Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Verbraucherschutz

Januar 2007

Risikopotenzial von drahtlosen Netzwerken

Bericht in Erfüllung des Postulates 04.3594 Allemann vom 8. Oktober 2004

Mitwirkung:
Bundesamt für Gesundheit (BAG)
Stefanie Gruber, Martin Meier, Mirjana Moser, Salome Ryf

Bundesamt für Kommunikation (BAKOM)
Rolf Burgherr, Mark Fitzpatrick, Markus Riederer

Bundesamt für Umwelt (BAFU)
Andreas Siegenthaler

Swissmedic, Schweizerisches Heilmittelinstitut
Daniel Reusser

Federführung:
Bundesamt für Gesundheit, Abteilung Strahlenschutz
Dr. Mirjana Moser

Weitere Informationen:
Diese Publikation ist auch in französischer und italienischer Sprache erhältlich
Der Bericht wird unter www.bag.admin.ch/wlan-bericht veröffentlicht.
.

Zusammenfassung

Der vorliegende Bericht wurde in Erfüllung des Postulates 04.3594 von Evi Allemann zum „Risikopotential von drahtlosen Netzwerken“ ausgearbeitet. Er gibt auf die im Postulat Allemann gestellten Fragen zu Strahlungspotential, Gesundheitsrisiken, Datensicherheit und Regelungsbedarf Auskunft. Im Bericht werden die meist verbreiteten Technologien wie Bluetooth, WLAN oder das neue WiMAX näher untersucht. Neben der Darstellung der aktuellen Technologien werden auch Szenarien hinsichtlich der Weiterentwicklung entworfen und Empfehlungen zum vorsorglichen Umgang mit diesen neuen Technologien gegeben.

Die Strahlenbelastung durch die heutigen Netzwerke ist relativ klein, sie liegt weit unterhalb der geltenden Grenzwerte. Trotzdem ist ein vorsorgliches Vorgehen angebracht. Gründe dazu sind die rasante technologischen Entwicklung mit leistungsfähigeren Geräten, die zunehmende Anwendung von Geräten nah am Körper sowie das gleichzeitige Betreiben mehrerer Geräte auf kleinem Raum. Zudem bestehen weiterhin Unsicherheiten bezüglich möglicher Gesundheitsrisiken, insbesondere was die Langzeitauswirkungen betrifft.

Eine besondere Problematik der drahtlosen Netzwerke ist ihre elektromagnetische Verträglichkeit. Die meisten drahtlosen Netzwerke senden im lizenzfreien Frequenzbereich wie viele andere Geräte auch. Dadurch kann es zu gegenseitigen Störungen kommen. Besondere Vorsicht ist deshalb bei den Anwendungen geboten, wie z.B. in der Medizin, bei welchen solche Funktionsstörungen zu einer Gesundheitsgefährdung führen könnten.

Auch in Bezug auf die Daten- und Informationssicherheit bergen drahtlose Netzwerke einige Gefahren. Diese sind grösser als bei leitergebundenen Netzen und es ist zudem für Laien schwieriger, die grundlegenden Sicherheitsmassnahmen anzuwenden. Eine entsprechende Information ist deshalb sehr wichtig.

Zum heutigen Zeitpunkt wird kein Regelungsbedarf festgestellt, weder was die steigende Anzahl an Hotspots anbelangt, noch hinsichtlich der Strahlung oder der Gesundheitsrisiken. Die weitere Entwicklung und Verbreitung dieser Technologien sowie die laufende Forschung in Bezug auf die Gesundheitsrisiken sollte jedoch von den zuständigen Behörden aufmerksam verfolgt werden.

Sowohl betreffend der Strahlung als auch der Sicherheit von drahtlosen Netzwerken besteht ein Sensibilisierungsbedarf. Im Bericht werden Empfehlungen zur Minimierung der Strahlenbelastung und zur Erhöhung der Datensicherheit gemacht. Der Bericht und die Empfehlungen sowie darauf basierende Faktenblätter werden auf der Internetseite des BAG publiziert. Insbesondere werden auch die Konsumentenorganisationen und die Ärzteschaft informiert.

1. Einleitung

Die drahtlose Kommunikation gehört unumstritten zu den zukunftsträchtigsten Marktsegmenten im Informationsbereich. Bei den drahtlosen Netzwerken wird ein ähnlicher Boom wie seinerzeit beim Mobilfunk erwartet. Indikator für diese Entwicklung ist die steigende Anzahl von Teilnehmern, welche die Vorteile des massiv verbesserten und mobileren Anschlusses an die digitale Welt nutzen: Durch drahtlose Netzwerke kann die Vernetzung von Computern und Computerperipherie untereinander und zum Internet ohne physische Kabelverbindung mittels einer Funkverbindung sichergestellt werden.

Dieser Boom wirft jedoch auch Fragen zur Sicherheit der neuen Technologien auf. Im technischen Bereich geht es dabei um die abhörsichere und unverfälschte Übertragung von Daten sowie die Störfestigkeit anderer elektrischer Geräte. Andererseits bestehen Fragen zu möglichen gesundheitlichen Wirkungen der elektromagnetischen Strahlung drahtloser Netzwerke mit teilweise neuartigen Charakteristiken.

Dem Antrag des Bundesrates vom 12.1.2005 folgend, hat der Nationalrat am 18.3.2005 das Postulat 04.3594 von Evi Allemann („Risikopotential von drahtlosen Netzwerken“) angenommen.
Im Postulat wird der Bundesrat beauftragt, *einen Bericht zum Risikopotenzial drahtloser Netzwerke (Wireless Local Area Networks “WLAN”, Bluetooth etc.) zu erstellen. Dabei sind sowohl die drahtlosen Netzwerke und Zugangspunkte in Büros und Privathaushalten sowie die öffentlichen Internetstationen (so genannte Hotspots) mit einzubeziehen. Der Bericht soll insbesondere aufzeigen:*

- *Strahlungspotenzial drahtloser Netzwerke,*
- *Gesundheitsrisiken (u.a. spezieller Fokus auf Privathaushalte mit Kleinkindern und mögliche Massnahmen),*
- *Umweltauswirkungen,*
- *Datensicherheitsaspekte,*
- *Allfälliger Regelungsbedarf für den derzeitigen Wildwuchs an privaten und öffentlichen Zugangspunkten (siehe www.swisshotspots.ch).*

Die Ergebnisse sind der Öffentlichkeit zielgruppenspezifisch in geeigneter Form bekannt zu machen.

Der vorliegende Bericht erteilt Auskunft auf die im Postulat Allemann gestellten Fragen[1]. Er setzt sich mit den aktuellen, meistverbreiteten Technologien wie Bluetooth, WLAN oder dem neuen WiMAX auseinander. Ausserdem entwirft der Bericht Zukunftsszenarien im Hinblick auf die möglichen Weiterentwicklungen und gibt Empfehlungen zum vorsorglichen Umgang mit diesen neuen Technologien.

Der Bericht wird auf der Internetseite des BAG veröffentlicht werden. Auf der BAG Internetseite werden ausserdem themenspezifische Faktenblätter veröffentlicht. Die Ärzteschaft wird mit einem Artikel im BAG-Bulletin zu dem Thema informiert. Konsumentinnen und Konsumenten werden in Zusammenarbeit mit dem Eidgenössischen Büro für Konsumentenfragen informiert.

[1] Als Ergänzung zum vorliegenden Bericht wird der Bericht „Nichtionisierende Strahlung und Gesundheitsschutz in der Schweiz“ zur Lektüre empfohlen, der als Antwort zum Postulat Sommaruga „Nichtionisierende Strahlen. Grenzwerte“ (00.3565) erarbeitet wurde. Er behandelt detailliert Expositionen, gesundheitliche Wirkungen und die rechtliche Situation im Bereich der nichtionisierenden Strahlung. www.bag.admin.ch/nis-bericht

2. Drahtlose Netzwerke: Funktionsweise und Strahlenbelastung

Definition

In einem drahtlosen Netzwerk werden Geräte statt mit Kabeln mit Funk, also mit hochfrequenter elektromagnetischer Strahlung, verbunden. Obwohl der Mobilfunk auch auf diese Weise funktioniert, werden damit eher Funkverbindungen auf kleineren Distanzen wie z.B. Netze von Computern und Computerperipherie untereinander und zum Internet bezeichnet.

Funktionsweise

In einem drahtlosen Netzwerk werden die Daten und Informationen drahtlos, mittels elektromagnetischer Wellen[2] (*Elektromagnetische Felder* EMF) übertragen. Dazu sind alle Geräte in einem drahtlosen Netzwerk mit einer Sende-Empfangs-Antenne ausgestattet. Um die gewünschten Informationen oder Daten von einem Sender an einen Empfänger zu übertragen, werden die Daten zuerst in ein Signal umgewandelt, dieses wird auf eine Trägerwelle eingeprägt und dann ausgestrahlt. Durch diese Einprägung wird die Trägerwelle verändert - moduliert. Es gibt unterschiedliche Modulationsarten und dementsprechend entstehen unterschiedliche Strahlungsmuster eines Funksignals. Ein anderes Gerät ist in der Lage das Signal zu empfangen, zu verstehen und in die ursprünglichen Daten oder Informationen umzuwandeln. Als Trägerwelle dienen hochfrequente EMF.

Die Verteilung der EMF um einen Sender hängt von der verwendeten Antenne ab. Eine Antenne kann in alle Richtungen gleichmässig strahlen (wie eine Glühbirne) oder sie kann nur in eine bestimmte Richtung strahlen (wie ein Scheinwerfer). Eine gerichtete Antenne hat einen grösseren Antennengewinn als eine gleichmässig, isotrop, strahlende. Die von der Antenne abgestrahlte Energie pro Zeit ist die Sendeleistung (in Watt, W). Häufig wird die EIRP[3] Sendeleistung verwendet. Sie beschreibt, wie stark eine isotrop strahlende Antenne senden müsste, um überall die gleich starke Strahlung zu erzeugen, wie die fragliche Antenne in ihrer Hauptstrahlrichtung. Die ERP[4] Sendeleistung beschreibt dasselbe für eine fiktive Dipolantenne.

Standards

Damit verschiedene Geräte in einem drahtlosen Netz miteinander kommunizieren können, definieren verschiedene Telekommunikationsstandards die Art und Weise der Datenübertragung (Trägerfrequenz, Modulation, Signalstärke, usw.).

Die wichtigsten Standards für drahtlose Netzwerke sind die Telekommunikationsstandards, die vom amerikanischen *Institute of Electrical and Electronics Engineers IEEE* herausgegeben werden.

In den folgenden Kapiteln werden die drei Standardfamilien für typische Netzwerke erörtert. Je nach Ausdehnung des Netzes unterscheidet man zwischen:

- Wireless Personal Area Networks (WPAN) für Anwendungen in einem kleinen Gebiet wie dem Arbeitsplatz (IEEE 802.15 Standards, bekannt als Bluetooth),
- Wireless Local Area Networks (WLAN) für etwas grössere Netzwerke zum Beispiel in einem Haus (IEEE 802.11 Standards, auch bekannt als WiFi),
- Wireless Metropolitan Area Networks (WMAN) für grössere regionale Netzwerke zum Beispiel in einer Stadt (Standard 802.16, bekannt als WiMAX[5]).

---

[2] Es werden Begriffe wie Wellen, Mikrowellen, elektromagnetische Strahlung, hochfrequente Strahlung verwendet. Physikalisch sind das alles elektromagnetische Felder (EMF) bestimmter Frequenzen – siehe: Abkürzungen und Begriffe, im Anhang, S. 31

[3] equivalent isotropically radiated power

[4] equivalent radiated power

[5] Der entsprechende europäische Standard vom European Telecommunications Standards Institute (ETSI) ist Hiperman.

Ein Überblick über diese Standards mit einigen Charakteristiken und der Situation in der Schweiz befindet sich in der Tabelle 1 .

Tabelle 1: *Standards für drahtlose Netzwerke*

	IEEE[6] Standard	**Max. Sendeleistung (EIRP)**	**Frequenz (MHz)**	**Konzessionspflicht**	**Reichweite (m)**	**Leistungsregulierung**	**Max. Bruttodatenrate (MBit/s)**
WPAN (Bluetooth)	802.15 Leistungsklasse1	100 mW	2400 – 2483,5	nein	100	ja, dynamisch	0,4 - 3
	802.15 Leistungsklasse 2	2,5 mW	2400 – 2483,5	nein	20	optional	0,4 - 3
	802.15 Leistungsklasse 3	1 mW	2400 – 2483,5	nein	10	optional	0,4 - 3
WLAN (WiFi)	802.11a	200 mW	5150 – 5250	nein	50	nein	54
	802.11b	100 mW	2400 – 2483,5	nein	bis 200	nein	11
	802.11g	100 mW	2400 – 2483,5	nein	50	ja, statisch	54
	802.11h	200 mW 1 W	5150 – 5350 5470 - 5725	nein	50	ja, dynamisch	54
WMAN (WiMAX)	802.16 Basisstation Teilnehmer	200 W/MHz 16/100W/MHz 4 W	3410 – 3600 5725 - 5875	ja in Planung	30000	ja	1 - 54

Weitere Standards wie z.B. HiperLAN, die vom *European Telecommunications Standards Institute ETSI* herausgegeben werden, haben keine Verbreitung auf dem Markt und werden deshalb in diesem Bericht nicht berücksichtigt.

Ermittlung der Strahlenbelastung

Die Dosis ist ein Mass für die Strahlenbelastung, die in direktem Zusammenhang mit den gesundheitlichen Auswirkungen steht. Die für hochfrequente EMF relevante Dosis ist die im Körper absorbierte Strahlungsenergie pro Zeitintervall und Körpergewicht. Sie wird durch den SAR-Wert (Spezifische Absorptionsrate in Watt pro Kilogramm W/kg) angegeben, welcher über jeweils 10g Gewebe und sechs Minuten gemittelt wird. Der SAR-Wert ist bei den Grenzwertempfehlungen der ICNIRP (International Commission on Non-Ionizing Radiation Protection) der Basisgrenzwert (ICNIRP Grenzwertempfehlung, siehe Kapitel 3.2).

Der SAR-Wert ist schwierig zu bestimmen. Einfacher ist eine indirekte Bestimmung über eine Immissionsgrösse wie dem elektrischen Feld (in Volt pro Meter, V/m) oder der Leistungsflussdichte (in Watt pro Quadratmeter W/m^2). Diese Grössen stellen bei den ICNIRP-Grenzwertempfehlungen die Referenzgrenzwerte dar. Sie dürfen nur angewendet werden, wenn die Strahlungsquelle entfernt vom Körper betrieben wird und der ganze Körper gleichmässig exponiert wird. Für Anwendungen in der Nähe des Körpers muss direkt der SAR-Wert bestimmt werden.

Exposition ist die Strahlung, welcher der Mensch während einer gewissen Dauer ausgesetzt ist.

[6] IEEE 802.11 (WLAN) http://standards.ieee.org/getieee802/802.11.html
IEEE 802.15 (Bluetooth) http://standards.ieee.org/getieee802/802.15.html
IEEE 802.16 (WiMAX) http://standards.ieee.org/getieee802/802.16.html

Sowohl Immissions- wie auch SAR-Werte sind von sehr vielen Faktoren abhängig wie Sendeleistung, Distanz vom Sender, Frequenz, Modulation usw. In der Tabelle 1 und in der Beschreibung der Technologien sind einige dieser Faktoren genauer angegeben.

Im Bericht werden meist die Worst Case-Szenarien aufgezeigt (z.B. maximale Sendeleistung, maximale Datenrate usw.) und mit den Grenzwerten verglichen. Die effektive Strahlenbelastung in realen Situationen liegt normalerweise unter diesen Worst Case-Werten.

Korrekte Messungen der Strahlung von drahtlosen Netzwerken sind sehr aufwändig und erfordern sehr gute Messinstrumente und Fachwissen. Wechselnde Datenraten, die Spreizung des Signals über mehrere Frequenzen etc. stellen grosse Herausforderungen an die Messung dar und können leicht zu systematischen Messfehlern führen.

2.1 Wireless Personal Area Networks (WPAN), Bluetooth

Anwendungen und Standards

Bluetooth (IEEE 802.15.1) ist der erste WPAN-Standard für Stimm- und Datentransfers über kurze Distanzen. Da Bluetooth-Sender sehr klein und billig sind und wenig Strom brauchen, sind schon sehr viele Geräte damit ausgestattet. Damit können zum Beispiel ein Mobiltelefon mit der Freisprecheinrichtung (Abbildung 1) oder ein Laptop und ein Desktop miteinander oder mit Peripheriegeräten wie Tastatur, Maus, Joystick, Lautsprecher, Drucker, Kamera etc. verbunden werden. Laufend werden neue Anwendungen entwickelt. Ende 2005 wurden weltweit wöchentlich an die 10 Mio. Bluetooth-Sender vertrieben und der Markt wächst laufend[7] .

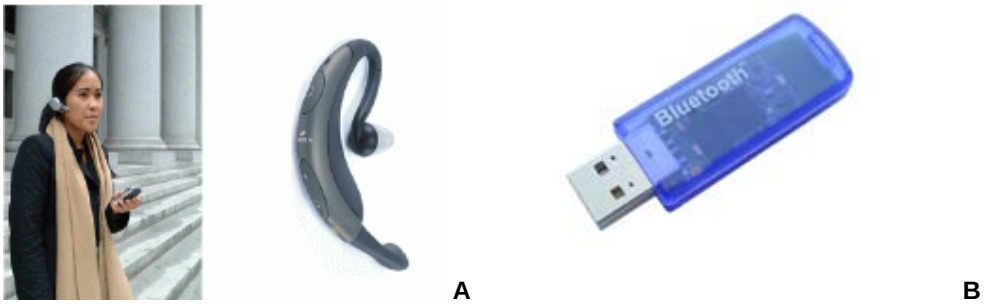


Abbildung 1 A: *Beispiel einer Bluetooth-Anwendung ist die drahtlose Kommunikation zwischen Handy und Freisprechvorrichtung [9].* ***B:*** *USB-Stecker mit Bluetooth-Sender*

Funktionsweise

Bluetooth sendet im lizenzfreien ISM-Band[8] bei einer Frequenz um 2,45 GHz. Das Frequenzband ist in mehrere Kanäle aufgeteilt. Um Störungen durch andere Bluetooth-Netze oder andere Funkanwendungen, die auf der gleichen Frequenz arbeiten, zu minimieren, wird das Signal nicht nur auf einem Kanal, sondern über mehrere Kanäle verteilt gesendet (gespreizt). Dafür wird im Allgemeinen maximal alle 625 µs der Kanal gewechselt (fast frequency hopping). In gleichen Zeitintervallen senden die Netzteilnehmer abwechslungsweise ihre Daten, wobei ein Benutzer bis zu fünf Zeitintervalle auf einmal besetzen darf. Dies führt zu einer unregelmässigen, gepulsten Charakteristik der Strahlung im Allgemeinen mit einer Pulsfrequenz bis zu 1600 Hz (1600 Pulse pro Sekunde).

[7] http://www.imsresearch.com
[8] Industrial Scientific Medical-Band, lizenzfreier Frequenzbereich

Kommen zwei Bluetooth-Geräte in Reichweite, so kommunizieren sie meist automatisch miteinander. In einem einfachen Netz können bis zu acht Geräte aktiv miteinander verbunden sein. Dabei übernimmt ein Gerät die Führung (Master) und organisiert den Funkverkehr im Netz. In aufgebauten Netzen sendet dieses Gerät auch, wenn kein Datenverkehr stattfindet, damit sich die anderen Geräte mit ihm synchronisieren können. Dazu sendet der Master regelmässig ein kurzes Signal aus. Die anderen Geräte (Slaves) können sich ausschalten, um Energie zu sparen, und nur ab und zu dem Funkverkehr im Netz zuhören.

Für verschiedene Anwendungen gibt es drei verschiedene Leistungsklassen (siehe Tabelle 1). Am weitesten verbreitet ist die schwächste Leistungsklasse 3.

Die effektive Sendeleistung ist meistens kleiner als die maximale. Aus verschiedenen Gründen ist es vorteilhaft, jeweils nur so stark zu senden, dass das andere Gerät das Signal gerade noch empfangen kann. So kann z.B. Batterie gespart werden und andere Anlagen werden nicht gestört. Ein Gerät kann die empfangene Sendeleistung messen und den Sender bitten, die Sendeleistung, falls möglich, zu steigern oder zu reduzieren (Leistungsregulierung). Somit sind die Sendeleistung und damit auch die Strahlenbelastung nicht konstant. Die Leistungsregulierung ist für die Leistungsklasse 1 obligatorisch, für 2 und 3 optional.

Strahlenbelastung

Immissionsmessungen

Im Auftrag des BAG wurden Messungen an verschiedenen Bluetooth-Sendern durchgeführt. Es wurden zwei verschiedene USB-Stecker-Antennen (Leistungsklasse 1 und 2)[9] und ein PDA (personal digital assistant, eine elektronische Agenda)[10] untersucht. Die Messungen wurden mit künstlich erzeugter maximaler Datenrate und maximaler Sendeleistung durchgeführt um den Worst Case zu simulieren.

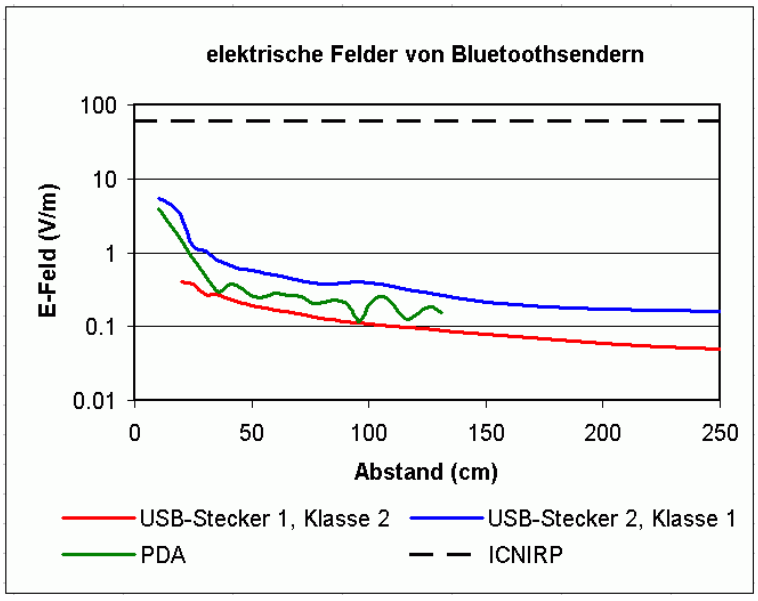


Abbildung 2: *Elektrisches Feld (E-Feld) als Funktion des Abstandes für zwei Bluetooth-USB-Stecker-Antennen verschiedener Leistungsklassen und einen PDA. Das Feld ist in einer logarithmischen Skala angegeben und nimmt mit zunehmendem Abstand sehr schnell ab.*

[9] Kramer A et al. Development of Procedures for the Assessment of Human Exposure to EMF from Wireless Devices in Home and Office Environments. 2005

[10] Kühn S et al. Development of Procedures for the EMF Exposure Evaluation from Wireless Devices in Home and Office Environments. Supplement 1: Close-to-Body and Base Station Wireless Data Communication Devices. 2006

Die gemessenen Feldstärken der Bluetooth-Sender sind in Abhängigkeit vom Abstand (in cm) in Abbildung 2 aufgezeigt. Sie schöpfen in dieser Worst Case-Situation weniger als 5% (Leistungsklasse 1) bzw. 1% (Leistungsklasse 2) der ICNIRP-Grenzwertempfehlung von 61 V/m aus.

Spezifische Absorptionsrate SAR
Um die Strahlenbelastung im Körper durch Geräte, welche nahe am Körper betrieben werden, zu simulieren, wurden die SAR-Werte in einem Körperphantom gemessen. Die Bluetooth-Sender wurden zu diesem Zweck direkt am Phantom angebracht. Es wurden die gleichen zwei USB-Stecker und der PDA wie bei den Immissionsmessungen untersucht (vgl. Abbildung 2). Zudem wurden die SAR-Werte zweier Freisprechvorrichtungen während einer Telefonverbindung mit einem Mobiltelefon in 1,5 m Entfernung gemessen (beide Leistungsklasse 3). Die Resultate sind in der Tabelle 2 zusammengefasst.

Tabelle 2: *SAR-Werte von verschiedenen Bluetooth-Sendern*

Gerät	Leistungsklasse	SAR (W/kg)
USB-Stecker 2	1	0,466
USB-Stecker 1	2	0,0092
PDA		0,01
Freisprechvorrichtung 1	3	0,00117
Freisprechvorrichtung 2	3	0,00319

Die gemessenen SAR-Werte liegen alle unterhalb der ICNIRP-Grenzwertempfehlung von 2 W/kg (Kopf, Körper) bzw. 4 W/kg (Extremitäten).

2.2 Wireless Local Area Networks (WLAN)

Anwendungen und Standards

In einem WLAN werden vor allem PCs und Laptops untereinander, mit Peripheriegeräten (Drucker, Scanner, usw.) und mit dem Access Point für den Internetzugang vernetzt. Dazu werden neue Laptops mit einem WLAN-Chip ausgestattet oder es kann eine WLAN-Karte in den PC oder Laptop eingeschoben werden (vgl. Abbildung 3). Es sind auch elektronische Agenden (PDA) auf dem Markt, die mit WLAN ausgestattet sind und auch als Mobiltelefon benutzt werden können.

Abbildung 3: *WLAN-Access Points und WLAN-Karten für PC und Laptop*[9]

Vorherrschende Standards bei WLAN[11] sind IEEE 802.11a, b, g und h (siehe Tabelle 1). Am meisten verbreitet ist der IEEE 802.11g Standard, welcher den IEEE 802.11b-Standard abgelöst hat. Erhältlich sind auch Geräte mit IEEE 802.11a, die jedoch nur mit reduzierter Leistung in Gebäuden betrieben wer-

[11] Zum Teil wird WLAN auch mit WiFi gleichgesetzt. WiFi ist jedoch nur ein Zertifikat gewisser Hersteller, das eine Interoperabilität der verschiedenen WLAN-Produkte garantieren soll.

den dürfen. In Europa wird stattdessen IEEE 802.11h eingeführt, momentan sind aber noch nicht viele Produkte auf dem Markt.

Funktionsweise

IEEE 802.11b und g senden im lizenzfreien ISM-Band um 2,45 GHz. Da viele andere Anwendungen ebenfalls diesen Frequenzbereich benutzen, ist die Störungsanfälligkeit gross. IEEE 802.11a und h senden im Frequenzbereich zwischen 5,15 GHz und 5,35 GHz, IEEE 802.11h zusätzlich zwischen 5,47 und 5,725 GHz. Diese Frequenzbereiche werden in der Schweiz (und Europa) auch für andere Dienste genutzt. Deshalb ist der Einsatz von Geräten des a-Standards nur mit reduzierter Leistung und in Gebäuden erlaubt. Der h-Standard wurde für Europa so angepasst, dass er die Frequenz sofort freigeben kann, wenn sie von einer anderen Anwendung gebraucht wird.

WLAN-Netze können entweder als Infrastrukturnetz oder als Ad-hoc-Netz betrieben werden. In einem Ad-hoc-Netz werden PCs oder andere Komponenten direkt miteinander verbunden. In einem Infrastrukturnetz läuft der Datenverkehr über einen zentralen Netzwerkknoten (Access Point). Über diesen kann das Netz auch an ein anderes Netz angebunden werden (Internet, Ethernet). Die meisten WLAN-Netze sind Infrastrukturnetze.

Möchte ein Gerät senden, so hört es zuerst für eine Weile zu, ob schon ein anderes Gerät am Senden ist. Ist dies nicht der Fall, so kann gesendet werden. Wie lange gesendet wird, ist nicht festgelegt und der Access Point hat keine Kontrolle darüber. Der Access Point sendet im Allgemeinen alle 100 ms während 0,5 ms ein Signal aus (den Beacon), damit sich die verschiedenen Geräte mit ihm synchronisieren können. Dadurch sendet der Beacon mit einer Repetitionsfrequenz von 10 Hz.

Um Batterie zu sparen, kann sich ein Gerät, das keinen Datenverkehr erwartet, in einen Ruhezustand begeben. In einem Ad hoc-Netz muss das Gerät für jeden Beacon aufwachen. In einem Infrastrukturnetz ist der Access Point über den jeweiligen Ruhezustand der Geräte informiert. Die Geräte wachen seltener auf, um einen Beacon abzuhören und zu erfahren, ob Daten für sie im Zwischenspeicher des Access Points bereitliegen.

Beim h-Standard wird die Sendeleistung automatisch je nach Empfangsqualität reguliert. Ausserdem kann bei Access Points des g- und h-Standards die Sendeleistung je nach abzudeckendem Gebiet reguliert werden. Innerhalb eines Standards hängt die tatsächlich abgestrahlte Leistung in erster Linie vom Datenverkehr ab. Wird von einem 100 mW-Access Point nur der Beacon ausgesendet, so beträgt die gemittelte Strahlungsleistung 0,5 mW. Werden jedoch viele Daten gesendet, so kann die abgestrahlte Leistung beinahe die maximal erlaubten 100 mW betragen.

Das von einer Antenne ausgesendete Signal nimmt mit der Distanz stark ab. Ausserdem kann das Signal durch Hindernisse wie Wände abgeschwächt oder reflektiert werden. Normale Reichweiten für einen 802.11b Sender mit 100 mW sind ca. 200 m im offenen Gelände und ca. 40 m in Gebäuden mit dünnen Wänden. Stahlbetonwände oder metallbedampfte Energiesparscheiben lassen die Strahlung praktisch nicht durch. Die Reichweite ist für Geräte mit dem h-Standard wegen der grösseren Sendeleistung im offenen Gelände grösser. Wegen der höheren Frequenz wird das Signal durch Wände jedoch stärker gedämpft, was zu einer reduzierten Reichweite in Gebäuden führt.

WLAN-Hotspots

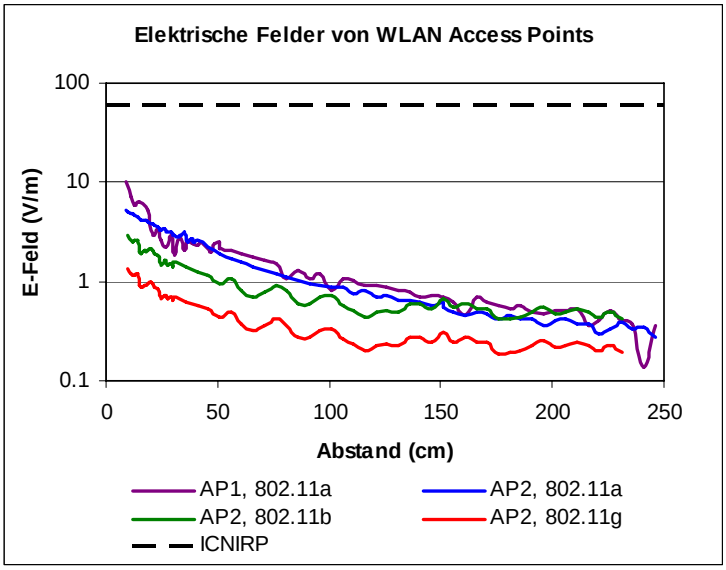
Ein Bereich, in dem der Internetzugang über WLAN zur Verfügung steht, wird als Hotspot bezeichnet. Hotspots können entweder öffentlich zugänglich sein (Bahnhöfe, Flughäfen etc.) oder nur einem eingeschränkten Nutzerkreis zur Verfügung stehen (Hotels). Der Zugang ins Internet bei Hotspots ist meist kostenpflichtig, es gibt aber auch Gratisangebote. Für die Versorgung in Gebäuden werden die Access Points typischerweise im Decken- oder Wandbereich – selten auch in Hohlböden – montiert, für die Aussenversorgung werden sie an der Aussenfassade oder auf dem Dach platziert. Falls an einem

Hotspot mehrere Access Points installiert sind, weisen diese zwischen einander einen Abstand von ca. 10 - 20 m auf.

Strahlenbelastung: Worst Case Szenarien

Immissionsmessungen

Im Auftrag des BAG wurden WLAN Access Points, PC-Karten und einen PDA der Standards 802.11a, b und g untersucht[9,10]. Es wurden die elektrischen Felder und die SAR-Werte bestimmt, immer unter Worst Case-Bedingungen mit maximaler Datenrate. Die elektrischen Felder wurden bei zwei verschiedenen Access Points, zwei verschiedenen PC-Karten und einem PDA gemessen (*Abbildung 4*). Gewisse WLAN-Geräte können mit verschiedenen Standards betrieben werden. So wurde beim Access Point 2 (*Abbildung 4*) der a-, der b- und der g-Standard ausgemessen. Vom h-Standard waren keine Geräte erhältlich, er ist jedoch unter Worst Case-Bedingungen mit dem a-Standard vergleichbar. Unter realen Bedingungen sollte die Strahlenbelastung durch den h-Standard kleiner sein, da dieser eine dynamische Sendeleistungsregulierung haben muss.



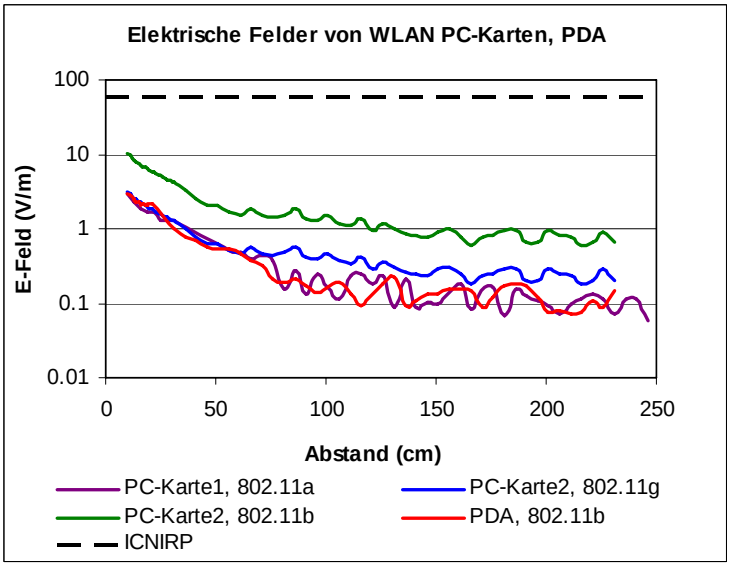


***Abbildung 4*:** *Elektrisches Feld (E-Feld) als Funktion des Abstandes für verschiedene WLAN Access Points, PC-Karten und PDA. Das Feld ist in einer logarithmischen Skala angegeben.*

Die elektrischen Felder nehmen mit dem Abstand zum Sender stark ab. Die Werte liegen immer unterhalb der ICNIRP-Grenzwertempfehlung von 61 V/m. Im Abstand von 20 cm schöpft keines der Geräte mehr als 10% der ICNIRP-Grenzwertempfehlung aus, bei 1 m nicht einmal 2,5%.

Die Immissionen von öffentlichen WLANs dürften etwa gleich gross sein wie die privater WLANs, da beide mit Sendern derselben Standards bestückt sind. In Tabelle 3 sind Werte von elektrischen Feldstärken von öffentlichen WLAN-Access Points zusammengefasst.

Tabelle 3 : *Elektrische Feldstärke von Access Points im öffentlichen Raum mit Sendeleistungen von 100/200 mW*[12]

Distanz zum Access Point (m)	elektrische Feldstärken (V/m)
1	0,7 – 3
2	0,4 – 1,5
5	0,1 – 0,7
10	0,05 – 0,4

Spezifische Absorptionsrate SAR

Zur Messung der SAR-Werte wurden die WLAN-Geräte an ein Körperphantom angebracht. In Tabelle 4 sind die SAR-Werte der Geräte zusammen gestellt. Da die Strahlenbelastung bei WLAN auch von der übermittelten Datenrate abhängt, sind diese auch aufgeführt. Es ist dabei zu beachten, dass die verschiedenen Standards verschiedene Datenübermittlungsmethoden haben, welche zu unterschiedlichen Strahlenbelastungen führen. Obwohl der g-Standard eine höhere Datenrate hat als der b-Standard, ist die Strahlenbelastung eher geringer als beim b-Standard.

Tabelle 4 : *SAR-Werte von Access-Points (AP), PC Karten und PDA*

802.11a		
Gerät	**Datenrate (Mb/s)**	**SAR (W/kg)**
AP 1	30	0,54
AP 2	6	0,18
AP 4	7,5	0,1
AP 5	28	0,36
PC-Karte 1	13,3	0,05
PC-Karte 2	13,3	0,07
PC-Karte 3	13,3	0,06

802.11b		
Gerät	**Datenrate (Mb/s)**	**SAR (W/kg)**
AP 3	6	0,44
AP 2	6	0,73
PC-Karte 4	6,3	0,43
PC-Karte 5	6	0,13
PDA	3,8	0,067

802.11g		
Gerät	**Datenrate (Mb/s)**	**SAR (W/kg)**
AP 3	26	0,25
AP 2	26	0,27
PC-Karte 4	21,5	0,11
PC-Karte 5	26	0,06

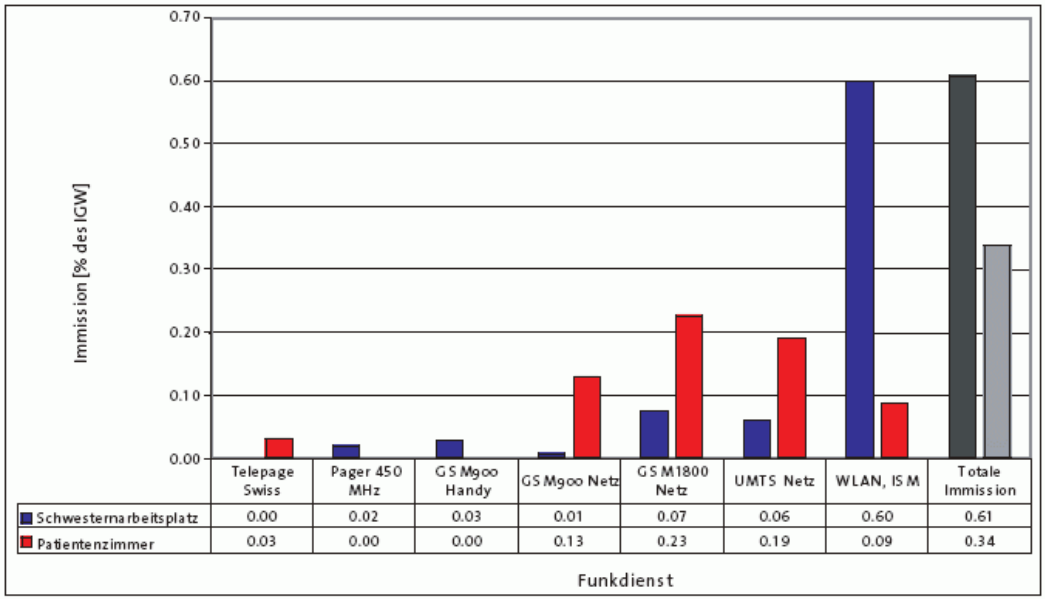
[12] „Elektrosmog in der Umwelt“, BUWAL, Bern 2005, Seite 54

Die SAR-Werte liegen alle unterhalb der ICNIRP-Grenzwertempfehlung von 2 W/kg (Kopf, Körper) bzw. 4 W/kg (Extremitäten). In der Realität spielen die SAR-Werte von Access Points wahrscheinlich keine grosse Rolle, da diese nicht in der Nähe des Körpers betrieben werden. PC-Karten oder der PDA dagegen können sehr wohl nahe am Körper betrieben werden.

Strahlenbelastung: Reale Szenarien

Immissionsmessungen

Immissionsmessungen während dem normalen WLAN-Betrieb wurden im Spital Thun durch Oertle et al.[13] durchgeführt. Das ganze Spital ist mit WLAN ausgerüstet, damit die elektronische Patientenakte auch am Patientenbett verfügbar ist. Die Messungen wurden an einem Schwesternarbeitsplatz und in einem Patientenzimmer durchgeführt. Zusätzlich zur normalen WLAN-Last wurde eine grosse Datei transferiert. Neben der WLAN-Strahlung wurde auch die Strahlung vom Mobilfunk- und Pager-Netz bestimmt.



	Telepage Swiss	Pager 450 MHz	GSMgoo Handy	GSMgoo Netz	GSM1800 Netz	UMTS Netz	WLAN, ISM	Totale Immission
Schwesternarbeitsplatz	0.00	0.02	0.03	0.01	0.07	0.06	0.60	0.61
Patientenzimmer	0.03	0.00	0.00	0.13	0.23	0.19	0.09	0.34

Abbildung 5: *(Quelle: [13]) Elektrische Feldstärken verschiedener Funkdienste im Vergleich zu den Immissionsgrenzwerten (IGW, entspricht den ICNIRP-Grenzwertempfehlungen).*

Am Schwesternarbeitsplatz, mit Sichtkontakt zum Access Point, trägt die WLAN-Strahlung am stärksten zur Strahlenbelastung bei und schöpft 0,6 % der ICNIRP-Grenzwertempfehlung für die Allgemeinbevölkerung aus. Im Patientenzimmer überwiegt die Mobilfunkstrahlung. Die Gesamtimmission im hochfrequenten Bereich liegt unterhalb eines Prozents der ICNIRP-Grenzwertempfehlung. In Abbildung 5 wird deutlich, dass beim Vorhandensein einer nahen Strahlungsquelle, wie dem WLAN im Schwesternzimmer, die Gesamtimmission zum grössten Teil von dieser stammt.

Im Auftrag des deutschen Bundesamtes für Strahlenschutz werden momentan durch die ARC Seibersdorf research GmbH Simulationen und Immissionsmessungen von WLAN-Hotspots durchgeführt[14]. In einem Café, ausgerüstet mit einem Access Point unter der Theke und zwei Laptops, wurden während dem Herunterladen von Daten Messungen an verschiedenen Orten im Raum durchgeführt. Damit die Messwerte mit dem ICNIRP-Referenzwert (siehe Kapitel 3.2 und Tabelle 5) verglichen werden konnten, wurde räumlich über den ganzen Körper und zeitlich über sechs Minuten gemittelt. Der höchste Wert von knapp 2 V/m wurde in der Nähe des Access Points hinter der Theke gemessen, was 3,2 % der IC-

[13] Oertle M et al. Elektromagnetische Felder im Akutspital: Wireless-LAN & Co als Risiko?. Praxis 2006; 95:933-941.

[14] Schmid G. et al. Bestimmung der realen Feldverteilung von hochfrequenten elektromagnetischen Feldern in der Umgebung von Wireless LAN-Einrichtungen (WLAN) in innerstädtischen Gebieten. 2. Zwischenbericht zum Forschungsvorhaben FM 8826

NIRP-Grenzwertempfehlung ausschöpft[15]. In diesem konkreten Fall könnte das Feld einfach reduziert werden, indem der Access Point an der Decke montiert würde.

2.3 Wireless Metropolitan Area Networks (WMAN), WiMAX

Anwendungen und Standards

Mit drahtlosen, stadtweiten Netzwerken (WMAN) sollen drahtlose Netzwerke über den lokalen Bereich hinaus erweitert werden. Im Gegensatz zu den drahtlosen lokalen Netzwerken (WLAN) mit Reichweiten von 40 – 200 m können WMAN Netzwerke mit Reichweiten von mehreren Kilometern ganze Städte abdecken.

Der WMAN-Standard IEEE 802.16 ist sehr offen gehalten und umfasst Frequenzen von 2 - 66 GHz. Um der Gefahr von zu unterschiedlichen Implementierungen und einem zersplitterten Angebot mit entsprechend höheren Herstellungskosten entgegenzuwirken, wurde von System- und Komponentenherstellern das WiMAX-Forum (WiMAX: Worldwide interoperability for microwave acess) gegründet. Es wählt aus den vielen Optionen, die der Standard 802.16 bietet, verschiedene Kombinationen aus und stellt sie als so genannte Profile zur Verfügung. Zurzeit sind von WiMAX drei Profile vorgesehen, die sich vor allem im Frequenzbereich unterscheiden (Stand August 04): Konzessionspflichtig: 2,5 GHz und 3,5 GHz, konzessionsfrei: 5,8 GHz. Je nach Interesse der WiMAX-Mitglieder können bei Bedarf weitere Profile definiert werden. Erste Geräte (Basisstationen und Endgeräte) sind im Januar 2006 von WiMAX zertifiziert worden. Mögliche Anwendungen der WiMAX sind auf der Abbildung *6* skizziert.

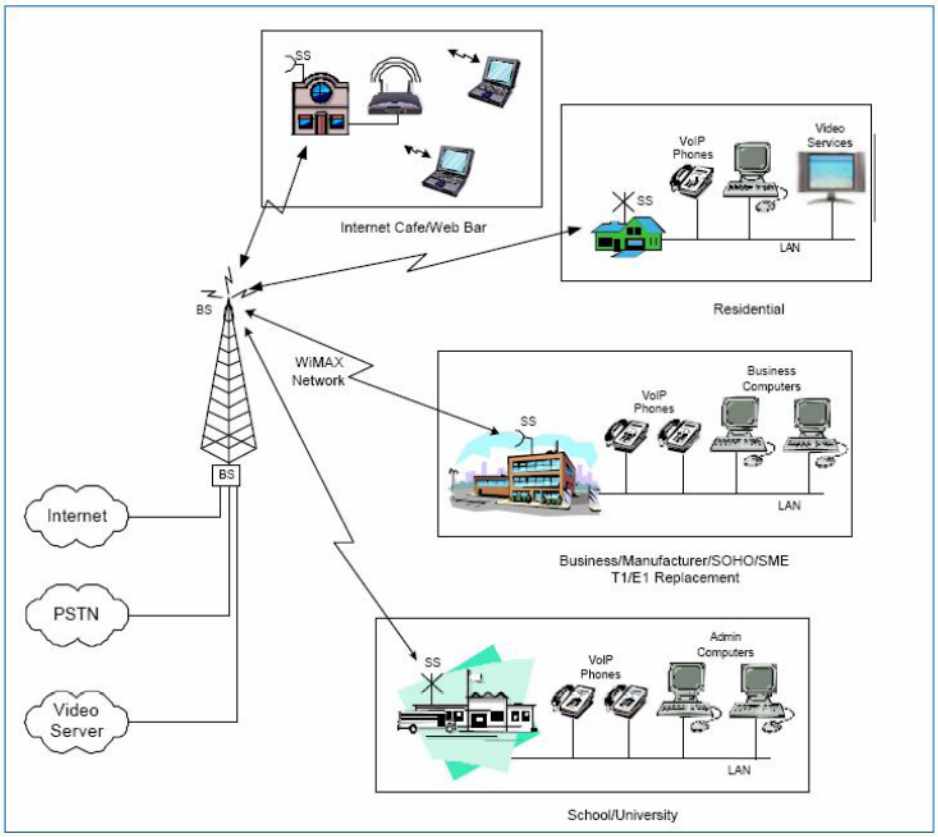


Abbildung 6: *Mögliche Anwendungen der WiMAX. Quelle:* [16]

[15] In der Publikation wird die Leistungsflussdichte angegeben, der Wert für das elektrische Feld ist daraus berechnet. Da die beiden Werte nicht linear zusammenhängen, ist auch die Grenzwertausschöpfung in Prozent unterschiedlich.

Konzessionen in der Schweiz

Am 07.06.2006 hat die Eidgenössische Kommunikationskommission (ComCom) eine WiMAX-Konzession bei 3,5 GHz an Swisscom Mobile vergeben[17]. Die Konzessionärin ist verpflichtet, bis spätestens am 31. Dezember 2007 den kommerziellen Betrieb aufzunehmen und bis Ende 2009 mindestens 120 Sende-/Empfangseinheiten zu betreiben. Beim Netzaufbau sind die Vorgaben der Verordnung über den Schutz vor nichtionisierender Strahlung (NISV, vgl. Kap. 5.3) einzuhalten.

Funktionsweise und Strahlenbelastung

Bei WiMAX handelt es sich um einen Breitbandanschluss (Broadband Wireless Access, BWA), welcher eine grössere Datenrate ermöglicht und deswegen primär für einen drahtlosen Zugang zum Internet vorgesehen ist (anstelle von Kabelmodem oder ADSL). Die Dienste sind vor allem in Gegenden sinnvoll, die nicht durch Kabel erschlossen sind. Die maximale Datenrate ist jedoch nur auf kürzere Strecken möglich. Sie ist von der verwendeten Kanalbandbreite abhängig und kann unter optimalen Bedingungen bis 75 Mbit/s bei einem 20 MHz Kanal betragen. Bei grösseren Distanzen sinkt jedoch die Datenrate. Je nach Konfiguration des Systems können die Distanzen von bis 30 - 40 km mit reduzierter Datenrate überbrückt werden.

Bei den heutigen Standards handelt es sich um feste Punkt-zu-Mehrpunkt Dienste. Bei der fixen Verwendung wird beim Kunden eine Sende-Empfangsanlage an der Aussenfassade des Hauses angebracht (Abbildung 7). Im Haus können die Endgeräte an einer Box angesteckt werden.

Abbildung 7 : *WiMAX Sende-Empfangsanlagen an Hausfassaden oder Dächern. Quelle:*[18]

Um den Endkunden die geplanten hohen Datenraten mit entsprechenden Kapazitäten anbieten zu können, werden ähnliche Netzstrukturen notwendig sein wie sie die heutigen Mobilfunknetze aufweisen. Dies bedeutet, dass eine grössere Anzahl Basisstationen aufgebaut werden muss. Obwohl in den konzessionierten Bändern Sendeleistungen bis 3 kW EIRP theoretisch möglich sind, ist die effektiv notwendige Sendeleistung stark von der Netzstruktur abhängig und wird durch den Betreiber festgelegt. Basisstationen mit Sendeleistungen von mehr als 6 W ERP, müssen den Anlagegrenzwert der NISV (6 V/m) einhalten. Es ist zu erwarten, dass WiMAX-Basisstationen Sendeleistungen von mehr als 10 W ERP aufweisen werden. Die Grenzwerte für WiMAX-Basisstationen entsprechen denjenigen für Mobilfunkbasisstationen.

WiMAX Netze befinden sich in der Aufbauphase, ob flächendeckende Netze erstellt werden ist aus heutiger Sicht fraglich. Die Grösse der Immissionen hängt stark vom entsprechenden Netzaufbau ab. Es kann aber davon ausgegangen werden, dass die Werte in ähnlicher Grössenordnung wie in entsprechenden Mobilfunknetzen liegen werden.

---

[16] www.wimaxforum.org
[17] http://www.bakom.ch/dokumentation/medieninformationen/00471/index.html?lang=de&msg-id=5474
[18] www.wimaxxed.at

2.4 Weiterentwicklung

Zurzeit herrscht sowohl bei der Erstellung neuer Telekommunikationsstandards als auch bei der Entwicklung und Herstellung von Geräten mit entsprechenden Sende-Empfangseinrichtungen ein reges Treiben. Für alle Dienste wird an einer Steigerung der Datenrate gearbeitet.

In Zukunft werden Kabelverbindungen zwischen Geräten mehr und mehr durch Bluetooth ersetzt werden. Dies ist auch für medizinische Anwendungen zur Übermittlung von Vitaldaten interessant. Mit Bluetooth kann die Anzahl Kabel am Patientenbett reduziert werden, die Patienten können sich freier bewegen. Die Reichweite von Bluetooth kann durch Multihopnetze vergrössert werden, bei denen das Signal zwischen Sender und endgültigem Empfänger durch andere Bluetooth-Sender weitergeleitet wird[19].

WLAN wird unter anderem dahingehend weiterentwickelt, dass auch zeitkritische Daten übertragen werden können, bei denen die Übertragungsqualität und Störsicherheit wichtig ist, z.B. um über das Internet zu telefonieren (voice over IP) oder um Filme und Musik in der Wohnung zu übermitteln.

Bei WiMAX ist vorgesehen, in Zukunft auch nomadische und mittelfristig mobile Dienste zuzulassen (IEEE 802.16e). Unter nomadischem Dienst versteht man die Nutzung eines Endgerätes an einem beliebigen Ort unter der Bedingung, dass der Standort des Endgerätes während der Nutzung ortsfest bleibt.

Neu werden auch WiMAX kompatible Chips hergestellt, die standardmässig in Laptops eingebaut werden können und somit in WiMAX versorgten Gebieten, mit grösserer Reichweite als die heutigen WLANs, drahtlosen Zugang zum Internet ermöglichen. Es ist anzunehmen, dass bei diesen Geräten auch mit höherer Strahlenbelastung zu rechnen ist.

Eine besondere Problematik liegt im Frequenzmanagement. Für WLAN-Anwendungen stehen heute im 5 GHz Band Frequenzen zur Verfügung, dabei sind Sendeleistungen bis 1 W möglich. Der höhere Frequenzbereich (ab 5,725 GHz) wird in der Schweiz momentan vorwiegend durch das Militär genutzt. Es sind Bestrebungen im Gang, diesen Bereich für BWA (Broadband Wireless Access) mit Sendeleistungen bis zu 4 W freizugeben. Es handelt sich um ein ISM-Band, d.h. darin dürfen auch verschiedene andere Anwendungen des Kurzstreckenfunks konzessionsfrei betrieben werden. Dem Vorteil der Konzessionsfreiheit stehen die Nachteile gegenseitiger Störung verschiedener Dienste und die geringe Sendeleistung gegenüber. Unter der Annahme, dass eine Koexistenz mit anderen Diensten möglich ist, könnten sich in diesem Band BWA-Anwendungen ausbreiten.

[19] Andreas Kuntz et al. ScatterNetz-Routing (SNR) - Multihopkommunikation für medizinische Bluetooth Ad Hoc Netzwerke. Proceedings der Gemeinsamen Jahrestagung der Deutschen, Österreichischen und Schweizerischen Gesellschaft für Biomedizinische Technik, 6.-9. September 2006, Zürich.

3. Gesundheitliche Auswirkungen

3.1 Thermische Auswirkungen hochfrequenter EMF

Die einzigen wissenschaftlich nachgewiesenen gesundheitlichen Auswirkungen hochfrequenter Strahlung sind thermische Effekte. Hochfrequente EMF dringen in den Körper ein und können das Gewebe erwärmen, indem die aufgenommene Strahlungsenergie in Wärme umgewandelt wird. In vielen Tierstudien wurde gezeigt, dass eine Teil- oder Ganzkörpererwärmung, welche zu einer Temperaturerhöhung von mehr als 1°C führt, irreversible Gewebeschädigungen verursachen kann. Auch die Daten über Reaktionen bei Menschen, welche bei Laboruntersuchungen an freiwilligen Probanden oder epidemiologischen Studien bei Arbeitern mit Radar oder Diathermiegeräten erzeugt wurden, zeigen deutlich, dass eine Gewebeerwärmung von mehr als 1°C Gewebeschädigung und fieberähnliche Reaktionen auslösen kann.

Die entsprechende dosimetrische Grösse für diese thermischen Effekte ist die pro Zeiteinheit und Körpergewicht im Körper absorbierte Energie, die *spezifische Absorptionsrate SAR* (in W/kg). Obwohl es unterschiedliche thermische Effekte gibt und die thermische Sensibilität verschiedener Gewebe stark variiert, geht aus allen Experimenten und Berechnungen eindeutig hervor, dass erst eine 30-minütige Exposition mit einer Ganzkörper-SAR von mehr als 4 W/kg zu einer Temperaturerhöhung von 1°C führen kann. Unter diesen Bedingungen vermögen nämlich die wärmeregulierenden Mechanismen im Körper (z.B. Schwitzen) die zusätzliche Wärme nicht mehr abzuführen.

Neben diesen thermischen Effekten können sehr stark gepulste EMF mit einer Pulsdauer von weniger als 30 μs und Frequenzen von 300 MHz bis 6 GHz Hörwahrnehmungen verursachen.

3.2 Internationale Grenzwerte für hochfrequente EMF (Schutz vor thermischen Auswirkungen)

Bei den hochfrequenten EMF sind die thermischen Effekte die einzigen, wissenschaftlich kausal nachgewiesenen Auswirkungen. Wie im vorherigen Kapitel erwähnt, handelt es sich dabei um akute Effekte, die ab einem SAR-Schwellenwert von 4 W/kg eintreten. Diese Effekte und der Schwellenwert bilden den Ausgangspunkt zur Festlegung der Grenzwerte.

Die meisten Länder haben basierend auf den Empfehlungen der ICNIRP (International Commission for Nonionizing Radiation Protection) gesetzliche Grenzwerte verankert. Die ICNIRP überprüft periodisch wissenschaftliche Publikationen bezüglich der physikalischen Charakteristika von EMF-Quellen und deren biologischen und gesundheitlichen Auswirkungen. Sie bewertet diese und gibt Schutzempfehlungen ab[20].

Die Labordaten wie auch begrenzte Versuche am Menschen zeigen, dass die wärmeregulierende Fähigkeit des Körpers einerseits individuell stark variiert und anderseits auch von verschiedenen weiteren Faktoren (z.B. Umgebungstemperatur, Konsum von Alkohol usw.) abhängig ist. Deswegen wendet die ICNIRP zur Berechnung des Grenzwertes einen Sicherheitsfaktor von 10 für beruflich exponierte Personen und von 50 für die allgemeine Bevölkerung an.

Diese Grenzwerte, welche für SAR als dosimetrische Grösse definiert sind, werden als Basisgrenzwerte bezeichnet. Weil die SAR nicht einfach zu bestimmen ist, wurden zur Expositionsbeurteilung einfacher zu messende Referenzgrenzwerte eingeführt. Sie gelten für eine gleichmässige Exposition des ganzen Körpers mit elektromagnetischen Feldern. Die Referenzgrenzwerte sind konservativ von den Basisgrenzwerten abgeleitet, ein Einhalten der Referenzgrenzwerte bedeutet in jedem Fall auch das Einhal-

[20] http://www.icnirp.de/

ten der Basisgrenzwerte. Die für drahtlose Netzwerke relevanten Basisgrenzwerte und Referenzwerte sind in Tabelle 5 angegeben.

Tabelle 5: *ICNIRP-Basisgrenzwerte und Referenzwerte für beruflich exponierte Personen und Allgemeinbevölkerung im Frequenzbereich 10 MHz - 10 GHz.*

Exponierte Person	**Durchschnittliche Ganzkörper SAR (W/kg)**	**elektrisches Feld (V/m)** Referenzwert für Ganzkörper SAR	**Lokaler SAR Kopf und Rumpf (W/kg)**	**Lokaler SAR Gliedmassen (W/kg)**
Beruflich exponierte Personen	0,4	137	10 (0,1 W/10g)	20 (0,2 W/10g)
Allgemeinbevölkerung	0,08	61	2 (0,02 W/10g)	4 (0,04 W/10g)

Diese Grenzwerte sind auch in der Schweiz gültig. Wie die durchgeführten Messungen zeigen (Kapitel 2) liegen die Expositionen durch heutige Netzwerke weit unterhalb der Grenzwerte.

3.3 Erforschung nicht-thermischer Effekte hochfrequenter EMF

Neben diesen nachgewiesenen thermischen Auswirkungen hochfrequenter EMF gibt es Hinweise auf andere Auswirkungen bei schwächeren Expositionen, unterhalb der Grenzwerte. Die Untersuchungen wurden vor allem im Zusammenhang mit Mobiltelefonie durchgeführt. Festgestellt wurde beispielsweise, dass hochfrequente EMF von Mobiltelefonen schwache Veränderungen der Hirnaktivität verursachen können. Unklar ist aber, ob und inwieweit diese Veränderungen die Gesundheit beeinflussen. Gegenwärtig lässt sich kein Zusammenhang zwischen einer häufigen Benutzung des Mobiltelefons und dem Auftreten von Hirntumoren herstellen. Auch der Einfluss der Strahlung von Mobilfunkantennen auf die Befindlichkeit von Anwohnerinnen und Anwohnern (Schlafstörungen, Kopfschmerzen und andere unspezifische Symptome) ist wissenschaftlich nicht nachgewiesen. Offen sind weiterhin die Fragen bezüglich einer postulierten Elektrosensibilität bestimmter Personen (gesundheitliche Beeinträchtigungen, die von den Betroffenen auf den Einfluss von EMF zurückgeführt werden) sowie einer allfälligen besonderen Empfindlichkeit von Kindern.

Evaluationen aller vorhandenen Daten über gesundheitliche Auswirkungen hochfrequenter EMF sind bei der IARC (International Agency for Research on Cancer) für das Krebsrisiko und bei der WHO allgemein bis 2008 geplant. Die Resultate werden in der IARC-Monographie bzw. den WHO-Environmental Health Criteria erscheinen. Parallel dazu arbeitet die ICNIRP an einer Neubeurteilung der wissenschaftlichen Basis und eventuell neuen Grenzwertempfehlungen.

3.4 Spezifische Problematik drahtloser Netzwerke

Bis heute wurden keine Studien durchgeführt, welche spezifisch die biologischen und gesundheitlichen Wirkungen der Strahlung von drahtlosen Netzwerken wie z.B. WLAN und Bluetooth untersucht haben.
Es werden jedoch allgemeine Studien zu nichtthermischen Effekten hochfrequenter EMF durchgeführt, welche es möglicherweise in Zukunft erlauben, auch Schlüsse über gesundheitliche Auswirkungen drahtloser Netzwerke zu ziehen.

Eine gesundheitliche Beurteilung drahtloser Netzwerke wird dadurch erschwert, dass die Expositionen bei verschiedenen Nutzungen komplett andere Eigenschaften aufweisen können, es gibt keine typische Exposition durch drahtlose Netzwerke. Stärkere lokale Expositionen treten dort auf, wo Sendeeinheiten sehr nah am Körper positioniert sind. Da die Stärke und Intensität der Strahlung stark distanzabhängig ist, sind die Ganzkörperexpositionen durch weiter entfernte Access-Points wiederum sehr schwach.

Zudem verläuft die technologische Entwicklung drahtloser Netzwerke rasant. Die Technologien drahtloser Netzwerke sind kurzlebig, werden schnell ersetzt und können innerhalb von 2 - 3 Jahren veralten. Neue Technologien weisen teilweise komplett andere Strahlungscharakteristika auf als Vorgängertechnologien. Wissenschaftliche Studien über gesundheitliche Wirkungen von spezifischen Technologien laufen deshalb Gefahr, dass die Technologien nach Studienabschluss gar nicht mehr bestehen.

Im Weiteren gibt es immer mehr multifunktionale Geräte (wie z.B. der untersuchte PDA), in denen verschiedene Dienste wie WLAN, Bluetooth und Mobilfunk kombiniert sind und zum Teil auch gleichzeitig genutzt werden können.

In Zukunft könnte die Strahlenbelastung grösser werden, da immer mehr Arbeitsplätze und Haushalte mit WLAN ausgestattet werden und zudem bei neueren Technologien die maximale Sendeleistung grösser ist. Es werden auch immer mehr flächendeckende WLANs über ganze Städte oder Teile von Städten[21] eingeführt. Zunehmen könnten auch Expositionen durch mehrere Geräte mit unterschiedlichen Strahlungscharakteristiken.

3.5 Indirekte Auswirkungen, elektromagnetische Verträglichkeit

Als indirekte Auswirkungen werden gesundheitliche Auswirkungen bezeichnet, welche nicht direkt durch die Strahlung, sondern durch Störung und somit Fehlfunktion eines, meist medizinischen, Gerätes verursacht werden. Die Funktionsresistenz elektromagnetischer Geräte gegenüber unterschiedlichen EMF wird als elektromagnetische Verträglichkeit (EMV) bezeichnet (siehe auch Kapitel 5.4.).

Im Prinzip sind zwei Störungsmuster unterscheidbar:

- Die Strahlung der drahtlosen Netzwerke stört die Funktion anderer elektronischer Apparate.
- Die drahtlosen Netzwerke werden durch elektrische Geräte, die im Mikrowellenbereich arbeiten, gestört. Die Strahlung dieser Geräte überdeckt die Strahlung der drahtlosen Netzwerke, was zu deren Fehlfunktion führen kann.

Bezüglich elektromagnetischer Beeinflussung von Medizinprodukten durch drahtlose Netzwerke gibt es einige wenige Studien, welche medizinische Geräte in Spitälern und elektronische Körperbeihilfen und Implantate betreffen.

Störung von Herzschrittmachern und Defibrillatoren durch WLAN[22]
Die Störempfindlichkeit von uni- und bipolaren Herzschrittmachern und Defibrillatoren durch WLAN wurde mit einem PDA untersucht, der bei maximaler Leistung von 100 mW direkt auf die einzelnen (nicht eingepflanzten) Implantate sendete. Es konnte keine Beeinflussung der Implantate festgestellt werden. Die Autoren empfehlen, die Studie mit Implantatträgern zu wiederholen, um in einer realen Situation die Resultate bestätigen zu können. Gemäss der Produktenorm müssen Herzschrittmacher und Defibrillatoren bis 2,5 GHz störfest sein. Es wäre deshalb sehr wichtig, die Untersuchung mit WLAN-Geräten des a- oder h-Standards bei 5 GHz durchzuführen.

Störung von anderen Geräten in Spitälern durch WLAN[23]
Eine Studie hat aufgezeigt, dass die meisten untersuchten Geräte immun gegen die Strahlung eines WLAN sind. Gestört wurden Ultraschall-Doppler-Geräte zur Überwachung der Herzfunktionen. Dabei wurden durch die WLAN-Strahlung zusätzliche akustische Interferenzen generiert, was möglicherweise zu Fehlinterpretationen des normalen Herzschlagrhythmus des Patienten führen kann.

[21] z.B. St.Gallen (www.openwireless.ch) oder Luzern („surf-on-the-fly“)
[22] Tri JL, Trusty JM, Hayes DL. Potential for Personal Digital Assistant interference with implantable cardiac devices. Mayo Clin.Proc. 2004;79:1527-30.
[23] Wallin MK, Marve T, Hakansson PK. Modern wireless telecommunication technologies and their electromagnetic compatibility with life-supporting equipment. Anesth.Analg. 2005;101:1393-400.

In einer Studie[24] fand sich ein Einfluss der WLAN im 2,45 und 5,2 GHz-Bereich auf Verdünnungssysteme und einen Ventilator. Die Autoren empfehlen, bei der Einführung von WLAN in Spitälern individuell die Immunität der verwendeten Apparate zu überprüfen.

In einer Studie[25] wurde der Einfluss eines g-Standard WLANs auf sechs verschiedene medizinische Geräte untersucht. Dabei wurden Abweichungen bei einer Infusionspumpe (2,4% Abweichung im Bolusvolumen) und einem Nerven- und Muskelstimulator (bis 10% Abweichung) gemessen. Die Änderungen waren aber kleiner, als dies der Produktestandard für diese Geräte zulässt.

Störung von elektronischen Geräten in Spitälern durch Bluetooth[26]
Die Beeinflussung elektronischer Geräte in Spitälern (Intensivstation oder Operationsraum) durch Bluetooth wurde in einer Studie untersucht. Von den getesteten Geräten wurde keines durch die Bluetooth-Strahlung beeinflusst. Die Autoren kommen zum Schluss, dass die Bluetooth-Technologie dazu beitragen könnte, die Kabelverbindungen um Patienten zu reduzieren. Sie empfehlen aber, die Funktion von Bluetooth-Applikationen in Spitälern mit robusten Tests abzusichern.

Störung von WLAN durch andere Geräte[27]
In einer Studie wurde die Störung von WLANs durch typische im Mikrowellenbereich arbeitende medizinische Geräte (Mikrowellenöfen, Elektrochirurgie, Telemetriesysteme) untersucht. Es wurde gezeigt, dass ein WLAN insbesondere dann überdeckt wird, wenn Mikrowellenöfen in der Nähe der Access-Points aufgestellt sind. Dies hat die Empfangsbedingungen sowie die Datenübertragungsraten verschlechtert. Die Autoren kommen zum Schluss, dass industrielle Mikrowellenöfen in Spitälern nicht neben den Access-Points eines WLAN zu positionieren sind.

Störung von Bluetooth durch andere Geräte
In der Studie zur Störung von elektronischen Geräten durch Bluetooth wurde auch die Störung von Bluetooth durch 44 andere Geräte ausgetestet. Es konnte keine Beeinflussung der Bluetooth-Verbindung gezeigt werden. Die Autoren machen jedoch darauf aufmerksam, dass Bluetooth-Verbindungen durch WLANs gestört werden können.

3.6 Zusammenfassung

Gemäss heutigem Kenntnisstand und aufgrund vorhandener Expositionsmessungen ist die durch drahtlose Netzwerke erzeugte hochfrequente Strahlung zu schwach, um durch Absorption über eine Erhöhung der Temperatur nachweisbare, akute gesundheitliche Wirkungen auslösen zu können. Langzeit- und nicht-thermische Auswirkungen sind zurzeit noch ungenügend erforscht. Aus den vorhandenen Studien über Auswirkungen hochfrequenter EMF im Niedrigdosisbereich, unterhalb der geltenden Grenzwerte, kann im Moment keine gesundheitliche Gefährdung durch drahtlose Netzwerke abgeleitet werden. Dies gilt auch für Kinder und Jugendliche.

Obwohl die einzelnen Geräte drahtloser Netzwerke relativ schwach strahlen, könnten stärkere lokale Strahlungen in Zukunft aus folgenden Gründen zunehmen: Zunehmende Dichte von Access-Points in Büroumgebungen, Verwendung von Access-Points in der Nähe von Arbeitsplätzen (z.B. Tischgeräte),

[24] Hanada E et al. Negligible electromagnetic interaction between medical electronic equipment and 2.4 GHz band wireless LAN. J Med Syst. 2002;26:301-8.
[25] Schröttner J et al. Are electro medical devices influenced by electromagnetic WLAN emissions? Proceedings der Gemeinsamen Jahrestagung der Deutschen, Österreichischen und Schweizerischen Gesellschaft für Biomedizinische Technik, 6.-9. September 2006, Zürich.
[26] Wallin MK, Wajntraub S. Evaluation of Bluetooth as a replacement for cables in intensive care and surgery. Anesth.Analg. 2004;98:763-7
[27] Tan KS, Hinberg I. Effects of a wireless local area network (LAN) system, a telemetry system, and electrosurgical devices on medical devices in a hospital environment. Biomed.Instrum.Technol. 2000;34:115-8.

zunehmende Verwendung von funkvernetzten Laptops an Arbeitsplätzen und im Privatbereich und die Verwendung von Standards mit höherer Datenrate, grösseren Reichweiten und höheren Sendeleistungen.

Aufgrund dieser Entwicklungen und der noch ungenügenden Datenlage bezüglich Gesundheitsrisiken besteht bei drahtlosen Netzwerken Forschungsbedarf, insbesondere in folgenden Bereichen:

- Bestimmung und Überwachung der Expositionen zukünftiger drahtloser Netzwerktechnologien. Die Tendenz bei drahtlosen Netzwerktechnologien geht in Richtung höherer Leistungen, die für eine grössere Reichweite und einer grösseren Datenrate benötigt werden. Hauptaugenmerk sollte dabei auf körpernahe Expositionen gelegt werden (Laptops, Bluetooth-USB-Stecker-Antennen, PDAs etc.), sowie auf kombinierte Expositionen.
- Gesundheitliche Auswirkungen von Teilkörperexpositionen typisch für Anwendungen bei drahtlosen Netzwerken (anders als Kopfexposition beim Mobiltelefon).
- Effekte nicht kontinuierlicher (gepulster) Strahlung mit Charakteristiken typisch für drahtlose Netzwerke.
- Strahlenempfindlichkeit von Kindern und Jugendliche und mögliche Auswirkungen drahtloser Netzwerke auf diese.

Bezüglich der Verwendung von drahtlosen Netzwerken in Spitälern besteht eine zu kleine Wissensbasis. Falls drahtlose Netzwerke in Spitälern verwendet werden, muss das Funktionieren der in den bestrahlten Bereichen verwendeten Medizinalgeräte sowie die Sicherstellung der Verbindungen über die Funkverbindung im Einzelfall rigoros geprüft werden. Die meisten EMV-Untersuchungen von Medizinprodukten wurden mit WLAN des b- oder g-Standards durchgeführt. Es sollten auch Untersuchungen mit WLAN im 5-GHz-Bereich durchgeführt werden, da diese nun auch vermehrt eingesetzt werden. Diese Sicherheitsaspekte sind in jedem Fall den Vorteilen einer Verwendung drahtloser Netzwerke voranzustellen.

4. Datensicherheit

4.1 Grundlegende Gefahren

Neben den bekannten Vorteilen haben drahtlose Technologien auch gewisse Nachteile, unter anderem im Bereich der Daten- oder Informationssicherheit. Die Informationssicherheit bzw. -unsicherheit ist bei allen Kommunikationssystemen ein Thema. Bei drahtlosen Netzwerken sind jedoch die Probleme im Vergleich zu drahtgebundenen Netzwerken verschärft. Nehmen wir das Beispiel des Abgreifens von Internetdaten. Wenn man an einem drahtgebundenen Internetanschluss arbeitet, gibt es einen bestimmten Kreis von Personen, die den Datenverkehr überwachen können, z. B. das technische Personal von Internetanbietern und anderen Netzbetreibern auf dem Übertragungsweg, Kriminelle mit physischem Zugang zur Netzinfrastruktur und Strafverfolgungsbehörden im In- und Ausland. Dies ist zwar ein beschränkter möglicher Lauscherkreis, aber man würde trotzdem lieber vermeiden, dass diese Personen sensible Daten wie e-Banking-Informationen einsehen können. Wenn der Internetanschluss über ein WLAN läuft, besteht eine erhöhte Gefahr, dass der Verkehr überwacht wird. Der Lauscherkreis wird in diesem Fall um alle Leute erweitert, die sich innerhalb der Reichweite des WLAN (unter Umständen in einem Umkreis von mehreren hundert Metern) aufhalten. Der drahtlose Internetanschluss ist in diesem Sinn unsicherer als der drahtgebundene. Man ist jedoch in beiden Fällen gut beraten, seine sensiblen Daten auf dem Weg durch das Internet zu schützen.

Die erhöhte Gefahr bei drahtlosen Netzwerken ist darauf zurückzuführen, dass man die Ausbreitung der Funksignale nicht nach Belieben einschränken kann. In vielen Fällen ist eine möglichst weite Ausbreitung des Funksignals auch erwünscht. Das Funksignal kann von einem Angreifer empfangen und verarbeitet werden. Ein Angreifer kann auch Funksignale für seine Zwecke in das Netzwerk einspeisen. Durch den Einsatz von speziellen Ausrüstungen kann ein Angriff auch aus einer Entfernung, die viel grösser ist als die übliche Betriebsreichweite des angegriffenen Systems, durchgeführt werden.

4.2 Informationssicherheit

Die Informationssicherheit wird oft in folgende vier Themen unterteilt: Vertraulichkeit, Authentisierung, Integrität, Verfügbarkeit. All diese Aspekte sind von der erhöhten Gefahr durch drahtlose Netzwerke betroffen. Im folgenden Abschnitt wird näher auf sie eingegangen.

Vertraulichkeit

Vertraulichkeit der Informationen bedeutet, dass die Informationen nicht von Unbefugten abgefangen bzw. überwacht werden. Sie ist besonders wichtig bei der Übertragung von schützenswerten Daten, wie z.B. des e-Banking. Ein besonderes Problem in diesem Bereich ist, dass das Mitschneiden (Aufzeichnen, Aufnehmen) in der Regel ein passiver Angriff ist und nicht direkt entdeckt werden kann. Beispiele einer Verletzung der Vertraulichkeit bei drahtlosen Systemen sind:

- Ein Telefongespräch an einer Anlage, bei der keine Verschlüsselung implementiert ist, wird von einem Angreifer in der Nachbarschaft aufgenommen, verarbeitet und abgehört.
- Die Signale einer drahtlosen PC-Tastatur werden von einem Angreifer aufgenommen und die Tastenschläge dekodiert ('keystroke logging'). Die Arbeit am PC kann rekonstruiert werden, Passwörter erfahren werden usw.
- Eine Firma baut ein drahtloses Lokalnetzwerk (WLAN) in ihren Geschäftsräumen. Ein Angreifer auf einem nahe gelegenen Parkplatz kann mit einem entsprechend ausgerüsteten Laptop den Verkehr auf diesem Netzwerk überwachen, selbst wenn im Netz die üblichen im Access Point eingebauten Sicherheitsmechanismen (z. B. WEP-Verschlüsselung, MAC-Filter) benutzt werden. Die dazu notwendigen Hacker-Anwendungen sind auf dem Internet frei verfügbar.

Authentisierung

Authentisierung soll die Identitäten von berechtigten kommunizierenden Instanzen bestätigen bzw. die Kommunikation für nicht berechtigte verunmöglichen. Eine Authentisierung kann für verschiedene Zwecke eingesetzt werden, z. B. für die Benutzung eines Netzwerks, die Benutzung einer Anwendung, den Zugriff auf Daten. Wenn der Authentisierungsmechanismus Sicherheitslücken aufweist, kann ein Angreifer auf Ressourcen zugreifen, obwohl er nicht dazu berechtigt ist. Beispiele eines Versagens der Authentisierung sind:

- Durch Abhören eines WLAN und gezieltes Einspeisen von bestimmten falschen Meldungen kann ein Angreifer die Identität eines berechtigten Benutzers im Netzwerk übernehmen und mit seinen Berechtigungen handeln.
- Ein Angreifer montiert im Abdeckungsgebiet eines WLAN einen fremden Access Point mit verstärktem Signal, um den Verkehr auf sich zu lenken und Authentisierungsdaten von Benutzern zu erhalten.
- Bei einem Bluetooth-Netz wird das Gerät und nicht der Benutzer authentisiert. Wenn ein Gerät in die Hände eines Angreifers fällt, geniesst er die gleichen Berechtigungen im Netz wie der echte Besitzer des Geräts.

Integrität

Integrität ist die Bestätigung, dass die übertragenen Daten vollständig und unverändert am Ziel ankommen. Dies kann aus verschiedenen Gründen wichtig sein, z. B. bei einem Vertrag aus rechtlichen oder bei wissenschaftlichen Daten aus wissenschaftlichen Gründen. Drahtlose Technologien sind anfällig für solche Angriffe, weil sie das Mitschneiden echter Daten und das Einspeisen veränderter Daten erleichtern. Beispiele einer Verletzung der Integrität sind:

- Bluetooth: Die Integritätssicherung schützt vor zufälligen Störungen von Daten, aber nicht unbedingt vor einer absichtlichen Veränderung der Daten. Ein Angreifer könnte einen Datenstrom gezielt abändern.
- Eine ähnliche Schwäche bei WLAN (nach dem häufig eingesetzten Standard IEEE 802.11) ermöglicht ebenfalls die absichtliche Mutation der übertragenen Daten.

Verfügbarkeit

Verfügbarkeit heisst, dass Netze und Dienste in Betrieb sind, Daten bereit stehen usw. Gefahren für die Verfügbarkeit sind technische Pannen, Natur- oder Zivilisationskatastrophen und auch Angriffe ('Denial of Service', DoS). Beispiele für Nichtverfügbarkeit sind:

- In einem Gefängnis wird von der Strafvollzugsbehörde ein Störsender eingesetzt, um den Empfang auf dem Areal zu stören und den Häftlingen die Kommunikation mit der Aussenwelt zu verunmöglichen.
- Ein Bluetooth-Gerät (z. B. Mini-Computer) wird immer wieder angesprochen (das angreifende Gerät verlangt Daten oder einfach eine Verbindung), bis seine Batterie entladen ist. Das Gerät steht nicht mehr zur Verfügung, und der Benutzer kann damit keine Verbindung zum Netzwerk mehr herstellen.
- Hochwasser verursacht einen grossflächigen Stromausfall. Nach wenigen Stunden ist die Notstromversorgung der meisten Mobilfunkbasisstationen, bzw. WiMAX-Basisstationen, im Katastrophengebiet erschöpft und es besteht nur noch eine sehr lückenhafte Abdeckung entsprechender Fernmeldedienste.

4.3 Weitere Probleme

In diesem Teil werden einige weitere Probleme beschrieben, die nicht in den obigen Abschnitt über die Informationssicherheit gehören.

Störungen über Funk

Viele drahtlose Systeme nutzen das ISM-Band (Industrial, Scientific and Medical) um 2,4 GHz. Dieses Frequenzband ist ein Bereich des Spektrums, der jedermann zur Verfügung steht und ohne Funkkonzession genutzt werden darf. Es gibt lediglich eine Regelung der Sendeleistung, die für alle Systeme im ISM-Band gilt. Die Befreiung von der Funkkonzessionspflicht hat wesentlich zum Erfolg der Funknetze wie WLAN und Bluetooth beigetragen. Die gleiche Freiheit bringt aber auch einen bedeutenden Nachteil. Viele Systeme teilen den gleichen Frequenzbereich ohne jegliche Koordination der Frequenzen. Dabei geht es nicht nur um Kommunikationsnetze aber auch um andere Geräte wie zum Beispiel Mikrowellenöfen. Die Folge ist die gegenseitige Störung der Kommunikationsnetze sowie ihre Störung durch andere Geräte. Diese Störungen können zu einer Minderung der Datenübertragungsrate oder gar Datenverlust führen.

Diebstahl von tragbaren Geräten

Laptop oder PDA werden oft in Verbindung mit drahtlosen Netzwerken und oft in der Öffentlichkeit benutzt. Solche Hightech Geräte sind bei Dieben sehr beliebt, wobei durch den Diebstahl eines solchen Gerätes möglicherweise viel mehr Schaden entsteht als nur der Verlust des Gerätes selbst. Alle Daten, die auf dem Gerät gespeichert sind, sind erstens verloren und können zweitens, sofern sie nicht verschlüsselt sind, offen gelegt werden. Berichte über den Verlust von sensiblen Geschäftsdaten wegen eines Laptop-Diebstahls erscheinen häufig in den Medien. Weitere Folgen sind zu befürchten, wenn der Benutzer Passwörter auf dem Gerät gespeichert hat. Wenn ein Unbefugter diese Passwörter findet, werden ihm weitere Tore geöffnet, z. B. das Einloggen in ein Firmennetzwerk mit allen Rechten des echten Benutzers.

Wenn ein tragbares Gerät in der Öffentlichkeit benutzt wird, werden sehr einfache Angriffe möglich. Durch die Beobachtung eines Benutzers kann man wichtige Daten aufnehmen, z. B. den Prozess zum Einloggen am Gerät oder am Netzwerk einschliesslich Benutzer-Identifikation und Passwörter.

Tragbare Geräte können einen Weg in ein Firmennetzwerk bieten, der die üblichen Sicherheitsmechanismen des Netzwerks umgeht. Das Gerät kann zum Beispiel an einem öffentlichen Netz von einem Virus infiziert werden und würde beim späteren Anschluss am Firmennetz dieses Virus in das Netzwerk einlassen.

Trittbrettfahrer

Trittbrettfahrer haben es leicht in ungesicherten drahtlosen Netzwerken. Ein drahtloses Lokalnetzwerk, bei dem die Sicherheitsmechanismen nicht eingeschaltet wurden, steht allen – also auch unrechtmässigen - Benutzern in seinem Abdeckungsgebiet zur Verfügung. Eine Person oder eine Firma, die ihr WLAN so offen lässt, kann zwar vor schweren Folgen wie dem Verlust von kritischen Daten verschont bleiben. Sie kann aber dafür das Problem haben, dass ihre teuer gekaufte Breitband-Internetverbindung ständig stark belastet ist und die eigenen Anwendungen kaum noch unterstützt.

Schlimmer wäre es, wenn die ungesicherten Netzwerkressourcen für illegale Zwecke benutzt würden. Über das Netzwerk könnte der Internetanschluss benutzt werden, um illegale Inhalte wie Pornographie, Musikstücke oder Spielfilme herunter zu laden oder Spamming, Hacking oder DoS-Angriffe durchzuführen. Rechtliche Folgen für den Netzbetreiber wären nicht ausgeschlossen.

4.4 Weiterentwicklung

In den letzten Jahren hat es bei den drahtlosen Netzwerken einen starken Aufschwung gegeben. Neue Technologien in Verbindung mit konzessionsfreien Frequenzbereichen haben eine weite Verbreitung von WLAN und Bluetooth ermöglicht. Die Entwicklung der Technologie geht weiter und neue Systeme werden bessere Leistungen aufweisen. Die Anzahl der Netze wird steigen. Ein Wachstum im Bereich

der drahtlosen Anschlussnetze (Wireless Local Loop, WLL; Broadband Wireless Access, BWA) wird ebenfalls erwartet. Immer mehr Personen werden ihren Kommunikationsbedarf über drahtlose Netze abwickeln. Parallel dazu nehmen die Gefahren im Internet zu: Eine klare Entwicklung zu einer Professionalisierung der Internetkriminalität wurde schon erkannt. Die Opfer werden künftig nicht nur unter einer Art Vandalismus zu leiden haben, sondern viel öfter mit einem finanziellen Schaden rechnen müssen. Bei der Bekämpfung dieser Gefahren, die ausser den drahtlosen Netzen auch das gesamte Internet betreffen, werden alle Beteiligten - Netzbetreiber, Dienstanbieter und Nutzer- eine Rolle zu spielen haben und ihre Rollen auch wahrnehmen müssen.

4.5 Zusammenfassung und Massnahmen

Drahtlose Netzwerke bieten praktische und flexible Kommunikationsmöglichkeiten. Sie bergen jedoch Gefahren für die Informationssicherheit. Diese Gefahren bestehen auch bei leitergebundenen Netzen, sie sind bei drahtlosen Systemen aber verschärft. Sowohl Nutzer wie Netzbetreiber sollten deshalb geeignete Massnahmen treffen, um ihre Daten zu schützen.

Die erste Massnahme, die gleichzeitig die Voraussetzung für alle anderen ist, geht dahin, das Bewusstsein aller Betroffenen, besonders aber der Nutzer, für Fragen der Informationssicherheit zu schärfen. Erst wenn die Gefahren bekannt sind, sind die Betroffenen überhaupt in der Lage, entsprechende Vorkehrungen zu treffen. Durch das richtige und korrekte Verhalten der Nutzer lässt sich schon sehr viel für die Informationssicherheit tun. Erst darauf aufbauend sind dann technische Massnahmen sinnvoll.

Die Nutzer haben verschiedene Möglichkeiten, aktiv und vorbeugend zu handeln. Endgeräte sollten durch geeignete Sicherheitsmassnahmen geschützt werden. Bei einem Laptop sind dies z.B. Virus- und Spyware-Schutz, Software-Firewall u.a. Sensible Daten sind nicht nur auf Übertragungswegen in Gefahr. Auch auf einem Speichermedium (z. B. Server, PC, Memory-Stick) können sie gefährdet sein. Hacking-Angriffe bzw. -Versuche sind für Informatikabteilungen an der Tagesordnung. Daten, die auf tragbaren Geräten wie Laptops oder PDA gespeichert sind, gehen bei einem Diebstahl zusammen mit dem Gerät verloren. Aus diesen Gründen ist es ratsam, sensible Daten verschlüsselt zu speichern.

Die Netzbetreiber, ob Privatpersonen mit kleinem oder Grossfirmen mit einem landesweiten Netzwerk, sollten die vorhandenen Sicherheitsmechanismen, die das jeweilige drahtlose System bietet, unbedingt nutzen. Selbst wenn diese lückenhaft sein können - ein schwacher Schutz ist besser als gar keiner. Die am besten geeigneten Massnahmen sind von Fall zu Fall unterschiedlich. Einige einfache Massnahmen für Privatpersonen sind im Kapitel 6.2 beschrieben. Die Sicherung der Funkstrecke behebt aber nicht die übrigen Sicherheitslöcher im Gesamtsystem. Das Sicherheitsproblem ist damit nicht gelöst.

Bei der Übertragung von sensiblen Daten ist es unentbehrlich, dass diese auf dem gesamten Übertragungsweg geschützt werden. Dies ist oft der Fall bei wichtigen Geschäftsdaten, wo dementsprechend hoch professionelle Lösungen eingesetzt werden. Bekannte Beispiele dafür sind das Virtual Private Network (VPN), das von Mitarbeitern für den externen Zugriff auf Firmennetzwerke über das Internet benutzt wird, und e-Banking-Systeme, welche die Finanzdaten von Kunden auf dem Weg vom PC zum Server der Bank schützen. Solche Systeme werden End-To-End-System genannt. Diese Lösungen bieten eine sichere Authentisierung und eine starke Verschlüsselung auf dem gesamten Übertragungsweg, unabhängig von der Technologie der einzelnen Übertragungsteilstrecken.

5. Rechtliche Regelung

5.1 Allgemein

Die Telekommunikationsaspekte der drahtlosen Netzwerke sowie einige Aspekte der Datensicherheit sind vorwiegend im Fernmeldegesetz und darauf basierenden Verordnungen geregelt. Dies gilt auch für den Gesundheitsschutz betreffend der Geräte als Komponenten der drahtlosen Netzwerke. Der Gesundheitsschutz im Sinne der Immissionsbegrenzung der Strahlung von stationären Anlagen ist im Umweltschutzgesetz, spezifisch in der Verordnung über den Schutz vor nichtionisierender Strahlung geregelt. In den folgenden Abschnitten werden diese Erlasse näher erläutert.

Die Regelung von drahtlosen Netzwerken bei der beruflichen Exposition oder bei Medizinprodukten wird nachfolgend nicht ausführlich behandelt. Informationen dazu sind im Bericht „Nichtionisierende Strahlung und Gesundheitsschutz in der Schweiz“ zu finden.[1] Bei Medizinprodukten wird nur der Aspekt der elektromagnetischen Verträglichkeit behandelt. Dieser Aspekt ist im Zusammenhang mit drahtlosen Netzwerken von besonderer Bedeutung.

Die Datensicherheit ist allgemein im Datenschutzgesetz[28] und punktuell in der Telekommunikationsgesetzgebung geregelt.

5.2 Telekommunikation (Gesundheitsschutz vor EMF bei Telekommunikationsgeräten)

Fernmeldegesetz FMG[29]

Das Fernmeldegesetz FMG regelt die fernmeldetechnische Übertragung von Informationen. Es zielt darauf ab, dass der Bevölkerung und der Wirtschaft vielfältige, preiswerte, qualitativ hoch stehende sowie national und international konkurrenzfähige Fernmeldedienste angeboten werden.

In Bezug auf drahtlose Netzwerke sind folgende Regulierungsaspekte von Interesse:

- Konzessionspflicht und Konzessionserteilung
- Frequenzverwaltung
- Anbieten, Inverkehrbringen und Inbetriebnahme sowie Erstellen, Betreiben und Kontrolle der Fernmeldeanlagen
- Störung bzw. elektromagnetische Verträglichkeit
- Schutz der Gesundheit und Sicherheit
- Fernmeldegeheimnis

Diese Aspekte sind in den entsprechenden Ausführungsverordnungen zum FMG genauer geregelt.

Ein revidiertes Fernmeldegesetz wurde am 24. März 2006 vom Parlament verabschiedet. Diese Änderung hat auch eine Überarbeitung der darauf basierenden Verordnungen zur Folge. Die geänderte Gesetzgebung tritt voraussichtlich am 1. April 2007 in Kraft. Die Änderungen betreffen drahtlose Netzwerke nur im Bereich der Dienstekonzession und haben keinen Einfluss auf die in diesem Bericht erörterten Aspekte der drahtlosen Netzwerke.

[28] Bundesgesetz von 19. Juni 1992 über den Datenschutz DSG, SR 235.1
[29] Fernmeldegesetz vom 30. April 1997, SR 784.10

Verordnung über Frequenzmanagement und Funkkonzessionen FKV[30], Verordnung über Fernmeldedienste FDV[31]

Gemäss Fernmeldegesetz[32] ist grundsätzlich jede Nutzung des Frequenzspektrums konzessionspflichtig. Allerdings kann der Bundesrat für Frequenznutzung von geringer technischer Bedeutung Ausnahmen vorsehen[33].

Die Verordnung über Fernmeldedienste regelt unter anderem den Umfang des Fernmeldedienstes, die Ausnahmen von der Konzessions- und Meldepflicht, die Nutzung des Funkfrequenzspektrums, die Konzessionen für Fernmeldedienste sowie die allgemeinen Rechte und Pflichten von Fernmeldedienstanbieterinnen.

Betreiber von drahtlosen Netzwerken benötigen eine Dienstekonzession[34] bzw. sind meldepflichtig[35], wenn diese für das Betreiben eines Fernmeldenetzes verwendet werden, mit welchen eine Anbieterin für Dritte (Teilnehmer oder andere Fernmeldedienstanbieterinnen) Fernmeldedienste (z.B. Sprachübertragung, Datenübertragungsdienste usw.) erbringt. Dabei spielt es keine Rolle, ob das drahtlose Netzwerk für den Teilnehmeranschluss oder für die Vernetzung von Fernmeldeanlagen eingesetzt wird.

Von der Konzessionspflicht ausgenommen sind Funkanlagen, die auf bestimmten Sammelfrequenzen und mit einer begrenzten Leistung benutzt werden[36]. Für die drahtlosen Netzwerke hat das BAKOM im ISM-(Industrial, Scientific and Medical) Band, konzessionsfreie Frequenzbereiche bei 2,4 GHz und 5 GHz freigegeben. Diese Ausnahme von der Konzessionspflicht gilt nur für bestimmte Leistungen. Sobald diese überschritten werden, lebt die Konzessionspflicht wieder auf. In diesen Frequenzbändern gibt es keinen Schutz vor Störungen durch andere Systeme. Die meisten drahtlosen Netzwerke, mit Ausnahme von WiMAX, arbeiten in diesem konzessionsfreien Bereich.

Verordnung über Fernmeldeanlagen FAV[37]

Das Anbieten, Inverkehrbringen und die Inbetriebnahme von Fernmeldeanlagen wird in der Verordnung über Fernmeldeanlagen FAV geregelt, die inhaltlich die Richtlinie 1999/5/EG über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität[38] umsetzt.

Als Fernmeldeanlagen gelten Geräte, Leitungen oder Einrichtungen, die zur fernmeldetechnischen Übertragung von Informationen bestimmt sind oder benutzt werden. Die fernmeldetechnische Übertragung erfolgt durch elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk (zwischen 9 kHz und 3000 GHz).[39]

Eine Fernmeldeanlage darf nur erstellt und betrieben werden, wenn sie zum Zeitpunkt, zu dem sie erstmals in Verkehr gebracht, erstellt oder in Betrieb genommen wird, den dafür geltenden Vorschriften entsprach und in diesem Zustand erhalten wurde.[40] Stationäre Fernmeldeanlagen müssen bei deren Betrieb zusätzlich den Anforderungen der Verordnung über den Schutz vor nichtionisierender Strahlung NISV[41] genügen (Sendeanlagen für Mobilfunk und Rundfunk).

---

30 Verordnung vom 6. Oktober 1997 über Frequenzmanagement und Funkkonzessionen, SR 784.102.1
31 Verordnung vom 31. Oktober 2001 über Fernmeldedienste, SR 784.101.1
32 Art. 22 Abs. 1 FMG
33 Art. 22 Abs. 3 FMG
34 Art. 4 Abs. 1 FMG
35 Art. 4 Abs. 2 FMG
36 Art. 8 Abs. 1 Bst. a FKV
37 Verordnung vom 14. Juni 2002 über Fernmeldeanlagen, SR 784.101.2
38 Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität
39 Art. 3 Bst. c und d FMG
40 Art. 32 FMG
41 SR 814.710

Grundsätzlich müssen folgende grundlegende Anforderungen[42] erfüllt werden:

- Schutz der Gesundheit und der Sicherheit der Benutzenden und anderer Personen
- elektromagnetische Verträglichkeit
- effektive Nutzung des zugewiesenen Spektrums

Die technischen Normen, bei deren Einhaltung vermutet wird, dass die grundlegenden Anforderungen erfüllt sind, bezeichnet das Bundesamt für Kommunikation (BAKOM)[43] nach dem europäischen Vorbild des „New And Global Approach". Die Normen, welche die Einhaltung der Grenzwerte für EMF von Geräten in drahtlosen Netzwerken definieren, sind in Tabelle 6 aufgeführt.

In Bezug auf EMF handelt es sich dabei hauptsächlich um die Einhaltung der international empfohlenen Grenzwerte (siehe Kapitel 4). Es gilt zu beachten, dass jedes einzelne Gerät den ganzen Grenzwert ausschöpfen kann.

Im Bereich des Schutzes betreffend die elektromagnetische Verträglichkeit dürfen Geräte bei bestimmungsgemässem Betrieb und Gebrauch andere Geräte nicht elektromagnetisch stören und so deren Funktionsfähigkeit beeinträchtigen. Jedes Gerät muss jedoch auch einen gewissen Eigenschutz gegen fremde Störungen aufweisen. In Bezug auf den Gesundheitsschutz ist dies insbesondere bei gewissen Medizinprodukten wichtig (z.B. Herzschrittmacher).

Der Vollzug betreffend des Gesundheitsschutzes vor hochfrequenten EMF, elektromagnetischer Verträglichkeit (EMV) sowie effektiver Nutzung des Spektrums obliegt dem BAKOM[44], während das Eidgenössische Starkstrominspektorat (ESTI) für die Aspekte der elektrischen Sicherheit und des damit verbundenen Gesundheitsschutzes zuständig ist.[45]

Technische Normen der CENELEC (Comité Européen de Normalisation Électrotechnique)
CENELEC-Normen spezifizieren die mess- und verfahrenstechnischen Vorgaben, mit denen der grundlegende Gesundheitsschutz im Bereich EMF von Produkten geprüft werden soll. Durch die europäische Normierungsorganisation CENELEC[46] wurden die in Tabelle 6 aufgeführten EMF-Normen, die den Bereich der hochfrequenten Strahlung mit einschliessen, sowie eine EMV-Norm für Medizinprodukte veröffentlicht.

[42] Art. 6 Abs. 1 i.V.m. Art. 7 Abs. 1 und 3 FAV
[43] Technische Normen für Fernmeldeanlagen
http://www.bakom.admin.ch/org/grundlagen/00563/00575/01142/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnq
[44] Art. 22 Abs. 1 FAV
[45] Verordnung vom 7. Dezember 1992 über das Eidgenössische Starkstrominspektorat, SR 734.24
[46] http://www.cenelec.org/Cenelec/Homepage.htm

Tabelle 6: *CENELEC-Normen, welche hochfrequente EMF regeln.*

Norm	Jahr	Titel
EN 50371	2002	Fachgrundnorm zum Nachweis der Übereinstimmung von elektronischen und elektrischen Geräten kleiner Leistung mit den Basisgrenzwerten für die Sicherheit von Personen in elektromagnetischen Feldern (10 MHz bis 300 GHz) - Allgemeine Öffentlichkeit
EN 50392	2004	Fachgrundnorm zur Demonstration der Konformität elektronischer und elektrischer Geräte mit den Basisgrenzwerten für die Exposition von Personen gegenüber elektromagnetischen Feldern (0 Hz - 300 GHz)
EN 50383	2002	Grundnorm für die Berechnung und Messung der elektromagnetischen Feldstärke und SAR in Bezug auf die Sicherheit von Personen in elektromagnetischen Feldern von Mobilfunk-Basisstationen und stationären Teilnehmergeräten von schnurlosen Telekommunikationsanlagen (110 MHz bis 40 GHz)
EN 50385	2002	Produktnorm zur Konformitätsüberprüfung von Mobilfunk-Basisstationen und stationären Teilnehmergeräten für schnurlose Telekommunikationsanlagen im Hinblick auf die Basisgrenz- und Referenzwerte bezüglich der Exposition von Personen gegenüber elektromagnetischen Feldern (110 MHz bis 40 GHz) – Allgemeinbevölkerung
EN 50400 / EN 50401	2006	Grundnorm / Produktnorm zum Nachweis der Übereinstimmung von stationären Einrichtungen für Funkübertragungen (110 MHz bis 40 GHz), die zur Verwendung in schnurlosen Telekommunikationsnetzen vorgesehen sind, bei ihrer Inbetriebnahme mit den Basisgrenzwerten oder den Referenzwerten bezüglich der Exposition der Allgemeinbevölkerung gegenüber hochfrequenten elektromagnetischen Feldern
EN 60601-1-2	2001 A1:2006	Medizinische elektrische Geräte -- Teil 1-2: Allgemeine Festlegungen für die Sicherheit - Ergänzungsnorm: Elektromagnetische Verträglichkeit - Anforderungen und Prüfungen

5.3 Umweltschutz (Gesundheitsschutz vor EMF bei stationären Anlagen)

Umweltschutzgesetz

Im Umweltschutzgesetz USG[47] sind neben Luftverunreinigungen, Lärm und Erschütterungen auch nichtionisierende Strahlen als Einwirkungen bezeichnet, die so zu begrenzen sind, dass sie für den Menschen und die Umwelt weder schädlich noch lästig sind. Das Schutzkonzept des Umweltschutzgesetzes ist zweistufig angelegt:

- Stufe Gefahrenabwehr:
  Immissionen, die schädlich oder lästig sind, sind nicht zulässig und müssen zwingend reduziert werden. Die Schädlichkeits- bzw. Lästigkeitsschwelle ist in Form von Immissionsgrenzwerten durch den Bundesrat verbindlich festzulegen.
- Stufe Vorsorge:
  Zusätzlich zur Verhinderung nachgewiesener schädlicher oder lästiger Wirkungen kennt das Umweltschutzgesetz den Vorsorgegrundsatz, wonach Einwirkungen, die schädlich oder lästig werden *könnten*, im Sinne der Vorsorge so weit zu reduzieren sind, als dies technisch und betrieblich möglich und wirtschaftlich tragbar ist. Dieser Auftrag gilt auch im Bereich unterhalb des Immissionsgrenzwertes. Eine konkrete Gefährdung muss dabei nicht nachgewiesen sein. Das Vorsorgeprinzip dient dazu, potenzielle Risiken - insbesondere Langzeitrisiken - zu vermindern, welche infolge des lückenhaften Kenntnisstandes nicht zufriedenstellend bewertet werden können.

Verordnung über den Schutz vor nichtionisierender Strahlung (NISV)

Die Verordnung über den Schutz vor nichtionisierender Strahlung[48] regelt ausschliesslich den Schutz vor elektromagnetischen Feldern (nichtionisierende Strahlen im Frequenzbereich von 0 Hz bis 300 GHz). Für die allgemeine Bevölkerung sind für den ganzen genannten Frequenzbereich Immissionsgrenzwerte für räumlich ausgedehnte Expositionen durch EMF festgelegt worden, ungeachtet deren Herkunft. Sie entsprechen den Empfehlungen der ICNIRP und sollen den Schutz des Menschen vor wissenschaftlich

[47] Bundesgesetz vom 7. Oktober 1983 über den Umweltschutz (Umweltschutzgesetz, USG) SR 814.01
[48] Verordnung vom 23. Dezember 1999 über den Schutz vor nichtionisierender Strahlung, SR 814.710 (NISV)

gesicherten, akuten schädlichen Einwirkungen sicherstellen. Die Immissionsgrenzwerte müssen überall dort eingehalten werden, wo sich Menschen - auch nur kurzfristig - aufhalten können. Sie gelten jedoch nur für Strahlung, die gleichmässig auf den ganzen menschlichen Körper einwirkt (Ganzkörperexpositionen).

Soweit es um konkrete emissionsbegrenzende Massnahmen und Zuständigkeiten geht, werden nur ortsfeste Anlagen erfasst (z.B. Hochspannungsleitungen, Fahrleitungen von Eisen- und Strassenbahnen, Sendeanlagen für Mobilfunk, drahtlose Teilnehmeranschlüsse oder Rundfunk). In Konkretisierung des Vorsorgeprinzips wurden zusätzlich so genannte Anlagegrenzwerte eingeführt, die strenger als die Immissionsgrenzwerte sind und sich an den technischen und betrieblichen Möglichkeiten zur Verringerung der Strahlung sowie deren wirtschaftlicher Tragbarkeit orientieren. Sie liegen um die Faktoren 10 bis 300 unterhalb der Immissionsgrenzwerte und gelten an Orten mit empfindlicher Nutzung (z.B. Wohnungen, Büros).

Der Vollzug des Umweltrechts obliegt grundsätzlich den Kantonen, soweit das Gesetz ihn nicht dem Bund vorbehält. Der Vollzug erfolgt dann durch den Bund, wenn Bundesbehörden andere Bundesgesetze anwenden und dabei Entscheide über Anlagen treffen, die NIS erzeugen (z.B. bei elektrischen Anlagen, Eisenbahnanlagen). Wo dies nicht der Fall ist, liegt die Zuständigkeit bei den Kantonen (z.B. Mobilfunkantennen, Rundfunksender, Betriebsfunkanlagen, Amateurfunkanlagen).

WLAN
Access Points von öffentlich zugänglichen Hotspots sind als stationäre Sendeanlagen zu betrachten und fallen somit in den Geltungsbereich der NISV.

Der Immissionsgrenzwert[49] ist so lange anwendbar, als der ganze Körper gleichmässig der Strahlung einer stationären Anlage exponiert ist. Bei heutigen WLAN Access Points sind bei Entfernungen, wo der Körper gleichmässig bestrahlt wird, die Imissionsgrenzwerte immer eingehalten.

Bei grösserer Annäherung an die Antenne, was bei WLAN Access Points in der Praxis vorkommt, handelt es sich um eine Teilkörperexposition. In diesem Fall ist der Immissionsgrenzwert der NISV nicht mehr anwendbar; an seiner Stelle gelten die Anforderungen der Verordnung über Fernmeldeanlagen (siehe Kapitel 5.2), bzw. der ICNIRP-Grenzwert von 2 W/kg für die lokale SAR. Auch dieser Grenzwert dürfte selbst bei kleinen Abständen eingehalten sein. Die Hersteller sind dafür verantwortlich, dass die Benutzer, welche die Installation vornehmen, über allfällige Mindestabstände informiert werden.

Da die maximal erlaubte Sendeleistung von WLAN Access Points unterhalb von 6 Watt ERP liegt, sind diese gemäss der NISV[50], von einer vorsorglichen Emissionsbegrenzung ausgenommen, d. h. sie müssen keinen Anlagegrenzwert einhalten. Es gibt allerdings Hinweise, dass die maximal erlaubte Sendeleistung der Access Points im ISM-Band von kleineren Betreibern (oft auch Gemeinden) nicht immer eingehalten wird (z. B. weil Antennen mit zu hohem Antennengewinn installiert werden). Wegen fehlenden technischen Kenntnissen und fehlender Erfahrung mit dem Thema nichtionisierende Strahlung ist solchen Hotspot-Betreibern vermutlich nicht bewusst, dass sie sich nicht rechtmässig verhalten. Solches Fehlverhalten könnte zu höheren Immissionen führen.

WiMAX
Basisstationen von WiMAX-Netzen unterliegen der NISV. Sie werden gleich behandelt wie Mobilfunkbasisstationen[51]. Für Basisstationen mit einer gesamten Sendeleistung von mehr als 6 Watt ERP muss bei der zuständigen Gemeinde ein Baugesuch eingereicht werden und die NIS-Belastung anhand eines Standortdatenblattes berechnet werden. Die Baubewilligung darf nur dann erteilt werden, wenn die NIS-Belastung durch die Sendeanlage an allen Orten mit empfindlicher Nutzung (Wohnräume, Schulen, un-

[49] Anhang 2 Ziffer 11 der NISV
[50] Anhang 1 Ziffern 61 und 71 der NISV
[51] siehe Vollzugsempfehlung zur NISV – Mobilfunk- und WLL-Basisstationen, BUWAL, 2002

überbaute Bauzonen) den Anlagegrenzwert einhält. Für Anlagen mit einer Sendeleistung von weniger als 6 Watt ERP kann die Behörde ein Meldeformular verlangen. Im konzessionsfreien Band mit maximalen Sendeleistungen von 1 W bzw. 2 W müssen die Basisstationen erst ab mehreren fix an einem Standort installierten Sendern, welche zusammen eine gesamte Sendeleistung von über 6 Watt ERP erreichen, den Anlagegrenzwert einhalten.

Über Teilnehmerantennen für den nomadischen Einsatz können noch keine Aussagen gemacht werden, da die konkrete technische Ausgestaltung dieser halbmobilen Systeme noch nicht bekannt ist.

5.4 Elektromagnetische Verträglichkeit bei Medizinprodukten

In der Schweiz werden Medizinprodukte, ähnlich wie Fernmeldeanlagen, nach dem europäischen „new and global approach“ geregelt; die gesetzlichen Grundlagen finden sich im Heilmittelgesetz (HMG)[52] und in der Medizinprodukteverordnung[53] (MepV). Der Bundesrat legt die grundlegenden Anforderungen an Medizinprodukte fest und das Schweizerische Heilmittelinstitut (Swissmedic) bezeichnet die technischen Normen, die geeignet sind, diese grundlegenden Anforderungen zu konkretisieren[54] - unter anderen auch die Anforderungen an elektromagnetische Verträglichkeit (siehe auch Kapitel 3.5). Die entsprechende Norm ist in der Tabelle 6 angefügt.

Gemäss dem „new and global approach“ übernehmen die Hersteller ein hohes Mass an Eigenverantwortung bei dem Verfahren der Inverkehrbringung eines Medizinproduktes. Sie sind nicht nur für die erfolgreich durchzuführenden relevanten Konformitätsbewertungsverfahren verantwortlich. Ihre Pflicht erstreckt sich über den gesamten Lebenszyklus der Produkte. Dabei hat die kontinuierliche Produktebeobachtung entscheidende Bedeutung. Beispielsweise müssen die Hersteller ihre Produkte risikoanalytisch auf Einflüsse neuer bzw. kommender Technologien, wie zum Beispiel Funknetzwerke mit neuen Frequenzbereichen, überprüfen. Je nach dem Ergebnis von allenfalls neu auftretenden Gefahren, müssen die Produkte aufgrund der geänderten Umstände angepasst oder gar weiterentwickelt werden.

Zur Erhöhung der Sicherheit betreibt Swissmedic ein so genanntes Vigilance-System: Hersteller und alle Inverkehrbringer von Medizinprodukten sind verpflichtet Swissmedic über schwerwiegende Vorkommnisse und Gefährdungen, sowie über Produkterückrufe und andere Herstellermassnahmen zu benachrichtigen. Ziel dieses Meldewesens von Zwischenfällen (Vigilance) ist es, das Wiederholen von Zwischenfällen zu verhindern. Die Untersuchung der Ursachen eines Vorkommnisses und die Durchführung allfälliger Korrekturmassnahmen sind Aufgaben des Herstellers und Inverkehrbringers. Diese Vorgänge werden von Swissmedic überwacht.

Sollten die drahtlose Netzwerke Funktionsstörungen von Medizinprodukten verursacht haben, sollten diese durch das Vigilance-System aufgefangen und korrigiert werden.

5.5 Zusammenfassung der rechtlichen Regelungen

In der Tabelle 7 sind die für verschiedene Aspekte der drahtlosen Netzwerke die wichtigsten vorhandenen Regelungen aufgelistet.

[52] Bundesgesetz vom 15. Dezember 2000 über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG), SR 812.21
[53] Medizinprodukteverordnung (MepV) vom 17. Oktober 2001, SR 812.213
[54] Art. 45 Abs. 3 und 4 HMG

Tabelle 7: *Für drahtlose Netzwerke (DN) relevante Regelungen* [55]

Thema	Erlass	Bemerkung
Standards Frequenzmanagement	FMG FKV	Die meisten DN senden in freien ISM Frequenzband - anfällig für Störungen
Konzessionen	FMG FDV FKV	Die meisten DN arbeiten konzessionsfrei (Ausnahme WiMAX)
Gesundheitsschutz Geräte	FAV	Grenzwerte für einzelne Produkte festgelegt in internationalen Produktenormen (Tabelle 6)
Gesundheitsschutz stationäre Anlagen (betrifft WLAN und WiMAX)	USG NISV	Immissionsgrenzwerte für alle Orte, wo sich Menschen aufhalten können + Anlagegrenzwerte für Orte mit empfindlichen Nutzung
Arbeitnehmerschutz für öffentliche stationäre Sendeanlagen	NISV	Immissionsgrenzwerte + Anlagegrenzwerte für Büros als Orte mit empfindlicher Nutzung
Arbeitnehmerschutz für Geräte und Anlagen im Betrieb	UVG	Immissionsgrenzwerte für berufliche Exposition (MAK-Werte)
Elektromagnetische Verträglichkeit	VEMV MepV	Europäische Produktenorm für elektromagnetische Verträglichkeit bei Medizinprodukten (Tabelle 6)
Datensicherheit	DSG FMG FDV	 Strafbestimmungen Fernmeldegeheimnis

5.6 Rechtlicher Regelungsbedarf

Da drahtlose Netzwerke nach aktuellem Wissensstand keine Gefährdung der Gesundheit darstellen, besteht aus gesundheitlicher Sicht kein weitergehender Regelungsbedarf für Geräte. Deshalb muss auch der so genannte Wildwuchs von Zugangspunkten zurzeit nicht eingeschränkt werden. Zugangspunkte mit Sendeleistung von mindestens 6 W ERP unterstehen zudem der vorsorglichen Emissionsbegrenzung der NISV, so dass bei stärkeren Hotspots die Anlagegrenzwerte zum Tragen kommen.

Nach aktuellem Wissenstand kann keine Aussage über langfristige gesundheitliche Wirkungen in Folge hochfrequenter Strahlung von drahtlosen Netzwerke gemacht werden kann. Im Sinne der Informiertheit der Konsumentinnen und Konsumenten über eine strahlungsarme Verwendung drahtloser Netzwerke wäre eine konsumentenfreundliche Strahlungsdeklaration der Produkte wünschenswert.

Wünschenswert wäre auch eine Neuregulierung in den Produktenormen, bei welcher nicht mehr der ganze ICNIRP-Grenzwert durch ein einziges Gerät ausgeschöpft werden kann. Damit soll sichergestellt werden, dass auch bei gleichzeitiger Nutzung mehrerer Geräte der Grenzwert nicht überschritten wird.

In Bezug auf die Datensicherheit bei drahtlosen Netzwerken besteht vielmehr ein Sensibilisierungsbedarf als ein Regelungsbedarf. Der Bund hat schon einiges dazu geleistet, z.B. im Rahmen der Informationsgesellschaft und durch die Melde- und Analysestelle Informationssicherung. Es bestehen auch private in der Datensicherheit tätige Organisationen wie z.B. der Verein Infosurance, der sich mit den Bedürfnissen der kleinen und mittleren Unternehmen beschäftigt.

Auch in Bezug auf elektromagnetische Verträglichkeit (EMV) besteht kein unmittelbarer Regelungsbedarf. Allerdings wurde festgestellt, dass die bestehende Norm für EMV bei Medizinprodukten nur Frequenzen bis 2,5 GHz berücksichtigt. Es besteht Bedarf, die Auflagen auch für höhere Frequenzen, wie sie bei drahtlosen Netzwerken vorkommen können, zu definieren.

[55] **FMG**: Fernmeldegesetz, **FKV**: Verordnung über Frequenzmanagment und Funkkonzessionen, **FDV**: Verordnung über Fernmeldedienste, **FAV**: Verordnung über Fernmeldeanlagen, **USG**: Umweltschutzgesetz, **NISV**: Verordnung über den Schutz vor nichtionisierender Strahlung, **UVG**: Bundesgesetz über die Unfallversicherung, **MAK**: Maximale Arbeitsplatzkonzentration, **VEMV**: Verordnung über die elektromagnetische Verträglichkeit, **MepV**: Medizinprodukteverordnung, **DSG**: Datenschutzgesetz

6. Empfehlungen zum strahlungsarmen und sicheren Umgang mit drahtlosen Netzwerken

6.1 Minimierung der Strahlung

Die Strahlenbelastung durch die heutigen Netzwerke ist sehr klein, sie liegt weit unterhalb der geltenden Grenzwerte. Den bestehenden Unsicherheiten bezüglich langfristiger gesundheitlicher Wirkungen als auch der Verwendung von immer leistungsfähigeren Geräten sowie körpernahen Technologien kann mit geeigneten Massnahmen begegnet werden. Da drahtlose Netzwerke nicht nur in Büros sondern auch in Privathaushalten verwendet werden, sind vorsorgliche Massnahmen insbesondere auch in Haushalten mit Kindern sinnvoll. Mit folgenden Massnahmen kann die persönliche Strahlenbelastung im Sinne einer Vorsorge minimiert werden:

- Das WLAN nur einschalten, wenn es gebraucht wird. Insbesondere beim Laptop ist es sinnvoll, das WLAN auszuschalten, weil sonst immer wieder nach einem Netz gesucht wird, was unnötige Strahlung verursacht und die Batterie entleert.
- Beim Telefonieren mit dem PDA vorzugsweise ein Headset (einen Kopfhörer) verwenden.
- Ein Bluetooth-Headset der schwächsten Leistungsklasse 3 benutzen und ausschalten, wenn es nicht benutzt wird.
- Den Laptop während der WLAN-Verbindung nicht am Körper halten.
- Den Access Point möglichst einen Meter entfernt von lang besetzten Arbeits-, Aufenthalts-, Spiel- oder Ruheplätzen platzieren.
- Den Access Point zentral platzieren, damit alle zu versorgenden Geräte einen guten Empfang haben.
- Den WLAN g-Standard dem b-Standard vorziehen. Wegen seiner effizienteren Datenübertragung ist bei diesem Standard die Strahlenbelastung reduziert.
- Falls eine Leistungsregelung möglich ist, sollte beim Access Point die Sendeleistung entsprechend dem zu versorgenden Gebiet optimiert werden.
- Ein WLAN-Sender soll nur mit einer vom Hersteller dafür bestimmten Antenne betrieben werden. Wird eine Antenne mit einem grösseren Antennengewinn verwendet, kann die maximal erlaubte Sendeleistung überschritten werden und es kann gegen das Fernmeldegesetz verstossen werden.

6.2 Erhöhung der Datensicherheit

Die nachfolgenden Hinweise sind als Informationsquelle für Heimanwender gedacht. Diese Massnahmen bilden nur einen ersten Schritt zur sicheren Internetnutzung über WLAN. Weiterführende Informationen zu Informationssicherheit für alle Anwender - von Privatpersonen bis zu Grossfirmen - bietet die Melde- und Analysestelle Informationssicherung (MELANI)[56].

Massnahmen für ein Heimnetzwerk

- Das Standardpasswort zur Verwaltung des Access Point sollte geändert werden.
- Die Verwaltung des Access Point sollte wenn möglich über ein Kabel, z.B. Ethernet, erfolgen und die Funktion für die Verwaltung über Funk ausgeschaltet werden.
- Mögliche Funktionen für die Fernverwaltung des Access Point über das Internet sollten ausgeschaltet werden.
- Die Netzwerkidentifikation (SSID) sollte geändert und das Aussenden der Netzwerkidentifikation (SSID Broadcast) ausgeschaltet werden.
- Die stärkste Verschlüsselung, die vom Access Point und von den Endgeräten unterstützt wird, sollte eingesetzt werden (vorzugsweise WPA 2 oder WPA, sonst WEP). Die längste Schlüssellänge bzw. ein starkes Passwort sollte benutzt werden.
- Wenn es im Netzwerk praktikabel und das notwendige Wissen vorhanden ist, sollten statische IP-Adressen anstatt DHCP (Dynamic Host Configuration Protocol) benutzt werden.

[56] http://www.melani.admin.ch

- Der MAC-Filter sollte benutzt werden, um den Zugang zum WLAN auf die bestimmten Endgeräte im Netzwerk einzuschränken.
- Wenn die Funktion im Access Point vorhanden ist und der Betrieb des Netzwerkes nicht dadurch beeinträchtigt wird, sollte die Sendeleistung verringert werden, um die Reichweite des WLAN zu vermindern.
- Das WLAN sollte nur bei Gebrauch eingeschaltet werden.

7. Anhang

7.1 Abkürzungen und Begriffe

Access Point	Basisstation in einem WLAN Funknetzwerk
Ad-hoc-Netzwerk	direkte Verbindung von WLAN-Clients ohne Access Point
BAFU	Bundesamt für Umwelt
BAKOM	Bundesamt für Kommunikation
Bandbreite	Zwei Bedeutungen: Kapazität eines Übertragungskanals Frequenzbereich eines Übertragungskanals
Beacon	Regelmässige Nachricht eines Access Points durch Senden eines Signals
BWA	Broadband Wireless Access
CENELEC	Comité Européen de Normalisation Électrotechnique, Normierungsgremium
Datenrate	Datenmenge, die pro Zeiteinheit transportiert wird
DoS-Angriff	Denial of Service, Angriff mit dem Ziel, einen Computer oder ein ganzes Netzwerk unbenutzbar zu machen
Dosis	ist die physikalische Grösse, welche diejenigen Eigenschaften der Strahlung, welche für bestimmte biologische Veränderungen relevant sind, am besten beschreibt. Dementsprechend sind für unterschiedliche biologische und gesundheitliche Auswirkungen unterschiedliche Dosisgrössen relevant.
E-Feld	Elektrisches Feld
EIRP	equivalent isotropically radiated power: Sendeleistung, mit welcher ein Isotropstrahler versorgt werden müsste, um in der Ferne dieselbe Feldstärke zu erzeugen wie eine Richtantenne in ihrer Hauptsenderichtung.
EMF	Elektromagnetisches Feld
Emission	ist die Strahlung, die von einer Strahlungsquelle ausgesendet wird.
EMV	elektromagnetische Verträglichkeit
ERP	Effective Radiated Power : Sendeleistung, mit welcher eine Dipolantenne versorgt werden müsste, um in der Ferne dieselbe Feldstärke zu erzeugen wie eine Richtantenne in ihrer Hauptsenderichtung.
ESTI	Eidgenössisches Starkstrominspektorat
Ethernet	eine Netzwerktechnologie
ETSI	European Telecommunications Standards Institute
Exposition	ist die Strahlung (Immission), der ein Objekt (Mensch, Tier, Pflanze, Boden oder Sachgut) während einer bestimmten Dauer (Expositionszeit) ausgesetzt ist. Man unterscheidet zwischen Ganzkörperexposition und Teilkörperexposition.
FAV	Verordnung über Fernmeldeanlagen
FDV	Verordnung über Fernmeldedienste
Fernfeld	Vgl. Nahfeld
Firewall	Gerät oder Software-Anwendung zur Überwachung und Regelung des Datenverkehrs im Netzwerk
FMG	Fernmeldegesetz
Freisprechvorrichtung	Kombination aus Kopfhörer und Mikrofon zum Anschliessen an ein Handy
Frequenz	Anzahl von Schwingungen pro Sekunde
Hacking	Unerlaubter Zugang zum oder Aufenthalt im Informatiksystem eines Dritten
HiperLAN	High Performance Radio Local Area Network, Standard zur Datenübertragung
Hotspot	lokales Areal (z. B. in Großstädten, auf Flughäfen, in Hotels), in dem Internet-Provider einen drahtlosen Zugang zum Internet zur Verfügung stellen
ICNIRP	International Commission of Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronics Engineers
Immission	ist die Strahlung an einem bestimmten Ort. Die Immission ist meistens niedriger als die Emission, da die Strahlung zwischen der Strahlungsquelle und dem Ort der Immission abgeschwächt werden kann.
Immunität	Fähigkeit eines Gerätes, unter Einwirkung elektromagnetischer Störsignale einwandfrei zu funktionieren
Infrastruktur-Netzwerk	WLAN-Netz, welches über einen Access-Points organisiert wird
Interoperabilität	Die Fähigkeit eines Gerätes, bei vergleichbarer Systemumgebung in einem Netz mit anderen Geräten desselben Standards sinnvoll kommunizieren zu können
ISM-Band	Industrial Scientific Medical-Band, frei zugänglicher Frequenzbereich
IT'IS	Foundation for Research on Information Technologies in Society, Zürich
Kanal, Übertragungskanal	Reservierter Zeit- bzw. Frequenzabschnitt für die Datenübertragung
MAC-Filter	Medium Access Control Filter, erlaubt nur bestimmte Exemplare eines Netzwerk-

	schnittstellentyps, d.h. bestimmte Geräte ans Netz
Master	Gerät, welches die Leitung des Funkverkehrs in einem Bluetooth-Netz übernimmt
Mbit/s	Megabit/Sekunde, pro Zeit übertragene Datenmenge
Memory-Stick, USB-Stecker	kleiner portabler Datenspeicher, USB: Universal Serial Bus
Nahfeld, Fernfeld	Im hochfrequenten Bereich unterscheidet man zwischen Nah- und Fernfeld, je nachdem, ob der Abstand zur Quelle kleiner oder grösser als die Wellenlänge der Strahlung ist. Im Fernfeld nimmt die elektrische Feldstärke linear mit der Entfernung ab (1/r), die Leistungsdichte quadratisch (1/r2)
NEV	Verordnung über elektrische Niederspannungserzeugnisse
NISV	Verordnung über den Schutz vor nichtionisierender Strahlung
PC-Karte	WLAN-Sender/-Empfänger-Einheit für einen Personalcomputer
PDA	Personal Digital Assistant, elektronische Agenda
SAR	Spezifische Absorptionsrate, die Einheit ist W/kg. Der SAR-Wert ist die physikalische Grösse und das Mass für die Absorption von hochfrequenter Strahlung in biologischem Gewebe. Sie ist sowohl von der Frequenz als auch von der Grösse des absorbierenden Körpers abhängig.
Server	zentraler Rechner in einem Netzwerk, der den Arbeitsstationen Ressourcen (z.B. Internetzugang) und Daten zur Verfügung stellt
Slave	Teilnehmer im Bluetoothnetz, im Gegensatz zum Master.
Spyware	Software, die das Verhalten von PC-Nutzern ausspioniert und dieses Wissen an andere weitergibt
Telemetriesystem	Automatische Übertragung von Messwerten oder -daten, über größere Entfernungen, Fernüberwachung
USG	Umweltschutzgesetz
UVG	Bundesgesetz über die Unfallversicherung
VEMV	Verordnung über elektromagnetische Verträglichkeit
WEP-Verschlüsselung	Wired Equivalent Privacy. WEP ist ein Standard zur Verschlüsselung von Funksignalen in einem drahtlosen Netzwerk (WLAN)
WiFi	Wireless Fidelity, Herstellerstandard für WLAN
WiMAX	Worldwide Interoperability for Microwave Access, Herstellerstandard für WMAN
WLAN	Wireless Local Area Network, Standard zur drahtlosen Datenübertragung über mittlere Distanzen (z.B. Haus)
WLAN-Karte	eingebauter WLAN-Sender/-Empfänger in einem Gerät
WMAN	Wireless Metropolitan Area Network, Standard zur drahtlosen Datenübertragung über grosse Distanzen (z.B. Stadt)
WPAN	Wireless Personal Area Network, Standard zur drahtlosen Datenübertragung über kurze Distanzen (z.B. Arbeitsplatz)

7.2 Postulat Allemann (04 3594) Risikopotenzial von drahtlosen Netzwerken

Wortlaut des Postulates vom 8. Oktober 2004

Der Bundesrat wird beauftragt, einen Bericht zum Risikopotenzial drahtloser Netzwerke (Wireless Local Area Networks “WLAN”, Bluetooth etc.) zu erstellen. Dabei sind sowohl die drahtlosen Netzwerke und Zugangspunkte in Büros und Privathaushalten sowie die öffentlichen Internetstationen (sog. Hotspots) mit einzubeziehen. Der Bericht soll insbesondere aufzeigen:

- Strahlungspotenzial drahtloser Netzwerke,
- Gesundheitsrisiken (u.a. spezieller Fokus auf Privathaushalte mit Kleinkindern und mögliche Massnahmen),
- Umweltauswirkungen,
- Datensicherheitsaspekte,
- Allfälliger Regelungsbedarf für den derzeitigen Wildwuchs an privaten und öffentlichen Zugangspunkten (siehe www.swisshotspots.ch).

Die Ergebnisse sind der Öffentlichkeit zielgruppenspezifisch in geeigneter Form bekannt zu machen.

Begründung

Immer mehr Menschen wissen das Plus an Flexibilität und Mobilität von drahtlosen Netzwerken zu schätzen. Die Zahl der öffentlichen Zugangspunkte auf das Internet (so genannten Hotspots) nimmt denn auch extrem rasch zu. Aber auch in Betrieben sowie in Privathaushalten erlebt die drahtlose Technologie einen regelrechten Boom. Sorglos wird diese an allen möglichen Orten eingesetzt: in Büros, in Privathaushalten, an Universitäten, in Hotels, an den Bahnhöfen und Flughäfen, in Zügen usw. Doch während beispielsweise im Zusammenhang mit Mobilfunkantennen oder Radio- und TV-Sendemasten heftig über Elektrosmog und die damit verbundenen Risiken debattiert und auch informiert wird, findet über mögliche Risiken der drahtlosen Netzwerktechnologie weder eine ausreichende Information noch eine ernsthafte Debatte statt.
Der Wunsch nach möglichst flexiblem und ortsunabhängigem Internetzugang ist gross, die Informationen zu den Auswirkungen drahtloser Netzwerke in der Schweiz dagegen sind kaum vorhanden. Gerade für die privaten Konsumentinnen und Konsumenten ist die aktuelle Situation sehr unbefriedigend, denn wollen sie sich rasch und objektiv über Vor- und Nachteile der drahtlosen Internettechnologie informieren, ist dies kaum möglich.
Umso wichtiger ist es, zum jetzigen Zeitpunkt Erkenntnisse über das Risikopotenzial drahtloser Netzwerke zu gewinnen und diese der Bevölkerung bekannt zu machen.

Stellungnahme des Bundesrates

Der Bundesrat erachtet die Erstellung eines Berichtes zum Risikopotential von drahtlosen Netzwerken als sinnvoll und notwendig. Drahtlose Netzwerke bilden einen wichtigen Bestandteil der neuen Informationstechnologien. Durch ihr rasantes Wachstum werden sie in kürzester Zeit allgegenwärtig sein. Die damit verbundenen Risiken für die Gesundheit und Umwelt sind aber noch ungenügend erforscht und nicht evaluiert. Im Auftrag des Bundesamtes für Gesundheit werden im Moment die Strahlungseigenschaften drahtloser lokaler Netzwerke untersucht. Mittels nationaler und internationaler Forschung werden potentielle Gesundheitsrisiken der elektromagnetischen Strahlung von Mobilkommunikationstechnologien untersucht. Es soll abgeklärt werden, inwieweit diese Forschungsresultate auf die drahtlosen Netzwerke übertragen werden können. Basierend auf diesen Grundlagen sollen Massnahmen empfohlen werden, welche gleichermassen einen hohen Gesundheitsschutz wie auch eine nachhaltige Technologieentwicklung ermöglichen. Zusätzlich sollen Datensicherheitsaspekte, Regelungsbedarf und der Bedarf nach Konsumenteninformation analysiert werden. Der Bericht soll in Zusammenarbeit mit allen in der Thematik involvierten Ämtern erstellt werden. Mit seinem Erscheinen ist bis Mitte 2006 zu rechnen.

7.3 Mitglieder der Arbeitsgruppe

Name	Adresse
Burgherr Rolf rolf.burgherr@bakom.admin.ch +41 32 327 5505	BAKOM Frequenzplanung - FM-FP Zukunftstr. 44 2501 Biel
Fitzpatrick Mark mark.fitzpatrick@bakom.admin.ch +41 32 327 5861	BAKOM Festnetzdienste und Grundversorgung - TC-FG Zukunftstr. 44 2501 Biel
Gruber Stefanie stefanie.gruber@bag.admin.ch +41 31 32 20098	BAG Abt. Recht 3003 Bern
Meier Martin martin.meier@bag.admin.ch +41 31 32 35694	BAG Abt. Strahlenschutz 3003 Bern
Moser Mirjana mirjana.moser@bag.admin.ch +41 31 32 29575	BAG Abt. Strahlenschutz 3003 Bern
Reusser Daniel daniel.reusser@swissmedic.ch +41 31 323 09 39	Swissmedic Abt. Medizinprodukte Hallerstr. 7 3009 Bern
Riederer Markus markus.riederer@bakom.admin.ch +41 32 327 5542	BAKOM Frequenzplanung - FM-FP Zukunftstr. 44 2501 Biel
Ryf Salome salome.ryf@bag.admin.ch +41 31 32 50983	BAG Abt. Strahlenschutz 3003 Bern
Siegenthaler Andreas andreas.siegenthaler@bafu.admin.ch +41 31 32 434 17	BAFU Abt. Luftreinhaltung und NIS 3003 Bern