab beispielsweise, dass der 1999 verabschiedete IEEE 802.11b der dominierende WLAN-Standard in Deutschland ist [BüGö03, 8]. Aufgrund der wesentlich höheren Datenübertragungsrate des im Jahr 2003 spezifizierten Standards IEEE 802.11g nahmen wir an, dass dieser Standard mittlerweile die höchste Verbreitung hat.

Abb. 4-12 zeigt, dass 50,7% der Unternehmen und Behörden, die WLAN-Infrastrukturen einsetzen, den Standard IEEE 802.11g und nur noch 37,3% den Standard IEEE 802.11b nutzen (Mehrfachnennungen waren möglich). Andere WLAN-Standards werden dagegen vergleichsweise wenig eingesetzt.

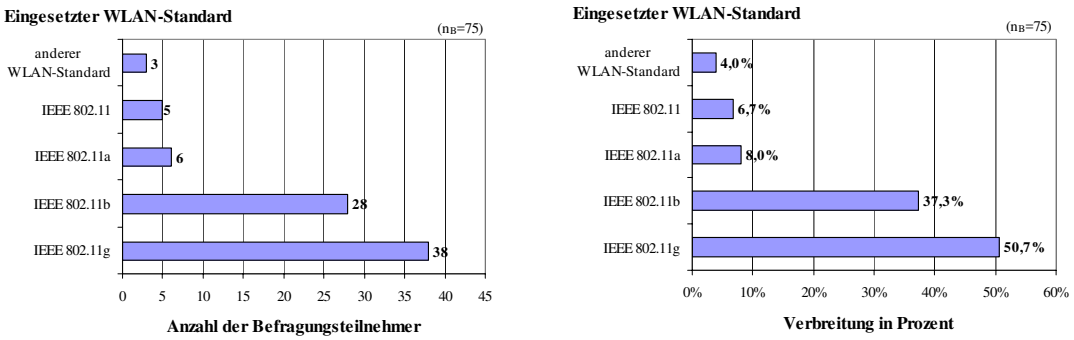

Abb. 4-12: Verbreitung von WLAN-Standards[60]

Unabhängig von der Wahl eines WLAN-Standards können WLAN-Infrastrukturen in zwei Modi betrieben werden.[61] Während beim Infrastruktur-Modus der Netzwerkverkehr der WLAN-Endgeräte über eine zentrale Instanz, den Access Points abläuft, kommunizieren im Ad-hoc-Modus die WLAN-Endgeräte direkt miteinander. Der Aufbau flächendeckender WLAN-Infrastrukturen in Unternehmen und Behörden erfordert die Verwendung des Infrastruktur-Modus [BSI05a, 14]. Aus diesem Grund gingen wir davon aus, dass in der Praxis der Ad-hoc-Modus eher selten anzutreffen ist.

Abb. 4-13 zeigt, dass 40,0% der Unternehmen und Behörden ihr WLAN im Infrastruktur-Modus betreiben. Den Ad-hoc-Modus nutzen hingegen nur 20% der Unternehmen und Behörden (Mehrfachnennungen waren möglich). Hypothese 5 ist damit bestätigt.

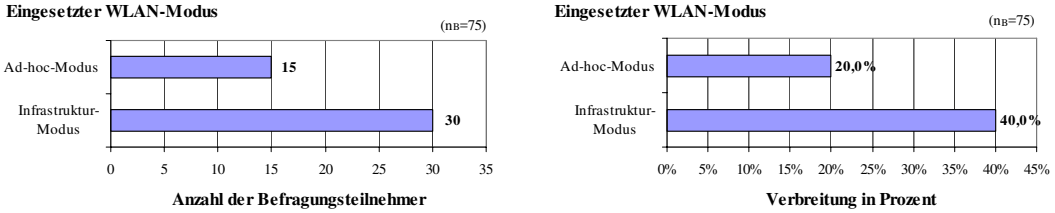

Abb. 4-13: Einsatz von Infrastruktur- vs. Ad-hoc-Modus[62]

Hypothese 6: Die Sicherheitsrelevanz der Nutzdaten, die über WLAN-Infrastrukturen übertragen werden, ist vergleichbar mit denen, welche über drahtgebundene LANs übertragen werden.

Um ein angemessenes Sicherheitsniveau in WLAN-Infrastrukturen zu ermöglichen, werden im IEEE 802.11-Standard und seinen Erweiterungen verschiedene Sicherheitsmaß-

60 Mehrfachnennungen waren möglich.
61 Vgl. dazu Abschnitt 2.2
62 Mehrfachnennungen waren möglich.

nahmen spezifiziert.[63] Darüber hinaus existieren weitere über die IEEE 802.11*-Standards hinausgehende Sicherheitsmaßnahmen.[64] Im weiteren Verlauf dieser Untersuchung sollen Gründe für den Einsatz bzw. Nichteinsatz von WLAN-Sicherheitsmaßnahmen ermittelt werden. Hierzu ermittelten wir jedoch zuerst, ob die über WLAN-Infrastrukturen übertragenen Daten genauso schutzbedürftig und damit sicherheitskritisch sind, wie Daten, die über die drahtgebundenen Netze übertragen werden. Wir gingen davon aus, dass die über WLAN-Infrastrukturen übertragenen Daten und die von drahtgebundenen Netzen in ihrer Sicherheitsrelevanz vergleichbar sind.

Abb. 4-14 zeigt, dass mit 53,3% die Mehrheit der befragten Unternehmen und Behörden mit WLAN-Infrastrukturen keinen Unterschied zwischen der Sicherheitsrelevanz von Daten sieht, die über das WLAN, und Daten, die über drahtgebundene Unternehmensnetze übertragen werden. Damit ist Hypothese 6 bestätigt. 25,3% der Befragungsteilnehmer gab an, dass die WLAN-Daten eine geringere Sicherheitsrelevanz besitzen. Nur 2,7% der Unternehmen und Behörden bewerten die über WLAN-Infrastrukturen übertragenen Daten mit einer vergleichsweise höheren Sicherheitsrelevanz.

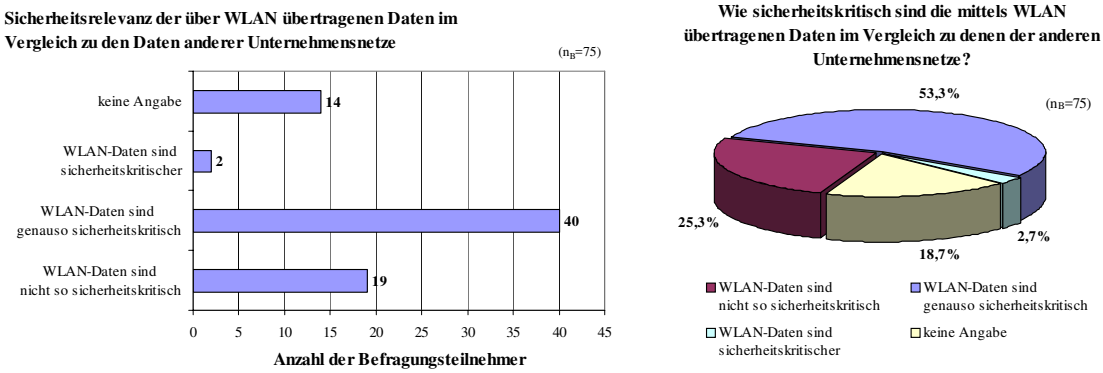

Abb. 4-14: Sicherheitsrelevanz der über WLAN-Infrastrukturen übertragenen Daten

4.3.4 Einsatz von Sicherheitsmaßnahmen in WLAN-Infrastrukturen

Von den Befragungsteilnehmern, die WLAN-Infrastrukturen einsetzen, füllten 36 die Fragen zu den WLAN-spezifischen Sicherheitsmaßnahmen vollständig aus. Die folgenden Auswertungen beziehen sich auf diese komplett ausgefüllten Fragebögen (n_C=36). 91,7% der Befragungsteilnehmer dieser kleineren Gruppe sind Unternehmen, 8,3% Behörden. Die Mehrheit der 32 Unternehmen gehört den Branchen Dienstleistungen (44,4%), Information

63 Vgl. zur Beschreibung der Sicherheitsmaßnahmen der IEEE-Standardfamilie Abschnitt 2.3

64 Vgl. dazu den Maßnahmenkatalog in Abschnitt 3.3

und Kommunikation (22,2%) und Industrie (19,4%) an. Demgegenüber sind die Branche Tourismus (2,8%) unterrepräsentiert. Unternehmen der Branchen Handel und Verkehr sind nicht vertreten. 41,7% der Unternehmen und Behörden dieser Gruppe (n_C=36) sind Kleinstinstitutionen (<10 Mitarbeiter), 16,7% kleine Institutionen (10-50 Mitarbeiter), 22,2% mittlere Institutionen (51-250 Mitarbeiter) und 19,4% große Institutionen (>250 Mitarbeiter).[65] Gegründet wurden 50,0% der Unternehmen und Behörden dieser kleinen Gruppe im Zeitraum zwischen 1990 und 1999, 25,0% zwischen 2000 und 2005 und 22,2% vor dem Jahr 1990. 75,0% der Befragungsteilnehmer (n_C=36) kommen aus Thüringen und 11,1% aus Nordrhein-Westfalen. Die Restlichen verteilen sich auf die Bundesländer Baden-Württemberg, Bayern, Berlin, Niedersachsen und Rheinland-Pfalz. Aus Sicht der Tätigkeiten/Positionen der Befragungsteilnehmer ist im Vergleich zu der Gruppe der WLAN-einsetzenden Befragungsteilnehmer (n_B=75)[66] festzustellen, dass der Anteil des IT-Fachpersonals mit 27,8% nochmals leicht höher sowie die Anteile der Befragungsteilnehmer aus der Geschäftsführung (36,1%) und dem Nicht-IT-Personal (16,7%) niedriger sind.

Hypothese 7: Unternehmen und Behörden setzen mehr technische als organisatorische Sicherheitsmaßnahmen ein.

Zur Absicherung von WLAN-Infrastrukturen sind sowohl technische als auch organisatorische Sicherheitsmaßnahmen notwendig. Organisatorische Veränderungen sind im Vergleich zu technischen Veränderungen oft mit höherem zeitlichen und personellen Aufwand verbunden. Wir nahmen aus diesem Grund an, dass technische Maßnahmen häufiger zum Schutz von WLAN-Infrastrukturen eingesetzt werden als organisatorische.

Tab. 4-2 zeigt die zehn am häufigsten eingesetzten Sicherheitsmaßnahmen. An den ersten beiden Positionen stehen softwaretechnische Maßnahmen. Dies ist nicht verwunderlich, da diese beiden Sicherheitsmaßnahmen zu denen in der Literatur am meisten Genannten zählen. Allerdings befinden sich bereits unter den TOP-10 insgesamt mehr organisatorische als technische Sicherheitsmaßnahmen. Darüber hinaus ermittelten wir durch Auswertung aller von den Befragungsteilnehmern eingesetzten Sicherheitsmaßnahmen, dass mehr organisatorische (53,4%) als technische Maßnahmen (35,6%) eingesetzt werden. Damit ist Hypothese 7 widerlegt.

---

65 Die vorgenommene Größenunterscheidung orientiert sich an den Empfehlungen der Europäischen Union [EU03].

66 Vgl. Abschnitt 4.3.3

ID	Maßnahme/Beschreibung	Klasse	Einsatzhäufigkeit in Prozent (n_C=36)
26	Werkseitige Grundeinstellungen an WLAN-Geräten ändern	Software-technische Maßnahme	83 %
28	Eigenen Netzwerknamen vergeben (kryptische SSID)	Software-technische Maßnahme	69 %
6	Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)	Org. Maßnahmen vor Inbetriebnahme	69 %
13	Administration der Access Points nicht über WLAN-Schnittstelle vollziehen	Org. Maßnahmen vor Inbetriebnahme	67 %
14	Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen	Org. Maßnahmen vor Inbetriebnahme	67 %
1	Notwendigkeit, Ziele und Anwendungszweck der WLAN-Infrastruktur begründen	Org. Maßnahmen vor Inbetriebnahme	67 %
22	Geeignete WLAN-Geräte (Signaltechnik: z. B. OFDM/ DSSS) und Standard (IEEE 802.11g, etc.) wählen	Hardware-technische Maßnahme	64 %
18	Physischer Zugriff zu Access Points nur autorisiertem Personal ermöglichen	Org. Maßnahmen während des Betriebs	61 %
44	Installation einer Personal Firewall auf den mobilen Endgeräten	Software-technische Maßnahme	58 %
2	Anforderungen an Sicherheitsziele festlegen	Org. Maßnahmen vor Inbetriebnahme	58 %

Tab. 4-2: Top-10-Liste der eingesetzten WLAN-Sicherheitsmaßnahmen

Neben den durch unseren Maßnahmenkatalog[67] vorgegeben Sicherheitsmaßnahmen konnten die Befragungsteilnehmer noch weitere von ihnen eingesetzte Sicherheitsmaßnahmen ergänzen. Tab. 4-3 enthält diese zusätzlichen Sicherheitsmaßnahmen. Es fällt auf, dass einige Befragungsteilnehmer Maßnahmen angaben, die bereits im Maßnahmenkatalog bzw. Fragenbogen enthalten waren, aber erst auf einer der Folgeseiten aufgeführt wurden. So ergänzten Befragungsteilnehmer beispielsweise bei den organisatorischen Sicherheitsmaßnahmen verschiedene software-technische, nach denen jedoch erst am Ende des Fragebogens gefragt wurde. Andere ergänzte Maßnahmen stellen Verfeinerungen von Sicherheitsmaßnahmen dar, die ebenfalls in unserem Katalog enthalten sind. Aus diesem Grund werden diese zusätzlich angegebenen Sicherheitsmaßnahmen in den folgenden Auswertungen nicht weiter berücksichtigt. Allerdings werden wir diese zusätzlichen Sicherheitsmaßnahmen bei der Überarbeitung/Vervollständigung unseres Maßnahmenkatalogs berücksichtigen.

[67] Vgl. Abschnitt 3.3 oder zur Übersicht Tab. 3-1

Klasse	Weitere von den Befragungsteilnehmern angegebene WLAN-Sicherheitsmaßnahmen
Organisatorische Maßnahmen vor der Inbetriebnahme	
	Die Mitarbeiter müssen unterschreiben, dass Sie unsere Bedingungen erfüllen.
	Funktionalität des WLAN zeitlich und örtlich begrenzt.
	IPSec; SSH und TLS Verschlüsselung / Authentifizierung der darüber laufenden Protokolle.
	QoS Betrachtungen, RSVP Implementierung, RADIUS Planung, Netzwerksimulation mit NS2.
	Separate Verschlüsselung von Kundendaten.
	WPA-PSK und Ausschluss unbekannter MAC-Adressen sowie Domainstruktur.
	Zugriff auf Unternehmens-LAN nur über VPN.
	Verschlüsselungstechnologien im Einsatz.
Organisatorische Maßnahmen während des Betriebs	
	Aktives Netzwerkmanagement organisieren und Verantwortungen definieren.
	eigene AP Software / Firmware im Einsatz, UNIX und Open Source Software OS auf allen Maschinen mit eigenem Sicherungskonzept.
	Firmwareupgrades der APs, Implementierung proprietärer Protokolle und neuer Security Ansätze für Remote Management in Testnetzen.
Hardware-technische Maßnahmen	
	AP mit Prism-Karten selbst gebaut und aktualisiert - je mit eigener bzw. aktualisierter Crypto-Umgebung nach Entwicklungsstand.
	Billing Überprüfung, damit die rechtmäßigen Anwender verifiziert werden. Wenn nicht bestätigt, dann keinen Zugriff mehr.
	Reichweite des Funknetzes durch bauliche Gegebenheiten von vornherein gering, weitere Maßnahmen deshalb nicht zwingend erforderlich.
	Verwendung eigener APs auf Linux-Basis.
	WLAN wird an einem Proxyserver, Firewall betrieben, an dem man sich anmelden muss. Der WLAN benutzt ein eigenes Netzwerk. Die IP Adressen sind mit Firmennetz nicht geroutet.
Software-technische Maßnahmen	
	Starke Authentifizierung in Kombination mit VPN.
	VPN für alle Netzwerkverbindungen.
	WLAN wird softwaretechnisch bei Bedarf aktiviert, ist baulich so gelegen, dass ein unbefugter Zugriff eigentlich nur vom Hubschrauber aus möglich ist.

Tab. 4-3: Weitere von den Befragungsteilnehmern angegebene WLAN-Sicherheitsmaßnahmen

Hypothese 8: Über ein Drittel der im Fragebogen genannten Sicherheitsmaßnahmen sind den Befragungsteilnehmern nicht bekannt.

WLAN-Ratgeber bzw. Dokumentationen zur WLAN-Sicherheit konzentrieren sich oft nur auf ausgewählte Sicherheitsmaßnahmen [Bach04; BSI03a; Endr04; Kopp04; Lanc04b].

Insbesondere erfolgt dabei eine Fokussierung auf die technischen Sicherheitsspezifikationen der IEEE 802.11-Standardfamilie[68]. Viele organisatorische, aber auch technische Aspekte der WLAN-Sicherheit außerhalb der Standards werden nur sehr knapp oder gar nicht behandelt. Dies führt dazu, dass viele WLAN-Betreiber und IT-Sicherheitsverantwortliche bestimmte Maßnahmen nicht kennen und demzufolge auch nicht einsetzen [BüGö03, S. 6]. Wir gingen davon aus, dass den Befragungsteilnehmern über ein Drittel der Sicherheitsmaßnahmen unseres Maßnahmenkataloges nicht bekannt sind.

Unsere Auswertungen ergaben, dass die Befragungsteilnehmer im Durchschnitt nur 56,3% der im Fragebogen genannten Sicherheitsmaßnahmen kennen, 43,7% der Maßnahmen sind ihnen unbekannt. Damit ist Hypothese 8 bestätigt. Die Unkenntnis von Sicherheitsmaßnahmen interpretieren wir als einen Hauptgrund für den Nichteinsatz von Sicherheitsmaßnahmen.

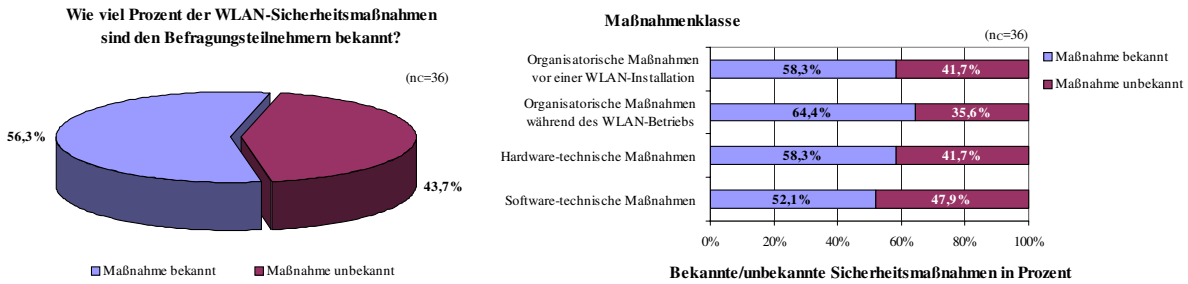

Abb. 4-15: Anteil der den Befragungsteilnehmern unbekannten WLAN-Sicherheitsmaßnahmen

Im Vergleich der vier Klassen von Sicherheitsmaßnahmen (Abb. 4-15, rechts) liegen die jeweiligen Bekanntheitsgrade der Maßnahmen nicht sehr weit auseinander. Bei software-technischen Sicherheitsmaßnahmen (52,1%) haben die Befragungsteilnehmer die größten Wissensdefizite. Bei der Analyse der Bekanntheitsgrade einzelner software-technischen Sicherheitsmaßnahmen konnten wir jedoch wesentlich größere Unterschiede ermitteln. Abb. 4-16 zeigt, dass die Maßnahme „Änderung der werkseitigen Grundeinstellungen“ mit einem Bekanntheitsgrad von 83,3% fast allen Befragungsteilnehmern bekannt ist. Dagegen gibt es aber auch weniger bekannte software-technische Maßnahmen. Hierzu zählen z. B. die „Maximierung des Beacon Intervalls“ und die „Verwendung von Block-Intra-BSS-Traffic in öffentlichen Bereichen“, welche jeweils nur 22,2% der Befragungsteilnehmer kennen.

68 Vgl. zur Sicherheitsspezifikation der IEEE 802.11-Standardfamilie Abschnitt 2.3

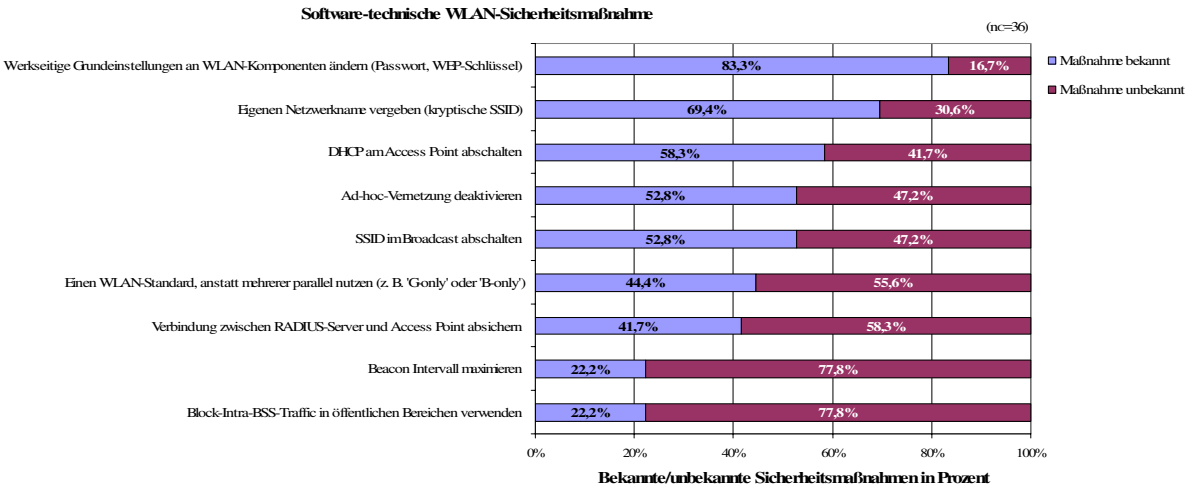

Abb. 4-16: Bekanntheitsgrade ausgewählter software-technischer WLAN-Sicherheitsmaßnahmen

Hypothese 9: Obwohl die Befragungsteilnehmer viele Sicherheitsmaßnahmen kennen, setzen sie über 20 Prozent der ihnen bekannten Maßnahmen nicht ein.

Viele Untersuchungen zur WLAN-Sicherheit ergaben, dass ein verhältnismäßig großer Anteil von WLANs nicht ausreichend oder überhaupt nicht geschützt ist [Bach04; BüGö03; RSA05; Saut04; Sili05]. Neben der Unkenntnis von WLAN-Sicherheitsmaßnahmen[69] vermuteten wir noch weitere Gründe für diese Sicherheitsdefizite. So gingen wir davon aus, dass trotz der Kenntnis von Sicherheitsmaßnahmen über 20 Prozent dieser bewusst nicht eingesetzt werden.

Abb. 4-17 zeigt, dass die Befragungsteilnehmer nur 77,7% der ihnen bekannten Sicherheitsmaßnahmen einsetzen. 22,3% der Sicherheitsmaßnahmen bleiben bewusst ungenutzt. Dies bestätigt Hypothese 9.

69 Vgl. zur Unkenntnis von WLAN-Sicherheitsmaßnahmen Abschnitt 4.3.4, Hypothese 8.

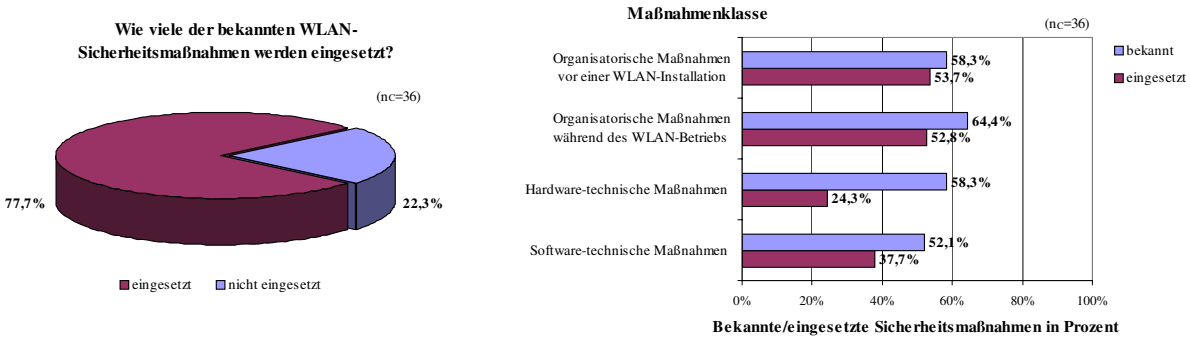

Abb. 4-17: Bekanntheitsgrade und Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen

Während bei den organisatorischen Maßnahmen vor und während des WLAN-Betriebs fast alle bekannten Sicherheitsmaßnahmen eingesetzt werden, existiert sowohl bei den hardware- als auch bei software-technischen Maßnahmen eine erhebliche Diskrepanz zwischen Bekanntheitsgrad und Einsatzhäufigkeit. Abb. 4-17 rechts zeigt, dass 52,1% der software-technischen Maßnahmen den Befragungsteilnehmern bekannt sind. Allerdings setzen sie nur 37,7% davon ein. Eine besonders große Diskrepanz tritt bei den hardware-technischen Maßnahmen auf. Dort kennen die Befragungsteilnehmer zwar 58,3% der Maßnahmen, setzen aber mit 24,3% nicht mal die Hälfte dieser ein.

Diese großen Diskrepanzen konnten wir auch bei der Analyse einzelner technischer Sicherheitsmaßnahmen bestätigen. Abb. 4-18 zeigt am Beispiel der Authentifizierungsverfahren, dass die bekannten Authentifizierungsverfahren nur sehr selten eingesetzt werden. So wird eine Authentifizierung über einen RADIUS-Server beispielsweise nur von 16,7% der Befragungsteilnehmer durchgeführt, obwohl 52,8% die Maßnahmen kennen.

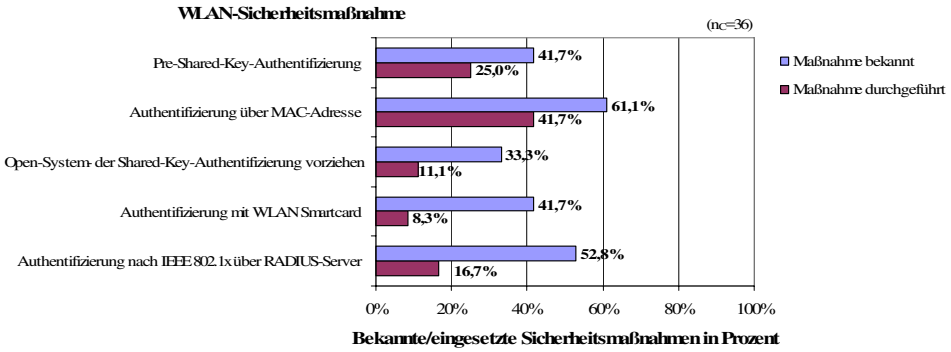

Abb. 4-18: Bekanntheitsgrade und Einsatzhäufigkeiten am Beispiel von Authentifizierungsverfahren

Hypothese 10: Wenn bekannte Sicherheitsmaßnahmen nicht eingesetzt werden, ist der am häufigsten genannte Grund dafür ein zu hoher Implementierungs- oder Betriebsaufwand.

Wie wir bereits in den Ausführungen zu Hypothese 9 feststellten, werden nicht alle WLAN-Sicherheitsmaßnahmen, die den Befragungsteilnehmern bekannt sind, eingesetzt. Es muss also neben der Unkenntnis von Sicherheitsmaßnahmen noch weitere Gründe für den Nichteinsatz geben. Aufgrund unserer eigenen Einschätzungen und den Ergebnissen von Expertendiskussionen nahmen wir an, dass neben der Unkenntnis von Maßnahmen ein zu hoher Implementierungs- bzw. Betriebsaufwand der Hauptgrund für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen ist.

Abb. 4-19 zeigt, dass nur bei 9,6% der Begründungen für den Nichteinsatz ein zu hoher Implementierungs- oder Betriebsaufwand angegeben wurde. Mit 22,7% der Antworten wurde von den Befragungsteilnehmern am häufigsten angegeben, dass sie auf die jeweilige Sicherheitsmaßnahme verzichten, weil diese in ihren WLAN-Infrastrukturen nicht praktikabel einsetzbar und damit für sie nicht relevant ist. In weiteren 7,6% der Begründungen gaben die Befragungsteilnehmer an, dass sie der Sicherheitsmaßnahme keine Erhöhung der Sicherheit zutrauen. Damit konnten wir Hypothese 10, die als häufigsten Grund einen zu hohen Implementierungs- oder Betriebsaufwand unterstellt, nicht pauschal für alle Sicherheitsmaßnahmen bestätigen.

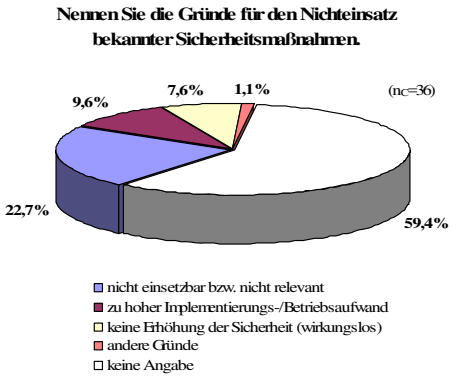

Abb. 4-19: Gründe für die Nichteinsatz von WLAN-Sicherheitsmaßnahmen

In einem weiteren Schritt analysierten wir die Begründungen für einzelne Sicherheitsmaßnahmen. Hierbei ermittelten wir, dass es durchaus Sicherheitsmaßnahmen gibt, für welche die Hypothese 10 zutrifft. Abb. 4-20 zeigt, dass insbesondere regelmäßig durchzuführende organisatorische Sicherheitsmaßnahmen aufgrund des hohen Implementierungs- bzw. Betriebsaufwandes von den Befragungsteilnehmern nicht eingesetzt werden. Dazu zählen bei-

spielsweise die Sicherheitsmaßnahmen „Physische Überprüfung der installierten Access Points auf Zugänglichkeit und Beschädigungen, um Netzausfälle und missbräuchliche Verwendungen zu verhindern“ (33,3%), „Regelmäßige Kontrolle und Wartung der Einstellungen der WLAN-Endgeräte, wie Firewall- und Betriebssystem-Konfiguration an den Endgeräten“ (29,4%) und „Regelmäßige Kontrolle und Überwachung des WLAN durch Netzwerkscans und Auswertung von Logdateien“ (27,8%). Aber auch aus anderen Maßnahmenklassen konnten wir derartige Maßnahmen ermitteln, z. B. „WLAN-Tapete zur Abschirmung nutzen“ (25,0%) oder „Verwendung eines Intrusion Detection Systems zur Überwachung des WLANs“ (22,7%).

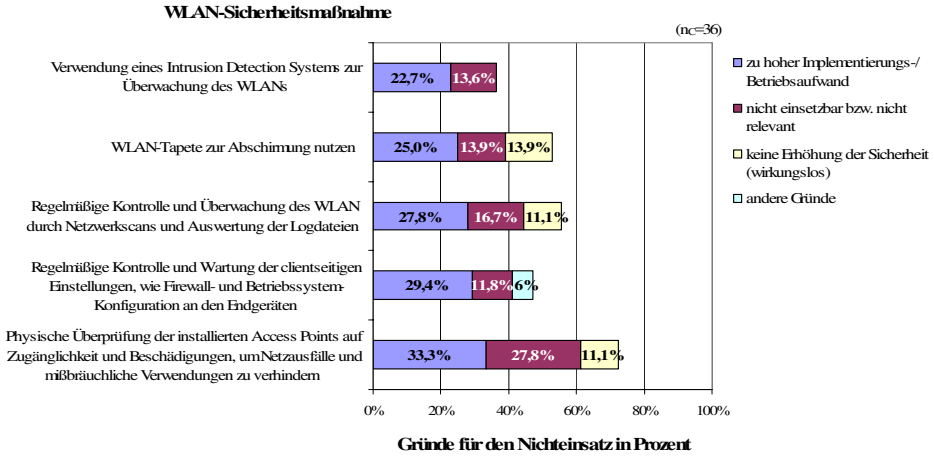

Abb. 4-20: Hoher Implementierungs- / Betriebsaufwand als häufigster Grund für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen

Zusätzlich zu den im Fragebogen vorgegebenen Begründungen für den Nichteinsatz konnten die Befragungsteilnehmer weitere Gründe angeben. Tab. 4-4 enthält diese Gründe. Aufgrund der geringen Nennungen konnten wir daraus allerdings keinen weiteren Hauptgrund für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen ableiten.

ID	Klasse		Maßnahme/Beschreibung	Weitere Gründe für den Nichteinsatz
…	**Organisatorische Maßnahmen während des Betriebs**			
21			Regelmäßige Kontrolle und Wartung der Einstellungen der WLAN-Endgeräte, wie Firewall- und Betriebssystem-Konfiguration an den Endgeräten	Eigenverantwortung der Anwender
...	**Software-technische Maßnahmen**			
...		Konfiguration und Administration der Endgeräte		
26			Werkseitige Grundeinstellungen an WLAN-Geräten ändern	Spielt keine Rolle
27			Ad-hoc-Vernetzung deaktivieren	Bei Bedarf

31			DHCP am Access Point abschalten	Nur für Ausnahmen
32			Verbindung zwischen RADIUS-Server und Access Point absichern	Für Teilbereiche
...		Authentifizierungsverfahren anwenden		
38			Authentifizierung mit WLAN Smartcard	In Planung
...		Verschlüsselungstechniken benutzen		
43			Netzwerktechnische Trennung zwischen WLAN und drahtgebundenem Netz (z. B. über Paketfilter, VPN oder VLAN)	Trennung ist nicht gewünscht
44			Installation einer Personal Firewall auf den mobilen Endgeräten	Liegt in der Verantwortung der Anwender
46			Datei- und Ressourcenfreigabe auf allen Endgeräten sowie Geräten, die vom WLAN aus erreichbar sind, restriktiv einschränken	Liegt in der Verantwortung der Anwender

Tab. 4-4: Weitere von den Befragungsteilnehmern angegebenen Gründe für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen

4.3.5 Zusammenhänge zwischen unternehmensspezifischen Merkmalen und WLAN-Sicherheitsmaßnahmen

Die folgenden Auswertungen basieren auf den Antworten der 36 Befragungsteilnehmer, welche die Fragen zu den WLAN-Sicherheitsmaßnahmen vollständig beantwortet haben (n_C=36).[70]

Hypothese 11: Unternehmen aus der IuK-Branche setzen im Vergleich zu Unternehmen aus anderen Branchen und Behörden mehr Sicherheitsmaßnahmen ein.

Wir gehen davon aus, dass Mitarbeiter von Unternehmen aus dem Bereich Information und Kommunikation (IuK) über ein umfangreicheres IT-Know-How im Vergleich zu anderen Branchen und Behörden verfügen. Aus diesem Grund vermuteten wir, dass bei Unternehmen der IuK-Branche mehr Sicherheitsmaßnahmen eingesetzt werden als in Unternehmen anderer Branchen und Behörden.

Abb. 4-21 zeigt, dass Unternehmen aus dem IuK-Bereich 55,1% der im Fragebogen enthaltenen WLAN-Sicherheitsmaßnahmen einsetzten. Dies ist im Vergleich zu den Unternehmen anderer Branchen und den Behörden ein deutlich höherer Wert. Damit ist Hypothese 11 bestätigt. Die mit 24,7% geringste Einsatzhäufigkeit von WLAN-Sicherheits-

[70] Zur Beschreibung der Gruppe der Befragungsteilnehmer, die alle Fragen zu den WLAN-Sicherheitsmaßnahmen ausgefüllt haben, vgl. Abschnitt 4.3.4.

maßnahmen stellten wir bei den Behörden fest. Dies kann als Indiz für ein mangelndes IT-Sicherheitsbewusstsein für den WLAN-Bereich interpretiert werden.

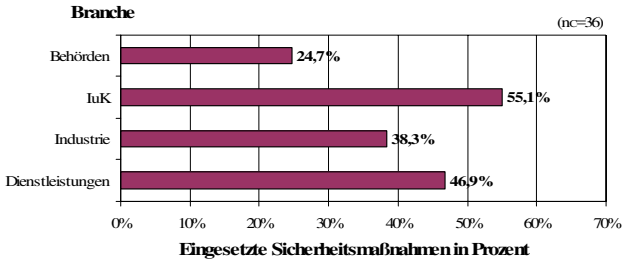

Abb. 4-21: Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Branche[71]

In einem weiteren Schritt untersuchten wir die Einsatzhäufigkeiten einzelner WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Branche.

Beispiel Authentifizierungsverfahren

Abb. 4-22 zeigt, dass 87,5% der Unternehmen aus der IuK-Branche Authentifizierungsverfahren nutzen. Im Vergleich zu Unternehmen anderer Branchen ist somit die Einsatzhäufigkeit wesentlich höher.

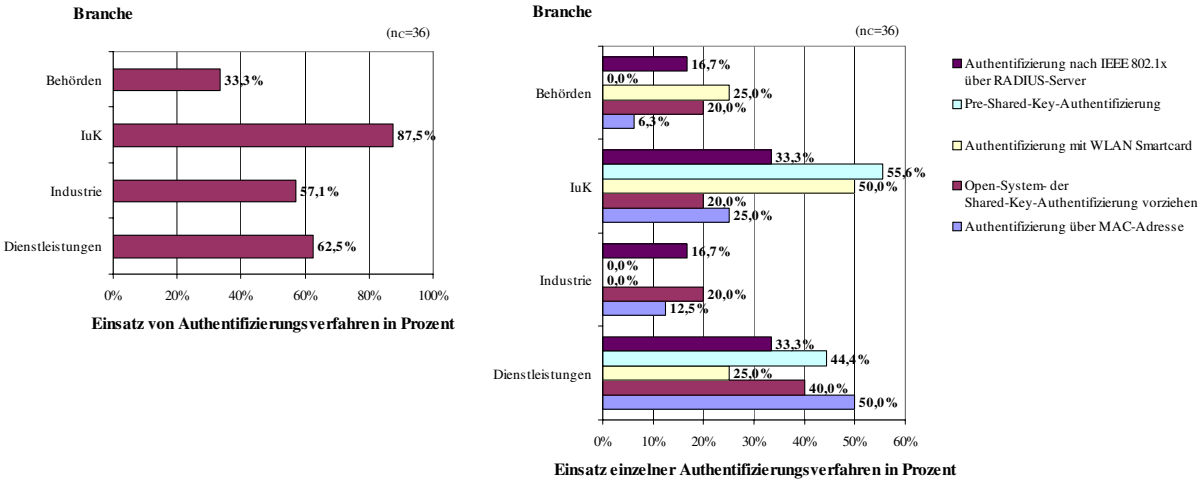

Abb. 4-22: Einsatzhäufigkeiten von Authentifizierungsverfahren in Abhängigkeit von der Branche[71]

Mit nur 33,3% nehmen auch hier die Behörden wiederum die letzte Position ein. Auch die Auswertung der einzelnen Authentifizierungsverfahren (Abb. 4-22, rechts) bestätigt den

71 Aufgrund der geringen Anzahl von Befragungsteilnehmern aus der Branche Tourismus werden diese hier nicht berücksichtigt. Unternehmen der Branchen Handel und Verkehr sind nicht vertreten. Vgl. Abschnitt 4.3.4

wesentlich intensiveren Einsatz dieser Maßnahmen bei IuK-Unternehmen (Mehrfachnennungen waren möglich).

Beispiel Verschlüsselungsverfahren

In Abb. 4-23 ist erkennbar, dass die Einsatzhäufigkeit von Verschlüsselungsverfahren bei den Unternehmen der IuK-Branche mit 75,0% sehr hoch ist. Jedoch erreichen hier die Unternehmen aus dem Dienstleistungsbereich mit 81,3% den Spitzenwert. Die geringste Einsatzhäufigkeit ermittelten wir wiederum bei den Behörden. Die Analyse der einzelnen Verschlüsselungsverfahren in Abb. 4-23 rechts zeigt, dass IuK-Unternehmen tendenziell stärkere Verschlüsselungsverfahren (WPA/WPA2) einsetzten. So gibt es in dieser Branche nur noch wenige Unternehmen, welche die sehr einfach anzugreifende WEP-Verschlüsselung verwenden. Die Ursache hierfür ist möglicherweise die höhere Affinität von Unternehmen der IuK-Branche zu IT-Sicherheitsthemen.

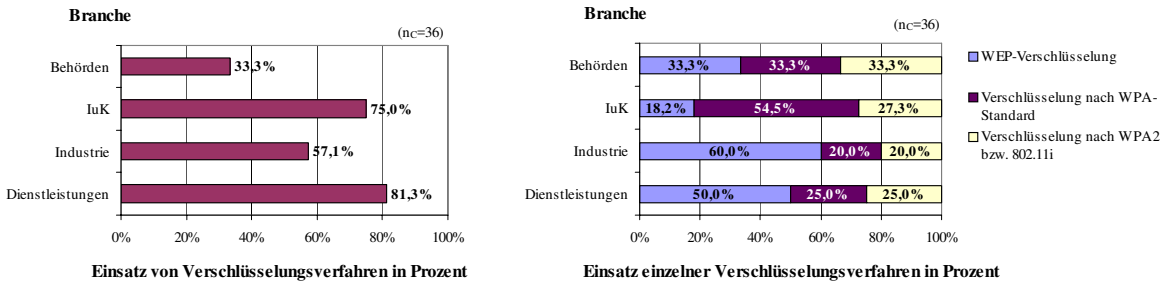

Abb. 4-23: Einsatzhäufigkeiten von Verschlüsselungsverfahren in Abhängigkeit von der Branche[72]

Hypothese 12: In Unternehmen und Behörden, die ein IT-Security-Management besitzen, ist der Einsatz von Sicherheitsmaßnahmen wesentlich höher als in Unternehmen und Behörden ohne IT-Security-Management.

Die Einrichtung eines IT-Security-Managements in einem Unternehmen oder einer Behörde dient der koordinierten Planung, Realisierung und Kontrolle der Sicherheit aller IT-Systeme. Es wird das Ziel verfolgt, die Sicherheit der IT-Systeme stets zu gewährleisten sowie zu verbessern. Dazu werden z. B. aus organisatorischer Perspektive bestimmte Rollen und Verantwortlichkeiten definiert, die ein den Anforderungen entsprechendes Sicherheitsniveau ermöglichen sollen. Voraussetzung dafür ist der kontinuierliche Aufbau von

72 Aufgrund der geringen Anzahl von Befragungsteilnehmern aus der Branche Tourismus werden diese hier nicht berücksichtigt. Unternehmen der Branchen Handel und Verkehr sind nicht vertreten. Vgl. Abschnitt 4.3.4

IT-Sicherheits-Know-how. Nicht jede Institution hat ein IT-Security-Management bzw. einen IT-Sicherheitsverantwortlichen. Bei 25 der 36 Befragungsteilnehmer (70%), welche die Fragen zu den WLAN-Sicherheitsmaßnahmen vollständig beantwortet haben, gibt es ein IT-Security-Management. Wir gingen davon aus, dass bei diesen Unternehmen und Behörden mehr Sicherheitsmaßnahmen eingesetzt werden als bei Unternehmen und Behörden ohne IT-Security-Management.

Abb. 4-24 zeigt, dass bei Institutionen mit IT-Security-Management durchschnittlich 50,6% der im Fragebogen aufgeführten Sicherheitsmaßnahmen eingesetzt werden. Dagegen sind es bei Unternehmen und Behörden ohne IT-Security-Management lediglich 25,0% der Maßnahmen. Dieses Ergebnis bestätigt Hypothese 12.

Die Untersuchung der einzelnen Maßnahmenklassen ergab einen besonders starken Zusammenhang zwischen dem Vorhandensein des IT-Security-Managements und dem Einsatz organisatorischer Sicherheitsmaßnahmen. Die Unterschiede bei den technischen WLAN-Sicherheitsmaßnahmen sind im Vergleich dazu eher gering bis moderat.

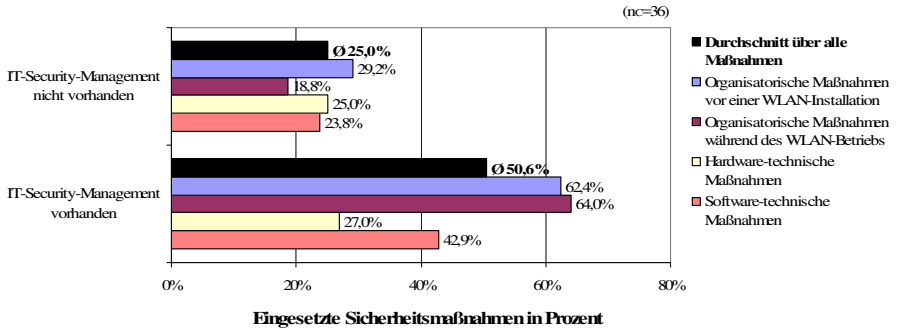

Abb. 4-24: Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Existenz eines IT-Security-Managements

Beispiel organisatorische Maßnahmen bei der Planung eines WLAN-Rollouts

Da der ermittelte Zusammenhang zwischen der Existenz des IT-Security-Managements und der Einsatzhäufigkeit bei den organisatorischen WLAN-Sicherheitsmaßnahmen[73] am stärksten zu beobachten war, untersuchten wir ausgewählte Maßnahmen dieser Kategorie näher. Abb. 4-25 zeigt, dass der Zusammenhang nicht pauschal auf alle organisatorischen Maßnahmen zutrifft. So sind bei den Sicherheitsmaßnahmen „Umgebungsfaktoren beachten“, „Messplanung durchführen“ und „Antennentyp und Aufstellort der Access Points so

[73] Vgl. zur Beschreibung der Sicherheitsmaßnahmen Tab. 3-1 bzw. die Abschnitte 3.3.1 und 3.3.2.

wählen, dass eine maximale Ausleuchtung gewährleistet ist“ keine gravierenden Unterschiede bei Befragungsteilnehmern mit und ohne IT-Security-Management erkennbar. Maßnahmen, wie „Einsatzorte/Einsatzbereich exakt festlegen und abgrenzen“, „Überlappungsfreie Kanalbelegung“ oder „Kontrolle und Überprüfung des WLAN durch abschließenden Netzwerkscan und Auswertung der Logdatei“ dagegen, werden häufiger oder sogar ausschließlich nur dann eingesetzt, wenn ein IT-Security-Management vorhanden ist.

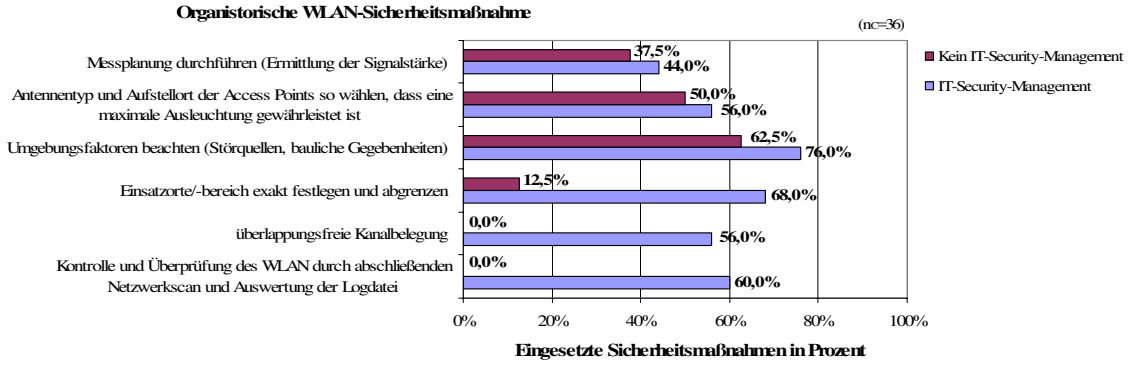

Abb. 4-25: Einsatzhäufigkeiten von organisatorischen Sicherheitsmaßnahmen in Abhängigkeit von der Existenz eines IT-Security-Managements

Hypothese 13: Größere Unternehmen und Behörden setzen im Vergleich zu kleineren Unternehmen und Behörden mehr Sicherheitsmaßnahmen in ihren WLAN-Infrastrukturen ein.

Größere Unternehmen und Behörden verfügen in der Regel über eine oder mehrere eigene IT-Abteilung(en) oder zumindest über eine größere Anzahl hochqualifizierter IT-Experten. Als Folge dessen werden ihnen im Vergleich zu kleineren Unternehmen umfangreichere IT-Kenntnisse zugeschrieben. Aus diesem Grund erwarteten wir, dass kleineren Unternehmen und Behörden eher weniger WLAN-Sicherheitsmaßnahmen bekannt sind und sie deshalb auch weniger Maßnahmen einsetzen.

Abb. 4-26 zeigt jedoch klar, dass wir diesen Zusammenhang nicht bestätigen konnten. Bei den Bekanntheitsgraden erzielen die größeren Unternehmen und Behörden mit 58,4% und 63,0% zwar die besseren Ergebnisse, jedoch sind die Unterschiede zu den kleineren relativ gering. In Bezug auf die Einsatzhäufigkeit sind die Unterschiede noch geringer. Im Gegenteil setzen hier die kleineren Unternehmen und Behörden mit 44,2% und 48,8% der Sicherheitsmaßnahmen sogar etwas mehr Maßnahmen als die größeren ein. Somit kann der erwartete Zusammenhang zwischen der Größe eines Unternehmens bzw. einer Behörde

und dem Einsatz von WLAN-Sicherheitsmaßnahmen nicht pauschal für alle Maßnahmen bestätigt werden.

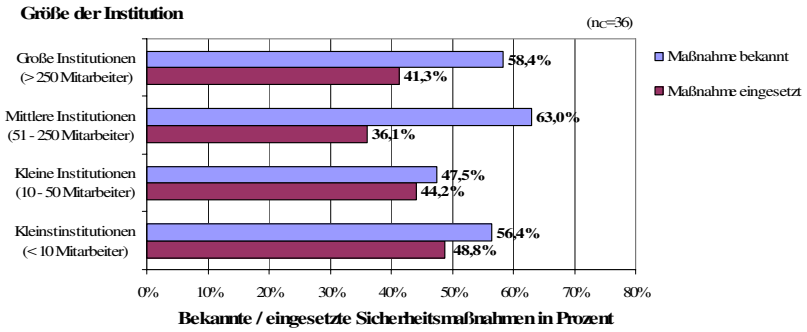

Abb. 4-26: Bekanntheitsgrade und Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in Abhängigkeit von der Größe der Institutionen

Bei der Analyse der Einsatzhäufigkeiten einzelner WLAN-Sicherheitsmaßnahmen konnten wir jedoch signifikante Abhängigkeiten von der Größe der Institution ermitteln und für einzelne Sicherheitsmaßnahmen die Hypothese 13 bestätigen. Abb. 4-27 zeigt vier Beispiele für derartige WLAN-Sicherheitsmaßnahmen. Es wird deutlich, dass es einerseits Sicherheitsmaßnahmen gibt, die verstärkt in großen Institutionen eingesetzt werden, wie beispielsweise die „Überlappungsfreie Kanalbelegung“. Andererseits existieren aber auch Sicherheitsmaßnahmen, die vorrangig in kleineren Unternehmen eingesetzt werden, wie z. B. „Zugangspasswörter bei WLAN und LAN unabhängig voneinander festlegen“, „Eigenen Netzwerknamen vergeben“ und „Werkseitige Grundeinstellungen an WLAN-Geräten ändern“.

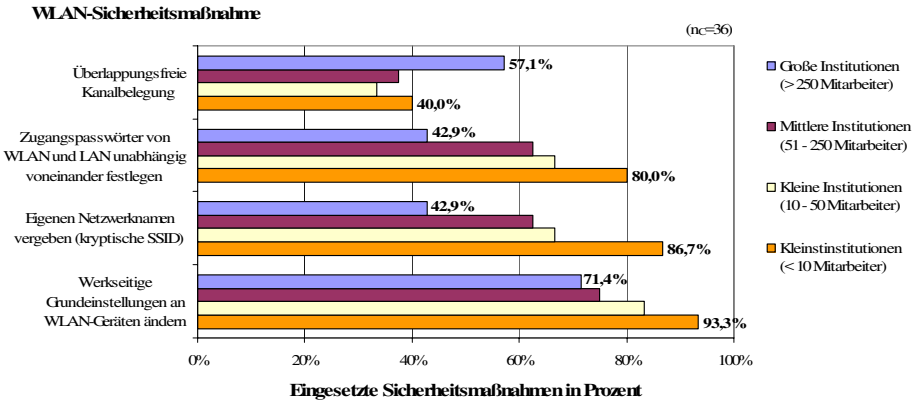

Abb. 4-27: WLAN-Sicherheitsmaßnahmen, deren Einsatz stark mit der Größe der Unternehmen und Behörden variiert

Hypothese 14: Unternehmen und Behörden, die eine WLAN-Infrastruktur bereits seit mehr als einem Jahr betreiben und damit über längere Erfahrungen verfügen, setzen mehr Sicherheitsmaßnahmen ein als Unternehmen und Behörden, die ihre WLAN-Infrastruktur erst seit einem Jahr betreiben.

Bei einem Einsatz von WLAN-Infrastrukturen über mehrere Jahre hinweg können Betreiber und Anwender wertvolle Erfahrungen im Umgang mit der WLAN-Technik und den Sicherheitsmaßnahmen sammeln. Dies führt in der Regel zu Lerneffekten. Deshalb gingen wir davon aus, dass in WLAN-Infrastrukturen, die seit mehr als einem Jahr betrieben werden, mehr Sicherheitsmaßnahmen als in neueren WLAN-Infrastrukturen zum Einsatz kommen.

Von den 36 Befragungsteilnehmern gaben 36,1% an, ihre WLAN-Infrastruktur erst seit einem Jahr oder kürzer zu nutzen. Demgegenüber setzen 61,1% ihre WLAN-Infrastruktur bereits seit mehr als einem Jahr ein.

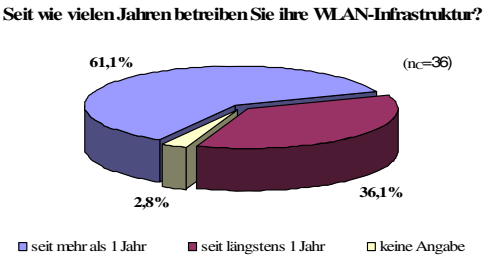

Abb. 4-28: Dauer der Nutzung von WLAN-Infrastrukturen

Abb. 4-29 zeigt, dass die Befragungsteilnehmer mit über einem Jahr Erfahrung nur 38,1% der im Fragebogen genannten Sicherheitsmaßnahmen einsetzen. Mit 51,9% der Sicherheitsmaßnahmen setzen Befragungsteilnehmer, die erst seit einem Jahr oder kürzer ihre WLAN-Infrastruktur nutzen, dagegen wesentlich mehr Maßnahmen ein. Damit konnten wir keinen Zusammenhang zwischen einer langen Nutzungsdauer und dem Einsatz von Sicherheitsmaßnahmen bestimmen. Hypothese 14 ist damit widerlegt.

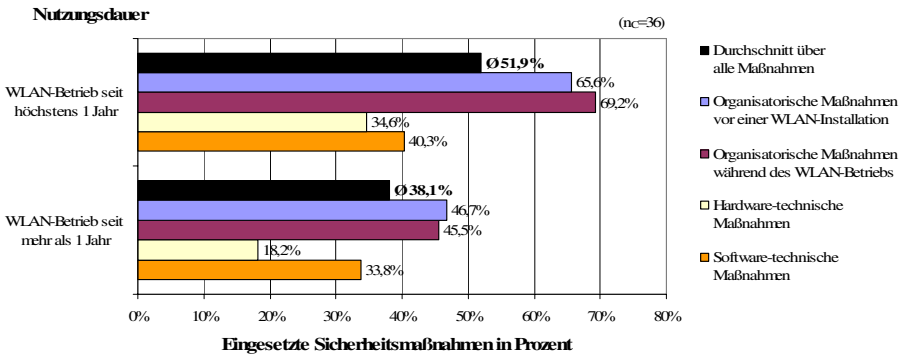

Abb. 4-29: Einsatz von Sicherheitsmaßnahmen in Abhängigkeit von der Dauer des WLAN-Betriebs

Im Gegensatz zur unserer Annahme zeigen die Ergebnisse, dass Unternehmen und Behörden mit mehr WLAN-Erfahrung wesentlich weniger Sicherheitsmaßnahmen einsetzen. In Abb. 4-29 ist erkennbar, dass das durchweg für alle Maßnahmenkategorien zutrifft. Eine Erklärung dafür könnten generell geringere Sicherheitsanforderungen in den vergangenen Jahren sein. Das heißt, Sicherheitsmaßnahmen, die noch vor zwei oder drei Jahren eingerichtet wurden, werden heute möglicherweise noch in unveränderter Form beibehalten, ohne dass deren Einsatz an die gestiegenen Sicherheitsanforderungen angepasst wird. Eine andere Erklärung könnte sein, dass erfahrene Betreiber nicht einfach alle ihnen bekannten Sicherheitsmaßnahmen einsetzen, sondern ganz gezielt bei der Auswahl vorgehen.

Unsere Analyse einzelner Sicherheitsmaßnahmen ergab, dass es aber durchaus Maßnahmen gibt, die häufiger bei WLAN-Infrastrukturen eingesetzt werden, die länger als ein Jahr existieren (siehe Abb. 4-30). Hierzu zählen beispielsweise die „Netzwerktechnische Trennung zwischen WLAN und drahtgebundenem Netz“, die „Installation einer Personal Firewall auf den mobilen Endgeräten“, die „Verwendung eines Intrusion Detection Systems zur Überwachung des WLANs“ sowie die „Datei- und Ressourcenfreigabe auf allen Endgeräten sowie Geräten, die vom WLAN aus erreichbar sind, restriktiv einschränken“. Gründe dafür können Trendentwicklungen sowie auch die unterschiedlichen zeitlichen Verfügbarkeiten einzelner - insbesondere technischer - Maßnahmen sein. So hat sich z. B. das Leistungs- und Produktspektrum von Personal Firewall Software und Intrusion Detection Systemen in jüngster Vergangenheit stark entwickelt.

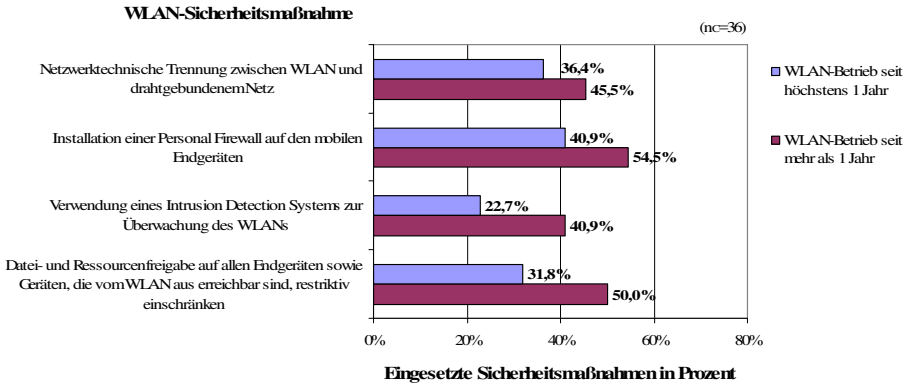

Abb. 4-30: WLAN-Sicherheitsmaßnahmen, die häufiger in WLAN-Infrastrukturen mit längerer Nutzungsdauer eingesetzt werden

Hypothese 15: Setzen Befragungsteilnehmer WLAN-Infrastrukturen in sicherheitskritischen Bereichen, wie Geschäftsführung, Entwicklung, Personal- oder Finanzbereich ein, sind mehr Sicherheitsmaßnahmen realisiert als bei Unternehmen und Behörden, die WLAN-Infrastrukturen nicht in diesen Bereichen einsetzen.

Innerhalb eines Unternehmens oder einer Behörde gibt es Bereiche mit unterschiedlichen Sicherheitsanforderungen. Zu sicherheitskritischen Bereichen zählen wir die Geschäftsführung, die Forschung und Entwicklung sowie den Personal- und Finanzbereich. Dort werden im Vergleich zu anderen Bereichen, wie Beschaffung, Marketing/Vertrieb, Produktion, Kundenservice oder IT, in der Regel wesentlich sensiblere Daten verarbeitet und übertragen. Wir gingen davon aus, dass beim Betrieb von WLAN-Infrastrukturen in sicherheitskritischen Bereichen meist mehr Sicherheitsmaßnahmen zum Einsatz kommen als in WLAN-Infrastrukturen in weniger sicherheitskritischen Bereichen.

20 der 36 analysierten Unternehmen und Behörden (55,6%) setzen ihre WLAN-Infrastrukturen in sicherheitskritischen Bereichen ein. Abb. 4-31 zeigt, dass wir jedoch zwischen dieser Gruppe und der Befragungsteilnehmern, die ihre WLAN-Infrastrukturen nur in weniger sicherheitskritischen Bereichen betreiben, kaum nennenswerte Unterschiede hinsichtlich der Anzahl der eingesetzten WLAN-Sicherheitsmaßnahmen ermitteln konnten. Einzig bei den Hardware-technischen Sicherheitsmaßnahmen liegt eine größere Differenz vor. Allerdings gaben hier die Befragungsteilnehmer an, dass sie in den weniger sicherheitskritischen Bereichen mehr Hardware-technische Sicherheitsmaßnahmen einsetzen. Dies entspricht nicht unserer Annahme und widerlegt damit Hypothese 15.

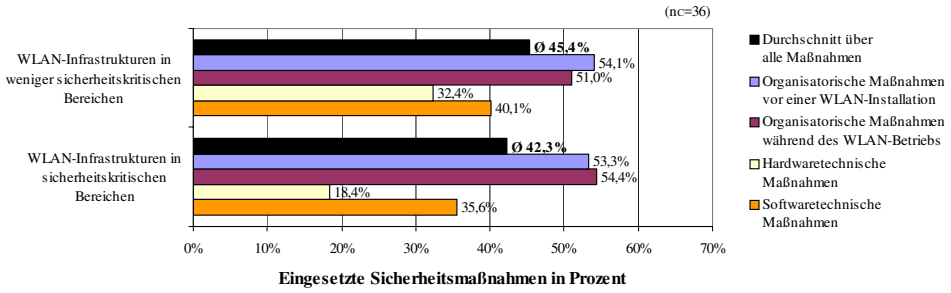

Abb. 4-31: Einsatz von Sicherheitsmaßnahmen in Abhängigkeit von Unternehmensbereichen

5 Zusammenfassung und Ausblick

Die Studie beschreibt Durchführung und Ergebnisse einer empirischen Untersuchung zur Verbreitung und Sicherheit von WLAN-Infrastrukturen in deutschen Unternehmen und Behörden. Es wurden Erkenntnisse über die Verbreitung der WLAN-Technologie, den Einsatz von WLAN-spezifischen Sicherheitsmaßnahmen, die Gründe des Nichteinsatzes von Sicherheitsmaßnahmen sowie Zusammenhänge zwischen unternehmensspezifischen Merkmalen und den Einsatz von Sicherheitsmaßnahmen zusammengefasst. Ausgangspunkt der empirischen Untersuchung ist ein von uns entwickelter Katalog WLAN-spezifischer Sicherheitsmaßnahmen. Dieser stellt den wesentlichen Bestandteil des für die Online-Befragung erstellten Fragebogens dar. Die Internet-basierte Befragung wurde von November 2005 bis Januar 2006 durchgeführt. Von 1.164 eingeladenen Unternehmen und Behörden nahmen 290 an der Untersuchung teil. Das entspricht einer Rücklaufquote von 24,9%. 75 der Befragungsteilnehmer nutzen WLAN-Infrastrukturen. Dies ergibt eine WLAN-Verbreitung von 25,9%. Von der Gruppe der WLAN-nutzenden Befragungsteilnehmer beantworteten 36 den Fragebogenteil zum Einsatz von WLAN-Sicherheitsmaßnahmen vollständig. Unsere Auswertungen ergaben folgende zentrale Ergebnisse:

- Bei den Befragungsteilnehmern ist seit 2002 eine kontinuierliche Zunahme der Verbreitung von WLAN-Infrastrukturen zu beobachten. Dieser Trend setzt sich auch 2006 fort. Im Jahr 2005 betrug die Wachstumsrate der WLAN-Nutzung unter den Befragungsteilnehmern 33,9%.
- Hauptsächlich große Unternehmen und Behörden setzen WLAN-Infrastrukturen ein. Jedoch planen insbesondere kleinere und mittlere Institutionen in naher Zukunft in zunehmendem Maße den Einsatz von WLAN-Infrastrukturen.

- Nachdem in den vergangenen Jahren der Standard IEEE 802.11b in WLAN-Infrastrukturen dominierte, setzt heute die Mehrheit (50,7%) der Befragungsteilnehmer mit WLAN-Infrastrukturen den neueren Standard IEEE 802.11g ein.
- Die Befragungsteilnehmer setzen zum Schutz ihrer WLAN-Infrastrukturen mehr organisatorische (53,4%) als technische Sicherheitsmaßnahmen (35,6%) ein.
- 43,7% der im Fragebogen genannten WLAN-Sicherheitsmaßnahmen sind den Befragungsteilnehmern nicht bekannt.
- Im Durchschnitt setzen die Befragungsteilnehmer nur 77,7% der ihnen bekannten Sicherheitsmaßnahmen ein, 22% bleiben ungenutzt. Insbesondere bei den Authentifizierungsverfahren liegen die Einsatzhäufigkeiten weit unter den Bekanntheitsgraden.
- Als Gründe für den Nichteinsatz von WLAN-Sicherheitsmaßnahmen nennen die Befragungsteilnehmer eine zu geringe Praktikabilität (22,7%), einen zu hohen Implementierungs-/ Betriebsaufwand (9,6%) sowie eine zu geringe Wirkung (7,6%) der Maßnahmen.
- Befragungsteilnehmer aus der IuK-Branche setzen mehr Sicherheitsmaßnahmen (55,1%) ein als Befragungsteilnehmer aus anderen Branchen (Dienstleistungen: 46,9%; Industrie: 38,3%) und Behörden (24,7%). Darüber hinaus ist bei Befragungsteilnehmern der IuK-Branche zu beobachten, dass sie im Vergleich zu Befragungsteilnehmern aus anderen Branchen und Behörden stärkere Verschlüsselungsverfahren (WPA/WPA2) nutzen.
- Bei Befragungsteilnehmern, die ein IT-Security-Management betreiben, ist der Einsatz von Sicherheitsmaßnahmen wesentlich höher (50,6%) als bei Befragungsteilnehmern ohne IT-Security-Management (25,0%). Insbesondere der Einsatz organisatorischer Maßnahmen ist von der Existenz eines IT-Security-Management stark abhängig.
- In punkto Bekanntheitsgrad und Einsatzhäufigkeit von Sicherheitsmaßnahmen stehen kleinere Unternehmen und Behörden den größeren in nichts nach.
- Befragungsteilnehmer, die längere Erfahrung mit WLAN-Infrastrukturen haben, setzen nicht mehr Sicherheitsmaßnahmen ein (38,1%) als Befragungsteilnehmer mit weniger Erfahrung (51,9%).

Angesichts der von uns gewählten Stichprobe (starker Fokus auf Thüringer Unternehmen, keine zufällige Auswahl der Befragungsteilnehmer) sowie der geringen Anzahl vollständig ausgefüllter Fragebögen hat die Untersuchung lediglich explorativen Charakter. Allgemeingültige Aussagen lassen sich nicht ableiten. Dennoch schätzen wir die von uns ermittelten Ergebnisse als erste konkrete Hinweise über die Verbreitung und die Sicherheit von WLAN-Infrastrukturen ein. Insbesondere konnten wir Bekanntheitsgrade, Einsatzhäufigkeiten und erste Zusammenhänge zwischen unternehmensspezifischen Merkmalen und einzelnen WLAN-Sicherheitsmaßnahmen ermitteln. Hierbei ist anzumerken, dass die Aussagen zur WLAN-Sicherheit lediglich auf der Anzahl der eingesetzten WLAN-Sicherheitsmaßnahmen beruhen. Es wird nicht berücksichtigt, wie stark die einzelnen Maßnahmen das WLAN-Sicherheitsniveau beeinflussen. Leider führt der Einsatz vieler Sicherheitsmaßnahmen nicht zwangsläufig zu einer hohen Sicherheit.

Wir planen, die Untersuchung mit einer größeren Stichprobe mit zufällig ausgewählten Unternehmen und Behörden zu wiederholen. Denkbar ist auch eine regelmäßige Wiederholung der Untersuchung. Dies würde es uns ermöglichen, Veränderungen und Trends bei der Sicherheit von WLAN-Infrastrukturen im Zeitablauf sowie beim Einsatz von einzelnen Sicherheitsmaßnahmen zu analysieren. Des Weiteren werden wir unseren Maßnahmenkatalog weiterentwickeln. Neben der stetigen Aktualisierung werden wir vor allem eine Bewertung der Qualität bzw. Wirkung der einzelnen Sicherheitsmaßnahmen vornehmen. Dies würde es uns erlauben, noch konkretere Aussagen zur Sicherheit in WLAN-Infrastrukturen zu treffen.

Literaturverzeichnis

[Arte04] Artem (Hrsg.): Handbuch – ComPoint Enterprise. http://www.funkwerk-ec.com/portal/downloadcenter/dateien/artem_compoint_enterprise/documentation/ar_ug_CPE_BR_d.pdf, Ulm 2004, Abruf: 2006-05-31.

[Bach04] Bachfeld, D.: Per Anhalter durchs Internet. In:c't Heft, Nr. 13 (2004), S. 92-97.

[BGWa01] Borisov, N.; Goldberg, I.; Wagner, D: Intercepting Mobile Communications: The Insecurity of 802.11. In: Proceedings of the 7th annual international conference on Mobile computing and networking. Rom (2001), p. 180-189, http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, Abruf: 2006-05-30.

[Blum03] Blumenthal, B.: Wireless LAN (IEEE 802.11) – Security Glossar. http://www.wireless-forum.ch/forum/download.php?id=190, 2003, Abruf: 2006-05-31.

[BoDö03] Bortz, J.; Döring, N.: Forschungsmethoden und Evaluation: für Human- und Sozialwissenschaftler. 3. Auflage, Springer Verlag, Berlin u. a., 2003.

[BSI03a] Bundesamt für Sicherheit in der Informationstechnik, Projektgruppe „Local Wireless Communication" (Hrsg.): Sicherheit im Funk-LAN (WLAN, IEEE 802.11). http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf, Bonn 2003, Abruf: 2006-05-30.

[BSI03b] Bundesamt für Sicherheit in der Informationstechnik, Projektgruppe „Local Wireless Communication" (Hrsg): Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte. http://www.bsi.bund.de/literat/doc/drahtloskom/drahtloskom.pdf, 2003, Abruf: 2006-05-31.

[BSI03c] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. http://www.bsi.de/literat/studien/trend2010/netze_kommunikation.pdf, 2003, Abruf: 2006-05-31.

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch: Handbuch für die sichere Anwendung der Informationstechnik. 6. Auflage, Bundesanzeiger, Köln, 2004.

[BSI05a] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Technische Richtlinie Sicheres WLAN (TR-S-WLAN) – Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen. Bonn, 2005.

[BSI05b] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Technische Richtlinie Sicheres WLAN (TR-S-WLAN) – Teil 3a: Auswahlkriterien für WLAN-Syteme. Bonn, 2005.

[BüGö03] Büttner, H.-G.; Gödde, D.: Wireless LAN – Studie zur Sicherheit von drahtlosen Netzwerken in deutschen Firmen. Ernst & Young IT-Security, http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/$file/WLAN.pdf, 2003, Abruf: 2006-05-30.

[Comc03] ComConsult (Hrsg.): Wireless LAN's: auf dem Weg zur strategischen Infrastruktur. http://www.comconsult-research.de/insider/bilder/WLANForum03Fazit1.pdf, 2003, Abruf: 2006-05-30.

[Davi04] Davies, J.: Drahtlose Netzwerke mit Microsoft Windows – Theorie und Praxis sicherer 802.11-Wireless-LANs mit Microsoft-Technologien. Microsoft Press, Unterschleißheim, 2004.

[DBCr01] Dunsmore, B.; Brown, J.; Cross, M.: Mission Critical! Internet Security. Syngress Publishing Inc., Rockland, 2001.

[Delb03] Delbrouck, D.: Rund 60 Prozent der Münchener WLANs sind unsicher. ZDNet-News, http://www.zdnet.de/news/tkomm/0,39023151,2133238,00.htm, 04/2003, Abruf: 2006-05-30.

[Dete03] Detecon International GmbH (Hrsg.): Trendletter Public WLAN – Hot Spot Report, Der Praxistest. http://www.detecon.com/load.php?url=L21lZGlhL3BkZi9maW5hbEhvdHNwb3RjaGVja18xMDAyMDQucGRm, 11/2003, Abruf: 2006-05-30.

[Dete04] Detecon International GmbH (Hrsg.): Key Notes. Security in mobilen Netzen. http://www.detecon.com/load.php?url=L21lZGlhL3BkZi9LZXlfTm90ZXNfV2VydGhlbmJhY2gucGRm, 03/2004, Abruf: 2005-06-09.

[DIN32705] Deutsches Institut für Normung (Hrsg.): Klassifikationssysteme: Erstellung und Weiterentwicklung von Klassifikationssystemen. DIN 32705, 1987.

[Ecol04] Ministerium für Umwelt und Naturschutz, Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen, ECOLOG-Institut für sozialökologische Forschung und Bildung (Hrsg.): Aktionsprogramm Umwelt und Gesundheit Nordrhein-Westfalen - Sachstandsermittlung zur Netzwerktechnologie WLAN. http://www.munlv.nrw.de/sites/arbeitsbereiche/immission/pdf/literatur.pdf, 10/2004, Abruf: 2006-05-25.

[Endr04] Endres, J.: Kein Durchgang! – WLAN-Router gegen Schwarz-Surfer schützen. In: c't Heft Nr. 13 (2004), S. 98-101.

[EU03] Europäische Union (Hrsg.): Empfehlung der Kommission vom 3. April 1996 betreffend die Definition der kleinen und mittleren Unternehmen (96/280/EG). http://europa.eu.int/scadplus/leg/de/lvb/n26001.htm, 2003, Abruf: 2006-05-25.

[FePf00] Federrath, H.; Pfitzmann, A.: Schutzziele in IT-Systemen. In: Datenschutz und Datensicherheit Nr. 12 (2000), S. 704-710.

[FMSh01] Fluhrer, S.; Mantin, I.; Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In: Lecture Notes in Computer Science Vol. 2259 (2001), p. 1-24.

[GeSc04] Gergeleit, M.; Schumann, R.: WLAN-Sicherheit jenseits von WEP - Relevant auch für die Automatisierung? http://www.rt-solutions.de/dat/SPS2004-Gergeleit.pdf, 2004, Abruf: 2006-05-30.

[Grot04] Grotzke, S. D.: WLAN - Der Einstieg ins kabellose Netz. C & L, Computer-&-Literatur-Verlag, Böblingen, 2004.

[Heis01] Heise Zeitschriften Verlag (Hrsg.): Flicken für Sicherheitslöcher in Funk-LANs. Heise Online News, http://www.heise.de/newsticker/meldung/print/23524, 2001, Abruf: 2006-05-30.

[Heis04] Heise Zeitschriften Verlag (Hrsg.): IEEE-Standard 802.11i für Wireless LAN ratifiziert. Heise Security News, http://www.heise.de/security/news/meldung/print/48624, 2004, Abruf: 2006-05-31.

[Heis05] Heise Zeitschriften Verlag (Hrsg.): Schnelles WLAN: Kompromiss in Aussicht. Heise Online News, http://www.heise.de/newsticker/meldung/61486, 07/2005, Abruf: 2006-05-30.

[Höch03] Höchel-Winter, C.: WLAN-Antennen optimal einsetzen, Funkqualität verbessern. http://www.comconsult-research.de/insider/bilder/IT-309-2s.pdf, 09/2003, Abruf: 2006-05-30.

[Hump04] Humpert, F.: IT-Sicherheit. In: HMD - Praxis der Wirtschaftsinformatik, Nr. 236 (April 2004), S. 7-18.

[IEEE03a] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://standards.ieee.org/getieee802/download/802.11-1999.pdf, 2003, Abruf: 2006-05-30.

[IEEE03b] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Layer in the 5 GHz Band. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf, 2003, Abruf: 2006-05-30.

[IEEE03c] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf, 2003, Abruf: 2006-05-30.

[IEEE03d] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 3: Specification for Operation in additional regulatory domains. http://standards.ieee.org/getieee802/download/802.11d-2001.pdf, 2003, Abruf: 2006-05-30.

[IEEE03e] Institute of Electrical Engineers (Hrsg.): 802.11F-IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. http://standards.ieee.org/getieee802/download/802.11F-2003.pdf, 2003, Abruf: 2006-05-30.

[IEEE03f] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf, 2003, Abruf: 2006-05-30.

[IEEE03g] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 5: Spectrum und Transmit Power Management Extensions in the 5 GHz Band in Europe. http://standards.ieee.org/getieee802/download/802.11h-2003.pdf, 2003, Abruf: 2006-05-30.

[IEEE04] Institute of Electrical and Electronics Engineers (Hrsg.): Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control

(MAC) Security Enhancements. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, 2004, Abruf: 2006-05-30.

[IEEE06] Institute of Electrical and Electronics Engineers: Wireless LANs Standards (802.11) – Documentation Homepage. http://standards.ieee.org/catalog/olis/lanman.html#wirelessLANS, 2006, Abruf: 2006-05-31.

[ISO05a] International Organization for Standardization (Hrsg.): ISO/IEC 27001:2005: Information technology, Security techniques, Code of practice for information se-curity management. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=, 2005, Abruf: 2006-05-25.

[ISO05b] International Organization for Standardization (Hrsg.): ISO/IEC 27001:2005: In-formation technology, Security techniques, Information security management systems – Requirements. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3=, 2005, Abruf: 2006-05-25.

[ITU91] International Telecommunication Union: X.800, Security Architecture for Open Systems Interconnection for CCITT Applications, 1991.

[Jöck04] Jöcker, P.: Computernetze - LAN - WAN - Internet. VDE-Verlag, 3. Auflage, Berlin u. a., 2004.

[KFGr99] Krallmann, H.; Frank, H.; Gronau, N.: Systemanalyse im Unternehmen: Partizipative Vorgehensmodelle, objekt- und prozeßorientierte Analysen, flexible Organisationsarchitekturen. 3. Auflage, Oldenbourg Verlag, München, Wien, 1999.

[Köhr04] Köhre, T.: Wireless LAN – Das kabellose Netzwerk – 10 maßgeschneiderte Workshops. Markt und Technik Verlag, München, 2004.

[Kopp04] Kopp, H.: Einsatz von WLAN in Unternehmen – Leitfaden. Electronic Commerce Center Mecklenburg-Vorpommern (Hrsg.), http://www.mittelstand-sicher-im-internet.de/content-details.php?118, 9/2004, Abruf: 2006-05-30.

[Krom02] Kromrey, H.: Empirische Sozialforschung: Modelle und Methoden der standardisierten Datenerhebung und Datenauswertung. 10. Auflage, Leske & Budrich Verlag, Opladen, 2002.

[Lanc04a] LANCOM Systems (Hrsg.): Techpaper 802.1x. http://www.lancom-systems.de/fileadmin/produkte/feature/techpaper/TP-WLAN-80211x-DE.pdf, 2004, Abruf: 2006-05-30.

[Lanc04b] LANCOM Systems (Hrsg.): Techpaper Überblick WLAN-Sicherheitsfunktionen. http://www.lancom-systems.de/fileadmin/produkte/feature/techpaper/TP-WLAN-security-DE.pdf, 2004, Abruf: 2006-05-30.

[Lanc04c] LANCOM Systems (Hrsg.): Techpaper WPA und 802.11i. http://www.lancom-systems.de/fileadmin/produkte/feature/techpaper/TP-WLAN-80211i-DE.pdf, 2004, Abruf: 2006-05-30.

[LeSt02] Lerg, A.; Stolz, A.: Das große Buch - Wireless LAN & Bluetooth. Data Becker Verlag, Düsseldorf, 2002.

[Mart04] Martin, B.: Checkliste WLAN. Stabsstelle IKT des Bundes, Bundeskanzleramt Österreich, http://www.cio.gv.at/it-infrastructure/wlan/Checkliste-WLAN_v10.pdf, 2004, Abruf: 2006-05-30.

[Mart73] Martin, J.: Security, Accuracy and Privacy in Computer Systems. Prentice-Hall PTR, 1973.

[Micr05] Microsoft Corporation (Hrsg.): IEEE 802.11 Wireless LAN Security with Microsoft Windows XP. http://www.microsoft.com/downloads/info.aspx?na=90&p=&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=67fdeb48-74ec-4ee8-a650-334bb8ec38a9&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2f1%2f6%2fa%2f16ae3c0f-a010-4370-a321-4e1ca8d95a95%2fWiFi_Security.doc, 2005, Abruf: 2006-05-30.

[Miro04] Mironov, R.: WLAN Sicherheits- und Perfomance-Kriterien. In: Funkschau, Nr. 17 (2004), S. 46.

[Müll02] Müller, B.: Sicherheit im Wireless LAN. http://www.tecchannel.de/hardware/1310/index.html, 2002, Abruf: 2006-05-25.

[PeKa04] Pietzko, S.; Kalkbrenner, A.: Standards im Wireless LAN. http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/WlanStandards, 2004, Abruf: 2006-05-25.

[PiRi94] Piveteau, J.-M.; Riess, H. P.: Eine generische Sicherheitsarchitektur für Telekommunikationsnetze. In: Bauknecht, K.; Teufel, S. (Hrsg.): Sicher-

heit in Informationssystemen. Proceedings der Fachtagung SIS'94 Universität Zürich-Irchel, Institut für Wirtschaftsinformatik, Verlag der Fachvereine, Zürich, 1994, S. 149.

[Poll04] Pollok, S.: WLAN? Aber sicher! http://www.incas.de/pdf/WLAN_aber_sicher.pdf, 2004, Abruf: 2006-05-27.

[PSWW00] Pfitzmann, A.; Schill, A.; Westfeld, A.; Wolf, G.: Mehrseitige Sicherheit in offenen Netzen. Vieweg Verlagsgesellschaft, Braunschweig u. a., 2000.

[Radm04] Radmacher, M.: Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks. Diplomarbeit an der Universität Duisburg-Essen, Fachbereich Wirtschaftswissenschaften, http://www.m-lehrstuhl.de/veranstaltung/WS_2004_AG/Diplomarbeit%20-%20Sicherheits-%20und%20Schwachstellenanalyse%20entlang%20des%20Wireless-LAN-Protokollstacks.pdf, Essen, 2004, Abruf: 2006-05-29.

[RPMü97] Ranneberg, K.; Pfitzmann, A.; Müller, G.: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley Verlag, Bonn u. a., 1997, S. 21-29.

[RSA04] RSA-Security Inc. (Hrsg.): The Wireless Security Survey of Frankfurt. http://www.rsasecurity.com/solutions/wireless/whitepapers/WSFR04_WP_0604.pdf, 05/2004, Abruf: 2006-05-30.

[RSA05] RSA-Security Inc. (Hrsg.): The Wireless Security Survey of San Francisco. http://www.securitymanagement.com/library/rsa_wireless0606.pdf, 03/2005, Abruf: 2006-05-30.

[Saut04] Sautner, F.: IT-Security-Studie 2004. InformationWeek. http://www.iw-live.de/security/media/it_security_2004_studieninfo.pdf, 2004, Abruf: 2005-05-30.

[Schn01] Schneier, B.: Secrets & Lies: IT-Sicherheit in einer vernetzten Welt. Dpunkt.Verlag, Heidelberg, 2001.

[SHEs99] Schnell, R.; Hill, P. B.; Esser, E.: Methoden der empirischen Sozialforschung. 6. Auflage, Oldenburg Verlag, München, 1999.

[Sili05] Silicon.de (Hrsg.): Wireless Networking Studie - WLAN entwickelt sich zum Kabel des kleinen Mannes. http://www.silicon.de/cms/extern.php?

lid=&pid=130&cid=11469&url=http://www.silicon.de/downloads/Wireless_Networking_04.pdf, 2005, Abruf: 2006-05-30.

[SMBa04] Sankar, K.; Miller, D.; Balinsky, A.: Cisco Wireless LAN Security. Cisco Press, Indianapolis, 2004.

[Stel93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes Beratungssystem für die Risikoanalyse. Dt. Universitätsverlag, Wiesbaden, 1993.

[StLe04] Stanossek, G.; Lenz-Hawliczek, J.: WLAN-Studie Berlin. http://www.berlin.de/senwiarbfrau/projektzukunft/mat/studien/studie_wlan_2004.pdf, 08/2004, Abruf: 2005-10-10.

[Stud06] Studerus Telecom AG (Hrsg.): Wireless LAN – Vernetzung von PCs über Funk. http://www.zyxel.ch/ratgeber.cfm?action=detail&id=10027&area=3&lang=d, 2006, Abruf: 2006-05-30.

[Wick04] Wick Hill (Hrsg.): Wireless Networking in Deutschland. http://www.nexthop.de/de/clients/wickhill/press/wh20040915.pdf, 10/2004, Abruf: 2006-05-30.

[Wifi03] Wi-Fi Alliance (Hrsg):Wi-Fi Protected Access: strong, standards-based, interoperable security for today's Wi-Fi Networks. http://www.wi-fi.org/membersonly/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf, 2003, Abruf: 2006-05-30."

[Wlan06] WLAN-SEC: Fragebogen. http://www.wlan-sec.de/Massnahmenkatalog.pdf, 2006, Abruf: 2006-05-30.

Anhang – Fragenbogen

I. Allgemeine Angaben zum Unternehmen

Bitte beantworten Sie zunächst einige allgemeine Fragen zu Ihrem Unternehmen.

I.1. In welcher Branche ist Ihr Unternehmen tätig?							
Dienstleistungen	**Handel**	**Industrie**	**Information und Kommunikation**	**öffentliche Einrichtung**	**Tourismus**	**Verkehr**	**keine Angabe**
☐	☐	☐	☐	☐	☐	☐	☐

I.2. In welchem Bundesland befindet sich der Hauptsitz Ihres Unternehmens?	

	weniger als 10	**zwischen 10 und 50**	**zwischen 50 und 250**	**mehr als 250**	**keine Angabe**
I.3. Wie viele Mitarbeiter sind in Ihrem Unternehmen beschäftigt?	☐	☐	☐	☐	☐

I.4. In welchem Jahr wurde Ihr Unternehmen gegründet?	

I.5. Welche Tätigkeit/Position üben Sie in Ihrem Unternehmen aus?	

	sehr wichtig	**wichtig**	**weniger wichtig**	**nicht wichtig**	**keine Angabe**
I.6. Wie wichtig ist die IT-Sicherheit in Ihrem Unternehmen?	☐	☐	☐	☐	☐

	ja	nein	keine Angabe
I.7. Gibt es ein IT-Security-Management bzw. einen IT-Sicherheitsverantwortlichen in Ihrem Unternehmen?	☐	☐	☐

	sehr hoch	hoch	mittel	niedrig	keine Angabe
I.8. Wie schätzen Sie das IT-Sicherheitsniveau in Ihrem Unternehmen ein?	☐	☐	☐	☐	☐

	ja	nein	ist geplant
I.9. Wird WLAN-Technologie in Ihrem Unternehmen eingesetzt? - bei „ja“ weiter mit Frage II.1 auf Seite 3 - bei „nein“ weiter auf Seite 12 - bei „ist geplant“ weiter mit Frage III.1.1. auf Seite 13	☐	☐	☐

II. WLAN-Spezifika des Unternehmens

Um später Abhängigkeiten zwischen unternehmensspezifischen Merkmalen und WLAN-Sicherheitsmaßnahmen ermitteln zu können, sind Angaben zur WLAN-Spezifika Ihres Unternehmens notwendig. Beantworten Sie bitte die folgenden Fragen zur WLAN-Spezifika.

II.1. Seit wie vielen Jahren wird WLAN-Technologie in Ihrem Unternehmen eingesetzt?	

	Zugang zum Internet	Zugang zu Anwendungen des Unternehmens	Bereitstellung von Dienstleistungen (z.B. Bezahldienste)	bisher nicht aufgeführte Anwendungszwecke	keine Angabe
II.2. Was ist der Anwendungszweck / Verwendungszweck Ihres WLANs? (mehrere Antworten möglich)	☐	☐	☐	☐	☐

II.3. In welchen Bereichen Ihres Unternehmens werden WLANs eingesetzt? (mehrere Antworten möglich)

Beschaffung	Finanzen/ Controlling	Forschung & Entwicklung	Geschäftsführung	IT-Bereich	Marketing & Vertrieb	Produktion/ Kundenservice	Personalbereich	bisher nicht aufgeführte Bereiche	keine Angabe
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

	weniger als 10% der Mitarbeiter	zwischen 10% und 40% der Mitarbeiter	zwischen 40% und 70% der Mitarbeiter	mehr als 70% der Mitarbeiter	keine Angabe
II.4. Wieviel Prozent der Mitarbeiter nutzen WLAN im Unternehmen?	☐	☐	☐	☐	☐

	Access Points	WLAN- fähige Endgeräte	keine Angabe
II.5. Wie hoch ist die Anzahl der WLAN-Komponenten in Ihrem Unternehmen?			☐

	Desktop PCs	Notebooks	PDAs / Smartphones	bisher nicht aufgeführte Arten von Endgeräte	keine Angabe
II.6. Welche Arten von WLAN-Endgeräten kommen in Ihrem Unternehmen zum Einsatz? (mehrere Antworten möglich)	☐	☐	☐	☐	☐

	ja	nein	keine Angabe
II.7. Ist das WLAN an ein anderes Netz in Ihrem Unternehmen angeschlossen?	☐	☐	☐

	Eigenbetrieb	Fremdbetrieb	keine Angabe
II.8. Wird das WLAN durch Ihr Unternehmen selbst oder durch eine Fremdfirma betrieben?	☐	☐	☐

	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	andere WLAN-Standards	keine Angabe
II.9. Welche WLAN-Standards werden in Ihrem Unternehmen eingesetzt? (mehrere Antworten möglich)	☐	☐	☐	☐	☐	☐

	Ad-hoc-Modus	Infrastruktur-Modus	keine Angabe
II.10. Welche WLAN-Einsatzmodi werden in Ihrem Unternehmen angewendet? (mehrere Antworten möglich)	☐	☐	☐

	stets in Betrieb	nur zur Kernarbeitszeit	nur bei Bedarf / auf Anfrage	keine Angabe
II.11. Welche Aussage können Sie zur Betriebszeit der WLAN-Infrastruktur treffen?	☐	☐	☐	☐

	die WLAN-Daten sind nicht so sicherheitskritisch	die WLAN-Daten sind genauso sicherheitskritisch	die WLAN-Daten sind sicherheitskritischer	keine Angabe
II.12. Wie sicherheitskritisch sind die mittels WLAN übertragenen Daten im Vergleich zu denen der anderen (drahtgebundenen) Unternehmensnetze?	☐	☐	☐	☐

	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	keine Angabe
II.13. Wie wichtig ist Ihnen die WLAN-Sicherheit in Ihrem Unternehmen?	☐	☐	☐	☐	☐

	sehr hoch	hoch	mittel	gering	keine Angabe
II.14. Wie schätzen Sie das WLAN-Sicherheitsniveau in Ihrem Unternehmen ein?	☐	☐	☐	☐	☐

III. WLAN-Sicherheitsmaßnahmen

III.1. Organisatorische Maßnahmen vor einer WLAN-Installation

Um Ihre WLAN-Infrastruktur den Sicherheitsanforderungen entsprechend angemessen abzusichern, sind organisatorische Maßnahmen erforderlich. Bereits vor der Inbetriebnahme einer WLAN-Infrastruktur können diese organisatorischen Maßnahmen helfen, die Sicherheit zu erhöhen.[74]

Schritt 1: Setzen Sie bitte in der ersten Spalte bei denjenigen Maßnahmen ein Häkchen, die Ihnen bekannt sind.

Schritt 2: Geben Sie bitte in der zweiten Spalte für die einzelnen Maßnahmen an, ob Sie diese durchgeführt haben.

Schritt 3: Geben Sie bitte für Maßnahmen, die NICHT von Ihnen durchgeführt bzw. eingesetzt wurden, den jeweiligen Grund dafür an. Nutzen Sie bitte dazu die vorgeschlagenen Antwortalternativen durch Angabe der Zahlen 1 bis 3 oder verwenden Sie das Eingabefeld frei zur Angabe anderer Gründe.

[74] Für weitere Erläuterungen zu den Sicherheitsmaßnahmen vgl. Abschnitt 3.3.1.

III.1.1. Sicherungskonzept für WLAN-Infrastruktur erstellen

	Welche der Maßnahmen sind Ihnen bekannt?	Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?	Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit	keine Angabe
Notwendigkeit, Ziele und Anwendungszweck der WLAN-Installation begründen	☐	☐		☐
Anforderungen an Sicherheitsziele festlegen	☐	☐		☐
Schutzbedarfsfeststellung und Risikoanalyse durchführen	☐	☐		☐
WLAN-Policy erstellen	☐	☐		☐

	Definition des WLAN-Nutzerkreises und Bedingungen für deren Zugang	Definition der Sicherheitsziele	Richtlinien zur Sicherung der Access Points	Richtlinien für das Schlüsselmanagement und die Authentifizierung	Richtlinien zur Sicherung der Clients	Richtlinien zum Reporting und Logging	keine Angabe
Falls eine WLAN-Policy existiert, enthält sie Richtlinien zu folgenden Punkten? (mehrere Antworten möglich)	☐	☐	☐	☐	☐	☐	☐

III.1.2. Optimales Rollout planen

	Welche der Maßnahmen sind Ihnen bekannt?	Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?	Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit	keine Angabe
Einsatzorte exakt festlegen und abgrenzen	☐	☐		☐
Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)	☐	☐		☐
Messplanung durchführen (Ermittlung der Signalstärke)	☐	☐		☐
Antennentyp und Aufstellort der Access Points so wählen, dass eine maximale Ausleuchtung gewährleistet ist	☐	☐		☐
überlappungsfreie Kanalbelegung (maximal 3 parallele Kanäle bei 802.11b, g und maximal 8 parallele Kanäle bei 802.11a)	☐	☐		☐
Kontrolle und Überprüfung des WLAN durch abschließenden Netzwerkscan und Auswertung der Logdatei	☐	☐		☐

III.1.3. Weitere organisatorische Maßnahmen vor einer WLAN-Installation

	Welche der Maßnahmen sind Ihnen bekannt?	Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?	Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit	keine Angabe
Testläufe im Vorfeld durchführen	☐	☐		☐
Notfallstrategien für den Ausfall entwickeln	☐	☐		☐

Administration der Access Points nicht über WLAN-Schnittstelle vollziehen	☐	☐		☐
Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen	☐	☐		☐
Sensibilisierung bzw. Schulung der Anwender	☐	☐		☐

Nennen Sie bitte weitere organisatorische Maßnahmen, die in Ihrem Unternehmen vor der WLAN-Installation durchgeführt wurden.

III.2. Organisatorische Maßnahmen während des WLAN-Betriebs

Nicht nur vor Inbetriebnahme einer WLAN-Infrastruktur sind organisatorische Sicherheitsmaßnahmen notwendig, sondern auch während des Betriebs muss regelmäßig die Sicherheit durch eine Reihe von organisatorischen Maßnahmen überprüft werden.[75]

Schritt 1: Setzen Sie bitte in der ersten Spalte bei denjenigen Maßnahmen ein Häkchen, die Ihnen bekannt sind.

Schritt 2: Geben Sie bitte in der zweiten Spalte für die einzelnen Maßnahmen an, ob Sie diese durchgeführt haben.

Schritt 3: Geben Sie bitte für Maßnahmen, die NICHT von Ihnen durchgeführt bzw. eingesetzt wurden, den jeweiligen Grund dafür an. Nutzen Sie bitte dazu die vorgeschlagenen Antwortalternativen durch Angabe der Zahlen 1 bis 3 oder verwenden Sie das Eingabefeld frei zur Angabe anderer Gründe.

[75] Für weitere Erläuterungen zu den Sicherheitsmaßnahmen vgl. Abschnitt 3.3.2.

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit**	**keine Angabe**
Einhaltung der Datenschutzbestimmungen	☐	☐		☐
Regelmäßige Kontrolle und Überwachung des WLAN durch Netzwerkscans und Auswertung der Logdateien	☐	☐		☐
Physischer Zugriff zu Access Points nur autorisiertem Personal ermöglichen	☐	☐		☐
Überprüfung der WLAN-Policy	☐	☐		☐
Physische Überprüfung der installierten Access Points auf Zugänglichkeit und Beschädigungen, um Netzausfälle und mißbräuchliche Verwendungen zu verhindern	☐	☐		☐
Regelmäßige Kontrolle und Wartung der clientseitigen Einstellungen, wie Firewall- und Betriebssystem-Konfiguration an den Endgeräten	☐	☐		☐

Nennen Sie bitte weitere organisatorische Maßnahmen während des WLAN-Betriebs, die in Ihrem Unternehmen durchgeführt werden.

III.3. Hardwaretechnische Maßnahmen

Zur Sicherung einer WLAN-Infrastruktur sind auch hardwaretechnische Maßnahmen einsetzbar.[76]

Schritt 1: Setzen Sie bitte in der ersten Spalte bei denjenigen Maßnahmen ein Häkchen, die Ihnen bekannt sind.

Schritt 2: Geben Sie bitte in der zweiten Spalte für die einzelnen Maßnahmen an, ob Sie diese durchgeführt haben.

Schritt 3: Geben Sie bitte für Maßnahmen, die NICHT von Ihnen durchgeführt bzw. eingesetzt wurden, den jeweiligen Grund dafür an. Nutzen Sie bitte dazu die vorgeschlagenen Antwortalternativen durch Angabe der Zahlen 1 bis 3 oder verwenden Sie das Eingabefeld frei zur Angabe anderer Gründe.

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit**	**keine Angabe**
geignete WLAN-Technik und Standard (IEEE 802.11g, etc.) wählen	☐	☐		☐
WLAN-Systemkomponenten und -Services nur bei Gebrauch einschalten bzw. zeitgesteuerten Zugriff aktivieren.	☐	☐		☐
WLAN-Tapete zur Abschirmung nutzen	☐	☐		☐
Registrierte WLAN-Karten über eine Ausleihe ausgeben und regelmäßig austauschen	☐	☐		☐

Nennen Sie bitte weitere hardwaretechnische Maßnahmen, die in Ihrem Unternehmen durchgeführt wurden.

[76] Für weitere Erläuterungen zu den Sicherheitsmaßnahmen vgl. Abschnitt 3.3.3.

III.4. Softwaretechnische Maßnahmen

Neben den hardwaretechnischen Maßnahmen sind auch softwaretechnische Maßnahmen einzusetzen, um WLAN-Infrastrukturen abzusichern.[77]

Schritt 1: Setzen Sie bitte in der ersten Spalte bei denjenigen Maßnahmen ein Häkchen, die Ihnen bekannt sind.

Schritt 2: Geben Sie bitte in der zweiten Spalte für die einzelnen Maßnahmen an, ob Sie diese durchgeführt haben.

Schritt 3: Geben Sie bitte für Maßnahmen, die NICHT von Ihnen durchgeführt bzw. eingesetzt wurden, den jeweiligen Grund dafür an. Nutzen Sie bitte dazu die vorgeschlagenen Antwortalternativen durch Angabe der Zahlen 1 bis 3 oder verwenden Sie das Eingabefeld frei zur Angabe anderer Gründe.

III.4.1. Konfiguration und Administration der Endgeräte

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit**	**keine Angabe**
Werkseitige Grundeinstellungen an WLAN-Komponenten ändern (Passwort, WEP-Schlüssel)	☐	☐		☐
Ad-hoc-Vernetzung deaktivieren	☐	☐		☐
Eigenen Netzwerkname vergeben (kryptische SSID)	☐	☐		☐
SSID im Broadcast abschalten	☐	☐		☐
Beacon Intervall maximieren	☐	☐		☐

[77] Für weitere Erläuterungen zu den Sicherheitsmaßnahmen vgl. Abschnitt 3.3.4.

DHCP am Access Point abschalten	☐	☐		☐
Verbindung zwischen RADIUS-Server und Access Point absichern	☐	☐		☐
Einen WLAN-Standard, anstatt mehrerer parallel nutzen (z. B. 'G-only' oder 'B-only')	☐	☐		☐
Block-Intra-BSS-Traffic in öffentlichen Bereichen verwenden	☐	☐		☐

III.4.2. Authentifizierungsverfahren anwenden

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit**	**keine Angabe**
Authentifizierung über MAC-Adresse	☐	☐		☐
Pre-Shared-Key-Authentifizierung	☐	☐		☐
Open-System- der Shared-Key-Authentifizierung vorziehen, um Kompromittierung des WEP-Schlüssels zu unterbinden	☐	☐		☐
Authentifizierung mit WLAN Smartcard	☐	☐		☐
Authentifizierung nach IEEE 802.1x über RADIUS-Server	☐	☐		☐

III.4.3. Verschlüsselungstechniken benutzen

	Welche der Maßnahmen sind Ihnen bekannt?	Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?	Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit	keine Angabe
WEP-Verschlüsselung	☐	☐		☐
Verschlüsselung nach WPA-Standard	☐	☐		☐
Verschlüsselung nach WPA2 bzw. 802.11i	☐	☐		☐

III.4.4. Weitere softwaretechnische Maßnahmen

	Welche der Maßnahmen sind Ihnen bekannt?	Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?	Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit	keine Angabe
Netzwerktechnische Trennung zwischen WLAN und drahtgebundenem Netz (z.B. über Paketfilter, VPN oder VLAN)	☐	☐		☐
Installation einer Personal Firewall auf den mobilen Endgeräten	☐	☐		☐
Verwendung eines Intrusion Detection Systems zur Überwachung des WLANs	☐	☐		☐
Datei- und Ressourcenfreigabe auf allen Endgeräten sowie Geräten, die vom WLAN aus erreichbar sind, restriktiv einschränken	☐	☐		☐

Nennen Sie bitte weitere softwaretechnische Maßnahmen, die in Ihrem Unternehmen durchgeführt wurden.

IV. Zukünftige Planung weiterer WLAN-Sicherheitsmaßnahmen

Nachdem Sie nun die Fragen zum Einsatz von WLAN-Sicherheitsmaßnahmen beantwortet haben, noch eine abschließende Frage.

	ja	nein	keine Angabe
IV.1. Planen Sie zukünftig den Einsatz weiterer WLAN-Sicherheitsmaßnahmen?	☐	☐	☐

Vielen Dank für Ihre Angaben!

Falls Sie die Ergebnisse der Studie direkt von uns erhalten möchten, geben Sie bitte die folgenden Kontaktdaten an (freiwillige Angaben):

Name	
Adresse	
Telefon	
E-Mail	

Andernfalls können Sie sich auch bei Ihrer jeweiligen Dachorganisation über die Ergebnisse der Studie informieren.

Ihr WLAN-SEC-Projektteam.

Der folgende Teil des Fragebogens gilt nur für den Fall, dass in Ihrem Unternehmen erst eine WLAN-Installation in Planung und noch nicht in Betrieb ist.

III. WLAN-Sicherheitsmaßnahmen

III.1. Organisatorische Maßnahmen vor einer WLAN-Installation

Um Ihre geplante WLAN-Installation reibungslos durchführen zu können, sind einige vorbereitende organisatorische Maßnahmen erforderlich.[78] Bitte gehen Sie bei der Beantwortung der Fragen wie folgt vor:

Schritt 1: Setzen Sie bitte in der ersten Spalte bei denjenigen Maßnahmen ein Häkchen, die Ihnen bekannt sind.

Schritt 2: Geben Sie bitte in der zweiten Spalte für die einzelnen Maßnahmen an, ob Sie diese durchgeführt haben.

Schritt 3: Geben Sie bitte für Maßnahmen, die NICHT von Ihnen durchgeführt bzw. eingesetzt wurden, den jeweiligen Grund dafür an. Nutzen Sie bitte dazu die vorgeschlagenen Antwortalternativen durch Angabe der Zahlen 1 bis 3 oder verwenden Sie das Eingabefeld frei zur Angabe anderer Gründe.

III.1.1. Sicherungskonzept für WLAN-Infrastruktur erstellen

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit 4=noch in Planung**	**keine Angabe**
Notwendigkeit, Ziele und Anwendungszweck der WLAN-Installation begründen	☐	☐		☐
Anforderungen an Sicherheitsziele festlegen	☐	☐		☐

[78] Für weitere Erläuterungen zu den Sicherheitsmaßnahmen vgl. Abschnitt 3.3.1.

Schutzbedarfsfeststellung und Risikoanalyse durchführen	☐	☐		☐
WLAN-Policy erstellen	☐	☐		☐

	Definition des WLAN-Nutzerkreises und Bedingungen für deren Zugang	**Definition der Sicherheitsziele**	**Richtlinien zur Sicherung der Access Points**	**Richtlinien für das Schlüsselmanagement und die Authentifizierung**	**Richtlinien zur Sicherung der Clients**	**Richtlinien zum Reporting und Logging**	**keine Angabe**
Falls eine WLAN-Policy existiert, enthält sie Richtlinien zu folgenden Punkten? (mehrere Antworten möglich)	☐	☐	☐	☐	☐	☐	☐

III.1.2. Optimales Rollout planen

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit 4=noch in Planung**	**keine Angabe**
Einsatzorte exakt festlegen und abgrenzen	☐	☐		☐
Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)	☐	☐		☐
Messplanung durchführen (Ermittlung der Signalstärke)	☐	☐		☐
Antennentyp und Aufstellort der Access Points so wählen, dass eine maximale Ausleuchtung gewährleistet ist	☐	☐		☐

überlappungsfreie Kanalbelegung (maximal 3 parallele Kanäle bei 802.11b, g und maximal 8 parallele Kanäle bei 802.11a)	☐	☐		☐
Kontrolle und Überprüfung des WLAN durch abschließenden Netzwerkscan und Auswertung der Logdatei	☐	☐		☐

III.1.3. Weitere organisatorische Maßnahmen vor einer WLAN-Installation

	Welche der Maßnahmen sind Ihnen bekannt?	**Welche der Maßnahmen wurden im Unternehmen bereits durchgeführt?**	**Maßnahme nicht durchgeführt, weil... 1=zu aufwendig 2=nicht zutreffend 3=keine Erhöhung der Sicherheit 4=noch in Planung**	**keine Angabe**
Testläufe im Vorfeld durchführen	☐	☐		☐
Notfallstrategien für den Ausfall entwickeln	☐	☐		☐
Administration der Access Points nicht über WLAN-Schnittstelle vollziehen	☐	☐		☐
Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen	☐	☐		☐
Sensibilisierung bzw. Schulung der Anwender	☐	☐		☐

Nennen Sie bitte weitere organisatorische Maßnahmen, die in Ihrem Unternehmen vor der WLAN-Installation geplant sind.

Vielen Dank für Ihre Angaben!

Falls Sie die Ergebnisse der Studie direkt von uns erhalten möchten, geben Sie bitte die folgenden Kontaktdaten an (freiwillige Angaben):

Name	
Adresse	
Telefon	
E-Mail	

Andernfalls können Sie sich auch bei Ihrer jeweiligen Dachorganisation über die Ergebnisse der Studie informieren.

Ihr WLAN-SEC-Projektteam.