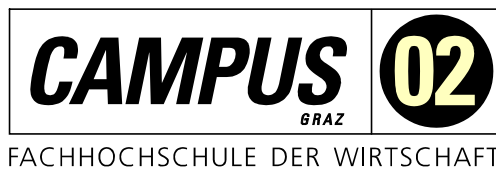


MASTERARBEIT

KONZEPTIONIERUNG EINER URBANEN WLAN-INFRASTRUKTUR

Ein umfassendes Modell zum Aufbau von öffentlichem
WLAN im städtischen Umfeld

ausgeführt am



Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Wolfgang Berger, B.Sc.

Personenkennzeichen: 1510320003

Graz, am 07. Dez. 2016

.....
Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Hiermit möchte ich mich bei all denjenigen bedanken, die mich bei der Erstellung dieser Masterarbeit einerseits fachlich, aber auch organisatorisch unterstützt haben. Ein besonderer Dank gebührt der Firma Citycom Telekommunikation GmbH, die mich in vielen Bereichen essentiell unterstützte und ohne welche diese Arbeit in der vorliegenden Form nicht möglich gewesen wäre. Ich möchte auch meinem firmenseitigen Betreuer und Teamleiter, Herrn Ing. Martin Greiner, für die fachliche Unterstützung und die entgegengebrachte Geduld sowie Rücksichtnahme danken. Vielen Dank ebenso Herrn DDI Peter Axnix für das Korrekturlesen sowie für diverse kritische Anregungen in Bezug auf meine Arbeit. Danke auch an meinem FH-Betreuer Herrn DI (FH) Christian Schmid, MSc für die konstruktive Kritik und Unterstützung bei der Gestaltung der Masterarbeit.

Ein weiteres Dankeschön gebührt meiner Familie und meinen Freunden, die mich im Zuge meiner bisherigen akademischen Laufbahn stets gefördert und unterstützt haben.

Wolfgang Berger, B.Sc.

Leibnitz, 07.12.2016

KURZFASSUNG

Öffentliches WLAN bringt einen erheblichen Mehrwert für moderne Städte weltweit. Obligatorisch für die Umsetzung eines solchen Projekts ist ein umfassendes Modell zur Konzeptionierung einer urbanen WLAN-Infrastruktur. Auf Basis der Analyse des öffentlichen WLANs der steirischen Landeshauptstadt Graz wurde ein Modell entwickelt, das als Leitfaden für Provider weltweit dienen kann. Ein bereits aktives Providernetzwerk ist als Grundvoraussetzung für die Inbetriebnahme des WLAN-Systems anzusehen, denn die Beschreibung zur Implementierung eines solchen Netzwerks ist nicht Gegenstand dieser Forschung. Die notwendigen Informationen zur Generierung des Modells basieren auf den Erkenntnissen durchgeführter Experteninterviews und aktueller technischer Literatur aus dem theoretischen Teil dieser Arbeit. Die befragten Sachkundigen lassen sich in drei Gruppen unterteilen. Gruppe eins besteht aus spezialisierten Facharbeitern in den Gebieten Netz-Design, Netzplanung und -wartung, sowie dem Betrieb von skalierenden und sicheren Rechenzentren. Experten der Gruppe zwei verfügen über fundiertes Wissen aus den Bereichen Wirtschaft und Tourismus in großen Städten. Gegenstand des Interviews der Gruppe drei sind die Themen Vertriebsmöglichkeiten und Projektmanagement. Aus technischer Perspektive ist abzuleiten, dass die Nutzeranzahl des WLAN-Systems auch ohne marketingtechnische Interventionen steigt, wenn das Modell zur Konzeptionierung einer urbanen WLAN-Infrastruktur angewendet wird. Aufgrund höherer Kapazitäten können mehr WLAN-Teilnehmer den Service verwenden. Für weitere akademische Arbeiten ist die Gesetzeslage zum Betrieb von öffentlichem WLAN ein offenes Forschungsthema. Im Detail muss analysiert werden inwiefern das steirische Baurecht, in Bezug auf die Installation von WLAN-Equipment, zu erweitern ist.

ABSTRACT

Public urban internet access delivers value-added service worldwide. A comprehensive model is needed to operate public wireless LAN successfully. This thesis focuses its analysis on a free WLAN service in Graz and develops a model to help other cities build and maintain open internet access. This research establishes a technical implementation scenario which is deployed based on an existing provider network. Necessary information for developing an urban WLAN model is gathered through expert interviews that are enhanced with the latest scientific insights presented in the theoretical part of the thesis. The interviewees are divided into three groups. Group one are professionals in the field of designing, planning and maintaining flexible and secure provider networks and operating data centres. The second group has expertise in economics and tourism in large cities. The third group possesses a deep understanding of sales and project management. The thesis results in a detailed model to implement WLAN in an urban environment. By using the model, foreign providers can deploy public internet access in cities efficiently. Furthermore, the user capacity of the system over a given period correlates with the system's technical implementation strategy, without any marketing-related interventions which are necessary to push the service forward. The legal perspectives of public internet access, for example the Styrian Construction Law regarding the installation of WLAN equipment in an urban environment, could be a suitable topic for future studies.

INHALTSVERZEICHNIS

1	EINLEITUNG	1
1.1	Wissenschaftliche Rahmenbedingungen	1
1.1.1	Problemdarstellung und Motivation	1
1.1.2	Zielsetzung und Resultat	2
1.1.3	Methode	3
1.1.4	Forschungsfrage	4
1.1.5	Hypothese	4
1.2	Städtische Informationssysteme	4
1.2.1	Fallbeispiel anhand der finnischen Großstadt Oulu	4
1.2.2	Motivation	5
2	TECHNISCHE ASPEKTE FÜR DEN BETRIEB VON KABELLOSEN NETZWERKEN	6
2.1	Der WLAN Standard IEEE 802.11	6
2.1.1	Kollisionsvermeidung in IEEE 802.11 Netzwerken	8
2.1.2	IEEE 802.11ac	10
2.1.3	WLAN als Entlastungstechnologie für Mobilfunknetzwerke	10
2.2	Interferenzen bei der Übertragung von Daten mittels WLAN	12
2.2.1	Selektion eines geeigneten WLAN-Kanals	12
2.2.2	Selbstoptimierendes WLAN	14
2.3	Energieeffiziente Gestaltung von WLAN-Umgebungen	15
2.3.1	Analyse des kabellosen Netzwerks	16
2.3.2	Energieoptimierungspläne	16
2.3.3	Energieoptimierung im städtischen Umfeld	17
2.4	Zentralisierte Verwaltung von Access Points	18
2.4.1	Control and Provisioning of Wireless Access Points (CAPWAP)	18
2.4.2	Proprietäre Software zur Verwaltung von Access Points	19
2.5	Sicherheit in kabellosen Netzwerken	21
2.5.1	Sicherheitsmaßnahmen zum autorisierten Zugriff auf kabellose Netzwerke	22
2.5.2	Autorisierungs- und Authentifizierungsverfahren im öffentlichen WLAN	25
2.5.3	Nutzungseinschränkungen durch Inhaltsanalysen	28

3	GESETZLICHE REGULIERUNGEN EINES ÖFFENTLICHEN WLAN NETZWERKS	33
3.1	Lizenzrechtliche Vorgaben und Rahmenbedingungen.....	33
3.1.1	Allgemeingenehmigung	34
3.1.2	Freigegebene Frequenzbänder	34
3.1.3	Empfehlungen der europäischen Kommission	36
3.2	Gesundheit und Immission	36
3.2.1	Festlegung und Einhaltung von Grenzwerten	37
3.2.2	WLAN-Funkanlagen	38
3.3	Privatrechtliche Haftungsrisiken beim Betrieb	38
3.3.1	Haftung in Abhängigkeit der WLAN-Sicherheit	39
3.3.2	Empfehlungen für österreichische WLAN-Provider	39
3.4	Nutzungsanalyse und Datenschutz der Internetuser	39
3.4.1	Cookies.....	40
3.4.2	Analysesoftware	42
3.4.3	Steuerung von Cookies durch den Nutzer	44
4	ANALYSE: DAS ÖFFENTLICHE WLAN DER STEIRISCHEN LANDESHAUPTSTADT GRAZ....	45
4.1	Urbanes WLAN in Graz	45
4.1.1	Die Entstehung des öffentlichen WLAN in Graz.....	46
4.1.2	Sicherheit im „Cityaccess“	47
4.1.3	Kundengewinnung durch Public-WLAN	48
4.1.4	Wirtschaftliche Betrachtung des „Cityaccess“	48
4.2	Ausrichtung der Dienstleistung am Markt.....	49
4.2.1	Das Captive Portal als Serviceplattform	49
4.2.2	Informationsgewinn durch Teilnehmeranalyse	50
4.2.3	Die Bewerbung der Dienstleistung als Herausforderung	50
4.2.4	Serviceetablierung unter Anbetracht der Stakeholder.....	50
4.3	Öffentliches WLAN als Service für den Tourismus- und Wirtschaftsstandort Graz	51
4.3.1	Öffentliches WLAN im Tourismus.....	51
4.3.2	Akquisition von Reisenden mittels WLAN	52
4.3.3	Angebotsoptimierung durch Herkunft- und Bewegungsanalysen von Touristen	52
4.3.4	Immission durch WLAN	52

4.4	Der Standorterhebungs- und Umsetzungsprozess	53
4.4.1	Die Initialisierung eines Standortes	53
4.4.2	Bauvorgaben bei der Installation	53
4.4.3	Service und Betrieb	55
4.4.4	Regulatorischer Änderungsbedarf	56
4.5	Technische Konzeptionierung der Servicestandorte	56
4.5.1	Herausforderungen aus Sicht der IT	56
4.5.2	Access Point-Hardware	57
4.5.3	Monitoring und Servicemanagement	58
4.5.4	Self-Service Funktionalitäten	58
5	MODELL EINES URBANEN WLAN-NETZWERKS	59
5.1	Aufbau und Infrastrukturkomponente	59
5.1.1	Softwarelösungen zur Servicekonzipierung	60
5.1.2	Darstellung der Architektur	60
5.2	Technische Implementierung eines Captive Portal- und Analysesystems	62
5.2.1	WLAN-System Konfigurationsprozess	62
5.2.2	Das WLAN-Analysesystem	63
5.2.3	Self-Service Funktionalitäten	64
5.3	Überwachung der Dienstleistung	65
5.3.1	Sicherheitsmanagement	65
5.3.2	Dienstleistungsüberwachung	66
5.4	Resultat	68
5.4.1	Graphische Modelldarstellung	68
5.4.2	Modellvalidierung	69
6	AUSBLICK UND FAZIT	73
	ANHANG A - BEISPIEL FÜR DEN WLAN-ANALYSECODE	75
	ANHANG B - PERSONAS	76
	ABKÜRZUNGSVERZEICHNIS	79
	ABBILDUNGSVERZEICHNIS	82
	TABELLENVERZEICHNIS	83
	LITERATURVERZEICHNIS	84

1 EINLEITUNG

Das erste Kapitel dieser Arbeit ist in zwei Teile aufgeteilt, wobei das erste Unterkapitel die wissenschaftlichen Rahmenbedingungen, bestehend aus der grundlegenden Problemstellung, sowie der Motivation dieser Arbeit, definiert. Einen weiteren Bestandteil dieses Kapitels bilden die Beschreibung der Methodik zur Erreichung der Zielsetzung, die Beantwortung der Forschungsfrage, sowie die Überprüfung der Hypothesen.

Die zweite Sektion der Einleitung beschreibt städtische Informationssysteme anhand der finnischen Stadt Oulu.

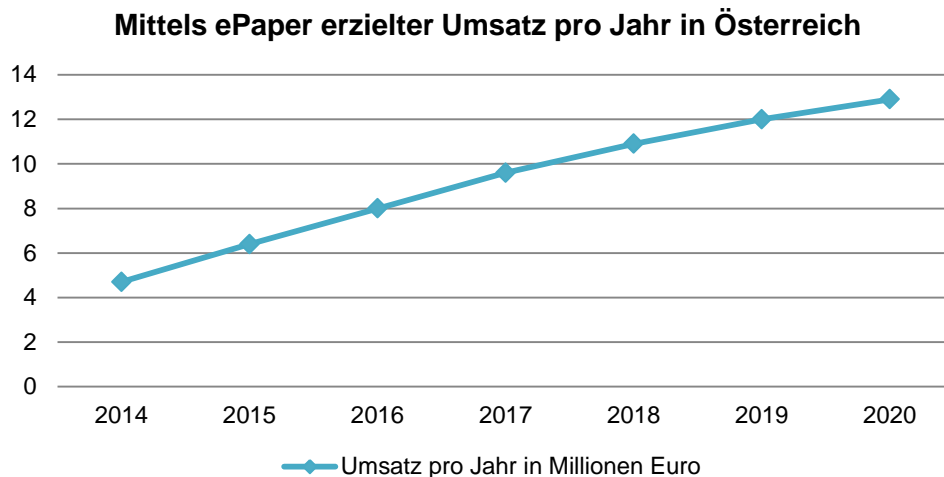
1.1 Wissenschaftliche Rahmenbedingungen

Die nachfolgenden wissenschaftlichen Rahmenbedingungen bilden einen organisatorischen Überblick über die wichtigen Metriken der Masterarbeit.

1.1.1 Problemdarstellung und Motivation

Gegenwärtig werden zunehmend digitale Medien zur Befriedigung des Informationsverlangens verwendet, da diese überregional erreichbar, leicht zugänglich und aktuell sind. Tagsüber wird keine Zeit exklusiv für den Konsum von Nachrichten reserviert. Vielmehr fungiert Informationsbeschaffung als Lückenfüller in Wartezeiten oder Pausen. Dieses Verhalten wird durch die weite Verbreitung von mobilen Geräten, wie Smartphones oder Tablets, ermöglicht. Nutzer tendieren zur vermehrten Inanspruchnahme von Nachrichtenseiten, wenn Informationen in sozialen Netzwerken, den Benutzern vorab und ohne explizites Interesse, präsentiert werden. (Wippersberg, 2016, S. 3)

Genau durch dieses Verhalten und den dadurch neuentwickelten innovativen Produkten, sowie Dienstleistungen, steigen die Anforderungen an das lokale Telekommunikationsnetz. Zeitungen, als klassische Informationsbeschaffungsmedien werden zunehmend um virtuelle Quellen erweitert, um den heute üblichen multimedialen Ansprüchen gerecht zu werden. Die nachfolgende *Abbildung 1* prognostiziert den mittels E-Paper erzielten Umsatz pro Jahr in Österreich.



*Abbildung 1 Der in Österreich erzielte Umsatz mittels E-Paper pro Jahr (in Millionen Euro)
Quelle: eigene Darstellung nach (Statista GmbH, 2015)*

Durch den kontinuierlich steigenden Informationsfluss bedarf es, neben leistungsstarken WLAN-Zugangspunkten (Wireless Local Area Network), vor allem einer fundierten Planung der dahinterliegenden Infrastruktur, um zukunftssichere Skalierung zu garantieren. Intelligente Übertragungstechnologien in Kombination mit neuartigen Software- und Hardwareprodukten ermöglichen den leistungsstarken Ausbau einer städtischen Infrastruktur.

Ungeachtet der technischen Realisierbarkeit einer urbanen WLAN Lösung, müssen primär die politischen, sowie rechtlichen Weichen gestellt und dadurch klare Rahmenbedingungen für das WLAN-System definiert werden. Insbesondere die Haftung des WLAN-Providers und die frei verwendbaren Funkkanäle zur Datenübertragung gelten als umstrittene Punkte für den Betrieb eines öffentlichen WLAN Netzwerks.

Eine Vielzahl europäischer Städte, darunter auch Graz, Linz, Wien und Oulu bieten bereits kostenlosen Internetzugang als Service für Bürger und Touristen an. Bürger, wie auch Touristen profitieren von der Ersparnis des eigenen mobilen Datenvolumens und vom freien Internetzugang im Allgemeinen.

Die persönliche Motivation des Autors liegt in der Umsetzung eines ganzheitlichen Konzepts für den Betrieb einer öffentlichen WLAN Lösung. Kommunikation ist ein Ausdruck der menschlichen Persönlichkeit. Umso wichtiger ist es, einen kostenfreien, zuverlässigen und leicht zugänglichen Service zu schaffen, um diese Art der Verständigung zu ermöglichen.

1.1.2 Zielsetzung und Resultat

Das Ziel der Masterarbeit ist die Entwicklung eines Modells für den performanten und sicheren Betrieb von frei zugänglichem WLAN in Städten. Dabei stehen der freie und benutzerfreundliche Zugang durch den Endanwender und auch die einfache Administrierbarkeit des Systems durch den WLAN-Provider, im Vordergrund.

Der praktische Nutzen besteht darin, dass Personen ein freier und performanter, aber jedoch reglementierter, Zugang zum Internet geboten wird. Das Resultat dieser Masterarbeit ist ein Modell, das sowohl organisatorische als auch technische Aspekte zur Planung und zum Betrieb einer WLAN-Lösung definiert.

1.1.3 Methode

Die Masterarbeit wird in Kooperation mit der Firma Citycom Telekommunikation GmbH verfasst, mit dem Ziel ein generell anwendbares Modell zur Konzeptionierung einer urbanen WLAN-Infrastruktur am Beispiel Graz zu entwickeln.

Zur Erreichung der Zielsetzung dienen Experteninterviews mit Personen aus folgenden Fachbereichen:

- Technische Expertise im Aufbau, Planung und Betrieb von großen Netzwerkinfrastrukturen sowie flexibler Rechenzentrumslösungen
- Wirtschaftliches Fachwissen im Bereich Tourismus sowie Aufbau von regionalen Telekommunikationsnetzen
- Expertenwissen aus Vertriebs- sowie Projektmanagementsicht

Im Fokus der Experteninterviews stehen die technische Umsetzung des Service, sowie die strategische Auswahl zukünftiger Servicestandorte. Ein weiterer wichtiger Teil der Interviews ist die Diskussion über den Mehrwert von öffentlichem WLAN für den Tourismus- und Wirtschaftsstandort Graz. Das Expertengremium bietet eine ausgewogene Mischung aus wirtschafts- und technikaffiner Expertise. In Kombination mit den Anforderungen einer modernen Kulturstadt lässt sich ein Modell für den performanten und sicheren Betrieb von frei zugänglichem WLAN definieren.

Aus technischer Sicht wird der Standorterhebungs- und Umsetzungsprozess diskutiert. Dies impliziert unter anderem die Erreichbarkeit des Standorts mittels Lichtwellenleiter- (LWL) Technik, den Aufbau- und Konfigurationsaufwand von Endgeräten, die Flächenabdeckung mittels WLAN, sowie die Notwendigkeit eines auf den Standort anpassbaren Captive Portal¹ und Analysesystems.

Im wirtschaftlichen Fokus steht die Bedeutung von öffentlichem Internetzugang für Menschen in Graz, sowie der Aufbau und Betrieb eines solchen Systems.

Die durch die Experteninterviews erlangten Informationen bilden den Rahmen für die Gestaltung des Modells für den performanten und sicheren Betrieb von frei zugänglichem WLAN. Zur Auswertung der Interviews durch den Autor dienen Transkripte und Audiomitschnitte der Gespräche.

¹ Als Captive Portal bezeichnet man eine nicht zu umgehende Website, die den Teilnehmenden eines WLAN Netzwerks initial nach dem Verbindungsaufbau, aus Gründen der Verrechnung oder zur Bestätigung der allgemeinen Nutzungsbedingungen, präsentiert wird.

1.1.4 Forschungsfrage

Was muss getan werden, um eine leistungsstarke, sichere und einfach zugängliche WLAN Infrastruktur im städtischen Umfeld abzubilden?

1.1.5 Hypothese

Ein öffentlich nutzbare WLAN-Lösung ist ein notwendiger Bestandteil einer modernen Stadt und kann von lokalen Providern nutzenoptimiert betrieben werden. Es besteht ein Zusammenhang zwischen der Auslastung eines WLAN-Standorts und dessen technischer Ausbauplanung.

1.2 Städtische Informationssysteme

Weltweit finden sich zahlreiche Metropolen, darunter der koreanische Seoul Gangnam Distrikt, die der Bevölkerung Informationsdienstleistungen, in Form von öffentlichem WLAN oder interaktiven und multimedialen Mediensäulen, anbieten. Die dahinterliegende Grundidee ist jene, dass Informationen allgegenwärtig werden. Hierbei unterscheidet man zwei Systeme. Solche, die auf Anfrage des Benutzers Informationen liefern und jene, die dem Anwender aktiv und prophylaktisch Fakten präsentieren. Ein essentieller Faktor eines städtischen Informationssystems ist die zielgruppenorientierte Auswahl der dargestellten Inhalte. Diese beziehen sich auf typographische Merkmale der Personen, sowie den Ort und die Zeit. (Schumann & Stock, 2015, S. 191 f.)

Durch öffentliches WLAN können Menschen das Internet nutzen, ohne ihr eigenes Datenvolumen zu verbrauchen, oder gar Roaming-Kosten bezahlen zu müssen.

In vielen Städten ist es gegenwertig üblich, spezielle Informationsapplikationen für mobile Geräte anzubieten. Beispielsweise kann man sich über Wetterprognosen, lokale Neuigkeiten oder dem Fahrplan der öffentlichen Verkehrsmittel informieren. (Schumann & Stock, 2015, S. 191 f.)

1.2.1 Fallbeispiel anhand der finnischen Großstadt Oulu

Oulu ist eine der am schnellsten wachsenden Großstädte Finnlands und ist vorwiegend technisch geprägt. Rund 800 Technologiekonzerne, wie beispielsweise Nokia haben einen Firmensitz in Oulu. Knapp 20% der Arbeitskräfte in Oulu arbeiten in der Elektronik und Computertechnik (ICT). Ein weiteres Potential für die Stadt bieten die insgesamt über 20.000 Studenten aus den regional ansässigen Universitäten. (Schumann & Stock, 2015, S. 195 ff.)

Neben den stationären Informationssäulen, genannt „*UBI-hotspots*“, bietet Oulu ein öffentlich nutzbares WLAN, genannt „*panOULU*“ an. Das „*panOULU*“ Netzwerk wird mit Hilfe von zahlreichen öffentlichen- und privaten Organisationen betrieben. Darunter befinden sich lokale Internet Service Provider (ISP), die Regierung, sowie industrielle Unternehmen. (Schumann & Stock, 2015, S. 195 ff.)

Seit 2001 hat sich die Anzahl an Access Points (AP) um ein Vielfaches erhöht. Seit dem Jahr 2012 stehen rund 1.350 Access Points zur Verfügung, was eine beträchtliche Abdeckung bedeutet. Die höchste Dichte der installierten APs ist an zentralen Plätzen in der Innenstadt aufzufinden. Rund 500 APs sind in einem Umkreis von 1km betriebsbereit. Der barrierefreie, kostenlose und einfache Zugriff durch den Endanwender steht definitiv im Vordergrund. Die finnische Großstadt Oulu geht hier allerdings noch einen Schritt weiter und hat mit dem Service „*panOULU Luotsi*“ ein Informationssystem geschaffen, das Informationen abgestimmt auf den Standort des Benutzers anbietet. (Schumann & Stock, 2015, S. 195 ff.)

Im Rahmen Ihrer Publikation führten Schuhmann und Stock (2015) eine Umfrage über das Nutzungsverhalten des öffentlichen WLAN in Oulu durch und kamen zu folgendem Ergebnis: Am häufigsten findet das WLAN Verwendung für Personen, die ihre Social-Media-Kanäle überprüfen, Mails versenden, Wetterprognosen abfragen, Busfahrpläne einsehen oder generelle Nachrichten abrufen möchten. Der Großteil der befragten Personen nützt den Laptop, um auf „*panOULU*“ zuzugreifen. Nur ein recht geringer Anteil greift auf Tablet-Computer als ICT-Gerät zurück. (Schumann & Stock, 2015, S. 201 f.)

Bezüglich der Sicherheit des „*panOULU*“ WLAN sind sich die Befragten nicht einig. Knapp die Hälfte findet, dass das Surfen im Internet über „*panOULU*“ nicht sicher ist. Es gibt bestimmte Tätigkeiten, die man lieber nicht in einem öffentlichen WLAN durchführen sollte, z.B. jene, wo Passwörter unverschlüsselt oder nur unzureichend gesichert übertragen werden, da diese mittels eines „*Packet Sniffer*“² und den entsprechenden Fachkenntnissen, ausgelesen werden können. (Schumann & Stock, 2015, S. 202 ff.)

Trotz der weitreichenden WLAN-Abdeckung in Oulu ist das „*panOULU*“-Netzwerk kein Konkurrenzprodukt zu den Internetangeboten der lokalen Provider. Gründe dafür sind einerseits die Internetgeschwindigkeit und andererseits die eingeschränkte flächenmäßige Abdeckung. Ein Großteil der Befragten ist vom öffentlichen WLAN Angebot überzeugt und wünscht sich ein solches Angebot auch in anderen Städten. Als einzige Kritikpunkte scheinen eine ausbaufähige WLAN-Abdeckung, sowie eine offensichtliche Kundmachung, dass „*panOULU*“ wirklich gratis ist, auf. (Schumann & Stock, 2015, S. 202 ff.)

1.2.2 Motivation

Das Beispiel anhand von Oulu zeigt, dass öffentliches WLAN zunehmend an Beliebtheit gewinnt und der Einsatz von frei zugänglichem WLAN kontinuierliches Wachstum erlebt. Trotz einiger Sicherheitsbedenken und ausbaufähigen Netzabdeckungen in manchen Städten, ist es naheliegend, dass auch die Steirische Landeshauptstadt Graz ihr öffentliches WLAN ausbauen wird, um den Einwohnern und Touristen bestmöglichen Informationszugang zu ermöglichen. Diese Masterarbeit beschreibt ein Modell für den performanten und sicheren Betrieb von frei zugänglichem WLAN und geht speziell auf übliche Fallstricke bei der Planung und Installation der Services ein.

² Software, die Netzwerkpakete aufzeichnet

2 TECHNISCHE ASPEKTE FÜR DEN BETRIEB VON KABELLOSEN NETZWERKEN

Gegenstand dieses Kapitels ist die Erfassung der technischen Informationen zur Entwicklung des WLAN-Systems. Zu Beginn wird der WLAN Standard IEEE 802.11 und dessen Spezifikationen genauer untersucht. Hier liegt der Fokus auf den unterschiedlichen Übertragungsraten und Möglichkeiten dieses Standards. Interferenzen bei der Übertragung von Daten mittels WLAN stellen IT-Fachkräfte vor große Herausforderungen. Die Selektion eines geeigneten WLAN-Kanals ist essentiell, um bestmögliche Übertragungsraten und Stabilität zu erzielen. Störfaktoren von kabellosen Datenverbindungen sind nicht statisch, weshalb ein theoretischer Ansatz zur Selbstoptimierung von WLAN beschrieben wird. Die energieeffiziente Gestaltung von kabellosen Umgebungen ist eine wichtige Teildisziplin beim Betrieb von WLAN-Netzzugängen. Energieeinsparungen lassen sich durch verschiedene Methoden, mit Hilfe der zentralisierten Verwaltung von Access Points, umsetzen. Kabellose Netzwerke bieten eine komfortable, aber auch potentiell unsichere Art und Weise an, um auf Internetressourcen zuzugreifen. IT-Administratoren müssen das WLAN-Konzept an die Zielgruppe des Netzwerks anpassen, um so das optimale Authentifizierungsverfahren zu wählen. Ein weiterer essentieller Planungspunkt ist die Implementierung von unternehmens- und gesetzeskonform Content-Filtering Maßnahmen, um Unternehmensdaten zu schützen und illegale Internetaktivitäten zu verhindern.

2.1 Der WLAN Standard IEEE 802.11

Das „*Institute of Electrical and Electronics Engineers*“ (IEEE) entwickelte den Standard IEEE 802.11 im Jahr 1997, um eine Alternative zu konventionellen kabelgebundenen Netzwerken zu schaffen. Der dem WLAN zugrundeliegende Standard IEEE 802.11 wurde in den letzten Jahren ständig überarbeitet und weiter verbessert. Der Erfolg von IEEE 802.11 liegt in der hohen Flexibilität, sowie der ausgeprägten Interoperabilität des Standards. Erste Derivate dieser Norm wurden für die Verwendung von unlizenziierten Frequenzbändern konzipiert. Infolgedessen operieren die meisten IEEE 802.11 Standards im 2,4 GHz und 5 GHz Frequenzband. Prinzipiell sind diese Frequenzbänder, unter Betrachtung kleinerer Frequenzanpassungen je Land, weltweit frei verfügbar, was dazu führt, dass Jedem die Bereitstellung eines WLAN-Netzwerks ermöglicht wird. Als Konsequenz steigt die Anzahl an WLAN-Netzwerken in dichtbesiedelten Gebieten zunehmend, wodurch Verbindungsstörungen zunehmen und die „*Quality of Service*“ (QoS) beeinträchtigt wird. (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 1)

Die Anforderungen an ein modernes WLAN steigen aufgrund von hochauflösenden Videos und anderen bandbreitenintensiven Anwendungen stetig. Längst nutzen Benutzer WLAN nicht nur zum Versenden von E-Mails oder zum Surfen im Internet, weshalb neben der Übertragungsfähigkeit auch die Übertragungssicherheit in Form von kurzen Latenzen zu berücksichtigen ist. (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 1 f.)

Tabelle 1 zeigt jene Derivate, die derzeit von der Masse der Endgeräte unterstützt werden. Die einzelnen Abwandlungen des IEEE 802.11 werden laufend verbessert oder durch neue Funktionalitäten aufgewertet. In der nachfolgenden *Tabelle 2* sind die neuesten Entwicklungen nach IEEE 802.11 aufgelistet.

Derivat	Verbreitung	Band	Übertragungsgeschwindigkeit
802.11a	veralteter Standard	5 GHz	54 MBit/s
802.11b	Standard, welcher vor allem bei alten Laptops Verwendung findet.	2,4 GHz	11 MBit/s
802.11g	Ähnlich wie 802.11b	2,4 GHz	54 MBit/s
802.11n	Gegenwärtig gängigster Standard, der von einer Vielzahl an Geräten unterstützt wird. Weiteres ist eine Abwärtskompatibilität gegeben.	2,4 GHz und 5 GHz	300 MBit/s

*Tabelle 1 Von der Masse an Endgeräten unterstützte 802.11 Derivate
Quelle: eigene Darstellung nach (Schreiner, 2012, S. 152)*

Derivat	Veröffentlichungsdatum	Band	Ziel
802.11aa	2012	2,4 GHz und 5 GHz	Robuste Übertragung von Audio und Video Inhalten
802.11ac	2014	5 GHz	WLAN mit sehr hoher Übertragungsrate im Bereich von unter 6 GHz
802.11af	2014	470-790 MHz (EU)	WLAN im TV Bereich
802.11ah	2016	54-72,76-88,174-216, 470-698,698-806 MHz(US) 902-928 MHz(US)	WLAN im unteren 1 GHz Bereich
802.11ax	2019	863-868 MHz(EU) 755-787 (China) 916.5-927.5 MHz(JP) 2,4 GHz und 5 GHz	Hoch effiziente WLANs (HEW)

*Tabelle 2 Ausblick kommender IEEE 802.11 Derivate
Quelle: eigene Darstellung nach (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 3)*

2.1.1 Kollisionsvermeidung in IEEE 802.11 Netzwerken

Bei einer aktiven Verbindung zwischen einer Station (STA) und einem Access Point (AP), beginnen beide Parteien mit der Übertragung von Paketen. Das Problem besteht darin, dass zwei aktive Stationen im selben Zeitfenster Daten über denselben Kanal hin zum Access Point transportieren könnten, was zu Kollisionen der Datenpakete führen würde. Das MAC-Protokoll von IEEE 802.11 verfügt über ein Verfahren zur Vermeidung von Kollisionen. CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) funktioniert ähnlich wie die Kollisionserkennung (CSMA/CD bzw. Carrier Sense Multiple Access Collision Detection) bei Ethernet. Der wesentlichste Unterschied besteht darin, dass CSMA/CA Kollisionen nicht nur erkennt, sondern diese im Vorhinein verhindert. Aufgrund der hohen Bitfehlerrate von Funkkanälen, erfordert IEEE 802.11 zudem Bestätigungen (Acknowledgements) und gegebenenfalls Übertragungswiederholungen, um eine reibungslose Verbindung bereitzustellen. *Abbildung 2* illustriert die Datenübertragung zwischen einer WLAN-Quelle und einem kabellosen Ziel. Bevor die Quelle mit der Datenübertragung beginnt, wird zuerst ein freier Kanal verifiziert und eine kurze Zeit abgewartet. Dieses Abwarten vor dem Senden von Daten wird als Distributed Inter-Frame Spacing (DIFS) bezeichnet und bildet neben dem Short Inter-Frame Spacing (SIFS) zwei Pufferzeiten für die korrekte Übertragung von Datenrahmen. (Kurose & Ross, 2012, S. 576 ff.)

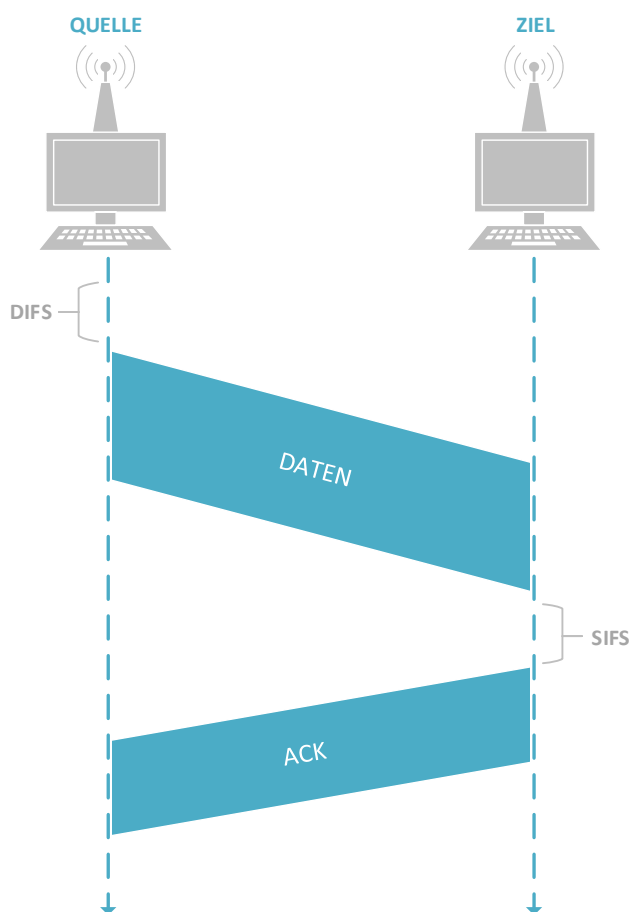


Abbildung 2 IEEE 802.11 CSMA/CA

Quelle: eigene Darstellung nach (Kurose & Ross, 2012, S. 578)

Der Umgang mit dem Hidden-Terminal-Problem soll sicherstellen, dass Clients, die mit demselben Access Point verbunden sind, sich jedoch durch das Problem des WLAN-Fading gegenseitig nicht erkennen, Daten auf demselben Kanal senden und so Kollisionen verursachen. Aus diesem Grund gibt es in der IEEE 802.11 Spezifikation die Kontrollrahmen Request-to-Send (RTS) und Clear-to-Send (CTS). Zuerst sendet der Client einen RTS-Rahmen (Broadcast) an den Access Point und alle im Netz befindlichen STAs. Dieser Rahmen beinhaltet die Zeit, die für die Übertragung des gesamten Daten- und Acknowledgement-Rahmens benötigt wird. Nach Erhalt dieses Rahmens schickt der Access Point einen CTS-Rahmen an alle im Netz befindlichen STAs. Dies dient dazu den RTS schickenden Client grünes Licht für die Datenübertragung zu geben und alle anderen Stationen anzuweisen, während des reservierten Zeitspektrums, keine Übertragungen anzustoßen. Die Verwendung von RTS- und CTS-Rahmen schafft den essentiellen Vorteil, dass im Falle einer unwahrscheinlichen Kollision nur die kurzen Kontrollrahmen kollidieren und nicht die ressourcenintensiveren Datenrahmen. Als Nachteil ist jedoch der erhöhte Kanalressourcenverbrauch anzumerken. Um in der Praxis Ressourcen zu sparen, legt jede Station einen bestimmten RTS-Schwellwert fest. Nur für Datenrahmen, die größer als dieser Schwellenwert sind, ist ein RTS/CTS erforderlich. (Kurose & Ross, 2012, S. 579 f.)

Abbildung 3 zeigt das Senden eines Datenrahmens unter Berücksichtigung des RTS/CTS-Mechanismus.

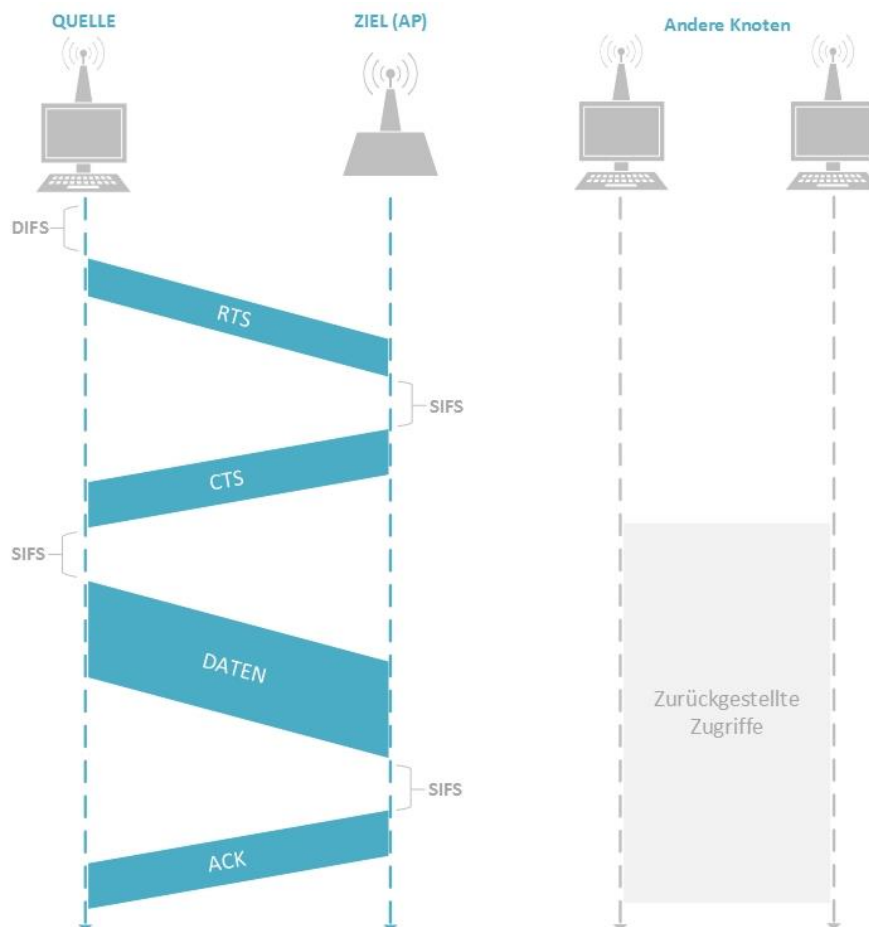


Abbildung 3 Kollisionsvermeidung mittels RTS/CTS
 Quelle: eigene Darstellung nach (Kurose & Ross, 2012, S. 581)

2.1.2 IEEE 802.11ac

Der WLAN-Standard IEEE 802.11ac ist sowohl im privaten-, als auch im unternehmerischen Kontext, zum bedeutendsten WLAN-Standard herangewachsen. Durch die Einführung neuer Layer-1-Technologien (Physikalischer Layer) und erweiterter MAC-Funktionalitäten, erhöhte sich die WLAN-Kapazität maßgeblich. Diese Neuerungen erlauben, im Vergleich zum Vorgänger Standard (IEEE 802.11n), eine vier Mal höhere Datenübertragungsrate von knapp 1 GBit/s. Im Gegensatz zu IEEE 802.11n unterstützt IEEE 802.11ac einen erhöhten, aber optimalen, Kanalbereich von bis zu 160 MHz. Mithilfe von „*channel bonding*“ (Gruppierung aufeinanderfolgender 20 MHz Kanäle) können hohe Übertragungsraten erzielt werden. Um den Umgang mit dem sogenannten „*Hidden-Terminal-Problem*“ zu verbessern, verfügt IEEE 802.11ac über erweiterte RTS/CTS Frames. Infolgedessen wird die maximal zur Verfügung stehende Kanalbandbreite auf Sender- und Empfängerseite bestimmt. Sollte der CTS-Frame eine kleinere Kanalbandbreite beinhalten als der RTS-Frame, wird dieser vom Sender angenommen. Als bedeutendste Neuerung gegenüber IEEE 802.11n ist die Einführung von „*Downlink multiuser MIMO*“ (MU-MIMO) zu erwähnen. Diese Technologie erlaubt die simultane Datenübertragung vom Access Point hin zu unterschiedlichsten Empfangsstationen (STAs). Im IEEE 802.11ac Standard können maximal acht Antennen, aufgeteilt in zwei Datenströme, bis zu vier unterschiedliche Benutzer pro Datenstrom, zur selben Zeit bedienen. Der Access Point spezifiziert Gruppen von STAs, die für den Empfang von Daten vorgesehen sind. Diese Informationen sind im neuen IEEE 802.11ac PHY-Header hinterlegt und werden isotrop an alle STAs gesendet (Broadcast). Die Art und Weise, wie die STAs gruppiert werden, obliegt dem jeweiligen Access Point, nachdem dieser das sogenannte „*channel state information feedback*“ von allen STAs abgefragt hat. (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 5)

2.1.3 WLAN als Entlastungstechnologie für Mobilfunknetzwerke

Öffentliche WLAN Hotspots können von lokalen Internet Service Providern oder öffentlichen Gemeinschaften betrieben werden und gewinnen zunehmend an Bedeutung. Anfänglich entwickelten sich seitens der Mobilfunkanbieter Bedenken bezüglich neuer Mitbewerber im Datenübertragungssektor. Ungeachtet dieser anfänglichen Bedenken nutzen Mobilfunkbetreiber WLAN, um die heutigen mobilen Datenmassen bewältigen zu können. WLAN nach IEEE 802.11 ermöglicht Mobilfunkanbietern eine Entlastung ihrer Haupt- und Zugangsnetzwerke. Zwar unterstützt LTE Mechanismen zum Auslagern von Datenströmen, allerdings fokussieren sich diese Technologien auf das Hauptnetzwerk des Providers („*core network*“). Durch die Einführung sogenannter „*offloading paths*“ können Daten, die eigentlich das Mobilfunknetz verwenden sollen, zum Lastenausgleich über externe WLAN-Strecken transportiert werden. Nachfolgende *Abbildung 4* zeigt den konzeptionellen Aufbau von WLAN als Entlastungstechnologie für Mobilfunknetzwerke: (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 20 f.)

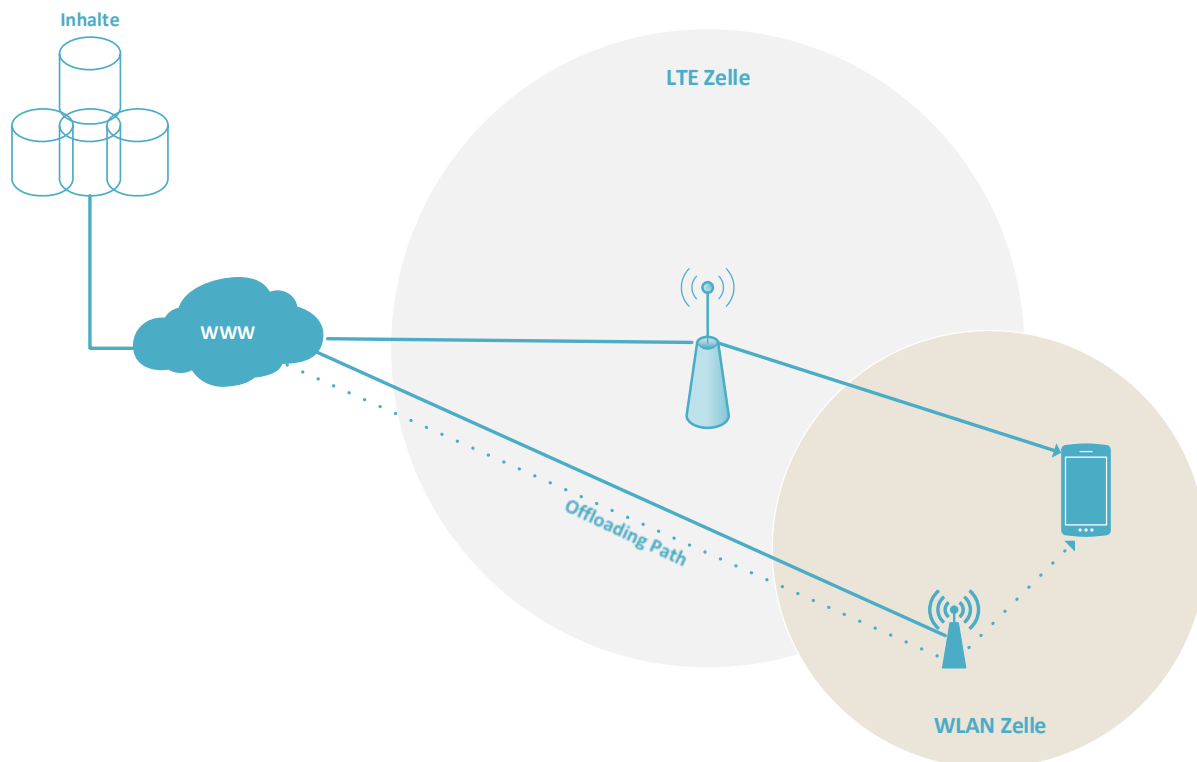


Abbildung 4 Entlastung von LTE mittels WLAN

Quelle: eigene Darstellung nach (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 20)

IP Flow Mobility and Seamless Offload (IFOM) unterstützt die nahtlose Zusammenarbeit mit IEEE 802.11 basierenden WLAN Netzwerken und LTE Verbindungen. IFOM bezieht sich auf IPv6 Technologien und erlaubt dabei richtliniengesteuertes und simultanes Routen von ausgewählten IP Paketen zwischen unterschiedlichen Übertragungstechnologien. Obwohl das Empfangsgerät mit dem WLAN Netzwerk kommuniziert, bleibt eine LTE Verbindung aufrecht. Um solch eine Logik zu verwalten, bedarf es einer zentralen Steuerungseinheit, genannt Access Network Discovery and Selection Function Server (ANDSF), im Hauptnetzwerk des Mobilfunkanbieters. Diese Steuerungseinheit stellt dem STA Informationen über die Verfügbarkeit und Qualität von benachbarten Netzwerken bereit und regelt den Prozess des Netzwerkwechsels. Die Verwendung mehrerer Interfaces stellt ein neues Konzept dar und Bedarf einer genauen Erforschung, um produktiv eingesetzt zu werden. Generell gibt es eine Vielzahl bestehender „*offloading*“ Methoden, um das Mobilfunknetzwerk zu entlasten. Die meisten Algorithmen zur Erforschung des „*offloading*“ Ansatzes beschäftigen sich mit Vorhersagen über den Aufenthaltsort von STAs in der umliegenden WLAN-Umgebung, Bewegungsströme, WLAN-Kapazität und den zu transferierenden Daten. (Bellalta, Bononi, Bruno, & Kassler, 2015, S. 20 f.)

2.2 Interferenzen bei der Übertragung von Daten mittels WLAN

WLAN ist elektromagnetische Strahlung, die über die Entfernung abnimmt. Das Fading nimmt drastisch zu, wenn sich feste Hindernisse oder andere störende Signalquellen zwischen Client und Access Point befinden. Nach (Cisco Systems, Inc, 2007, S. 1) sind beispielsweise Funktelefone, Mikrowellenherde, Bluetooth Geräte, kabellose Videokameras, kabellose Spiele-Controller aber auch fluoreszierende Lampen typische Störfaktoren eines kabellosen Netzwerks.

Durch die Resonanz des Wassers in Fußbodenheizungen werden WLAN Signale (2,4 GHz Bereich) wesentlich gestört, wodurch die stockwerkübergreifende Verbindungsqualität zwischen dem Access Point und einer Empfangsstation beeinträchtigt wird.

Selbst die Durchführung eines Radio Frequenz Scans (RF), garantiert nicht, dass man alle Interferenzen findet, da diese oft nur temporär bei der Verwendung eines Gerätes auftreten. (Cisco Systems, Inc, 2007, S. 2) Elektromagnetische Wellen reflektieren an Gegenständen in der Umgebung, wonach sich unterschiedliche Signalwege zwischen der Sende- und der Empfangsstation bilden und das Signal unscharf transportiert wird. Diesen Umstand bezeichnet man als Mehrwegeausbreitung. (Kurose & Ross, 2012, S. 564)

Die Interferenzen bei der Übertragung von Daten mittels IEEE 802.11 können keinesfalls durch die Bereitstellung mehrerer Access Points, im engen geographischen Sinne, gelöst werden. Sollen mehrere APs im engen Umfeld betrieben werden, so muss die Sendestärke jedes Access Points gedrosselt werden, um nicht gegenseitige Interferenzen zu produzieren. Selbst die Verwendung von 5 GHz fähigen STAs reduziert Interferenzen nicht. Heutzutage gibt es eine Vielzahl an kabellosen Geräten, die ebenfalls das 5 GHz Band verwenden. Die einfachste Möglichkeit interferenzgenerierende Geräte zu verhindern ist die Erstellung einer Firmenrichtlinie, die den Betrieb von Bluetooth-Headsets oder Mikrowellenherde verbietet. Des Weiteren könnten spezielle Räumlichkeiten geschaffen werden, die frei von Störungen sind, um beispielsweise erfolgskritische Systeme kabellos zu betreiben. (Cisco Systems, Inc, 2007, S. 3 ff.)

2.2.1 Selektion eines geeigneten WLAN-Kanals

Die geographische Dichte an Access Points erfordert Methoden für die intelligente Ausnutzung freier Kanäle, um Interferenzen weitgehend zu minimieren. Es ist eine schwierige Aufgabe, den optimalen Kanal unter Anbetracht von Upstream- und Downstream-Verbindungen zu finden. Nachfolgend wird ein Modell zur geeigneten Selektion freier Kanäle beschrieben. Dieses Modell bringt erhebliche Verbesserungen im Vergleich zu den beiden nachfolgend angeführten Vorgehensweisen zur Selektion eines geeigneten WLAN Kanals (Client-Assisted Channel Assignment Optimization und Least Congested Channel Selection). (Kwon, Choi, Kim, & Chung, 2015, S. 45)

Um die Systemgeschwindigkeit in hoch frequentierten Netzwerken zu steigern, fokussieren sich die Forschungstätigkeiten der High-Efficiency WLAN Task Group (HEW TG) auf die Entwicklung des IEEE 802.11ax Standards. Mithilfe von MAC-Technologien werden Interferenzen benachbarter STAs vermieden. MAC basierte Kanalentscheidungstechnologien werden in zentralisierte und verteilte Methoden aufgeteilt. Zentralisierte Methoden verwenden einen Access Point Controller, der auf Kosten von CPU-Leistung, alle Informationen der angeschlossenen Access Points sammelt und den optimalen Kanal je Access Point zuteilt. Im Gegensatz dazu bestimmen APs in verteilten Systemen, den aus ihrer Sicht optimalen Kanal, selbst. Die Kanalzuteilung erfolgt anonym, also ohne jegliche Mitteilungen an die benachbarten STAs, weshalb das Finden eines passenden Kanals eine erhebliche Herausforderung darstellt. Interferenzen zwischen Access Points und Clients hängen im Wesentlichen von der Anzahl an assoziierten und nicht assoziierten STAs am AP ab. Die Kanalinformationen nicht assoziierter STAs können aufgrund der fehlenden Implementierung im IEEE 802.11-Standard nicht ausgelesen werden. (Kwon, Choi, Kim, & Chung, 2015, S. 46)

Least congested channel selection (LCCS)

Das LCCS Prinzip sucht nach Kanälen, die eine minimale Anzahl an STAs beinhalten. Jeder Access Point sendet über den verwendeten Kanal ein sogenanntes „*beacon packet*“ aus, welches als Hinweis für die Anzahl an verbundener STAs dient. Jeder Access Point sendet diese Pakete aus und erhält auch Pakete von benachbarten APs. Das Problem besteht darin, dass die Informationen nur von angrenzenden Access Points verwertet werden können. Ein weiteres Problemfeld von LCCS ist die Erkennung der am wenigsten ausgelasteten Kanäle bei „*downstream*“ und „*upstream*“ Übertragungen. Die Auslastung bei LCCS bezieht sich nur auf die Anzahl der STAs im Kanal und nicht auf die Auslastung des Kanals im Sinne der Datenübertragung. Um dieses Problem zu adressieren, wurde das „*client-assisted channel assignment optimization*“ (CACAO) Schema entwickelt. (Kwon, Choi, Kim, & Chung, 2015, S. 47)

Client-assisted channel assignment optimization (CACAO)

CACAO verwendet den IEEE 802.11k Standard für das Ressourcenmanagement der Kanäle. STAs haben die Fähigkeit, benachbarte APs über die Auslastung der umliegenden Kanäle zu informieren. Diese Informationen sind nicht vollständig korrekt, da auch STAs, die mit dem assoziierten AP nicht interferieren, gemeldet werden. In großen Netzwerken, die eine Vielzahl von Access Points beinhalten, erhöht sich so der Overhead für die Auswahl des richtigen Kanals erheblich. Das ständige Wechseln der Kanäle ist somit suboptimal für die Performance des Systems. (Kwon, Choi, Kim, & Chung, 2015, S. 48)

Schema nach (Kwon, Choi, Kim, & Chung, 2015)

Das Schema nach (Kwon, Choi, Kim, & Chung, 2015) beschreibt die Auswahl des geeigneten Kanals durch eine Adaption des „*beacon frame*“. Als zusätzliches Informationselement wurde das sogenannte „*channel load information element*“ beigefügt. Diese Erweiterung besteht aus folgenden Feldern: „*element ID, length, service set identifier (SSID), channel number, channel load list*“. Das Feld „*element ID*“ weist auf die Existenz des „*channel information element*“ im Body des Frames hin. Das Element „*length*“ beschreibt die Länge des „*channel information element*“. Das Feld „*channel load list*“ besteht aus zwei Subelementen. Das erste Subelement beinhaltet die SSID des benachbarten Access Points, das Zweite kennzeichnet die Nummer der STAs, die diesen benachbarten Access Point kennen. (Kwon, Choi, Kim, & Chung, 2015, S. 48)

Das vorgestellte Schema besteht aus zwei Phasen, der Initialphase und der Kanal-Auswahlphase, welche jeweils für die Kanalabschätzung und dessen optimale Auswahl für das System, zuständig sind. In der Initialphase sendet der Access Point ein „*beacon frame*“ mit einem initialen „*channel load information element*“, aber jedoch leerem „*channel load list*“ Feld aus. Um dieses Feld zu befüllen, fordert der Access Point die assoziierten STAs auf, eine „*active channel scanning*“ Prozedur durchzuführen, wonach diese Prozedur von den STAs gemäß IEEE 802.11 Standard ausgeführt wird. Jeder STA setzt den assoziierten Access Point über die „*channel scanning information*“, mit den SSIDs von benachbarten APs, in Kenntnis. Danach bestimmt der AP die Anzahl an STAs, die eine SSID gemeldet haben. Infolgedessen aktualisiert der Access Point die zwei Subelemente der „*channel load list*“ (SSID und Anzahl an STAs). (Kwon, Choi, Kim, & Chung, 2015, S. 48)

Mit Hilfe der periodisch durchgeführten Kanal-Auswahlphase schätzt der Access Point die Anzahl an störender STAs in jedem Kanal und wählt den optimalsten Kanal aus. Der AP und dessen assoziierte STAs führen periodisch ein „*passive channel scanning*“ aus, um den „*beacon frame*“ von angrenzenden APs mitzuhören und deren Kanallastinformationen zu kennen. Sollten die Access Points ihre SSID im ersten Subelement der „*channel load list*“ finden, überprüfen sie den Wert des zweiten Subelements, das die Anzahl an störender STAs im Umfeld beinhaltet. Wenn eine STA, die bereits mit einem AP verbunden ist, außerhalb des Umfelds eines benachbarten Access Point liegt, kann dieser keine Interferenzen erkennen. Um dieses Problem zu lösen, überprüfen die STAs das „*channel load list*“ Feld und melden die Anzahl an störender STAs für jeden Kanal ihrem assoziierten Access Point. Daraufhin zählt der Access Point die Anzahl an interferierenden STAs und bestimmt den am wenigsten gestörten Kanal, was in weiterer Folge zu erheblichen Performancesteigerungen führt. (Kwon, Choi, Kim, & Chung, 2015, S. 50)

2.2.2 Selbstoptimierendes WLAN

Die Optimierung eines WLAN Netzwerks stellt eine Herausforderung für den derzeitigen Forschungsstand dar. (Lee & Kim, 2016, S. 61) erkannten das gegenwertige Problem der verstopften Kanäle im 20/40 MHz-, als auch im 80/160-MHz Bereich.

Nicht zuletzt durch die zunehmende Verbreitung von IEEE 802.11ac im 5 GHz-Bereich, welche eine höhere Anzahl an WLAN-Geräten bedienen und eine performantere Datenübertragung realisieren kann, wird das Problem der verstopften Kanäle zunehmend verstärkt. (Lee & Kim, 2016, S. 61) analysierten den ACI-Effekt (Adjacent Channel Interference) auf das Carrier Sense (CS) und der automatischen Verstärkungsregelung (AGC) von WLAN. Zur Adressierung des Problems wurde ein eigener Schwellenwert entwickelt, welcher in der „*interference-aware self-optimizing*“ (IASO) „*carrier sensor jointly optimizing initial gain and multi-channel multi-level carrier sensing*“ Theorie Anwendung findet. IASO bringt erhebliche Verbesserungen in Bezug auf Latenz, Datenübertragungsrate, Energieeffizienz und dynamischer Reichweite. (Lee & Kim, 2016, S. 61)

2.3 Energieeffiziente Gestaltung von WLAN-Umgebungen

Kabellose Netzwerkgeräte entwickeln sich zunehmend als unabdingbare Kommunikationsschnittstelle zwischen Menschen im privaten und öffentlichen Umfeld. Das Problem besteht darin, dass Access Points unbenutzt betrieben werden, um durch Benutzer generierte Spitzenlasten abdecken zu können. Access Points, aus der UniFi AC Produktreihe der Firma Ubiquiti, haben einen maximalen Energieverbrauch von 6,5 bis 22 Watt. Der Stromverbrauch hängt stark vom Typ des WLAN-Senders und dessen tatsächlicher Auslastung ab. So verbrauchen leistungsstarke Hotspots mehr Strom, als Access Points, die nur für eine geringe WLAN-Teilnehmeranzahl ausgelegt sind. (Ubiquiti Networks, Inc. (a), 2016, S. 6 ff.)

Primär Organisationen, die ein dichtes WLAN-Netzwerk betreiben, beschäftigen sich daher mit Methoden, um den Stromverbrauch der installierten Access Points zu optimieren. Aktuell existieren zwei Algorithmen, zur erfahrungswertgesteuerten Energieoptimierung von WLAN-Stationen. Der „*off-line*“ Algorithmus schätzt den Bedarf an WLAN basierend auf zuvor gemessenen und verarbeiteten Informationen. Dies impliziert historische Daten über eingeschaltete Access Points, verbundene Benutzer und übertragende Daten je Zugangspunkt. Unter Einbezug dieser Erfahrungswerte wird ein statischer Plan für das Powermanagement des APs entwickelt. Dank der geringen Komplexität dieser Vorgehensweise und der hohen Energieeinsparung ist der „*off-line*“ Algorithmus als eine potentiell geeignete Strategie zu betrachten, wobei jedoch die Gefahr der Unter- bzw. Überschätzung besteht. Im Gegensatz zum „*off-line*“ Algorithmus schätzt der „*on-line*“ Algorithmus den WLAN Bedarf der User basierend auf Echtzeitmessungen des generierten Datenverkehrs. Die hohe Flexibilität dieses Ansatzes ermöglicht, unter Anbetracht höherer Rechenaufwände, eine optimale Energieeinsparung. Bevor mit der Optimierung des Energieverbrauchs begonnen werden kann, muss eine Bewegungsmatrix der WLAN-Teilnehmer, unter Anbetracht deren Datennutzungsintensität im WLAN, erstellt werden. Basierend auf den erlangten Erkenntnissen erfolgt die Planung einer Energieoptimierungsstrategie. (Ganjia, et al., 2014, S. 1 f.)

2.3.1 Analyse des kabellosen Netzwerks

Um die Bewegungsanalyse in kabellosen Netzwerken festzustellen, muss eine Synergie zwischen der „*polling-based*“ Methode, auf Basis von SNMP und der „*event-based*“ Methode, auf Basis von Assoziationsinformationen und Log-Nachrichten, erstellt werden. Durch regelmäßige SNMP-Anfragen an den Access Point können eine Vielzahl relevanter Metriken abgefragt werden. Die Zeit zwischen den einzelnen Anfragenachrichten wird durch die eventbasierte Methode kompensiert, um die Präzision der Ergebnisse sicherzustellen. Die administrationsfreundliche Darstellung der Analyseergebnisse übernimmt üblicherweise ein WLAN-Controller. Dieser hat den Vorteil, dass sowohl anfragebasierte als auch eventbasierte Informationen zentral verarbeitet und exportiert werden können. Infolgedessen bedarf es keiner Konfigurationsänderung des bestehenden Netzwerks oder der Installation spezieller Auditgeräte. (Ganjia, et al., 2014, S. 4)

Typische Metriken, die durch einen WLAN-Controller aufgezeichnet werden sind:

- Name des Users, dessen IP und MAC-Adresse
- Assoziationsbeginn und Ende pro User, sowie dessen konsumierte Datenmenge
- SSID und IEEE 802.11 Protokoll

(Ganjia, et al., 2014, S. 4)

2.3.2 Energieoptimierungspläne

Grundsätzlich unterscheidet man zwischen statischen, dynamischen und nutzermobilitätsbasierenden Strategien, um den Energieverbrauch zu senken. Statische Strategien basieren auf historischen Werten und achten nicht auf die momentane Auslastung der Access Points. Beispielsweise können sämtliche Access Points über Nacht oder nach 22:00 Uhr abgeschaltet werden, um so eine signifikante Energieeinsparung zu erzielen. Ein partielles Abschalten, in wenig frequentierten Arealen, ist ein sinnvoller Ansatz, um Energie zu sparen, die Kommunikation jedoch nicht gänzlich lahmzulegen. Dieses Vorgehen erzielt in öffentlichen Gebäuden und Schulen, außerhalb der Betriebszeiten, optimale Energiesparergebnisse, ohne dabei den Service der Liegenschaft zu beeinflussen. (Ganjia, et al., 2014, S. 6 ff.)

Die dynamische Methode erkennt den Bedarf an WLAN durch Benutzer und regelt so die Stromzufuhr zu den einzelnen Access Points, die auch wirklich benötigt werden, um einen gewissen Bereich abzudecken. Vorzugsweise sind jene Access Points, die sich im Eingangsbereich oder in Durchzugswegen befinden aktiv. Sollte ein User im Netz erkannt werden, erweitert sich die WLAN-Abdeckung durch mehrere APs dynamisch. Durch diese Strategie kann zusätzlich Energie eingespart werden, da APs, die zurzeit nicht benötigt werden, einer dynamischen Deaktivierung unterliegen. (Ganjia, et al., 2014, S. 10 ff.)

Nutzermobilitätsbasierende Strategien fassen eine Menge von Access Points zusammen, die von einem User durchschnittlich verwendet werden. Diese Informationen werden im Profil des Benutzers abgespeichert. Um letztendlich Energie zu sparen, werden Cluster von Access Points definiert. Der Cluster Head bietet hierbei die WLAN-Grundabdeckung. Die Idee besteht darin, dass wenn sich ein Benutzer mit einem AP in seinem User Set verbindet, nur jene APs im Cluster aktiviert werden, die sich ebenfalls im User Set des Benutzers befinden („*user-profile-based approach*“), da hier Potential für Roaming entsteht. Alle anderen, nicht benötigten Access Points, werden im Gegensatz zu traditionellen clusterbasierten Ansätzen, erst gar nicht mit Strom versorgt. Jene unbenützten APs, die sich sowohl im User Set, als auch im Cluster befinden, werden nach einer gewissen inaktiven Zeit deaktiviert. Daher ist es wichtig, dass sich der User primär mit dem Cluster Head assoziiert und die anderen Access Points im Cluster nur bei Bedarf aktiviert werden. (Ganjia, et al., 2014, S. 14 f.)

2.3.3 Energieoptimierung im städtischen Umfeld

Die Forschungsergebnisse von (Ganjia, et al., 2014) fokussieren sich primär auf Energieeinsparungen in organisierten Unternehmungen. Dies hat den Vorteil, dass klare Strukturen und immer wiederkehrende Mobilitätspatterns leichter abgeschätzt werden können, um die Access Point On/Off-Strategie zu trainieren. Klar definierte Ereignisse wie Mittagspausen oder Öffnungszeiten bilden einen sicheren Rahmen für Interventionen auf Netzwerkebene.

Im urbanen Umfeld lassen sich solche Ereignisse wesentlich schwerer abschätzen, obwohl jedoch Gemeinsamkeiten klar zu erkennen sind. Beispielsweise können zusätzliche Access Points an Hauptbahnhöfen und Nahverkehrsdrehscheiben aktiviert werden, um den Strom an Pendlern nach Feierabend abzufertigen. In Einkaufsstraßen können Access Points jedoch nicht nach Ladenschluss deaktiviert werden. Es ist nicht auszuschließen, dass Passanten und Fußgänger das öffentliche WLAN außerhalb der Geschäftszeiten verwenden wollen. Darüber hinaus verfügen Städte über eine wesentlich breitere Nutzerbasis und eine höhere Dynamik als geschlossene Organisationen. Die Verwaltung von User Sets würde enorme Datenmengen erzeugen und die Sinnhaftigkeit der Energieersparnis relativieren. Indikatoren für die Erhöhung der WLAN-Kapazität wären Großveranstaltungen, Märkte oder ähnliche dichtfrequentierte Ereignisse. Um intelligente On/Off-Strategien zu entwickeln bedarf es einer durch Controller gestützten Access Point-Verwaltung. Da das Netzwerk in Städten zunehmend wächst und sich die Anforderungen ständig ändern, ist oft nicht jeder Access Point per Controller steuerbar, sondern muss dediziert verwaltet werden, was zu einer zusätzlichen Komplexitätssteigerung führt.

2.4 Zentralisierte Verwaltung von Access Points

Wachsende kabellose Netzwerke verlangen eine zentralisierte Überwachungs- und Verwaltungslösung, um die Performance, Verfügbarkeit und Sicherheit des Service sicherzustellen. Durch eine zentralisierte Netzwerkverwaltung können Probleme leichter erkannt und behoben werden. Die Verwendung von zentralen WLAN-Controllern manifestiert den Begriff „*Access Point*“ grundlegender. APs arbeiten somit nur mehr als reine Zugriffspunkte, die extern gesteuert werden.

2.4.1 Control and Provisioning of Wireless Access Points (CAPWAP)

Die Internet Engineering Task Force verfügt über eine Expertengruppe, die sich mit Schwierigkeit von zentralisierten Verwaltungsszenarien auseinandersetzt. Die „*Control and Provisioning of Wireless Access Points*“ (CAPWAP) definiert Standardlösungen für die Überwachung, Kontrolle und Verwaltung von großen IEEE 802.11 Netzwerken. (Bernaschi, et al., 2011, S. 1283)

Das Ziel des gleichnamigen Protokolls CAPWAP ist die Bereitstellung eines einzigen Kontrollzugriffspunkt für eine Vielzahl an Access Points. Obwohl das CAPWAP Protokoll auf der IEEE 802.11 Architektur aufbaut, gibt es keine Technologieeinschränkungen durch die verwendete Frequenz bzw. Kanaltechnologie. Neben der zentralisierten Steuerung und Autorisierung von Richtlinienverwaltung, sollen durch CAPWAP geschaffene Controller, Access Points entlasten, sodass jene nur mehr durch zeitkritische Aktivitäten belastet werden. Alle rechenintensiven Vorgänge geschehen am Netzwerk-Controller und nicht mehr direkt auf jedem Access Point. Infolgedessen sollen generische Kapselungs- und Transportmechanismen zur Verfügung gestellt werden. Die CAPWAP-Implementierung nutzt das (User Datagram Protocol) UDP als Transportprotokoll und besteht einerseits aus den CAPWAP-Datennachrichten („*data messages*“) und andererseits aus den CAPWAP-Kontrollnachrichten („*control messages*“). Des Weiteren verfügt CAPWAP über ein eigenes Protokoll zur automatischen Assoziation zwischen dem WLAN-Controller und den Access Points. Im Gegensatz zum Simple Network Management Protocol (SNMP) ist CAPWAP speziell für die Verwaltung von Access Points entwickelt. SNMP ist ein generellerer Ansatz zur Administration von Netzwerkgeräten. Eine SNMP-Adaption zur Steuerung von Access Points ist aus administrationstechnischer Sicht nicht empfehlenswert, da CAPWAP speziell für diesen Anwendungsfall entwickelt wurde. (Bernaschi, et al., 2011, S. 1284)

(Bernaschi, et al., 2011, S. 1285) definieren eine Adaption von CAPWAP, namens „OpenCapwap“, bestehend aus der in *Tabelle 3* ersichtlichen Komponenten.

Bestandteil	Beschreibung
AC daemon	Implementiert CAPWAP-Kontrollfunktionen und steuert externe Anwendungen.
WTP daemon	Implementiert die von CAPWAP zur Verfügung gestellten kabellosen Endpunkttechnologien und interagiert mit externen Anwendungen.
External application (AC Side)	Erstellt eine Liste von WTPs (Wireless Termination Point), die mit dem Controller verbunden sind, sendet und empfängt Daten.
External application (WTP Side)	Steht im Datenaustausch mit dem OpenCapwap WTP daemon.

Tabelle 3 OpenCapwap Bestandteile.

Quelle: eigene Darstellung nach (Bernaschi, et al., 2011, S. 1285)

Mit OpenCapwap, in Kombination mit dem auf GNU/Linux basierenden System „OpenWrt“, wird eine zentralisierte und quelloffene Verwaltung von drahtlosen Zugriffspunkten ermöglicht. OpenWrt ist ein spezielles, quelloffenes Betriebssystem für ältere, generische Access Points. Die Verwaltungslösung besteht aus zwei Applikationen, dem UCI Server (auf WTP Seite) und einer Remote UCI (auf Seite des Controllers). Mit Hilfe des Unified Command Interface (UCI) können die WTPs letztendlich konfiguriert werden. (Bernaschi, et al., 2011, S. 1286)

2.4.2 Proprietäre Software zur Verwaltung von Access Points

Unternehmensfokussierte Hersteller von Access Points, stellen passend zum Produktportfolio, proprietäre Software zur Administration von WTPs zur Verfügung. Diese Steuerungssoftware kann herstellerabhängig *on-premise* oder *off-premise* betrieben werden. Der Vorteil von proprietärer Software liegt darin, dass IT-Administratoren auf die optimal abgestimmte Software zum Produkt zurückgreifen können. Es sind keine komplizierten und wartungsintensiven Analysen zu eventuellen Problembehebungen nötig, da Support geboten wird. *Abbildung 5* zeigt das Dashboard des UniFi Enterprise System Controller von Ubiquiti Networks. Die in Java geschriebene Webapplikation vereint alle Vorteile einer Controller-gestützten Lösung in einem benutzerfreundlichen Frontend. Hersteller tendieren dazu, in den entwickelten Administrationsoberflächen ein Rundpaket ihrer Leistungen anzubieten, um so eine ganzheitliche Administration zu realisieren. Dabei übernimmt der Controller neben der optimalen Aufteilung der STAs auf die jeweiligen Frequenzbänder, sofern die Access Points dies automatisch zulassen, auch erweiterte Analyseaufgaben. *Abbildung 6* illustriert eine Nutzungsstatistik im Gesamten und pro Access Point. *Abbildung 7* zeigt den schematischen Plan eines Büroraums, um eine ungefähre WLAN Abdeckung zu demonstrieren. (Ubiquiti Networks, Inc. (b), 2016)

Der UniFi Enterprise Controller verfügt zusätzlich über eine Google Maps-Unterstützung. Dieses Feature ist vor allem bei der Gestaltung eines urbanen WLAN-Netzwerks äußerst nützlich. Darüber hinaus erleichtert ein WLAN-Controller die Verwaltung mehrerer SSIDs in Kombination mit strukturierten VLAN-Umgebungen (Virtual Local Area Network). Außerdem unterstützt die UniFi Enterprise Controller Software das Band Steering (Technologie zur Aufteilung verbundener STAs auf das 2,4 GHz oder das 5 GHz Netz bei dualbandfähigen WLAN-Geräten), sowie die Airtime Fairness-Technologie. (Ubiquiti Networks, Inc. (b), 2016)

Airtime Fairness teilt jedem verbundenen Teilnehmer, unabhängig von dessen theoretischer Übertragungsgeschwindigkeit, gleich viel Zeit für den Datentransfer zu. Infolgedessen resultiert eine höhere Performance für WLAN-Geräte der aktuellen Generation (IEEE 802.11n und besser), sofern ältere WLAN-Geräte, mit dem gleichen Access Point verbunden sind. (Ruckus Wireless, Inc., 2014)

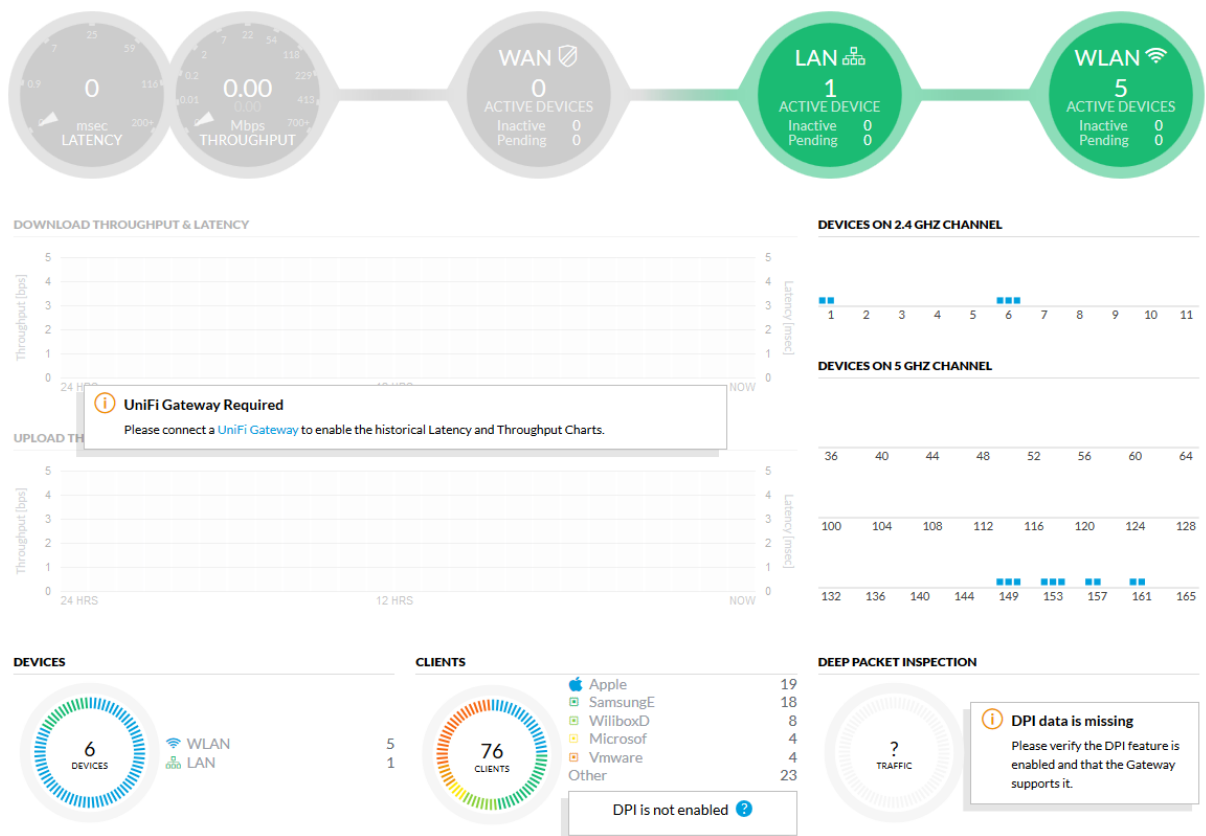


Abbildung 5 UniFi Enterprise Controller Dashboard
Quelle: vom Autor erstellt

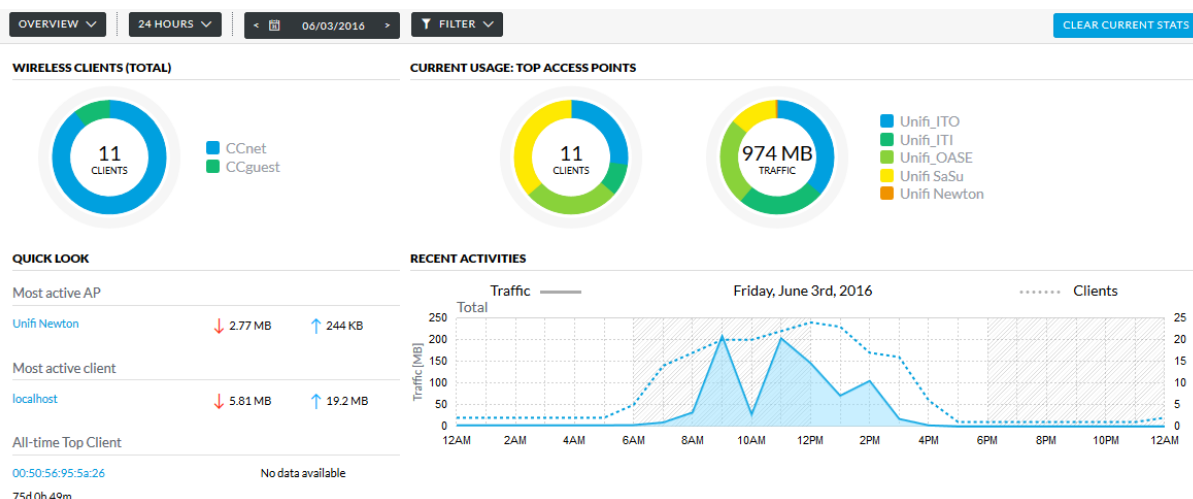


Abbildung 6 UniFi Enterprise Controller Nutzungsanalyse
Quelle: vom Autor erstellt

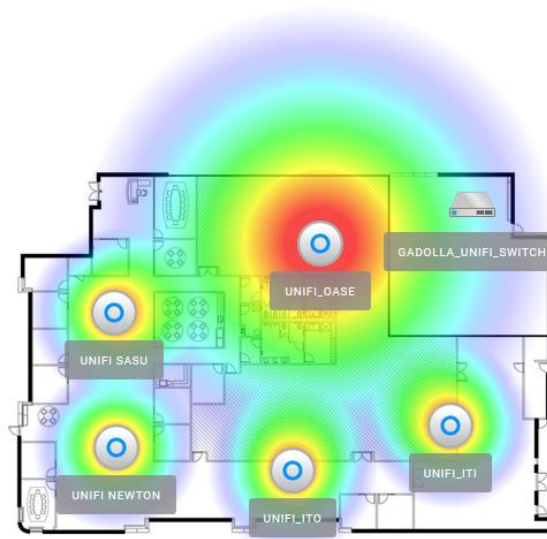


Abbildung 7 UniFi Enterprise Controller WLAN Abdeckung
Quelle: vom Autor erstellt

2.5 Sicherheit in kabellosen Netzwerken

Die weite Verbreitung von Wi-Fi fähigen Geräten führt zum Anstieg von WLAN-Netzwerken im öffentlichen und privaten Umfeld. Dieses Kapitel fokussiert sich auf die Sicherheit der Datenübertragung in kabellosen Netzwerken. Trotz weitreichender Verbreitung von HTTPS-Webseiten (Hypertext Transfer Protocol Secure) und dem damit einhergehenden Sicherheitsgewinn, ist es nicht ratsam, streng vertrauliche Internetaktivitäten, wie z.B. Online Banking, in öffentlichen WLAN-Netzwerken durchzuführen. In Bezug auf WLAN-Sicherheit werden zwei Sicherheitskonzepte unterschieden. Im ersten Konzept werden Sicherheitsmaßnahmen zum autorisierten Zugriff auf kabellose Netzwerke beschrieben.

Die Nutzerbasis ist bekannt, denn es sind Authentifizierungsinformationen für die Nutzung des Dienstes erforderlich. Das zweite Konzept beschreibt ein öffentlich zugängliches und unverschlüsseltes WLAN, das von einer unbekanntem Nutzerbasis verwendet wird. Hierbei steht der freie und einfache Zugang im Vordergrund.

2.5.1 Sicherheitsmaßnahmen zum autorisierten Zugriff auf kabellose Netzwerke

Nach der Einführung des IEEE 802.11-Standards begann die Entwicklung einer sicheren Standarderweiterung für die vertrauliche Kommunikation in drahtlosen Netzwerken. Der im Jahr 2004 freigegebene IEEE 802.11i-Standard verfügt über eine Vielzahl von Verbesserungen im Bereich der Authentifizierungsmechanismen und der Schlüsselverteilung. Das weitgehend unsichere Wired Equivalent Privacy-Verfahren (WEP) wurde durch modernere und besser durchdachte Verfahren ersetzt. (Kurose & Ross, 2012, S. 783)

WEP verwendet das RC4-Verschlüsselungsschema und das CRC-32 Verfahren, um die Datenintegrität sicherzustellen. Der von WEP verwendete „*shared key*“ hat eine Länge von 5 bis 13 Bytes. (Mekhazniaa & Zidania, 2015, S. 173)

Wi-Fi Protected Access (WPA) ist die sichere und überarbeitete Version des IEEE 802.11i-Standards. WPA basiert auf dem Temporary Key Integrity Protocol (TKIP) und ermöglicht eine zufällige Schlüsselgenerierung, um Attacken basierend auf statistischen Analysen zu verhindern. Weiteres verfügt WPA, im Gegensatz zu WEP, über erweiterte Sicherheitseigenschaften, wie Schlüsselhashfunktionen und den Message Integrity Check (MIC). (Mekhazniaa & Zidania, 2015, S. 173)

Moderne kabellose Netzwerke setzen auf den Nachfolgestandard von WPA. WPA2 bündelt eine Vielzahl von sicherheitsrelevanten Neuerungen im Bereich der Client Authentifizierung und der Datenintegrität. Sicher konfigurierte drahtlose Netzwerke werden üblicherweise durch den Überbegriff Robust Security Network (RSN) zusammengefasst. Wird für die Authentifizierung ein Four-Way-Handshake verwendet, so spricht man von Robust Security Network Association (RSNA). Prinzipiell unterscheidet man bei WPA2 zwei verschiedene Authentifizierungsmethoden. Die erste Methode setzt die Kenntnis eines sogenannten Pre-Shared Key (PSK) voraus, um sich authentifizieren zu können. Dieser Schlüssel ist für jeden Benutzer gleich, weshalb WPA2-PSK meist in kleineren Unternehmen oder Privathaushalten eingesetzt wird. Bei der zweiten Methode verfügt jeder Benutzer über eigene Authentifizierungsinformationen, die zentral von einem Authentifizierungsserver nach dem IEEE 802.1X Standard abgewickelt werden. (Sotzek, 2012, S. 15 f.)

Jeder Access Point, der die IEEE 802.1X-Authentifizierung unterstützt, muss netzwerktechnischen Kontakt zu einem zentralen Authentifizierungsserver haben, um die vom Benutzer bereitgestellten Anmeldeinformationen zu überprüfen. Durch die erweiterte Abstraktion der Authentifizierung, weg vom Access Point, resultieren erleichterte Managementmöglichkeiten, was den Wartungsaufwand reduziert, die Sicherheit erhöht und Kosten senkt. *Abbildung 8* beschreibt die aus vier Phasen bestehende Authentifizierung mittels IEEE 802.11i. (Kurose & Ross, 2012, S. 783)

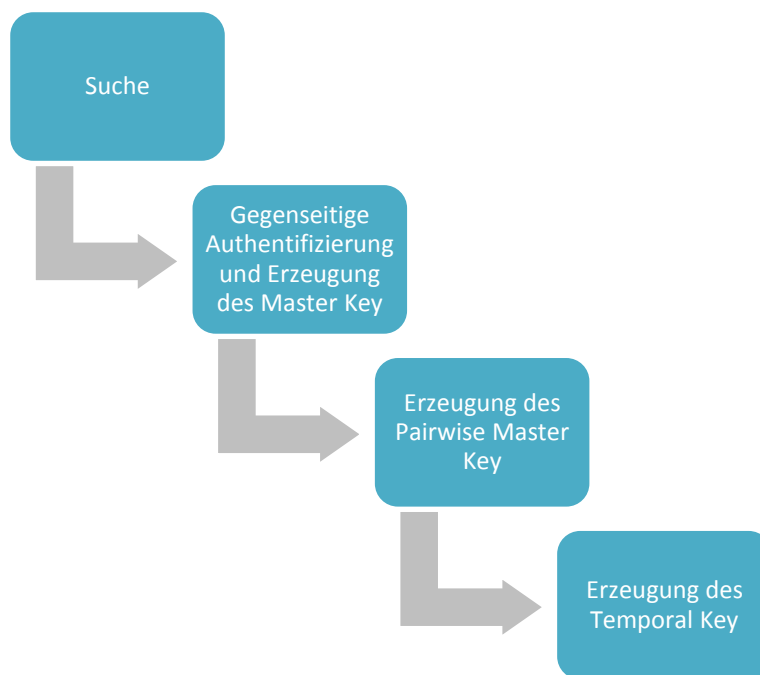


Abbildung 8 IEEE802.11i Authentifizierung
Quelle: eigene Darstellung nach (Kurose & Ross, 2012, S. 783 ff.)

Bei der Suche gibt der Access Point die zur Verfügung stehenden Verschlüsselungstypen an die Teilnehmer des WLANs weiter. Der Klient entscheidet anschließend, welcher Typ für die Verbindung verwendet wird. In der zweiten Phase findet die Authentifizierung des Users beim Authentifizierungsserver statt. Der Access Point fungiert hierbei als Nachrichtenweiterleiter. Die Kommunikation bzw. die Nachrichtenformate zwischen dem „*Supplicant*“ (Benutzer) und dem Authentifizierungsserver werden durch das Extensible Authentication Protocol (EAP) definiert. Der Klient sendet die mittels EAPoL (EAP over LAN) verpackten Nachrichten an den Access Point, der diese Nachrichten entpackt, in RADIUS verpackt und anschließend mittels UDP/IP an den Authentifizierungsserver (auch RADIUS Server genannt) sendet. In diesem Fall bildet der „*Authenticator*“ (Access Point) den Zugriffspunkt zum RADIUS Server, der sich für gewöhnlich in einer sicheren Netzwerkumgebung befindet. (Kurose & Ross, 2012, S. 783 f.)

Neben EAP-TLS existieren diverse weitere Derivate und Authentifizierungsmethoden, wie z.B.:

- MSCHAP-V2
- EAP-OTP
- EAP-FAST
- LEAP
- EAP-MD5
- EAP
- EAP-GTC
- PEAP

Im dritten Schritt erstellen Klient und Authentifizierungsserver, unter Verwendung ihres Master Key (MK), einen gemeinsamen, geheimen Pairwise Master Key (PMK). Dieser Key ist nun beiden Parteien bekannt, wodurch sie nun gegenseitig authentifiziert sind. Mit Hilfe des gemeinsam erstellten Primary Master Key können die Parteien nun weitere Schlüssel, zur Verschlüsselung von Daten auf der Sicherungsschicht, erstellen. (Kurose & Ross, 2012, S. 784 f.)

Authentifizierung im Forschungsnetzwerk eduroam

„eduroam“, als Teil des pan-europäischen Forschungsnetzwerks GÉANT, offeriert Studenten teilnehmender akademischer Einrichtungen sicheren Internetzugang. Verwaltet wird „eduroam“ durch das National Research and Educational Network Policy Committee (NREN PC). Die Authentifizierung der Netzwerkteilnehmer erfolgt über die Heiminstitution mit den dort bereitgestellten Anmeldedaten. Die Autorisierung, um auf lokale Netzwerkressourcen zuzugreifen, erfolgt durch das besuchte Netzwerk. (Milinović, Winter, Srce / CARNet, RESTENA, & SA3 T2 group, 2012, S. 5 f.)

Eine hierarchisch aufgebaute RADIUS-Serverinfrastruktur (Remote Authentication Dial-In User Service) transportiert die Authentifizierungsanfragen vom Benutzer einer besuchten Organisation hin zur eigenen Institution und retour. Typischerweise administriert jede Organisation einen eigenen RADIUS-Server, welcher die bereitgestellten Anmeldeinformationen mit einer lokalen Benutzerdatenbank abgleicht. Dieser RADIUS-Server ist mit einem zentralen und nationalen RADIUS-Server verbunden, welcher wiederum mit einem europäischen oder globalen RADIUS-Server kommuniziert. Durch die im Benutzernamen eines Klienten enthaltene Domäne, im Kontext auch „realm“ genannt, kann der RADIUS-Server die Authentifizierungsanforderungen zur korrekten Heimorganisation leiten. STAs verwenden den IEEE 802.1X-Standard und EAP, um einen sicheren Tunnel für die Authentifizierung bereitzustellen. *Abbildung 9* illustriert den „eduroam“ Authentifizierungsweg von der besuchten- bis hin zur heimischen Organisation. (Milinović, Winter, Srce / CARNet, RESTENA, & SA3 T2 group, 2012, S. 6)

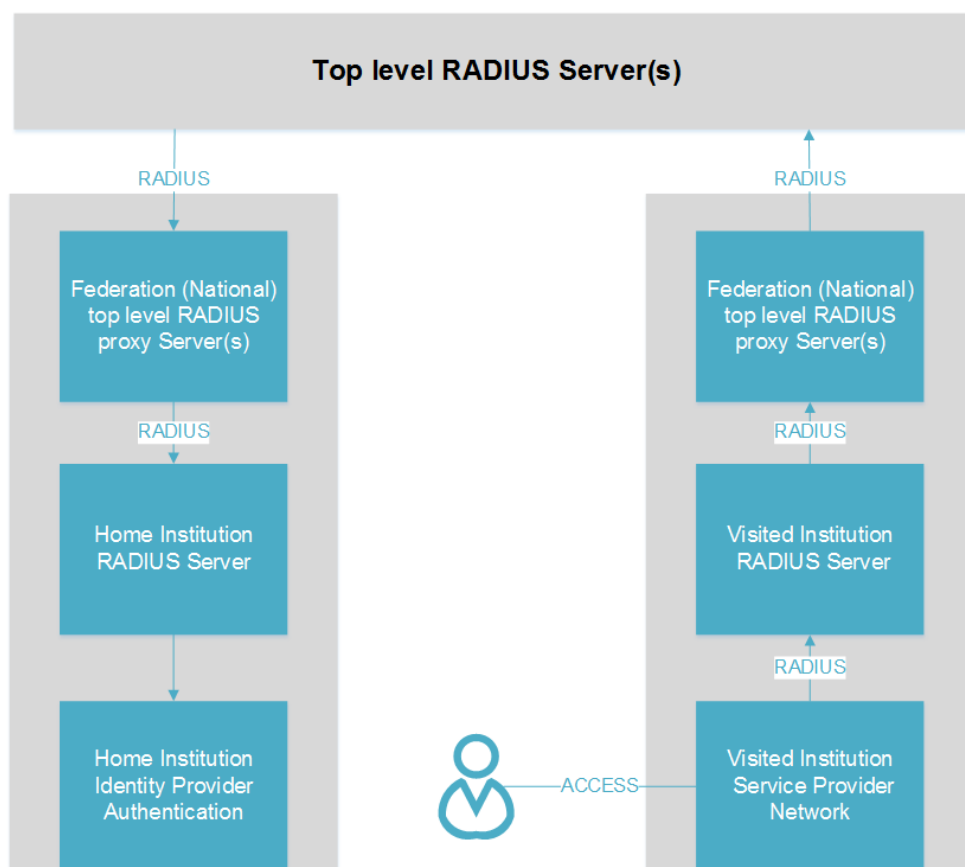


Abbildung 9 „eduroam“ RADIUS Authentifizierungsweg

Quelle: eigene Darstellung nach (Milinović, Winter, Srce / CARNet, RESTENA, & SA3 T2 group, 2012, S. 9)

2.5.2 Autorisierungs- und Authentifizierungsverfahren im öffentlichen WLAN

Öffentliches und unverschlüsseltes WLAN in Städten ist komfortabel, kann aber sogleich auch eine Gefahr für die Privatsphäre der Teilnehmer im Netzwerk darstellen. Nachfolgend wird der Mensch, als das wirkungsvollste Sicherungsinstrument für persönliche Daten betrachtet. Anschließend werden kontrollierten Zugangsverfahren zu öffentlichen WLAN Zugangspunkten diskutiert. Hierbei unterscheidet man wiederum zwischen zwei verschiedenen Zugangsarten, einerseits die Bestätigung der Allgemeinen Geschäftsbedingungen (AGBs) auf sogenannten Captive Portal-Seiten, zum anderen die privilegiertere Authentifizierung mittels Voucher Code.

Der Mensch als wichtigste Sicherheitsebene

(Ochang, Irving, & Ofem, 2016) untersuchten das Sicherheitsbewusstsein von durchschnittlichen Usern kabelloser Netzwerke. Die erlangten Erkenntnisse zeigen, dass nicht IT affine Benutzer oftmals nicht verstehen, wie sie ihre Daten in kabellosen Netzwerken schützen können. Diese Nutzerbasis hat selten oder nie von WLAN-Richtlinien gehört und findet auch nicht, dass dies Teil ihrer Aufgabe im beruflichen Umfeld ist. Sie erkennen nicht, dass Technik alleine nicht ausreicht, um Sicherheit zu bescheinigen. IT affine Anwender sind sich den Gefahren in WLAN Netzwerken bewusst und achten auf ihr Verhalten. (Ochang, Irving, & Ofem, 2016, S. 24 ff.)

Endanwender müssen keine Sicherheitsexperten sein. Vielmehr ist es essentiell, ein Sicherheitsbewusstsein zu bilden und einfache Tipps im Umgang mit öffentlichem Internet zu kennen. Es ist sehr ratsam, nur verschlüsselte Webseiten zu verwenden. Dazu gibt es hilfreiche Browsererweiterungen, wie Force-TLS und HTTPS-Everywhere, die den Benutzer bei der sicheren Navigation im Internet unterstützen. Prinzipiell geht es bei Verschlüsselung darum, dass die Kommunikation zwischen einem Server und der Empfangsstation nicht für Dritte einsehbar ist. Serverzertifikate beweisen dem User, dass der Server wirklicher jener ist, der er vorgibt zu sein. Diese Zertifikate werden von globalen Zertifizierungsstellen für Domänen ausgestellt. Die verschlüsselte Übertragung erfolgt schließlich mittels HTTPS. Es ist wichtig, dass die gesamte Internetseite über HTTPS abrufbar ist. Oftmals sind nur Login-Seiten geschützt, die weiteren Websiteaufrufe im eingeloggten Zustand werden jedoch unverschlüsselt übertragen. Trotz der gesicherten Übertragung von Inhalten, währenddessen der Benutzer eingeloggt ist, sollte keinesfalls auf den Abmeldevorgang vergessen werden, da nur so die Sitzung sicher beendet werden kann. Wissenschaftliche Untersuchungen zeigten, dass auch mobile Applikationen (Mobile Apps) Daten oftmals unverschlüsselt übertragen. Für den Endanwender ist diese Übertragung nicht ersichtlich, was eine erhebliche Sicherheitsbeeinträchtigung darstellt. (OnGuardOnline.gov, 2014)

Apple wirkt dieser Gefahr durch die zwingende Einführung von App Transport Security (ATS) bis Ende 2016 entgegen. Standardmäßig können keine unverschlüsselten Verbindungen mehr in Apps auf iOS 9 und OS X 10.11 aufgebaut werden. Dabei setzt Apple, die als sicher geltenden Technologien TLSv1.2 mit Perfect Forward Secrecy (PFS), entsprechend lange RSA (Rivest, Shamir und Adleman) und ECC (Elliptic Curve Cryptography) Schlüssel, sowie SHA2 (Secure Hash Algorithm) Zertifikate, voraus. (Ballard & Cooper, 2016)

Autorisierter Zugriff auf das Netzwerk durch Captive Portal-Systeme

Die Portal-Authentifizierung wird auch als Web- oder DHCP Web-Authentifizierung bezeichnet und authentifiziert die Verbindungsteilnehmer unter der Verwendung eines üblichen Webbrowsers. Bevor die Uservalidierung stattfindet, bekommt der assoziierte STA eine IP-Adresse vom DHCP-Server im Netzwerk zugewiesen, um letztendlich die Captive Portal-Webseite vom Portal Server anzeigen zu können. (Huawei Technologies Co., Ltd., 2012, S. 5)

Das Captive Portal-System (CP) greift in die HTTP-Verbindung des Teilnehmers ein und leitet diesen zu einer entsprechenden Captive Portal-Seite weiter. Dies geschieht nur, sofern nicht bereits eine Authentifizierung vorliegt, wonach typischerweise keine Weiterleitung mehr stattfindet. (Extreme Networks, 2016, S. 9) Für die Funktionalität eines solchen Systems muss der Teilnehmer zwingend eine HTTP-Anfrage absenden. Bei HTTPS-Verbindungen kann das Captive Portal-System nicht in die Verbindung eingreifen und die Weiterleitung durchführen.

Je nach Betriebssystem- bzw. Softwareanbieter gibt es unterschiedliche Varianten ein Captive Portal-System zu erkennen, sodass ein Teilnehmer nicht stets den Verbindungsaufbau zu einer mittels HTTPS gesicherten Webseite versucht und scheitert. Wird eine Verbindung mit einem öffentlichen WLAN-Hotspot hergestellt, so sendet der Webbrowser Google Chrome eine Anfrage an „http://www.gstatic.com/generate_204“ und überprüft den erhaltenen Antwortcode. Wird diese Anfrage weitergeleitet, öffnet Google Chrome das weitergeleitete Ziel in einem neuen Browser-Tab, denn es könnte sich um eine Anmeldeseite handeln. (Google (a), 2016)

(Extreme Networks, 2016, S. 11) unterscheidet zwischen vier Captive Portal-Varianten:

- Internal Captive Portal
- Guest Portal
- Guest Splash Screen Portal
- External Captive Portal

Beim Prinzip des Internal Captive Portal leitet der CP-Server den User auf eine vom CP-Server gehostete Authentifizierungsseite um. Der User authentifiziert sich mit den entsprechenden Anmeldeinformationen bei einem backend-RADIUS Server. Hierbei läuft der RADIUS-Server separiert vom CP-Server. Wird eine Verbindung mit dem Guest Portal hergestellt, so wird der User wiederum vom CP-Server auf eine vom CP-Server gehostete Webseite umgeleitet. Eine Authentifizierung erfolgt ebenfalls auf dieser Webseite, unter Verwendung einer vom CP-Server verwalteten Datenbank. Der gesamte Prozess verlässt den CP-Server nicht weshalb Anbieter, wie Extreme Networks, ihre CP-Server mit einer leicht zu bedienenden GUI (Graphical User Interface) versehen, um die Usability zu verbessern. Dies hat den Vorteil, dass auch nicht IT-versierte Personen über einen eingeschränkten Administrations-Account Benutzer für die WLAN-Anmeldung erstellen und verwalten können. (Extreme Networks, 2016, S. 11 f.)

Im Gegensatz zu den bereits diskutierten Portalvarianten sind für die Nutzung von WLAN, welches durch einen Guest Splash-Screen gesichert ist, keinerlei Anmeldeinformationen erforderlich. Um Internetzugang zu erhalten, müssen Teilnehmer üblicherweise die Allgemeinen Geschäftsbedingungen des WLAN-Providers akzeptieren. Dieser Captive Portal-Ansatz eignet sich besonders für die Bereitstellung von WLAN mit einer sehr großen Anzahl an unbekannten Nutzern. Wie auch beim Guest Portal, wird der Guest Splash-Screen durch den CP-Server bereitgestellt. Die Charakteristik des External Captive Portal liegt darin, dass die Authentifizierungswebsite nicht vom CP-Server, sondern von einem externen Web-Server ausgeliefert wird. Infolgedessen ermöglicht diese Captive Portal-Art höchste Flexibilität bei jedoch hohem Verwaltungs- und Implementierungsaufwand. Web-Developer haben die anspruchsvolle Aufgabe die Session Informationen der WLAN-Teilnehmer korrekt zu verwalten und entsprechende Authentifizierungsmechanismen (intern, sowie extern) bereitzustellen. Die interne Authentifizierung gleicht die Anmeldeinformationen mit dem CP-Server ab, welcher wiederum an einem RADIUS Server angebunden ist. Bei erfolgreicher Authentifizierung leitet der External Captive Portal Server den WLAN-Teilnehmer in das Internet weiter. Ziel ist hier die Separierung von Web- und RADIUS-Interaktionen. Der externe Authentifizierungsmechanismus liegt direkt in der Obliegenheit des External Captive Portal Server. Hierbei kann auf eine Vielzahl von Mechanismen, wie Active Directory Authentication, Splash-Screen Authentication, RADIUS oder proprietäre Datenbanksysteme, zurückgegriffen werden. Der External Captive Portal-Server muss letztendlich dem CP-Server den Status der Benutzerauthentifizierung mitteilen, welcher wiederum definierte Richtlinien (Policies) auf die WLAN-Teilnehmer anwendet. (Extreme Networks, 2016, S. 13 ff.)

Privilegiertere Authentifizierung mittels Voucher Code

Die Authentifizierung mittels Voucher Code wird häufig eingesetzt, um Benutzern zeitlich limitierten Zugang zum Internet anzubieten, ohne dabei spezifische Benutzernamen und Passwörter erstellen zu müssen. Mögliche Einsatzgebiete sind Hotels, Besprechungsräume oder Flughäfen. Jeder Voucher Code verfügt über ein vordefiniertes Gültigkeitsintervall, welches unabhängig vom Verbindungszustand des Benutzers abläuft. Voucher Codes werden durch das Public/Private Key RSA-Verfahren erstellt und mittels einer sogenannten „*Magic Number*“ verifiziert. (The pfSense Project, 2014)

Web Jail & Walled Garden

Die Terminologien „*Web Jail*“ und „*Walled Garden*“ beschreiben Restriktionen, aber auch Freiräume, in denen sich ein User im Netzwerk bewegen kann. Beispielsweise können nicht authentifizierte Benutzer nur spezielle Webseiten aufrufen oder Protokolle nutzen. Jedenfalls müssen nicht authentifizierte Teilnehmer Zugang zur Authentifizierungswebseite erhalten, um sich letztendlich anmelden zu können. Ein Szenario für die Verwendung eines solchen Ansatzes wäre die Erlaubnis, vor der Authentifizierung nur auf Update-Server zugreifen zu können, um den Sicherheitsrichtlinien des Netzwerks zu entsprechen. (Extreme Networks, 2016, S. 19)

2.5.3 Nutzungseinschränkungen durch Inhaltsanalysen

Im Unternehmensumfeld zählt die Analyse des Netzwerkverkehrs zu den Kernaufgaben, um die Produktivität der Mitarbeiter sicherzustellen, sensible Firmendaten im Unternehmen zu behalten (Data Leakage Prevention) oder Infektionen durch Viren oder Malware vorzubeugen. Darüber hinaus ist es wichtig, dass die zur Verfügung stehende Netzwerkbandbreite sowohl für tägliche und operative Aufgaben im Unternehmen, als auch für geschäftskritische Applikationen frei bleibt. Dazu zählt unter anderem die Unterbindung von privaten Downloads oder der Datenaustausch über einschlägige und meist illegale Plattformen. Unternehmen stehen zusätzlich vor der Herausforderung Social-Media-Kanäle zuzulassen, jedoch private Kommunikationen zu minimieren. Beispielsweise benötigt die Verkauf- und Marketing Abteilung Zugang zu diversen Plattformen, um das Unternehmen am Markt zu platzieren. Hier bedarf es konkreter Firmenrichtlinien zur Effizienzsteigerung. (Nicoletti, 2013, S. e101)

Laut der weltweit agierenden Unternehmensberatungsfirma IDC gelten ca. 30-40% des unternehmerischen Internetverkehrs als nicht geschäftsrelevant. Laut „*The Center of Internet Studies*“ ergriffen rund 60% der befragten Unternehmen disziplinierte Maßnahmen gegen die eigenen Mitarbeiter. Ein unsachgemäßes Verhalten der Angestellten kann den Ruf des Unternehmens erheblich schädigen, da Gerichtsverhandlungen publik werden und Kunden so das Vertrauen zu den Produkten des Unternehmens verlieren. (Nicoletti, 2013, S. e102)

Aus der Sicht eines öffentlichen WLAN-Service Providers gelten prinzipiell dieselben Anforderungen an das Netzwerksystem. Zusätzlich wird verstärkt Wert auf das Unterbinden illegaler Downloads und das Erreichen nicht geeigneter Webinhalte (Pornographie, Gewalt, Drogen, Waffen) gelegt. System erhaltende Dienste laufen außer Reichweite der WLAN-Teilnehmer, wodurch hier keine Gefährdung durch übermäßige Bandbreitenauslastung entstehen kann. Zusätzliche Bandbreitenlimitierungen pro User können komfortable an den Access Points konfiguriert werden. Aufgrund der hohen Anzahl an WLAN-Benutzer ist das Überprüfen des gesamten Netzwerkverkehrs auf Viren bei einem unentgeltlichen und frei zugänglichen WLAN-Netzwerk unter Berücksichtigung begrenzter Ressourcen nicht tragbar.

Kategorisierungsstrategien von Webinhalten

Filterungssysteme nutzen eine Kombination verschiedenster Techniken und Daten zur Kategorisierung von Inhalten. Keyword- und URL-Listen (Uniform Resource Locator) werden manuell von kommerziellen Anbietern oder der Öffentlichkeit aktualisiert und bieten einen grundlegenden Basisschutz. Kontinuierliche Veränderungen von Websites und eine Vielzahl an Sprachen und Domainnamen limitieren Keyword- und URL-Listen zunehmend. Als Erweiterung zu den eben genannten Techniken dienen Analysemethoden wie die „*Bayesian Analysis*“ oder das „*Content Based Image Filtering (CBIF)*“. Die „*Bayesian Analysis*“ untersucht Wörter im Kontext. Hierfür muss die Analyse ausreichend mit Testdaten trainiert werden, sodass bestmögliche Resultate zu erwarten sind. Das Training erfordert menschliche Interventionen, bis die Analyse soweit ist, selbst Muster zu erkennen und so bisher unbekannte Websites zu klassifizieren. (Nicoletti, 2013, S. e104 ff.)

Visuelle Inhalte erfordern andere Methoden zur Inhaltsüberprüfung. CBIF analysiert den Hautfarbenanteil eines Bildes, um so pornographisches Material zu identifizieren. Als erster Schritt wird die Hautfarbe, welche aus einer Kombination aus Rot, Gelb und Braun besteht und die Bildtextur bestimmt. Beim zweiten Analyseschritt werden jene Bilder, die über geringe Hautanteile verfügen, in eine Datenbank aufgenommen und akzeptiert. Die verbleibenden Bilder werden automatisch segmentiert und deren Signatur wird berechnet. Zuletzt erfolgt ein Vergleich neuer Bilder mit jenen, die bereits in der Datenbank der akzeptierten Bilder liegen. Hierbei können entsprechende Grenzen für den Bildvergleich definiert werden, sodass beispielsweise Bilder, die jenen in der Datenbank zu 40% ähneln automatisch akzeptiert, andere wiederum zur manuellen Durchsicht markiert oder komplett verworfen werden. (Nicoletti, 2013, S. e104 ff.)

Content-Filtering aus technischer Perspektive

Auf technischer Ebene lässt sich Content-Filtering mittels Proxy-Server und Firewalls realisieren. Beide Varianten greifen von unterschiedlichen Netzwerkebenen, aus der Sicht des „*Open Systems Interconnection Model (OSI)*“, in den Datenverkehr ein. Im Gegensatz zu Proxy-Server, welche auf Applikationsebene arbeiten (OSI-Layer 7), operieren Firewalls auf Netzwerk- und Transportebene (OSI-Layer 3 & 4). (Nicoletti, 2013, S. e106)

Proxy-Server können den Datenverkehr auf Applikationsebene untersuchen und so beispielsweise nur HTTP-Verbindungen auf TCP Port 80 genehmigen, während Firewalls lediglich Verbindungen auf TCP Port 80 prüfen können, ohne die darüberliegende Anwendung zu kennen. Trotz der vielseitigen Einsatzszenarien von Proxy-Server als Reverse-Proxy oder Forward-Proxy bedarf es einer aufwendigen Administration des Dienstes, da sonst zunehmend Fehlerquellen und Sicherheitslücken entstehen. (Nicoletti, 2013, S. e107)

Durch die Entwicklung von „*Next-Generation Firewalls (NGFW)*“ sind IT-Administratoren in der Lage Proxy-Dienste mit einer klassischen Stateful-Firewall zu verbinden und so ebenfalls auf Applikationsebene zu filtern. Der einzige Unterschied besteht darin, dass ein Proxy-Server die Anfrage des Netzwerkteilnehmers entgegennimmt und selbst eine Anfrage weiter ans Internet leitet, während eine Next-Generation Firewall nur den Header der Anfrage modifiziert, Inspektionen durchführt und die originale Anfrage des Teilnehmers an das Internet sendet. NGFWs werden häufig in Verbindung mit „*Unified Threat Management (UTM) Appliances*“ gebracht, da diese Systeme ebenfalls für die Analyse des Netzwerkverkehrs konzipiert sind. Dazu zählen Ansätze wie Anti Virus-Überprüfungen, Intrusion-Detection-Systeme (IDS) bzw. Intrusion-Prevention-Systeme (IPS), Website Filterung und Applikationskontrolle. Unternehmen wie Fortinet, Websense oder Blue Coat vertreiben in diesem Sektor kommerzielle Produkte. (Nicoletti, 2013, S. e107 f.)

Diverse Suchmaschinenanbieter, wie Yahoo, Bing und Google, bieten Benutzern und Netzwerkadministratoren die Möglichkeit ausschließlich gefilterte Suchergebnisse zu erhalten. Dazu müssen Administratoren den Proxy-Server so konfigurieren, dass bei jeder Suchanfrage der Parameter „*&safe=strict*“ mitübertragen wird. Dies funktioniert allerdings nur bei HTTP-Suchanfragen. (Google (b), 2016)

Benutzer können alternativ SafeSearch in ihrem Browser aktivieren. Um diese Einstellung persistent zu halten und um unautorisiertes Deaktivieren zu verhindern, muss ein Google Konto erstellt werden. (Google (b), 2016) Zwingendes Ziel in jedem Netzwerk ist die sichere Übertragung von Webinhalte mittels HTTPS. Hierfür bietet Google eine spezielle Safe-Search-VIP (Virtuelle IP-Adresse) an, welche auf mehrere Google-Server verweist. IT-Administratoren müssen den DNS-Eintrag (Domain Name System) für „*www.google.com*“ (inklusive aller Google Top-Level-Domains³) in einen CNAME (Canonical Name) für „*forcesafesearch.google.com*“ ändern, um SafeSearch obligatorisch bereitzustellen. (Google (c), 2016)

Maßnahmen zur Umgehung von Webfiltern

(Nicoletti, 2013, S. e114) beschreibt fünf verschiedene Proxy-Server Architekturen zur Umgehung von Inhaltsfiltern.

- Client-basierte Proxy
- Offene Proxy
- HTTP Web-basierte Proxy
- Sichere öffentliche und private Web-basierte Proxy
- Sichere anonyme Web-basierte Proxy

Client-basierte Proxy-Programme erstellen einen lokalen Proxy-Server, welcher auf einen Nicht-standard-Port gebunden ist. Dieses Programm konfiguriert den Webbrowser des Computers um, sodass der gesamte Browserverkehr über den lokalen Proxy-Server an einen externen, verschlüsselten Proxy-Server übertragen wird. Content-Filtering Geräte des Netzwerks können den lokalen Datenverkehr am Computer nicht einsehen. Diese erkennen nur ein eigens adaptiertes und verschlüsseltes Protokoll des Proxy-Programms, welches Anfragen des Netzwerkbenutzers durch einen externen Proxy-Server tunnelt. IT-Administratoren können diese Umgehungsmethode verhindern, indem sie die Firewall-Lognachrichten nach ungewöhnlich hohen Aktivitäten auf nicht-standard Ports überprüfen. (Nicoletti, 2013, S. e114 f.)

Die Konfiguration von offenen Proxy-Servern geschieht direkt im Web-Browser des Benutzers. In diesem konkreten Fall werden offene Proxy-Server auch als explizite Proxy-Server bezeichnet, da diese durch Benutzer mit administrativen Rechten, gesetzt werden können. Alle angefragten Web-Inhalte werden direkt an den Proxy-Server übertragen. Dieser erhält infolgedessen die angefragten Informationen und leitet sie an den Client weiter. Maßnahmen zur Blockierung eines offenen und explizit gesetzten Proxy-Servers werden durch Blockierung der entsprechenden Einstellungen im Browser realisiert. IT-Administratoren müssen bedenken, dass Clients eigentlich gar keinen direkten Internetzugriff benötigen. Nur der Proxy-Server, darf Verbindungen ins Internet aufbauen. Anbieter HTTP web-basierter Proxy-Server stellen eine Webseite mit einem simplen URL-Eingabefeld, zum anonymisierten Aufruf von Webseiten, bereit. Content-Filtering Systeme sehen nur den Datenverkehr zwischen dem Client und der Proxy-Webseite. (Nicoletti, 2013, S. e116)

³ https://www.google.com/supported_domains (abgerufen am 30. November 2016)

Sichere öffentliche/private und anonyme Proxy-Dienste funktionieren ähnlich wie HTTP web-basierte Proxy-Dienste. Der Unterschied liegt darin, dass sichere Proxy-Server den Verbindungsaufbau mittels HTTPS zulassen. Um die Nutzung von sicheren Proxy-Diensten zu verhindern, müssen IT-Administratoren in den SSL Datenverkehr des Netzwerkes eingreifen und die Verbindung zu anderen Proxy-Servern unterbinden. Dieses Vorgehen erfordert eine detaillierte Implementierungsstrategie und ausreichend Ressourcen. An diesem Punkt ist die aufklärende Expertise von IT-Fachleuten gefragt. Sie müssen der breiten Masse an Internet-Benutzern zu verstehen geben, dass Web-Proxy nicht zwingend die eigene Anonymität bewahren. Kriminelle können einen vermeintlich vertrauensvollen Proxy-Dienst betreiben, um Anmeldeinformationen oder andere sensible Daten auszuspähen. Dies ist möglich, da sämtlicher Datenverkehr über den Proxy-Server abgeführt wird. (Nicoletti, 2013, S. e116)

Ogleich der Einsatz von Webfiltern positiv für den Daten- und Jugendschutz ist, werden Content-Filter in manchen Teilen der Welt als Unterdrückungsinstrument missbraucht. In Teilen der arabischen Regionen, wie dem Iran, Bahrain, Jemen oder Libyen, verbieten Internet Service Provider auf Verlangen des Staates den Zugang zu sozialen Netzwerken oder anderen Diensten zur freien Meinungsäußerung. Aus diesem Grund bedarf es Lösungen, um anonymen und unzensierten Zugang zu allen Inhalten des Internets zu erlangen und nicht politisch verfolgt zu werden. Durch die Lizenzgestaltung von Open-Source-Software können Softwareentwickler Anonymisierungsprogramme so adaptieren, dass lokale Anforderungen in Bezug auf die niedrige zur Verfügung stehende Bandbreite, umsetzbar sind. (Shirazi, 2011, S. 920 f.)

Laut (Shirazi, 2011) verwendet die iranische Digital-Community drei verschiedene Arten zur Sicherung des Datenverkehrs und Erhaltung der Anonymität im Netz. Proxy-Server dienen zur Maskierung der IP-Adresse und des Standortes, Verschlüsselungssoftware chiffriert den Netzwerkverkehr und weitere Programme, die verschiedenste Sicherheitsfeatures kombinieren, bilden eine sichere Plattform. Web-Proxy-Server haben den Vorteil, dass diese meist außer Landes gehostet sind und so über eine schnellere Internetanbindung und neuere Hardwarebauteile verfügen. Allerdings sind staatliche Service Provider in der Lage, den Zugang zu diversen Web-Proxy-Server zu unterbinden. Lokal entwickelte Open-Source-Software ermöglicht einen verschlüsselten Datenaustausch, was einerseits sicher ist, andererseits jedoch die lokale Infrastruktur beinahe untragbar belastet. Ziel ist es also ein System zu entwickeln, welches sowohl Sicherheit gewährleistet, plattform- bzw. betriebssystemübergreifend funktioniert, von nicht IT-versierten Personen bedienbar ist, als auch aus Benutzersicht ressourcenschonend (Bandbreitenbedarf, Installationsgröße, Rechenleistung) operiert. (Shirazi, 2011, S. 922)

Die Umfrageergebnisse von (Shirazi, 2011) zeigen, dass das client-basierte Proxy-Programm „UltraSurf“ zu den effektivsten Open-Source-Werkzeugen gegen Content-Filtering zählt. Der Geschwindigkeitsvorteil von Proxy-Servern wird durch strenge Filterungsmaßnahmen seitens der Regierung und der damit verbundenen Verbindungsprobleme zunehmend minimiert. Ursprünglich wurde „UltraSurf“ für die Anforderungen chinesischer Internetnutzer entwickelt, welche allerdings über mehr Internetbandbreite verfügen. (Shirazi, 2011, S. 925)

Neben der freien Bandbreite ist jedenfalls die kontinuierliche Konnektivität, des staatlichen Internet Service Provider, zum Internet ausschlaggebend. Im Jahr 2009 isolierte die iranische Regierung das Land, aufgrund politischer Turbulenzen, gänzlich vom Internet. (Shirazi, 2011, S. 925)

Die zur Verfügung stehende Bandbreite ist sehr wichtig für die reibungslose Funktionalität von Anonymisierungsdiensten, da zusätzlicher Overhead bei der Datenübertragung entsteht. *Abbildung 10* zeigt, die durchschnittliche Verbindungsgeschwindigkeit der Internetanschlüsse in Österreich vom 3. Quartal 2007 bis zum 1. Quartal 2016 (in kbit/s). Im ersten Quartal 2016 geht man hier von einer Downloadgeschwindigkeit von 13.149 kbit/s aus.

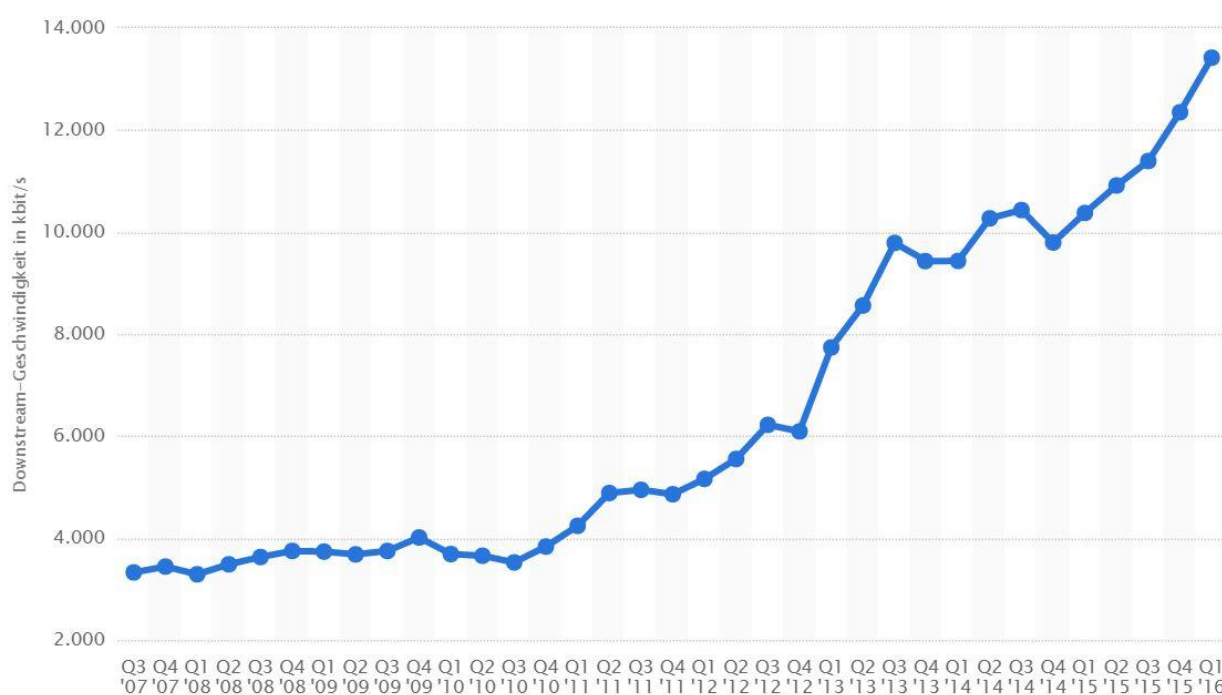


Abbildung 10 Durchschnittliche Internetgeschwindigkeit in Österreich (in kbit/s)
 Quelle: (Akamai Technologies, 2016)

Zur Zeit der Recherchen durch (Shirazi, 2011, S. 921) standen den iranischen Internetnutzern im Vergleich eine durchschnittliche Downloadrate von rund 660 kbit/s zur Verfügung. Im ersten Quartal 2011 verfügten österreichische Web-User bereits über eine durchschnittliche Downloadgeschwindigkeit von 4.238 kbit/s. Daraus resultiert ein Geschwindigkeitsunterschied um das 6,4-fache gegenüber dem Iran.

3 GESETZLICHE REGULIERUNGEN EINES ÖFFENTLICHEN WLAN NETZWERKS

Durch die zunehmende Verbreitung von WLAN-Funkstationen müssen regulatorische Rahmenbedingungen für deren Betrieb und Installation geschaffen werden. In Österreich beschäftigen sich die entsprechenden Stellen mit den lizenzrechtlichen Vorgaben und Rahmenbedingungen, damit Provider ein öffentliches WLAN erstellen können. Die Allgemeingenehmigung stellt eine wesentliche Säule der Rahmenbedingungen dar. Damit einheitliche und europaübergreifende Richtlinien für den Betrieb von WLAN gegeben sind, werden spezielle freigegebene Frequenzbänder angeboten. Darüber hinaus komplettieren die Empfehlungen der europäischen Kommission den Betrieb von WLAN. Der Aufbau von Funkanlagen muss jedenfalls auch aus gesundheitlicher Sicht betrachtet werden, um jegliche Gesundheitsgefährdung für die Bevölkerung auszuschließen. Sind die baurechtlichen Rahmenbedingungen aus Providersicht abgeschlossen müssen sich diese jedenfalls Gedanken über privatrechtliche Haftungsrisiken beim Betrieb machen. Dazu zählen Haftungsrisiken beim Missbrauch des WLAN-Netzwerks durch Dritte, sowie die Wahrung der Privatsphäre von Benutzern auf Captive Portal-Seiten durch rechtskonformes Setzen von Cookies.

3.1 Lizenzrechtliche Vorgaben und Rahmenbedingungen

In Österreich besteht eine generelle Bewilligung, die den Betrieb von kabellosen und lokalen Funknetzwerken erlaubt. Gemäß den ebenso geltenden europäischen Bestimmungen muss ein drahtloses Zugangssystem definierten technischen Merkmalen entsprechen, welche in diversen Funk-Schnittstellenbeschreibungen festgelegt sind. Kunden von kabellosem Equipment müssen gemäß „§ 10 Abs.3 des Bundesgesetzes über Funkanlagen und Telekommunikationsendeinrichtungen (entspricht dem Artikel 6(3) der Richtlinie 1999/5/EG)“ über die zulässige Verwendung in Österreich informiert werden. Die benötigten Informationen und technischen Spezifikationen müssen in der Gerätebeschreibung ersichtlich sein. (Bundesministerium für Verkehr, Innovation und Technologie, 2010, S. 1)

Österreichisches Recht sieht vor, dass die Erbringung von kabellosen Telekommunikationsdiensten gemäß den Bestimmungen des Telekommunikationsgesetzes (TKG) 2003 §§ 14ff behandelt werden und daher eine Anzeigepflicht bei der Regulierungsbehörde gemäß TKG 2003 § 15 besteht. Weiterfolgend ist die „Empfehlung der Kommission vom 20. März 2003 zur harmonisierten Gewährung des öffentlichen Funk-LAN-Zugangs zu öffentlichen elektronischen Kommunikationsnetzen und –diensten in der Gemeinschaft“ von Bedeutung. (Bundesministerium für Verkehr, Innovation und Technologie, 2010, S. 2 f.)

3.1.1 Allgemeingenehmigung

Die Rundfunk und Telekom Regulierungs-GmbH (RTR GmbH) ist in Österreich die zuständige Stelle für Provider von öffentlichen Telekommunikationsdiensten und -netzen. Gemäß TKG 2003 § 15 Abs. 2 muss eine schriftliche Anmeldung bei der RTR erfolgen, um die Bereitstellung, Betriebsaufnahme oder etwaige Änderungen der beabsichtigten Kommunikationsdienstleistungen zu melden. Die Anmeldung umfasst grundsätzliche Informationen des beantragenden Unternehmens, wie den Namen, die Anschrift und die Rechtsform. Darüber hinaus benötigt die RTR detaillierte Angaben, welche die Kurzbeschreibung des Netzes oder des Dienstes und den voraussichtlichen Termin der Aufnahme, Änderung oder Einstellung des Dienstes, umfassen. (Rundfunk und Telekom Regulierungs-GmbH)

Online steht eine Liste der aktuell anzeigepflichtigen Unternehmen zur freien Einsicht bereit.⁴

3.1.2 Freigegebene Frequenzbänder

In Österreich wird die zur Verfügung stehende Frequenz für WLAN von der RTR verwaltet. Prinzipiell unterscheidet man hierbei zwischen WLAN in den 2,4 GHz- und 5 GHz-Bereichen, welche wiederum in kleinere Kanäle unterteilt sind. Sowohl für WLAN im 2,4 GHz, als auch im 5 GHz-Bereich gilt: Wird das kabellose Netzwerk nicht zu gewerblichen Zwecken bereitgestellt, so besteht keine Anzeigepflicht gemäß § 15 TKG 2003. (Rundfunk und Telekom Regulierungs-GmbH, 2013)

WLAN in den 2,4 GHz-Spektren

Die 2,4 GHz-Spektren erstrecken sich von den Kanälen 1 (2,412GHz) bis 13 (2,472). Der Abstand benachbarter WLAN-Kanäle beträgt nur 5 MHz, wodurch sich benachbarte Kanäle überlappen. Im 20 MHz Bereich sind nur vier Kanäle (1, 5, 9, 13), im 40 MHz Bereich lediglich zwei Kanäle (3, 11) exklusiv nutzbar. (Rundfunk und Telekom Regulierungs-GmbH, 2013) *Abbildung 11* illustriert den Umfang der 2,4 GHz-WLAN-Spektren. Die Ordinatenachse gibt die Leistung, gemäß der äquivalenten isotropen Strahlungsleistung (EIRP) inklusive Antennengewinn, in Milliwatt (mW), an.

⁴ <https://www.rtr.at/de/tk/ListeAGGTK> (abgerufen am 12. September 2016)

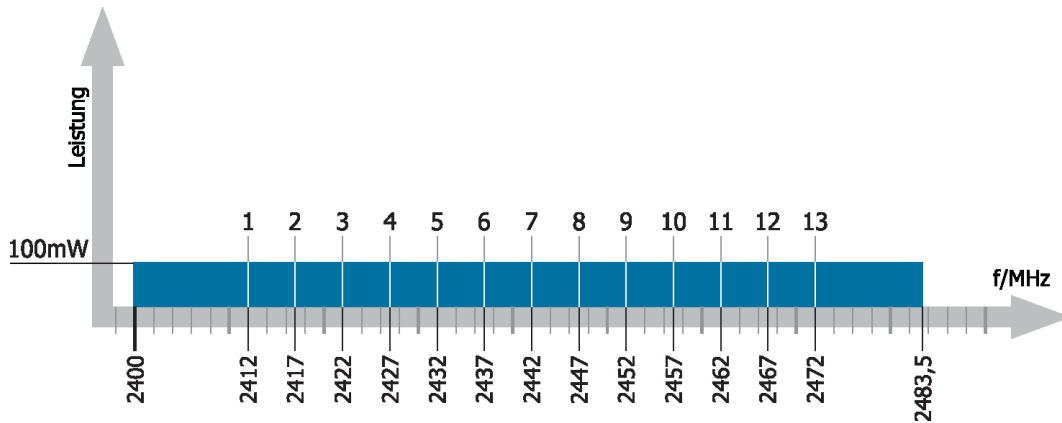


Abbildung 11 WLAN in den 2,4 GHz-Spektren
Quelle: (Rundfunk und Telekom Regulierungs-GmbH, 2013)

WLAN in den 5 GHz-Spektren

Die 5 GHz-Spektren beschreiben WLAN in den Kanälen 36 bis 48 (5,18 GHz - 5,24 GHz), jeweils im Abstand von vier Kanälen. Zusätzlich unterstützen manche 5 GHz fähige Geräte die Kanäle 100 bis 140 (5,50 GHz - 5,70 GHz), ebenso im Abstand von jeweils vier Kanälen. (Rundfunk und Telekom Regulierungs-GmbH, 2012)

Abbildung 12 illustriert den Umfang der 5 GHz-WLAN-Spektren. Die Ordinatenachse gibt die Leistung, gemäß der äquivalenten isotropen Strahlungsleistung inklusive Antennengewinn, in Milliwatt (mW), an.

Die Subklasse 54 definiert die Nutzungsklasse des Frequenzbereichs zwischen 5,47 GHz - 5,725 GHz, die sowohl für den „indoor“ als auch den „outdoor“ Bereich gilt. Wichtig ist, dass die maximale Sendeleistung von 1 Watt, inklusive der Gewinnantennen, nicht überschritten werden darf, um den interferenzfreien Betrieb von Radarsystemen, die in diesem Frequenzbereich operieren, sicherzustellen. Anzumerken sei, dass die Störung des WLAN-Signals durch Radarsysteme ist nicht auszuschließen ist. (Bundesministerium für Verkehr, Innovation und Technologie, 2010, S. 2)

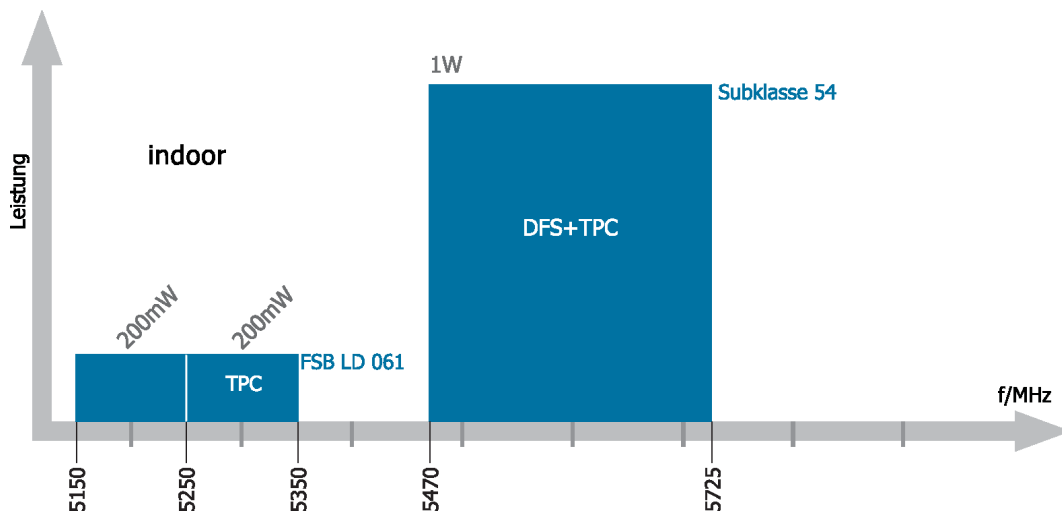


Abbildung 12 WLAN in den 5 GHz-Spektren
Quelle: (Rundfunk und Telekom Regulierungs-GmbH, 2012)

3.1.3 Empfehlungen der europäischen Kommission

(Liikanen, 2003) beschreibt unter Anerkennung bereits existierender Richtlinien, den gesetzlichen und wirtschaftlichen Umgang mit kabellosen Netzwerken. Ziel ist die regulatorischen Rahmenbedingungen zugunsten von kabellosen Netzwerkanbietern zu optimieren, Frequenzen korrekt aufzuteilen, Hindernisse abzubauen und Fairness bei der Zulassung von Providern walten zu lassen. Die Empfehlung der Kommission legt dar, dass die Störung des WLAN-Signals von allen Teilnehmern anerkannt wird, sofern keine möglicherweise geschützten Nutzer beeinträchtigt werden. Der Wegfall individueller Nutzungsrechte, sowie die Freigabe der 5 GHz-Bereiche, verringert die Teilnehmeranzahl in den überfüllten 2,4 GHz-Bereichen und vermeidet unnötige Genehmigungsverfahren. Die Bereitstellung öffentlicher WLAN-Dienste darf nur von einer Allgemeingenehmigung abhängig gemacht werden. Die Empfehlung der Kommission adressiert Mitgliedsstaaten keine individuellen Nutzungsrechte für die 2,4 GHz -und 5 GHz-Spektren auszustellen. (Liikanen, 2003, S. L 78/12 - L 78/13)

3.2 Gesundheit und Immission

WLAN, Mobilfunk, Radiowellen und Schnurlostelefone wirken täglich auf den Körper ein. Vor allem in dicht besiedelten Arealen sind vermehrt WLAN-Access Points und Mobiltelefone aktiv. In diesem Kapitel wird der Einfluss von kabellosen Verbindungen auf den menschlichen Organismus betrachtet. Regulatorische Rahmenbedingungen dienen zum Schutz der Bevölkerung und definieren zulässige Höchstwerte.

Abbildung 13 illustriert, dass knapp 50% der Befragten aus Deutschland vermuten, dass Mobiltelefone einen gewissen Einfluss auf ihre Gesundheit haben. Damit liegen die Deutschen über den EU27 Durchschnitt von 41%. (Europäische Kommission (b), 2010)

Mobilfunk: Meinungen über den Effekt auf die Gesundheit

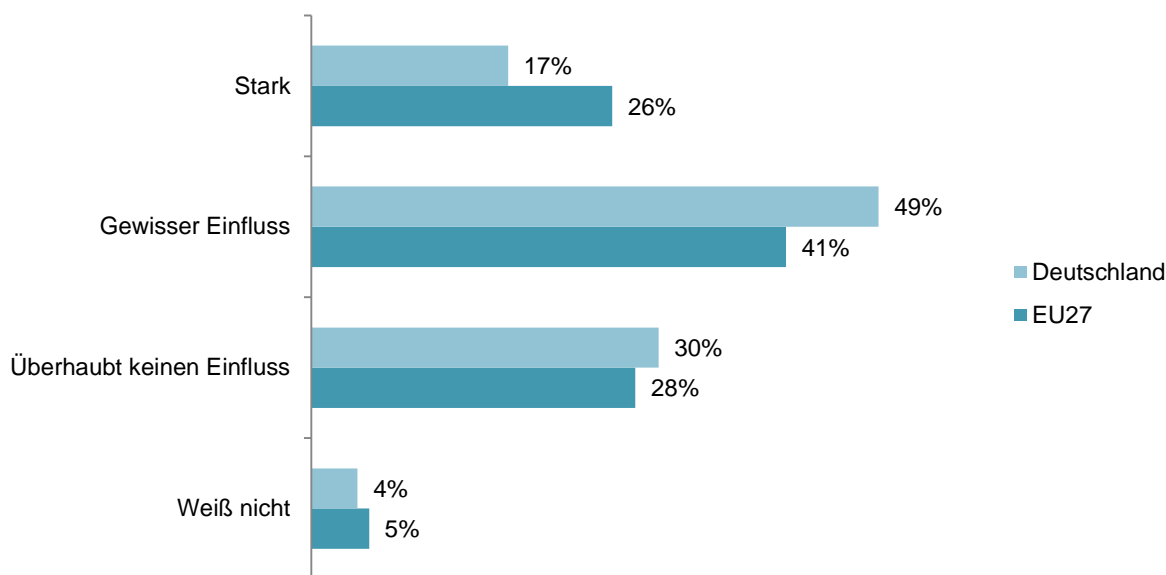


Abbildung 13 Mobilfunk: Meinungen über den Effekt auf die Gesundheit
Quelle: eigene Darstellung nach (Europäische Kommission (b), 2010)

3.2.1 Festlegung und Einhaltung von Grenzwerten

Dringen elektromagnetische Wellen in den Menschen ein entsteht Wärme. Für das Maß eines Grenzwertes wird die pro Zeiteinheit im Gewebe absorbierte Energie herangezogen. Die daraus resultierende spezifische Absorptionsrate (SAR) wird in Watt pro Kilogramm (W/kg) angegeben. Dosimetrische Messungen und Analysen zeigen, dass ein SAR-Wert von 1-4 W/kg zu einer Temperaturerhöhung von ca. 1°C führt. Gemäß dem Forum Mobilkommunikation gelten unterschiedliche Grenzwerte, je nach Personengruppe. „Beruflich Exponierte“ befinden sich im erwerbstätigen Alter, sind gesund und wurden vom Arbeitgeber über die Gefahren durch übermäßige Strahlenbelastung in Kenntnis gesetzt. Für diese Personengruppe gilt ein Grenzwert von 0,4 W/kg. Im Gegensatz dazu besteht die „Allgemeinbevölkerung“ aus Menschen unterschiedlichster Gesundheitszustände und biologischen Entwicklungsstufen. Zum Schutz dieser Personengruppe beläuft sich der Grenzwert auf 0,08 W/kg. Die Strahlenabsorption durch den menschlichen Körper hängt stark von der Frequenz ab. Je höher die Frequenz, desto geringer die Eindringtiefe. (FMK Forum Mobilkommunikation (a))

Im TKG 2003 §§ 54 Abs. 1 Ziffer 1d und 73 Abs. 2 wird der Schutz der Bevölkerung vor Funkanlagen und deren ungestörten Betrieb geregelt. Der in der Vornorm E8850 festgelegte Grenzwert ist als Schutz-Wert heranzuziehen. Der Wert selbst ist im Gesetzestext nicht zu finden, da dieser je nach wissenschaftlichem Forschungsstand variieren kann und infolgedessen immer eine Gesetzesänderung notwendig wäre. Für die Einhaltung des Grenzwertes sind die Provider einer Funkanlage verantwortlich. Entsprechende Arbeitssicherheitsrichtlinien stellen sicher, dass keine unbefugten Personen in die direkte Nähe von Antennenanlagen gelangen können, da hier die Wellenbelastung am höchsten ist. Die Kontrolle obliegt hierbei der Fernmeldebehörde. (FMK Forum Mobilkommunikation (b))

3.2.2 WLAN-Funkanalagen

In Europa begrenzt das European Telecommunications Standards Institute (ETSI) in der Norm EN 300 328 die maximale Sendeleistung. Die vom Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) betrachteten Studien analysierten die Strahlenbelastung durch WLAN und kamen zu dem Ergebnis, dass das Lastverhältnis entsprechend gering ist und somit den Richtlinien der International Commission on Non Ionizing Radiation Protection (ICNIRP) entspricht. Außerhalb von Laborbedingungen betrachtet ist das Lastverhältnis sogar noch geringer, als in den Studien beschrieben. Entsprechende Versuche wurden erfolgreich an britischen Schulen durchgeführt. (SCENIHR Scientific Committee on Emerging and Newly Identified Health Risks, 2015, S. 37)

Die Weltgesundheitsorganisation (WHO) bestätigt, dass der durch Funkwellen verursachte Temperaturanstieg des menschlichen Körpers zu gering ist, um die Gesundheit zu beeinflussen. Studien haben gezeigt, dass die durch WLAN verursachte Immission an öffentlichen Orten die international üblichen Standards um das Tausendfache unterschreiten. Der menschliche Körper wird durch Radio und TV Funkwellen, aufgrund der niedrigeren Frequenz, bis zu 5mal mehr belastet. Verschiedene Funkmodulationen (analog/digital) haben bisweilen keinen Einfluss auf die Gesundheit eines Menschen gezeigt. Die Annahme, dass durch WLAN oder Mobilfunk mehr Menschen krank werden ist jedoch nicht einfach belegbar. Hierzu müssen weitere Langzeitstudien durchgeführt werden. (World Health Organization, 2006)

3.3 Privatrechtliche Haftungsrisiken beim Betrieb

Bislang mussten sich die österreichischen Gerichte noch nicht zur zivil- oder strafrechtlichen Verantwortlichkeit eines WLAN-Service Provider äußern. Das bloße zur Verfügung stellen eines Computers mit Internetanschluss alleine reicht nicht aus, um gesetzwidriges Verhalten zu begründen. Es muss eine Verletzung von Prüf- und Sorgfaltspflichten vorliegen. Infolgedessen ist abzuleiten, dass Gastwirte oder Hoteliers nicht für die rechtswidrige Nutzung des Internetzugangs seitens der Kunden zur Verantwortung gezogen werden können. Aus österreichischer Sicht existiert vor allem Literatur zur Vorratsdatenspeicherung in WLAN-Netzwerken, denn es mangelt aus jetziger Sicht an konkreten Rechtsprechungen in Bezug auf die Haftung des WLAN-Betreibers. (Thiele, 2015, S. 6 f.)

Verglichen mit Österreich existieren in Deutschland verschärfte Gesetze zur Haftungsbestimmungen in kabellosen Netzwerken, was als eindeutiger Standortnachteil zu bewerten ist. Daraufhin wurden deutsche Gesetze geformt, die es Cafés und Hotels erlaubt, WLAN anzubieten, ohne Haftungsrisiken zu befürchten. (Thiele, 2015, S. 9)

3.3.1 Haftung in Abhängigkeit der WLAN-Sicherheit

Anbieter verschlüsselter WLAN-Umgebungen müssen sich keinesfalls Sorgen über Haftungsrisiken bezüglich des Fehlverhaltens von Dritten Gedanken machen. Der Inhaber des Netzwerks muss beweisen den Gesetzesverstoß nicht selbst begangen zu haben. WLAN-Service Anbieter müssen die Sicherheitseinstellungen des Netzwerks nicht ständig aktualisieren und somit auch zugriffssicher halten, sofern zum Zeitpunkt der initialen Bereitstellung des Dienstes adäquate und zeitgemäße Maßnahmen zum Schutz des Netzwerks geschaffen wurden. (Thiele, 2015, S. 11) Laut Art 15 der E-Commerce-Richtlinie dürfen dem Anbieter von WLAN keine allgemeinen Überwachungspflichten abverlangt werden. Bereitsteller öffentlicher Netzwerke sind als Access-Provider zu klassifizieren, wonach das ECG (E-Commerce-Gesetz) § 13 gilt. Der Anbieter ist nicht zu belangen, sofern dieser nicht in den Datenverkehr eingreift, Veränderungen oder andere Einflüsse vornimmt. Provider ungesicherter WLAN-Netze müssen nicht im Vorhinein annehmen, dass Rechtsverletzungen über das Netz begangen werden. Wird der Betreiber über Rechtsverletzungen in Kenntnis gesetzt, so muss dieser entsprechende Vorkehrungen zur Unterbindung treffen, um nicht im Rahmen der Gehilfenhaftung mitverantwortlich zu sein. *„Nach § 19 Abs. 1 ECG gelten die Haftungsfreistellungen nicht gegenüber Unterlassungsansprüchen. [...] Zur Frage, ob die Haftungsfreistellungen tatsächlich Unterlassungsklagen ggü. Accessprovider nicht ausschließen, liegen in Österreich noch keine Entscheidungen vor [...]“* (Ney, 2015)

3.3.2 Empfehlungen für österreichische WLAN-Provider

Österreichische WLAN-Provider sollten die Benutzer vorab über ihre Pflicht, das Netzwerk nicht missbräuchlich zu verwenden, in Kenntnis setzen. Sie behalten sich das Recht vor, Protokolldaten zur Strafverfolgung an Behörden weiterzuleiten. Aus technischer Perspektive können Download und Upload von großen Datenmengen unterbunden werden, um File-Sharing Aktivitäten unattraktiv zu gestalten. Darüber hinaus ist ein automatischer Verbindungsabbruch nach einer gewissen Zeit zu empfehlen. Zusätzlich ist der Einsatz von geeigneten Content-Filter Maßnahmen unverzichtbar. (ARGE DATEN - Österreichische Gesellschaft für Datenschutz (a))

3.4 Nutzungsanalyse und Datenschutz der Internetuser

Nutzungsanalysen von Web-Usern sind insbesondere mit der damit einhergehenden Beachtung der Datenschutzkonformität durchzuführen. Website-Betreiber nutzen Cookies, um die Zielgruppe einer Website genauer zu kennen und entsprechende Marketingstrategien zu entwickeln oder ihre Dienste zu optimieren. Entsprechende Analysesoftware befähigt IT-Administratoren komplexe Analyseszenarien umzusetzen, während die Reporterstellung aus Businesssicht einfach funktioniert. Die Informationen dieses Kapitels fokussieren sich unter anderem auf den Aspekt jegliche Analysedaten selbst zu verwalten und diese nicht auszulagern bzw. extern zu hosten.

Die Steuerung von Cookies durch den Endanwender stellt ein essentielles Recht auf Privatsphäre dar, wonach ein entsprechendes Steuerungspanel seitens des Website-Betreibers geschaffen werden muss.

Laut einer Umfrage der Organisation Insight Intelligence vom Jänner 2016 in Schweden akzeptieren rund 50% der befragten Personen Cookies, ohne die Allgemeinen Nutzungsbedingungen der Website gelesen zu haben. *Abbildung 14* illustriert diesen Sachverhalt und zeigt, dass nur 28% der Umfrageteilnehmer Cookies primär ablehnen und danach die Website weiterverwenden, sofern dies noch möglich ist. (Insight Intelligence, 2016)

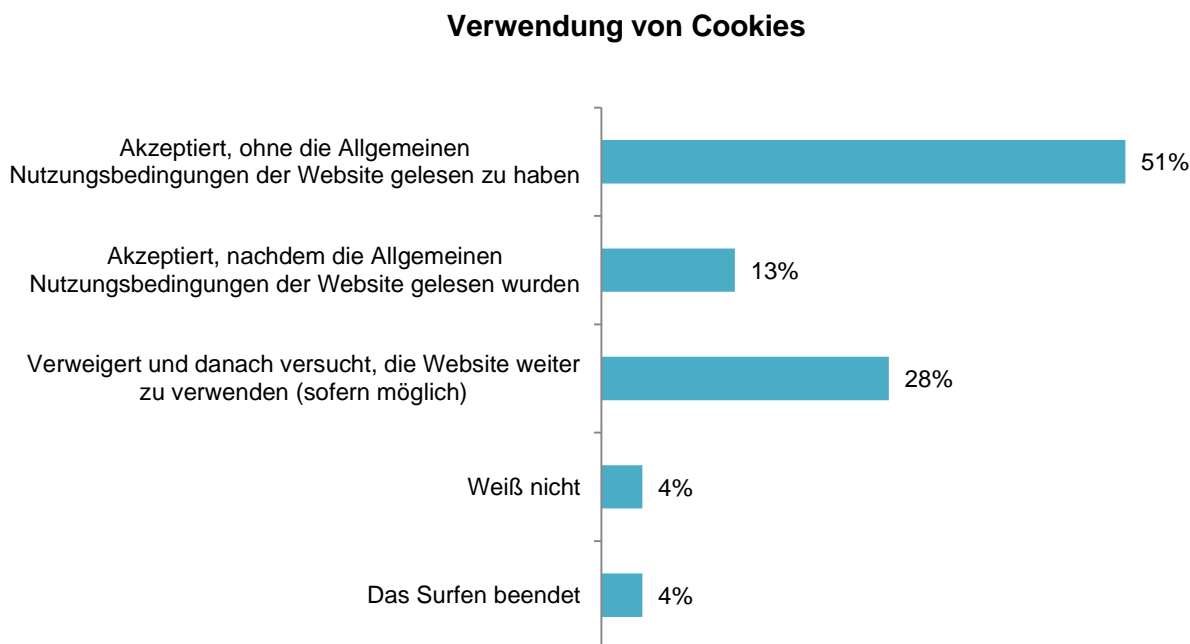


Abbildung 14 Verwendung von Cookies
Quelle: eigene Darstellung nach (Insight Intelligence, 2016)

3.4.1 Cookies

Als Cookies bezeichnet man kleine Konfigurationsdateien, die als Textdateien auf dem Rechner eines Users, beim Aufrufen einer Website, abgelegt werden. Cookies beinhalten Informationen über den Besucher und werden unter anderem zu dessen Wiedererkennung oder zur Speicherung von websitespezifischen Konfigurationen verwendet. Die österreichische Rechtsgrundlage für die Verwendung von Cookies wird im TKG 2003 § 96 Absatz 3 geregelt. Durch die breite Einsatzmöglichkeit und der damit einhergehenden Nutzungsvielfalt von Cookies bedürfen diese einer expliziten Zustimmung des Benutzers. Zusätzlich müssen Inhaber einer Website, in einer Sektion des Impressums, ausdrücklich auf die Verwendung von Cookies hinweisen. Prinzipiell gilt die Cookie-Regelung für jeden Website-Betreiber, da schon das Bereitstellen von „*Informationsmaterial als Dienst für die Informationsgesellschaft iSd § 3 Z 1 E-Commerce-Gesetz (ECG)*“ gilt und daher zustimmungspflichtig ist. Darüber hinaus gelten gesonderte Richtlinien für kommerzielle Betreiber von Web-Shops, Suchmaschinen oder Online-Werbeanbietern. (ARGE DATEN - Österreichische Gesellschaft für Datenschutz (b))

Eine Berufung auf browserspezifische und daher clientseitige „Do Not Track“ Einstellungen ist nach der EU-Richtlinie 2002/58/EG und dem TKG 2003 nicht zulässig. Man unterscheidet zwischen zustimmungspflichtigen, nicht zustimmungspflichtigen und bedingt zustimmungspflichtigen Cookies. (ARGE DATEN - Österreichische Gesellschaft für Datenschutz (b))

Tabelle 4 beschreibt die jeweiligen Cookie-Einsatzgebiete und gibt die Optionalität der Zustimmung durch den User an:

Cookies	Beschreibung	Zustimmungspflicht
Warenkorb-Cookies	Speicherung des Warenkorbinhalts	Nein
Sicherheits-Cookies	Protokollierung fehlgeschlagener Anmeldeversuche	Nein
Multimedia-Cookies	Präsentation von Multimediainhalten	Nein
Tracking-Cookies	Website übergreifende Nachverfolgung von Benutzern	Ja
Werbe-Cookies	Darstellung zielgruppenorientierter Annoncen	Ja
Analyse-Cookies	Erstellung von Reports	Ja
Authentifizierungs-Cookies	Identifikation authentifizierter Benutzer	Bedingt
Darstellungs-Cookies	Speicherung von Darstellungsattributen (z.B. Sprache der Website, mobile Version)	Bedingt
Social Plugin-Cookies	Ermöglichen die Freigabe von Inhalten über soziale Netzwerke	Bedingt

Tabelle 4 Arten von Cookies

Quelle: (ARGE DATEN - Österreichische Gesellschaft für Datenschutz (b))

Letztendlich ist der Verwendungszweck aus Sicht des Website-Benutzers für die Zustimmungspflicht ausschlaggebend. Besonders Betreiber, von durch Werbung finanzierter Webseiten, beachten diesen Umstand nicht ausreichend. Für die Website-Betreiber ist die Verwendung von Werbe-Cookies unerlässlich, da diese den Erhalt des Internetauftritts finanzieren. Aus Benutzersicht ist dies jedoch völlig irrelevant, wodurch jedenfalls eine Zustimmungspflicht gegeben ist. Ein Verstoß gegen die Bestimmungen des TKG 2003 kann mit einer Geldstrafe von bis zu 37.000 Euro geahndet werden. (ARGE DATEN - Österreichische Gesellschaft für Datenschutz (b))

Stellungnahme der Artikel-29-Datenschutzgruppe

Entsprechend Artikel 29 der Richtlinie 95/46/EG, für den Schutz personenbezogener Daten natürlicher Personen, setzt die Europäische Union ein in Datenschutzfragen unabhängiges Beratungskonsortium ein. Die Aufgaben dieses Gremiums sind im Artikel 30 der Richtlinie 95/46/EG, sowie im Artikel 13 der Richtlinie 2002/58/EG, definiert. (Artikel-29-Datenschutzgruppe, 2013, S. 1)

Ziel der europäischen Datenschutzgruppe ist die Schaffung eines einheitlichen und gültigen Einwilligungsprozesses zur Nutzung von Cookies, um größtmögliche Transparenz für den Website-Nutzer zu schaffen. Die unterschiedlichen Auslegungen der europäischen Mitgliedsstaaten müssen zwingend vereinheitlicht werden. So müssen deutliche Hinweise über die verwendete Cookie-Art auf der Website zu finden sein. Es ist essentiell, User deutlich darüber in Kenntnis zu setzen, dass durch die Nutzung der Website Cookies auf dem Endgerät abgespeichert werden und dass der User durch bloße Nutzung der Website diesem Sachverhalt zustimmt. Zusätzlich muss dem Nutzer jedoch ermöglicht werden, Cookie-Präferenzen abzugeben. Ebenso wichtig ist, dass diese Präferenz zu einem späteren Zeitpunkt jedenfalls adaptierbar bleibt. Ein Regelwerk, um bestimmte Cookies zu akzeptieren oder die Speicherung gänzlich zu verweigern, muss bereitgestellt werden. (Artikel-29-Datenschutzgruppe, 2013, S. 2)

Der Begriff „Einwilligung“ erfordert ebenfalls einer genaueren Spezifikation, damit ein einheitliches, die Mitgliedsstaaten übergreifendes, Verständnis möglich wird. So muss eine korrekte Einwilligung des Benutzers folgende Punkte erfüllen: (Artikel-29-Datenschutzgruppe, 2013, S. 3)

- „Spezifische Informationen“
- „Zeitablauf“
- „Aktive Entscheidung“
- „Ohne Zwang“

Die europäische Datenschutzgruppe definiert, dass die obigen Elemente „[...] spezifische Informationen, vorherige Einwilligung, durch aktives Verhalten des Nutzers geäußerte Willensbekundung sowie die Möglichkeit der Entscheidung ohne Zwang [...]“, für den rechtskonformen Einsatz von Cookies dringend erforderlich sind. (Artikel-29-Datenschutzgruppe, 2013, S. 3)

3.4.2 Analysesoftware

Google Analytics ist mitunter der bekannteste Service zur Analyse von Benutzern auf Internetseiten. Die einfache Bedienung, sowie schnelle Inbetriebnahme des Dienstes und das Wegfallen von Softwarekosten bieten nicht IT-versierten Personen eine solide und wirkungsvolle Basis zur Anwenderanalyse. Im Gegenzug entwickelte Matthieu Aubry, gestützt durch eine engagierte Community, die Open-Source Analyseplattform Piwik. (Piwik PRO GmbH, 2016, S. 5)

Google Analytics

Software-as-a-Service (SaaS) Produkte, wie Google Analytics, haben den Vorteil, dass aus Sicht des Betreibers einer Website keine aufwendigen Installationen notwendig sind. Daraus ergeben sich Effizienz-, Kosten- und Skalierungsvorteile. Die Software wird von Google gewartet und der Website-Betreiber braucht nur einen gängigen Webbrowser, um die aufgezeichneten Informationen einzusehen und zu verwalten. Dies impliziert, dass jegliche Daten auf Google-Server gespeichert und möglicherweise für Dritte einsehbar sind. (Piwik PRO GmbH, 2016, S. 9)

Der genaue Standort der Daten ist ungewiss, was aus Datenschutzsicht eine Problematik darstellt. (Piwik PRO GmbH, 2016, S. 9) Google ist in der Lage die gesammelten Informationen mit anderen Diensten aus der eigenen Angebotspalette zu kombinieren, umso umfassende Benutzerprofile zu erstellen. Seitens Google werden die Daten zur Verbesserung bestehender Google-Dienste verwendet. Die Services des Internet-Giganten Google sind aus heutiger Sicht omnipräsent, was zu einer Ansammlung von enormen Datenmengen und damit einhergehender Verantwortung führt. Die mittels Google Analytics verarbeiteten Daten werden vertraulich behandelt, jedoch weist die Google-Privacy-Policy ausdrücklich darauf hin, dass Website-Betreiber keine zur Identifikation von Personen dienenden Daten an Google senden dürfen. (Piwik PRO GmbH, 2016, S. 11 f.)

Nachfolgender Ausschnitt aus den Google Analytics Nutzungsbedingungen unterstreicht die Tendenz, dass Google als Datensammler par excellence fungiert und lässt Vermutungen offen, warum Google Analytics ohne Kosten für Website-Betreiber angeboten wird: (Google (d), 2016) & (Piwik PRO GmbH, 2016, S. 14)

„Google and its wholly owned subsidiaries may retain and use, subject to the terms of its privacy policy (located at <https://www.google.com/policies/privacy/>), information collected in Your use of the Service. [...]”

Piwik

Das Analyseprogramm Piwik wird in drei verschiedenen Ausprägungen angeboten. Website-Betreiber können die Community-Version der Software oder die funktionsreichere Pro-Version direkt auf einen entsprechend vorbereiteten⁵ Webserver installieren. Alternativ dazu bietet die Piwik PRO GmbH eine gehostete Variante, nach demselben Softwaremodell wie Google Analytics, genannt Piwik PRO Cloud, an. (Piwik PRO GmbH, 2016, S. 5) Die lokale Installation von Piwik erfordert erweiterte IT-Kenntnisse und ist daher nur für Unternehmen, die über eine eigene IT-Abteilung verfügen, ratsam. (Piwik PRO GmbH, 2016, S. 10)

Der Vorteil besteht jedoch darin, dass Unternehmen genau wissen, wo ihre sensiblen Daten und die Daten ihrer Kunden aufbewahrt sind. Ebenso können länderspezifische Datenschutzrichtlinien eingehalten werden.

Die Europäische Kommission betreibt auf Basis der Open-Source Software Piwik einen selbst gehosteten Analysedienst, genannt *„Europa Analytics“*. Dadurch können EU konforme Datenschutzrichtlinien aufrechterhalten werden. Aus technischer Sicht bedeutet dies, dass Analysedaten ausnahmslos auf den eigens betriebenen MySQL-Server (Structured Query Language) der Europäischen Kommission gespeichert sind und somit europäischem Recht unterliegen. Maßnahmen, wie die Anonymisierung von Quelldaten und das Anbieten von „Opt-out“-Verfahren klassifizieren den optimalen und datenschutzkonformen Einsatz von Analysesoftware. „Opt-out“ bietet Website-Benutzer die Möglichkeit nicht mehr mithilfe von Cookies analysiert zu werden. Wird dies zu einem späteren Zeitpunkt wieder gewünscht, so kann mittels „Opt-in“ revidiert werden. (Europäische Kommission (a))

⁵ <http://piwik.org/docs/requirements/> (abgerufen am 14. September 2016)

3.4.3 Steuerung von Cookies durch den Nutzer

Sowohl Google Analytics, als auch Piwik bieten IT-Administratoren die Möglichkeit „Opt-in“- bzw. „Opt-out“-Verfahren zu implementieren. Google Analytics erfordert hierfür ein spezielles Browser-Plugin, welches durch manuelle Intervention auf Benutzerseite installiert werden muss. Piwik ermöglicht das Einbinden eines „Opt-out“-Schalters direkt auf der Website. Dadurch können Benutzer selbst über ihre Analysepräferenz entscheiden. (Piwik PRO GmbH, 2016, S. 31)

Abbildung 15 zeigt den datenschutzkonformen Webauftritt der Firma Oracle. Ein vorbildliches Cookie-Steuerungspanel bietet Besuchern größtmögliche Transparenz.

Ihre Wahlmöglichkeiten hinsichtlich Cookies auf dieser Website. **ORACLE**

Wählen Sie aus, ob diese Website lediglich funktionelle Cookies und/oder Marketing-Cookies, wie nachfolgend beschrieben, verwenden darf.

— — **ERFORDERLICHE COOKIES**
Diese Cookies sind für die Kernfunktionen der Website erforderlich und werden automatisch aktiviert, wenn Sie diese Website nutzen.

— — **FUNKTIONELLE COOKIES**
Diese Cookies ermöglichen uns die Analyse der Website-Nutzung, damit wir deren Leistung messen und verbessern können.

— — **MARKETING-COOKIES**
Diese Cookies werden von uns und Dritten genutzt, um Werbung anzubieten, die Ihren Interessen entspricht.

Gestattete Funktionalität

- Speichern die Anmeldeinformationen und sorgen für sichere Anmeldung
- Ermöglicht einen sicheren Login
- Speichern Ihren Aufgaben- oder Transaktionsfortschritt
- Speicherung des Fortschritts bei Bestellvorgängen
- Analysieren die Website-Nutzung, um kundenspezifischen Inhalt zu liefern
- Speicherung Ihrer Anmeldedaten
- Führen Analysen durch, um die Website-Funktionalität zu optimieren
- Speicherung des Warenkorb-Inhalts
- Ermöglichen Dritten das Angebot von Tools für Gesellschaftsmedien
- die einheitliche Darstellung von Seiten-Inhalten

NICHT gestattete Funktionalität

- Liefern Ihnen interessensabhängige Angebote oder Werbung
- Ermöglicht das Teilen von Seiten über Soziale Netzwerke
- Ermöglicht das Schreiben von Kommentaren
- das Anzeigen von Angeboten, die Ihren Interessen entsprechen

◀ ABBRECHEN ✓ PRÄFERENZEN SENDEN

Datenschutzerklärung | Powered by TRUSTe

Abbildung 15 Cookie-Steuerungspanel auf der Website der Firma Oracle⁶
Quelle: vom Autor erstellt

⁶ <https://www.oracle.com/at/index.html> (abgerufen am 19. September 2016)

4 ANALYSE: DAS ÖFFENTLICHE WLAN DER STEIRISCHEN LANDESHAUPTSTADT GRAZ

In diesem Kapitel werden zusätzliche, obligatorische Elemente eines strukturierten Modells zum Aufbau von öffentlichem WLAN im städtischen Umfeld erläutert. Graz, als steirische Landeshauptstadt, verfügt über ein breit ausgebautes und öffentliches WLAN-Netzwerk. Mithilfe qualitativer Experteninterviews wird das dortige WLAN-System beleuchtet und kritisch analysiert. Die Befragten stammen aus dem Umfeld der Firma Citycom Telekommunikation GmbH und bilden ein abwechslungsreiches Fachgremium in den Bereichen, Wirtschaft, Technik und Marketing. Unter Einbezug der technischen und rechtlichen Voraussetzungen kann so letztendlich in *Kapitel 5* ein umfassendes und generell anwendbares Modell für eine urbane WLAN-Infrastruktur erstellt werden.

Die Auswertung der Experteninterviews erfolgt nach dem Schema von (Meuser & Nagel, 2009, S. 467 f.) anhand thematischer Einheiten und inhaltlicher Zusammengehörigkeit. Hierbei fokussiert sich jedes Interview auf den Wissenshorizont des jeweiligen Experten. Der *„gemeinsam geteilte institutionell-organisatorische Kontext“* der Experten schafft die Vergleichbarkeit der Interviewtexte. Die Gesamtheit der beteiligten Fachläute verfügt über ein grundsätzliches Verständnis der Thematik, welches durch personenbezogenes Spezialwissen komplettiert wird.

4.1 Urbanes WLAN in Graz

Zur Erstellung eines Modells für urbane WLAN-Netzwerke sind Informationen über aktuelle WLAN-Projekte in Städten erforderlich. Die Firma Citycom Telekommunikation GmbH betreibt mehrere öffentliche WLAN-Standorte, welche unter dem Namen „Cityaccess“ zusammengefasst sind. „Cityaccess“ als Begriff setzt sich aus der Betreiberfirma Citycom und dem Wort Internetaccess zusammen. (Huber, 2016, S. 2)

Für die administrative Analyse dieses WLAN-Netzwerks sind detaillierte Informationen, von der Geschäftsführung der Firma Citycom über die Entstehung dieses Service, erforderlich. Die im Experteninterview erfragten Sachverhalte stehen im Fokus auf das Projekt „Cityaccess“, der Gesamtheit der Standorte, sowie projektspezifische Rahmenbedingungen für die Entstehung und den Betrieb der Dienstleistung.

4.1.1 Die Entstehung des öffentlichen WLAN in Graz

Zu Beginn des Projekts existierten seitens der Geschäftsführung Skepsis bezüglich der Notwendigkeit von öffentlichem WLAN, da sowohl die Verbreitung an mobilen Endgeräten gering ausfiel, als auch Unklarheit über die Zielgruppe herrschte. In der initialen Entstehungsphase des „Cityaccess“ zeigte sich, dass WLAN primär für Touristen relevant war, da der Großteil der Grazer Bevölkerung über mobile Datenpakete verfügte. Dieser Umstand hat sich allerdings in den letzten Jahren gewandelt, wonach öffentliches WLAN auch zunehmend für Grazer bedeutsam wird. (Huber, 2016, S. 1)

WLAN-Standorte werden aufgrund von Aufträgen der Stadt erhoben. Dazu zählen beispielsweise Events oder vertriebliche Projekte. Ziel ist die kostengünstige Bereitstellung und Erschließung von Gebieten. Da das Projekt „Cityaccess“ grundsätzlich kein kommerzielles Produkt ist, gilt es einen Konsens zwischen der gewünschten Nachfrage und der wirtschaftlichen Betrachtung des Standorterhebungs- und Umsetzungsprozesses zu schaffen. Der primäre Fokus der Servicebereitstellung liegt auf Parks, öffentliche Plätze und Kultureinrichtungen. Hier ist eine Erlaubnis zur Installation von Hot Spots leichter zu erlangen, als in der Altstadt von Graz. (Huber, 2016, S. 2)

Abbildung 16 zeigt die Installation einer WLAN-Antenne am multimodalen Knoten Hasnerplatz in Graz, die von der Firma Citycom betrieben wird.



Abbildung 16 Öffentliches WLAN am Grazer Hasnerplatz
Quelle: Citycom Telekommunikation GmbH

Zudem ist eine Kooperation mit dem Forschungsnetzwerk „eduroam“ angedacht. Grundlegende technische Rahmenbedingungen können mit wenig Aufwand umgesetzt und finanziert werden. Allerdings fehlt diesbezüglich ein konkreter Auftrag der Stadt oder des Gemeinderats. (Huber, 2016, S. 2)

Öffentliches WLAN gehört zu den wesentlichsten Services einer modernen Stadt, weshalb derzeit Pläne für einen weitreichenden und flächendeckenden WLAN-Ausbau in Graz ausgearbeitet werden. (Huber, 2016, S. 4)

4.1.2 Sicherheit im „Cityaccess“

Sicherheit ist ein wichtiger Bestandteil eines öffentlichen WLAN-Netzes. Die Schaffung technischer Rahmenbedingungen hierfür obliegt dem jeweiligen IT-Beauftragten. Das Projekt „Cityaccess“ ist so gestaltet, dass mehrere Firewalls und Content-Filtering Maßnahmen dem User höchsten Schutz bieten. Schlussendlich ist jedoch jeder User selbst für die eigene Sicherheit im Netzwerk verantwortlich. Selbst beim sorgsamem Umgang mit persönlichen Informationen ist die Gefahr Opfer von Datenspionage zu werden, in einem öffentlichen Netzwerk größer, als im privaten WLAN. Durch bedachtes Handeln seitens des Nutzers kann diese Unsicherheit jedoch erheblich reduziert werden. (Huber, 2016, S. 1)

Installation und Betrieb von öffentlichem WLAN werden durch Instanzen des jeweiligen Zuständigkeitsbereichs geregelt. Daher gilt, dass die von der Altstadtkommission und anderen weisungsbefugten Behörden auferlegten Installations- und Betriebsbedingungen eingehalten werden müssen, um den Service betreiben zu dürfen. Seitens der RTR-GmbH besteht kein Einfluss auf die Dienstleistung, lediglich die Vorhaben der Citycom sind an die RTR-GmbH zu melden. (Huber, 2016, S. 2)

Unter Anbetracht der derzeitigen österreichischen Rechtsprechung ist der Provider eines öffentlichen WLAN-Dienstes nicht für das Fehlverhalten der Internet-User verantwortlich. Die Firma Citycom muss beim Missbrauch des Dienstes mit den Behörden kooperieren und im Zuge eines Verfahrens eventuell bestimmte Nutzer sperren. Jene Daten, die mittels Piwik erhoben werden, dienen rein statistischen Zwecken. Die Daten werden nicht mit anderen Traffic-Daten oder persönlichen Informationen von Usern verknüpft. Die Analyse beschränkt sich auf gerätespezifische Attribute und deren Verteilung je Standort. Da die Daten auf den hauseigenen Server der Citycom abgespeichert sind, verlassen die Analysedaten keinesfalls Österreich. (Huber, 2016, S. 4)

4.1.3 Kundengewinnung durch Public-WLAN

Öffentliches WLAN ist nicht unmittelbar als Werkzeug für die Gewinnung von neuen Kunden zu sehen. Im Kontext der Firma Citycom dient es als Bestandteil einer Imagekampagne. Als lokaler Internet-Service-Provider benötigt die Citycom keine klassische Produktwerbung und kann dennoch fokussiert auf die eigenen Kerngeschäfte hinweisen. Die Bereitstellung von Public-WLAN ist nicht als Produkt zu sehen. (Huber, 2016, S. 2) Sehr wohl dient öffentliches WLAN als Technologie für das Sponsoring von Veranstaltungen. (Huber, 2016, S. 3)

4.1.4 Wirtschaftliche Betrachtung des „Cityaccess“

Das Public-WLAN in Graz wird zurzeit nicht kommerziell betrieben. Umso wichtiger ist die kostenoptimierte Bereitstellung der Dienstleistung. Die Kosten eines Standortes, die sich aus Bau, Betrieb, Akquisition und Administration zusammensetzen, belaufen sich im Durchschnitt auf einige Tausend Euro. Dieser Betrag kann je nach Standorterschließungsaufwand variieren. Gerade die Herstellung der Glasfaserverbindung vom Standort bis zu den Citycom Rechenzentren ist ein erheblicher Kostenfaktor. Nicht zu unterschätzen ist auch die Arbeitszeit zur Konzipierung und Inbetriebnahme des Standorts, sowie einige Hundert Euro pro Access Point. (Huber, 2016, S. 3)

Die temporäre Deaktivierung von WLAN-Antennen (On/Off-Strategien) resultiert in keiner Kosteneinsparung. Die dahinterliegende Infrastruktur verbraucht in Relation zu einem Access Point ohnehin viel mehr Strom. Auch die Entlastung des Internet-Uplinks ist nicht kostenrelevant. Zudem wären der administrative Mehraufwand und potentiell unerwünschte Ausfallszeiten, aufgrund allfälliger nächtlicher Events, nicht tragbar. (Huber, 2016, S. 3)

Die Verantwortlichen der Stadt Salzburg verfolgen einen konträren Ansatz. Das WLAN wird zwischen 24:00 Uhr und 05:00 deaktiviert.⁷

Derzeit besteht kein Bedarf durch Partnerschaften mit lokalen Mobilfunkanbietern das „Cityaccess“ als Trägermedium für „LTE-over-WiFi-offloading“ heranzuziehen, da Graz ohnehin bereits über ein breit ausgebautes LTE-Netz verfügt. (Huber, 2016, S. 3)

⁷ http://www.stadt-salzburg.at/internet/service/aktuell/aussendungen/2011/salzburg_surft_gratis_wifi_im_stadtraum_335024.htm
(abgerufen am 03. Oktober 2016)

4.2 Ausrichtung der Dienstleistung am Markt

Obgleich die Vorgaben technischer und rechtlicher Natur für die Inbetriebnahme der Dienstleistung zwingend einzuhalten sind, ist jedenfalls die durchdachte Ausrichtung des Angebots am Markt besonders von Bedeutung. Die Grundlage dieses Kapitels bildet das Interview mit einem Experten, welcher knapp 20 Jahre Erfahrung mit WLAN im öffentlichen Raum, IT-Projektmanagement und Gestaltung von Qualitätsmanagementprozessen in IT-Landschaften vorweisen kann. Im Fokus des Gesprächs steht das Potential von öffentlichem WLAN für Graz und dessen Stakeholder. Unter Anbetracht der einzelnen Servicebestandteile, sowie der Wirkung der Dienstleistung, insbesondere auf die Stakeholder, werden die Schwierigkeiten bei der Ausrichtung am Markt hervorgehoben. Ergänzend werden Informationen über die Verwendung des Captive Portal als Serviceplattform, sowie der Informationsgewinn für weitere Softwareprojekte durch die Analyse von WLAN-Teilnehmern diskutiert.

4.2.1 Das Captive Portal als Serviceplattform

WLAN wird als wesentlicher Bestandteil einer modernen Stadt wahrgenommen und kann als Träger für diverse kommunale Dienstleistungen dienen. Kostenloses, öffentliches und vor allem leicht zugängliches WLAN kann als wirkungsvolles Instrument zur Darstellung städtischer Dienstleistungen verwendet werden. Alle in einer Stadt verbauten Sensoren, beispielsweise zum Auslesen des Zähler- oder Wasserstandes, können mit einem flächendeckenden, kabellosen Netzwerk verbunden werden, um so die Entwicklung einer Smart City voranzutreiben. Zum Begriff einer Smart City zählt auch der intelligente und verantwortungsbewusste Umgang mit Abfall. Derzeit erfolgt die Entwicklung einer Serviceplattform in Kooperation mit dem Umweltamt der Stadt Graz zur Darstellung von Informationen und Abfuhrterminen. Das Captive Portal, als wirkungsvolles Marketinginstrument, kann zur marketingtechnischen Ausrichtung solcher Dienstleistungsangebote herangezogen werden. Die jeweiligen Servicebetreiber könnten sich erheblichen Aufwand und kostspielige Werbekampagnen sparen. Das WLAN-System des „Cityaccess“ muss eine modulare Oberfläche für Marketingmaßnahmen der Stadt Graz und dessen Partner bieten. (Droneberger, 2016, S. 2)

4.2.2 Informationsgewinn durch Teilnehmeranalyse

Die in den Analysedaten des „Cityaccess“ ersichtlichen Gerätespezifikationen von WLAN-Teilnehmern hilft App-Entwicklern bei der zielgerichteten und vor allem plattformspezifischen Programmierung von Anwendungen für die Stadt Graz. Beispielsweise wird das mobile Betriebssystem Windows Mobile nahezu gar nicht verwendet, wonach auch keine mobilen Anwendungen speziell für diese Plattform angepasst werden müssen. Stattdessen setzt man auf HTML5-Webapplikationen (Hypertext Markup Language), welche architekturübergreifend funktionieren oder fokussiert sich auf populärere Mobilumgebungen. Wünschenswert wäre zudem die Auswertung demographischer Userdaten, wie Altersgruppe und Geschlecht, da diese Eigenschaften maßgeblich für die Entwicklung weiterer Services der Stadt Graz Verwendung finden würden. Ebenso wünschenswert ist die Analyse des Netzwerkverkehrs zur Erkennung bestimmter Applikationen, welche online verwendet werden. Wichtig ist, dass die Analysedaten stets in der Hoheit der Holding Graz bzw. der Citycom bleiben. Erfahrungsgemäß sinkt die Akzeptanz eine App zu benutzen, wenn Google Analytics als Analysewerkzeug implementiert wurde. Ebenso muss dem Nutzer die Möglichkeit einer Analyseverweigerung unbedingt eingeräumt werden. (Droneberger, 2016, S. 2 f.)

4.2.3 Die Bewerbung der Dienstleistung als Herausforderung

Zurzeit gibt es nur sehr eingeschränkte Marketingmaßnahmen zur Bekannthetsförderung des „Cityaccess“. Vereinzelt wurden an einigen Standorten Hinweisschilder angebracht, um auf den Service aufmerksam zu machen. Hier besteht definitiv Änderungsbedarf, sobald die technische Revision abgeschlossen ist und die Dienstleistung in voller Leistungsstärke angeboten werden kann. Im Rahmen von Sponsoring-Tätigkeiten wird das jährliche Grazer Elevate Festival gerne unterstützt. Die dahinterstehende Verbindung innovativer und querdenkender Persönlichkeiten trägt maßgeblich zur Bekanntmachung des öffentlichen WLAN der Stadt Graz bei. Noch bevor die Holding Graz im Marketingbereich tätig wurde, haben die Betreiber der Elevate Festival-Website aktiv Werbung für den Service gemacht und diesen gutgeheißen. Zudem wären Social-Media-Kampagnen, sowie Werbeanzeigen an den multimedialen Displays in den Straßenbahnen der Stadt Graz sehr sinnvoll. (Droneberger, 2016, S. 3 f.)

4.2.4 Serviceetablierung unter Anbetracht der Stakeholder

Die Firma Citycom Telekommunikation GmbH ist Teil der Holding Graz - Kommunale Dienstleistungen GmbH, wonach den öffentlichen Raum betreffende Entscheidungen mehrere Instanzen durchlaufen und dadurch geprüft werden. Wichtig ist, dass das öffentliche WLAN der Stadt Graz intern einen gewissen Stellenwert im Konzern einnimmt, damit die ausgearbeiteten Konzepte greifen und auch nach außen hin erfolgreich kommuniziert werden. Primäre Managementaufgabe ist das Vereinigen aller Stakeholder und Werbetreiber, um gemeinsam einen nachhaltigen Service zu schaffen. (Droneberger, 2016, S. 5 f.)

4.3 Öffentliches WLAN als Service für den Tourismus- und Wirtschaftsstandort Graz

Frei zugängliches und öffentliches Internet ist ein obligatorischer Bestandteil einer modernen Stadt, wie Graz. In diesem Kapitel wird öffentliches WLAN aus Sicht des Geschäftsführers der Graz Tourismus und Stadt Marketing GmbH betrachtet. Im Fokus steht der Service für den Reisenden, jedoch auch der Mehrwert, den öffentliches WLAN für den Wirtschaftsstandort Graz schafft.

4.3.1 Öffentliches WLAN im Tourismus

Die Nachfrage nach performantem und öffentlichem WLAN ist derzeit ununterbrochen präsent, was zudem durch die aktuellen Roaming-Tarifmodelle lokaler Mobilfunkanbieter verstärkt wird. Im Vordergrund stehen der kostenlose und vor allem der hürdenlose Internetzugang, welcher ortsübergreifend gegeben sein muss. Spezieller Fokus liegt hierbei auf Knotenpunkte wie Flughäfen oder Bahnhöfe. WLAN ist dort zur Verfügung zu stellen, wo sich die Touristen hauptsächlich aufhalten. Dies impliziert wichtige Plätze und Sehenswürdigkeiten, jedoch auch deren Verbindungswege. Zudem verwenden Gastronomiebetriebe WLAN zur Kundengewinnung. Hierzu kann von der Wirtschaftskammer Kärnten eine entsprechende Förderung⁸ bezogen werden. Um großflächiges WLAN anbieten zu können, finden momentan in New York weitreichende Umbauarbeiten von Telefonzellen zu Hotspots⁹ statt. Auf diese Art und Weise kann äußerst rasch eine weitreichende Vernetzung realisiert werden. Öffentliches WLAN gehört zu den üblichen Dienstleistungen, die eine Stadt anbieten muss, weshalb Touristen oftmals nicht explizit auf den vorhandenen Service hingewiesen werden müssen. (Hardt-Stremayr, 2016, S. 1 f.) In Graz befinden sich jedoch Informationsschilder, die auf öffentliches WLAN hinweisen.

Laut (Hardt-Stremayr, 2016, S. 2) ist die standortspezifische Bereitstellung von Zusatzinformationen oder etwaige Registrierungsrestriktionen keinesfalls förderlich. Die Besucher wollen möglichst schnell und unkompliziert ihren Informationsbedarf decken. Standortabhängiges Zusatzmaterial am Captive Portal muss ein wirkliches Interesse und Informationsbedürfnis befriedigen, um nicht störend zu wirken. Ebenfalls sind Newsletter in diesem Kontext keine empfehlenswerte Variante zur Touristeninformation. (Hardt-Stremayr, 2016, S. 2 f.)

⁸ <http://www.wkk.or.at/tourismus/wlan/downloads/foerderantrag.pdf> (abgerufen am 11. Oktober 2016)

⁹ <https://www.link.nyc/> (abgerufen am 11. Oktober 2016)

4.3.2 Akquisition von Reisenden mittels WLAN

Ein städtisches WLAN muss den aktuellen Bandbreitenanforderungen von Social-Media-Kanälen gerecht werden, denn nur so können Touristen oder Blogger ihren Inhalt schnell teilen und so wiederum indirekt und vor allem kostenlos Werbung bereitstellen, um neue Touristen anzuwerben. Graz, als Stadt im „*Creative-Industry-Bereich*“, kann somit neue Personengruppen anziehen und die lokale Wirtschaft, durch Unterstützung von Startups, fördern. (Hardt-Stremayr, 2016, S. 2)

Auch Helge Fahrnberger, Geschäftsführer der Toursprung GmbH, ist der Meinung, dass das Teilen von Stadtbildern über soziale Netzwerke einen immensen Mehrwert für das Stadtmarketing generiert und gratis Sichtkontakte erzeugt. Bei einer Kostengegenüberstellung zwischen WLAN und Werbung durch klassische Printmedien, resultiert ein erheblicher Mehrwert zu Gunsten des kabellosen Internet. (Fahrnberger, 2014, S. 35)

Gerade dort, wo viel fotografiert wird und Bilder über diverse Plattformen geteilt werden, muss leistungsstarkes WLAN-Equipment installiert sein. Die Website „www.sightsmap.com“ stellt hierfür eine eindrucksvolle Online-Karte mit jenen Orten, an denen viele Fotos entstehen, bereit. (Hardt-Stremayr, 2016, S. 4)

Zudem wäre eine Kooperation mit dem Forschungsnetzwerk „eduroam“ optimal, um die Universitätsstadt Graz zu fördern. Öffentliches WLAN muss auf jedem Campus und in jedem Studentenheim zur Verfügung stehen. Die Akquisition von neuen Unternehmen, internationalen Studenten und Forschern muss als oberste Priorität gewertet werden, denn hierdurch profitiert der Wirtschaftsstandort Graz maßgeblich. (Hardt-Stremayr, 2016, S. 4)

4.3.3 Angebotsoptimierung durch Herkunft- und Bewegungsanalysen von Touristen

Mithilfe detaillierter Analysedaten könnten die Bewegungsströme von Touristen nachverfolgt werden, was zu einem besseren Serviceangebot und Abwicklung von Veranstaltungen beitragen kann. Es wurde bereits erfolglos versucht diese Informationen von einem lokalen Mobilfunkanbieter zu erhalten. Die belgische Stadt Brüssel verfügt im Gegensatz über ein durchdachtes Analysesystem zur Erkennung von Personen, die sich auf diversen Plätzen aufhalten. Unter Einbezug dieser Daten können im Vergleich zu den klassischen Fragebögen, zuverlässige Hochrechnungen im tagestouristischen Sektor generiert werden. (Hardt-Stremayr, 2016, S. 3)

4.3.4 Immission durch WLAN

Im touristischen Bereich ist das Unbehagen durch WLAN-Wellen nicht stärker ausgeprägt, als in anderen Arealen, da sich Touristen nur zeitlich begrenzt an einem Standort aufhalten. Hier zählen vielmehr die zur Verfügung stehende Bandbreite und der Abdeckungsradius von WLAN-Anlagen. (Hardt-Stremayr, 2016, S. 3 f.)

Die durch WLAN-Immission hervorgerufene Belastung an Kurorten oder bestimmten touristischen Einrichtungen ist standortbezogen nicht größer ausgeprägt, als an anderen Stellen, wonach Beschwerden durch Touristen nur Einzelfallcharakter haben. (Hardt-Stremayr, 2016, S. 3 f.)

4.4 Der Standorterhebungs- und Umsetzungsprozess

Der Standorterhebungs- und Umsetzungsprozess zählt zu den wichtigsten Teilaspekten bei der Gestaltung eines WLAN-Systems. Die rechtskonforme und bautechnisch durchdachte Platzierung und der Betrieb sind fundamental für den Erfolg der Dienstleistung. Wie in *Kapitel 3* erläutert müssen bestimmte Rahmenbedingungen zwingend eingehalten werden. Nachfolgendes Experteninterview wurde mit einem Spezialisten für die Planung von Telekommunikationsstandorten, welcher auf seine über 20-jährige Expertise in den Bereichen Infrastrukturanlagen, Projektierung, Errichtung, Service, Betrieb und Wartung von solchen Anlagen zurückgreifen kann, durchgeführt.

4.4.1 Die Initialisierung eines Standortes

Zu Beginn eines Bauprojekts steht immer der standortspezifische Bedarf nach einem kabellosen Internetzugang. Die Initialisierung eines Standortes muss aus zwei Blickwinkeln betrachtet werden. Aus bautechnischer Sicht gilt es zu evaluieren, wo das WLAN-Equipment aufgebaut werden kann. Die Herausforderung hierbei ist vor allem die optimale Anbringung der WLAN-Antenne mitsamt dem restlichen Softwareverarbeitungsteil. Aus privatrechtlicher Sicht betrachtet ist in Österreich das Grundeigentumsrecht von essentieller Bedeutung. Es bedarf einer privatrechtlichen Vereinbarung mit dem Inhaber der Liegenschaft, welche als Tragwerk für WLAN-Equipment dienen soll. Dieser Vertrag umfasst sowohl „*Art, Umfang und Wesen*“ der Funkstation, als auch die monetäre Entschädigung des Liegenschaftsinhabers. (Axnix, 2016, S. 1 f.)

4.4.2 Bauvorgaben bei der Installation

Die Erfüllung öffentlich-rechtlicher Gegebenheiten ist ein obligatorischer Bestandteil beim Installieren von WLAN-Umgebungen, weshalb spezifische Genehmigungsverfahren existieren. In Österreich gibt es bundesländerübergreifend unterschiedliche Richtlinien für die Beurteilung von Antennen und Kabelanlagen. Die steirische Bauordnung und das Altstadterhaltungsgesetz¹⁰ (AEG) in Graz bilden zwei wesentlichen Rahmenbedingungen zur Installation von Funkanlagen. Darüber hinaus gibt es in Städten eine Vielzahl denkmalgeschützter Gebäude. (Axnix, 2016, S. 2 f.)

¹⁰ <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrStmk&Gesetzesnummer=20000162> (abgerufen am 26. September 2016)

Der Denkmalschutz ist im Grundbuchauszug vermerkt und wird vom Bundesdenkmalamt streng kontrolliert. Die Behörde muss daher in den Standorterschließungsprozess eingebunden werden. Begehungen vor Ort, sowie die optimale Integration von Antennen an Gebäuden, sind wichtige Voraussetzungen, um eine Genehmigung zu erhalten. Beim Planen muss darauf geachtet werden, die bereits existierende Infrastruktur des Gebäudes optimal auszunutzen, sowie auch bautechnische Merkmale, wie Regenabflussrohre als Trägermedium für Antennen zu gebrauchen. Aus funktechnischer Perspektive ist dies keinesfalls suboptimal, da sich WLAN-Signale nicht kugelförmig ausbreiten und daher bloß die signalschwache Rückseite zum Gebäude zeigt. Generell gilt: Je unauffälliger die Installation erscheint, desto einfacher ist die Genehmigung der Funkanlage beim Bundesdenkmalamt. Der Antragsteller ist gegenüber dem Bundesdenkmalamt in Beweispflicht, dass durch das Anbringen einer WLAN-Antenne das „(...) äußere Erscheinungsbild und die Grundcharakteristik (...)“ des Gebäudes nicht beeinflusst werden. Hier gilt es einen Konsens zwischen dem Schutz einer Liegenschaft und der zukunftsorientierten Bereitstellung von kabellosem Internet zu schaffen. (Axnix, 2016, S. 2 f.)

Abbildung 17 zeigt die optimale Installation eines WLAN-Access Points, sodass weder das äußerliche Erscheinungsbild, noch die Grundcharakteristik der Grazer Murbrücke beeinflusst wird. Abbildung 18 illustriert einen WLAN-Access Point am Dach des Rondeaus am Grazer Jakominiplatz. Obwohl die Positionierung der WLAN-Funkanlage offensichtlicher ist, als beispielsweise bei der Grazer Murbrücke, fällt diese aufgrund der baulichen Gegebenheiten des Standorts keinesfalls störend auf.



Abbildung 17 Öffentliches WLAN am Citybeach (Grazer Murbrücke)

Quelle: Citycom Telekommunikation GmbH



Abbildung 18 Öffentliches WLAN am Grazer Jakominiplatz
Quelle: Citycom Telekommunikation GmbH

4.4.3 Service und Betrieb

Die Servicierung von Funkanlagen ist ein wesentlicher Bestandteil eines erfolgreichen WLAN-Netzwerks. Es ist wichtig, dass die Anlagen einerseits leicht zugänglich sind und dass andererseits entsprechende Vereinbarungen mit den Liegenschaftsinhabern bezüglich der Serviceintervalle getroffen werden. Ziel ist es nicht, den Privaten durch häufige Interventionen unnötig zu behindern. (Axnix, 2016, S. 2)

Für den konformen Service und Betrieb einer Anlage muss die für den Standort zuständige Person stets einen Überblick über die getroffenen Vereinbarungen (privatrechtlich und behördentechnisch) behalten. Es ist nötig den Interventionszeitpunkt zu kennen, da „(...) *Verträge im Allgemeinen befristet vereinbart werden.*“ Darüber hinaus ist es wichtig, gesonderte Bescheid-Auflagen zu kennen, um die Standortsicherung zu gewährleisten. (Axnix, 2016, S. 3)

4.4.4 Regulatorischer Änderungsbedarf

Trotz der durch die Mobilfunktechnik initiierten gesetzlichen Anpassungen im privatrechtlichen Bereich fehlt es immer noch an klaren Ablaufstrukturen und Genehmigungsverfahren im WLAN-Sektor. Der Begriff WLAN ist als solches momentan im steirischen Baurecht¹¹ noch nicht verankert, lediglich „(...) Kabelanlagen, Antennenanlagen, sichtbare Antennentragwerke (...)“ werden zurzeit spezifiziert. Hier fehlt es an notwendigen Rahmenbedingungen, die klare und vor allem bundesländerübergreifende Richtlinien schaffen. (Axnix, 2016, S. 4)

4.5 Technische Konzeptionierung der Servicestandorte

Die technisch einwandfreie Konzeptionierung des Service bildet eine fundamentale Grundlage für den Betrieb, sowie den Erfolg der Dienstleistung. In diesem Kapitel wird der technische Hintergrund des Grazer WLAN-Systems „Cityaccess“ kritisch beleuchtet, sowie das Verbesserungspotential diskutiert. Das Interview wurde mit einem Spezialisten im Bereich virtueller Rechenzentrumsinfrastrukturen durchgeführt.

4.5.1 Herausforderungen aus Sicht der IT

Die Konzeptionierung und in weiterer Folge auch der Betrieb eines öffentlichen WLAN-Systems stellt die Abteilung IT-Operations der Firma Citycom vor eine Herausforderung, die ein gut durchdachtes Systemdesign erfordert, um den wachsenden Bedarf an Bandbreite und die zunehmende Nutzerbasis zu bewältigen. Das öffentliche WLAN der Stadt Graz steht derzeit vor einer technischen Revision. Beim aktuellen WLAN-System sind sowohl die Ausfallsicherheit, als auch die Skalierbarkeit nicht gegeben. Alle Systemkomponenten, wie beispielsweise die Firewall, der DNS-Server, der Proxy-Server, der VLAN-Server und das Captive Portal werden von einer virtuellen Maschine verarbeitet. Dieser Server verfügt über keine graphische Administrationsoberfläche, was im Fehlerfall zu einer zwangsläufigen, händischen Intervention durch die Techniker der Citycom führt. Auch die Initialisierung neuer Standorte erweist sich infolgedessen als äußerst aufwendig und intransparent. Dasselbe gilt auch für die Verwaltung der Access Points. Derzeit ist ebenso eine manuelle Konfiguration der WLAN-Antennen notwendig, da es aufgrund der großen Herstellervariation im Netz keinen einheitlichen WLAN-Controller gibt. (Greiner, 2016, S. 1 f.)

In Zukunft soll das WLAN-System skalierbar ausgerichtet werden und einen Single-Point-Of-Failure konzeptionell, bestmöglich ausschließen. Darüber hinaus ist die graphische Administration aller beteiligten Komponenten essentieller Bestandteil für die Bedienung durch neu eingeschultes Personal. (Greiner, 2016, S. 1 f.)

¹¹ <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrStmk&Gesetzesnummer=20000070> (abgerufen am 27. September 2016)

Aus der Sicht des Endnutzers muss die Netzwerkinfrastruktur transparent konzipiert sein, um standortinternes Wechseln zwischen den einzelnen Access Points reibungslos zu ermöglichen. Ein standortübergreifendes und ununterbrochenes Internetsurfen ist derzeit aus administrativer Sicht und technischer Konzeptionierung nicht möglich. Zum einen sind die „Cityaccess“-Standorte räumlich zu weit voneinander getrennt und zum anderen entstehen Probleme hinsichtlich der Nutzungsstatistikauswertung. (Greiner, 2016, S. 1 f.)

Als wesentliche Herausforderung an ein öffentliches WLAN-System ist die Überprüfung der übermittelten Inhalte anzusehen. Content-Filtering Maßnahmen schützen den User und verbieten den Zugriff auf diverse Dienste und Web-Inhalte. Ein kommerzielles Unified Threat Management der Firma Fortinet¹² filtert den Web-Traffic des „Cityaccess“. Wünschenswert wäre ein zweischichtiges System, das bereits am Captive Portal möglichst nahe am Nutzer wirkt. (Greiner, 2016, S. 3 f.)

Aus Sicht eines Telekommunikationsanbieters muss die Datenhoheit stets bei der Firma Citycom liegen. Die durch den „Cityaccess“ erlangten Analysedaten sollen nicht länger via Google Analytics verarbeitet werden. Stattdessen ist die Einführung des Analysesystems Piwik auf eigener Infrastruktur fixer Bestandteil der technischen Revision des „Cityaccess“. (Greiner, 2016, S. 4)

Darüber hinaus muss die zur Verfügung stehende Bandbreite abgeklärt und konfiguriert werden. Derzeit sind für das WLAN-System 100 Mbit/s verschaltet. Im Zuge der Revision wird das Limit zunächst auf 300 Mbit/s angehoben, kann jedoch bis Ende 2017 auf 500 Mbit/s ansteigen, da zusätzliche Nutzerzahlen und auch ein verändertes Nutzungsverhalten hin zu bandbreitenintensiven Anwendungen erwartet werden. (Greiner, 2016, S. 4)

4.5.2 Access Point-Hardware

Für die großflächige Installation von WLAN-Equipment ist zwangsläufig ein gewisser Automatismus in Form eines dedizierten WLAN-Controllers erforderlich. Ziel ist die standortspezifische und gruppierte Administration von mehreren Access Points. Relevante Netzwerkeinstellungen, wie beispielsweise die SSID, müssen vom WLAN-Controller ohne händisches Zutun auf neue Access Points des Standortes ausgerollt werden, um so im Fehlerfall Access Points auszutauschen und automatisch zu provisionieren. Das WLAN-Steuerungssystem muss zwingend in einer virtualisierten Umgebung operieren, da zusätzliche Hardwareausgaben inakzeptable sind. (Greiner, 2016, S. 2)

¹² <http://de.fortinet.com/> (abgerufen am 18. Oktober 2016)

Nachfolgend zeigt *Tabelle 5* die optimalen Eigenschaften eines Access Points für den urbanen Einsatz in Graz.

Eigenschaften	Werte
Hersteller	Maximal zwei bis drei unterschiedliche Hersteller im urbanen Netzwerk
Varianten	Die Hersteller müssen ein breites Sortiment an indoor- und outdoor-fähigen Geräten anbieten, um auf die Skalierung pro Standort einzugehen.
Frequenzen und WLAN-Modus	Dualbandfähig (2.4 GHz und 5 GHz). Der Standard IEEE 802.11ac ist im urbanen Umfeld empfehlenswert.
Erscheinungsbild	Der Access Point muss möglichst unscheinbar sein, gut in das Stadtbild passen und eine einfache Montage erlauben.
Management	Eine zentrale Konfiguration mittels eines entsprechenden virtuellen WLAN-Controllersystems ist obligatorisch.

Tabelle 5 Access Point-Spezifikationen
Quelle: (Greiner, 2016, S. 3)

4.5.3 Monitoring und Servicemanagement

Die Überwachung der Netzwerkhardware ist essentiell für die Erkennung möglicher Performanceprobleme oder Defekte. Derzeit überwacht ein MRTG-Monitoring (Multi Router Traffic Grapher) System mittels ICMP-Ping (Internet Control Message Protocol) und per SNMP (Simple Network Management Protocol) die Access-Points. (Greiner, 2016, S. 2)

4.5.4 Self-Service Funktionalitäten

Nach Abklärung der technischen Spezifikationen bedarf es einer genaueren Analyse der derzeitigen Self-Service Funktionalitäten. Die Administration von Textdateien auf Kommandozeilenebene ist für nicht IT-versierte Personen keine Option und würde sicherheitstechnisch, aufgrund der erforderlichen Rechtevergabe, katastrophal sein. Derzeit übernehmen die Techniker der Citycom sowohl den technischen Betrieb, als auch die textuelle und visuelle Ausrichtung der Captive Portal Seite. Es bedarf einer transparenten Lösung zur Auslagerung bestimmter Tätigkeiten an Dritte. Beispielsweise könnten HTML-Templates für Werbeagenturen bereitgestellt oder Redirect-Systeme mittels eines DNS-Portals realisiert werden. Dies gilt aber jedenfalls pro Standort. Ziel ist die kompakte und einfache Administration des gesamten Systems. (Greiner, 2016, S. 3)

5 MODELL EINES URBANEN WLAN-NETZWERKS

Das nachfolgende Modell kombiniert die Informationen der vorherigen Kapitel und vereint diese in einem generell anwendbaren, technischen Implementierungskonzept. Zu Beginn wird der Aufbau der Serverinfrastruktur inklusive empfohlener Software beschrieben. Das Darstellungskonzept kann ohne signifikante Adaptierungen in jeder Provider-Umgebung installiert werden. Die technische Implementierung eines Captive Portal- und Analysesystems bildet den Kernbestandteil einer WLAN-Umgebung, weshalb hier genauere Vorgehensweisen und Best-Practice-Ansätze verdeutlicht werden. Das Sicherheits- und Servicemanagement setzt sich mit der Überwachung einer WLAN-Infrastruktur auseinander. Hierbei wird eine Sammlung verschiedener Indikatoren zur Serverüberwachung geprüft. Dies impliziert sowohl das Content-Filtering, als auch die Aufzeichnung von Bandbreiten-Metriken im Netzwerk. Abschließend erfolgt die Validierung des Modells mit Hilfe des Value Proposition Canvas und drei repräsentativer Personas. Mithilfe dieses Konzepts erhalten Städte weltweit ein strukturiertes Vorgehensmodell und sparen sich somit aufwendige und daher auch kostenintensive Konzeptionsschritte. Dadurch, dass ausschließlich Open Source Software eingesetzt wird, gewinnt das Modell zusätzlich an Mehrwert.

5.1 Aufbau und Infrastrukturkomponente

Eine leistungsstarke Providerinfrastruktur bildet das Rückgrat eines robusten WLAN-Systems und gilt daher als Voraussetzung für den Betrieb eines urbanen und kabellosen Netzwerks. Der Fokus dieses Kapitels liegt auf der Konzeptionierung einer WLAN-Lösung im Serverinfrastrukturbereich unter Verwendung eines bereits existierenden und produktiven Providerbackbones. Aufgrund der identifizierten Anforderungen in *Kapitel 4* werden alle Servicekomponenten auf virtualisierter Umgebung installiert. Die Virtualisierungs-Plattform hängt von der Präferenz des jeweiligen Serviceproviders ab. Prinzipiell sollten proprietäre Lösungen, wie VMware¹³, Microsoft Hyper-V¹⁴ oder XenServer¹⁵ verwendet werden, um eine robuste Plattform sicherzustellen. Allerdings können die Servicebestandteile auch über Open Source Virtualisierungs-Technologien, wie KVM (Kernel-based Virtual Machine) bereitgestellt werden. Darüber hinaus bildet die Konfiguration von Speicher- und Netzwerkredundanzen aus Rechenzentrumssicht einen obligatorischen Servicefaktor, der vorab zu gewährleisten ist.

¹³ <http://www.vmware.com/de.html> (abgerufen am 01. November.2016)

¹⁴ <https://www.microsoft.com/de-de/server-cloud/solutions/virtualization.aspx> (abgerufen am 01. November 2016)

¹⁵ <http://xenserver.org/> (abgerufen am 01. November 2016)

5.1.1 Softwarelösungen zur Servicekonzipierung

Als zentrale Steuereinheit dient das auf FreeBSD basierende Open Source Betriebssystem pfSense¹⁶. Diese Software ist eine virtualisierbare Firewall und verfügt zusätzlich über alle obligatorischen Funktionalitäten zum Betrieb eines Netzwerks, wie beispielsweise einem DHCP-Server, einem DNS-Server, einem Proxy-Server, einem DNS-Forwarder und auch Mechanismen zur Bandbreitenanalyse pro Interface. Die Software zeichnet sich zudem durch Captive Portal-Funktionalitäten, umfangreiche Zusatzpakete und durchdachte Skalierbarkeit aus. (Greiner, 2016) verweist zudem auf die graphische Administrierbarkeit des Systems und stellt dies als essentielles Feature dar. Jeder WLAN-Standort verfügt über zwei dedizierte VLANs, wobei ein VLAN als standortübergreifendes Management-VLAN dient und das zweite VLAN standortbezogen einzigartig bleibt. Es wird jedem Standort ein eigenes, privates IP-Subnetz zugeteilt.

(Bernaschi, et al., 2011, S. 1288) erwähnt ebenso die Verwendung von pfSense als Steuerungssystem für das „*Provincia di Roma WiFi network*“, das kabellose Netzwerk der Provinz Rom. Zum Betrieb der virtualisierten Firewall wird eine GNU/Linux Distribution mit KVM als Hypervisor eingesetzt.

Weitere Bestandteile eines kabellosen Netzwerks sind Server, die statische Inhalte für die Darstellung der Captive Portal-Seite ausliefern und als Analysewerkzeug für WLAN-Teilnehmer fungieren, aber auch dedizierte Maschinen zur Verwaltung von WLAN-Access Points und Server zur Statusüberwachung der kompletten Dienstleistungssysteme mittels SNMP und Uptime-Ping. Auch hier ist es wichtig, dass alle Komponenten vollständig virtualisierbar und konsolidiert in einem Rechenzentrum lauffähig sind. Als Betriebssystem für diese Dienstleistungsserver soll aus Sicherheitsgründen Debian GNU/Linux in der aktuell vorliegenden Version 8.6 (Codename Jessie) verwendet werden. Ebenso ist auch die Installation anderer Linux Distributionen wie Ubuntu, Fedora, CentOS oder Red Hat Enterprise Linux, in der jeweils aktuellsten Version, möglich.

5.1.2 Darstellung der Architektur

Basierend auf den Untersuchungsergebnissen der vorherigen Kapitel zeigt *Abbildung 19* einen Best-Practice-Architekturvorschlag für urbane WLAN-Systeme. Das gesamte WLAN-Konstrukt ist vollständig virtualisiert aufgebaut. Die virtuellen Maschinen sind Hypervisor-intern über einen virtuellen Switch verbunden, welcher VLAN-Tags zur Netzwerkseparierung verwendet. Die pfSense, als zentrales Steuerungsinstrument, verwaltet das komplette Netzwerk und führt den Datenverkehr der Teilnehmer über ein Uplink-Interface ins Internet ab. Neben dem Uplink-Interface verfügt die Firewall über einen VLAN-Trunk Port, auf welchem einerseits die standort-spezifischen VLANs aufgeschaltet werden, andererseits auch das netzwerkübergreifende, einheitliche Management-VLAN.

¹⁶ <https://pfsense.org/> (abgerufen am 01. November 2016)

Alle Dienstleistungsserver sind über das Management-VLAN der Firewall an das Internet angebunden. Entsprechende Firewall-Regeln erlauben nur servicerelevante Operationen der WLAN-User auf den Dienstleistungsservern. Der Content Share verfügt zudem über eine separate öffentliche IP-Adresse, um Dritte die Möglichkeit einzuräumen Bilder und andere Inhalte, aus Zwecken des Captive Portal-Designs, hochzuladen. An den jeweiligen Standorten stehen Provider-CPEs (Customer Premises Equipment), die die notwendigen VLANs tagged nach dem Standard IEEE 802.1Q an einen Switch oder direkt an die Access Points übergeben.

Sollten WLAN-Standorte nicht durch das providereigene Netzwerk physikalisch erreichbar sein, kann vor Ort ein VPN-Concentrator installiert werden, welcher über das Internet einen sicheren Tunnel zur pfSense und somit zum WLAN-Netzwerk aufbaut. Darüber hinaus würden auch Richtfunkstrecken den Servicebedarf in nicht ausreichend erschlossenen Gebieten abdecken. In diesen beiden Fällen bedarf es einer detaillierten Evaluierung, um die Netzwerke performant und sicher zu verbinden.

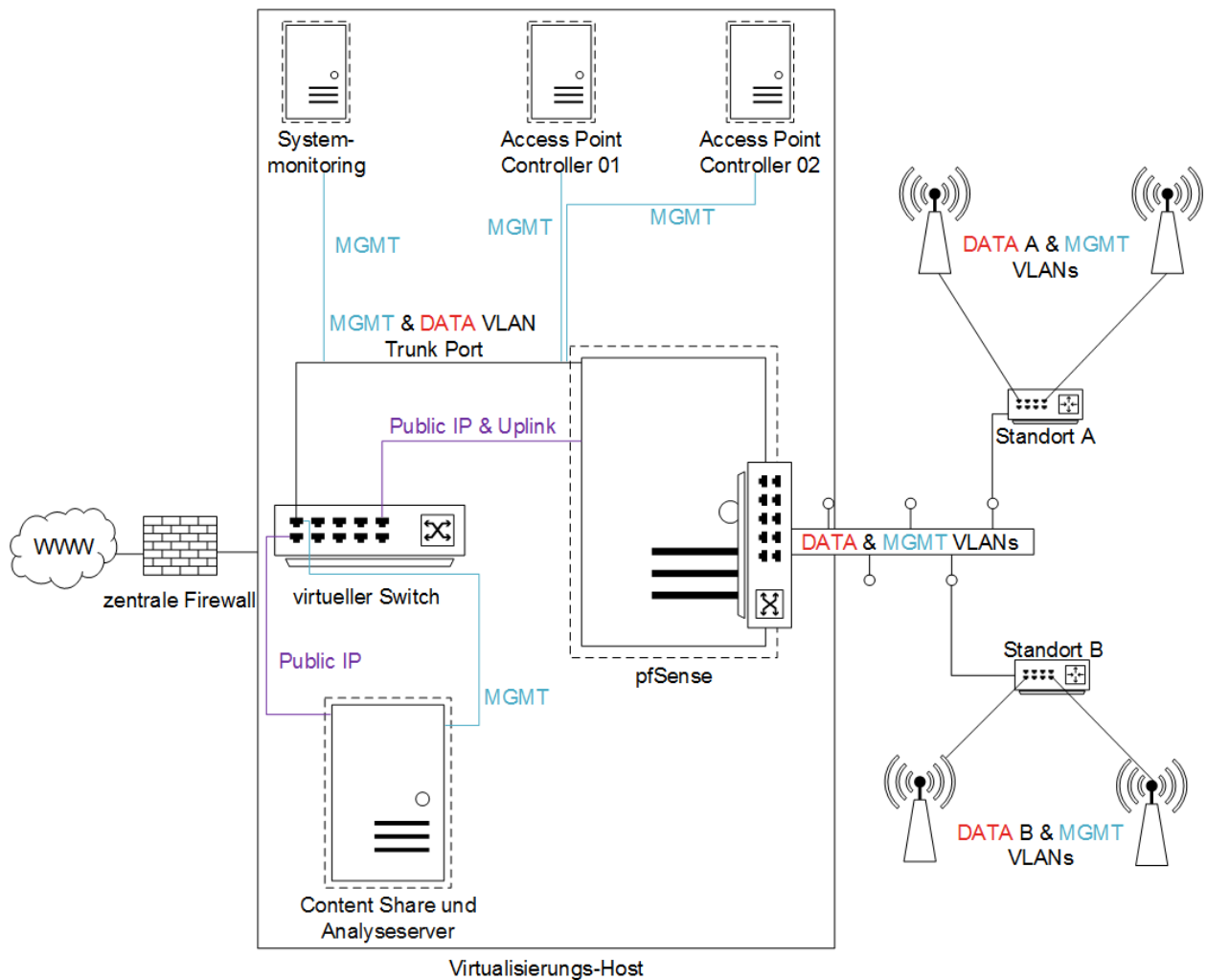


Abbildung 19 WLAN-Architektur
Quelle: vom Autor erstellt

5.2 Technische Implementierung eines Captive Portal- und Analysesystems

Nachdem die Infrastrukturkomponenten installiert wurden und die Basiskonfiguration der Server abgeschlossen ist, erfolgt die technische Implementierung des Captive Portal- und Analysesystems. Zu Beginn dieses Kapitels zeigt ein graphischer Konfigurationsprozess, welche Schritte zu erledigen sind, sodass das WLAN-System produktiv funktioniert. Die Schwierigkeit besteht darin die WLAN-Teilnehmer pro Standort zu analysieren und zugleich größtmögliche Bedienungsflexibilität und Sicherheit anzubieten. Ein modernes WLAN-System muss die Auslagerung von organisatorischen Tätigkeiten an Dritte erlauben, ohne dabei Zugriff auf sensible Systeme freizugeben, weshalb Self-Service Funktionalitäten erfolgskritisch für eine WLAN-Umgebung sind. Vor allem in einer urbanen Umgebung mit vielen Stakeholdern müssen klare Zugangsmechanismen zu Verwaltungsressourcen geschaffen werden.

5.2.1 WLAN-System Konfigurationsprozess

Abbildung 20 illustriert den Konfigurationsablauf eines neuen WLAN-Standortes. Zu diesem Zeitpunkt wird angenommen, dass alle bauspezifischen und netzwerktechnischen Vorkonfigurationen, die in einem Providernetzwerk zu erledigen sind, abgeschlossen wurden und dass das Management-VLAN bereits am neuen Standort aktiv ist. Ein wichtiger Punkt ist die Unterscheidung zwischen Firewall-Regeln und Captive Portal-Regeln. Nicht authentifizierte User können auf keine Ressourcen im Netzwerk zugreifen, ganz gleich ob Internet-Inhalte oder netzwerkinterne Dienste, wie den Dienstleistungssever. Das führt dazu, dass die Captive Portal-Seite nicht ordnungsgemäß dargestellt werden kann, da die pfSense aus Skalierungs- und Performancegründen nur ein HTML-Grundgerüst ausliefert und die Webseite erst am Client-Gerät aufgebaut wird. Deshalb ist die Konfiguration eines Walled Garden erforderlich. Ein Walled Garden definiert einen eingezäunten Bereich, in dem sich nicht authentifizierte WLAN-Teilnehmer bewegen können. Als grundlegende Voraussetzung muss jedoch der Netzwerkzugriff bereits auf IP-Ebene erlaubt sein, weshalb hierfür entsprechende Firewall-Regeln zu definieren sind. Sind beide Regeln korrekt konfiguriert und wurde eine Piwik-Analyseseite erstellt und eingerichtet, wird die WLAN-Teilnehmeranalyse vom System vorgenommen und dynamischer Inhalt für das Rendern der Captive Portal-Seite ausgeliefert. Der genaue Ablauf des Analyseprozesses wird im nachfolgenden Teilkapitel ausführlicher erläutert.

Abschließend müssen die Access Points am WLAN-Standort konfiguriert werden. Dies impliziert die Definition einer einheitlichen SSID, der Kanalnutzung, der rechtskonformen Sendestärke und die Konfiguration des einzigartigen Standort-VLANs, um den Datenverkehr schlussendlich abzuführen. Hier zeigen sich die Vorzüge eines zentralen WLAN-Controllers, da nicht jeder Access Point einzeln konfiguriert wird, sondern Access Points in Gruppen zusammengefasst und administriert werden.

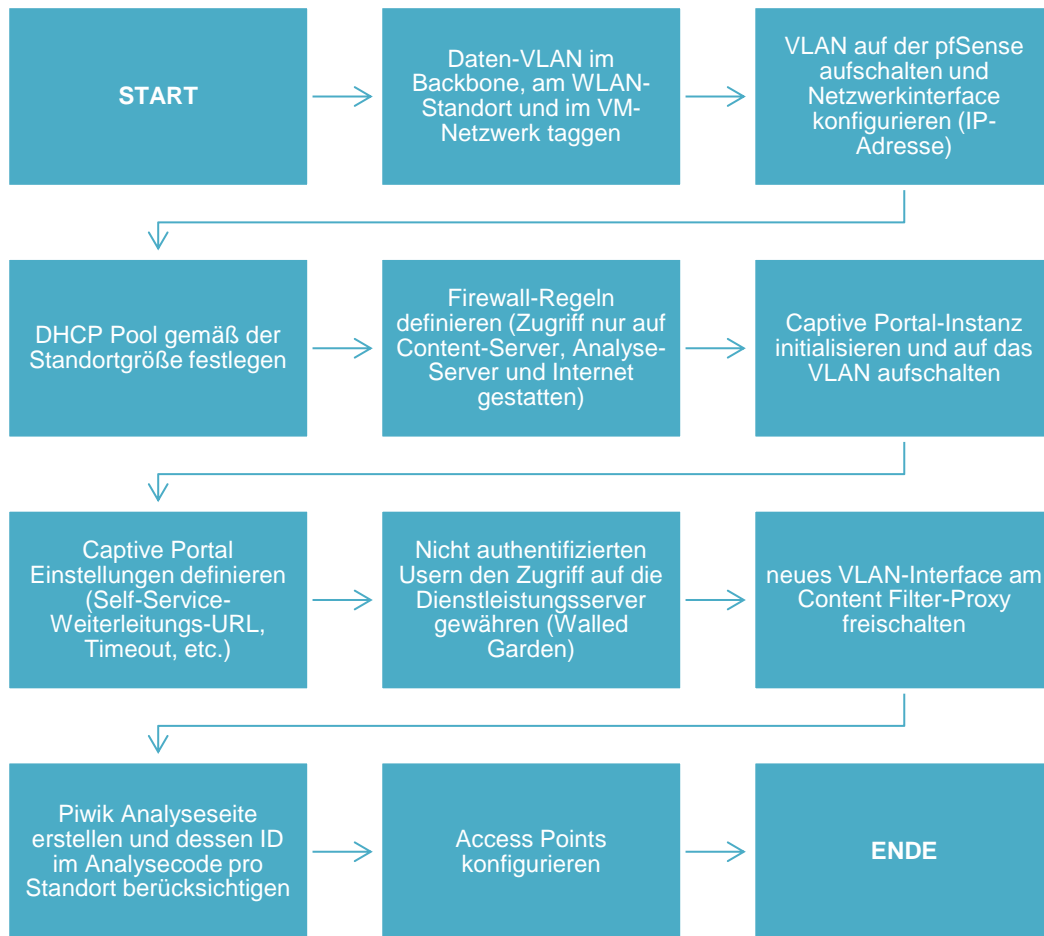


Abbildung 20 Technischer Konfigurationsablauf eines WLAN-Standorts
Quelle: vom Autor erstellt

5.2.2 Das WLAN-Analysesystem

Die Herausforderung bei der Gestaltung des WLAN-Analysesystems liegt in der granularen Analysierbarkeit der einzelnen Standorte, ohne dabei doppelten Analysecode für jeden Standort abzuspeichern. Gemäß den identifizierten Anforderungen an ein städtisches WLAN-System wird der JavaScript-Analysecode der selbst gehosteten Piwik Plattform verwendet. WLAN-Teilnehmer bekommen von der pfSense das HTML-Grundgerüst der Captive Portal-Seite übermittelt, welches unter anderem auch auf eine PHP-Datei (PHP: Hypertext Preprocessor) am Content Share-Server referenziert. Diese PHP-Datei generiert für jeden User den standortspezifischen Analysecode. Dies hat den Vorteil, dass IT-Administratoren nur eine Datei zu warten haben, wenn beispielsweise ein neuer Standort zu erstellen ist. User haben keinen Zugriff auf die gesamte Standortliste, da die PHP-Anfrage nur einen allgemein verfügbaren Programmcode zurückgibt und die Liste der Standorte somit verbirgt. Das Beispiel für einen solchen Ablauf ist im *Anhang A* beigefügt. *Abbildung 21* zeigt, dass Daten von allen Standorten gesammelt und von einem zentralen System verarbeitet werden. In weiterer Folge sind somit granulare Nutzungsberichte pro Standort verfügbar.



Abbildung 21 Standort-spezifische WLAN-Nutzungsanalyse
Quelle: vom Autor erstellt

5.2.3 Self-Service Funktionalitäten

Betreiber eines urbanen WLAN-Systems müssen bestimmte Self-Service Funktionalitäten für Angehörige und Interessensträger der Stadt und der Politik bereitstellen, damit der Mehrwert des Dienstes in Form von Besucherzahlen messbar wird. Daher sind Mechanismen zur Steuerung und Analyse des Systems ein integraler Bestandteil für das Modell.

Nachdem der WLAN-Teilnehmer die AGBs bestätigt hat, wird dieser auf eine Werbe- bzw. Informationsseite weitergeleitet. Diese Seite muss jedenfalls durch Dritte über eine sichere und leicht zu bedienende Schnittstelle austauschbar sein. Um dies zu realisieren, kann von IT-Administratoren eine entsprechende Domäne registriert werden (z.B. stadtwlanredirect.at). Pro Standort wird am Captive Portal eine URL zur Weiterleitung hinterlegt (z.B. vlan1234.stadtwlanredirect.at). Nicht IT-affine Personen können über das graphische DNS-Portal der gekauften Domäne schnell und einfach einen HTTP-redirect einrichten und so den WLAN-Teilnehmer dynamisch auf eine neue Webseite verweisen ohne hierbei Zugriff auf die Captive Portal-Administration zu haben. Technisch wird beim DNS HTTP-redirect ein virtueller Host auf einem Webserver erzeugt, welcher die Weiterleitung, zur vorab definierten Webseite, am Gerät des WLAN-Users anstößt.

Das Analysewerkzeug Piwik verfügt über ein mehrstufiges Berechtigungsschema, welches die Rechtevergabe pro Analyst und Standort realisiert. Diese Funktionalität ist von enormer Bedeutung für Stakeholder und ermöglicht eine genaue Analyse der WLAN-Auslastung pro Standort. Darauf aufbauend könnten in weiterer Folge städtische Marketingmaßnahmen geplant werden. (Droneberger, 2016, S. 2) und (Hardt-Stremayr, 2016, S. 3) bezeichnen WLAN-Analysedaten als einen obligatorischen Faktor eines öffentlichen WLAN-Netzwerks und heben die Bedeutung für ihren Tätigkeitsbereich hervor.

5.3 Überwachung der Dienstleistung

Ein städtisches WLAN-System wird von einer Vielzahl unterschiedlichster Personen genutzt, weshalb die Überwachung der Dienstleistung ein wichtiger Bestandteil der Modellentwicklung ist. Einerseits müssen Zugriffsbeschränkungen auf das Management-Netzwerk sichergestellt werden und andererseits ist gerade in einem öffentlichem WLAN Content-Filtering besonders wichtig. Aufgrund der scheinbaren Anonymität der WLAN-Teilnehmer sinkt womöglich die Hemmschwelle illegale Aktivitäten im Netzwerk vorzunehmen. Im Zuge von präventiven Maßnahmen muss auch Kinder und Jugendliche der Zugang zu ungeeigneten Materialien und Informationen verwehrt werden.

Eine weitere Herausforderung ergibt sich aus der Überwachung der Dienstleistung hinsichtlich von Netzwerk- und Serverauslastungen. Um Engpässe schnell zu erkennen und entsprechend reagieren zu können, bedarf es intelligenter Monitoring-Systeme.

5.3.1 Sicherheitsmanagement

Netzwerkzugriffsbeschränkungen sind für die Sicherheit des Systems von oberster Bedeutung. WLAN-Teilnehmer sollen nur in die für sie vorgesehenen System-Areale Zugriff erhalten. Dabei muss die Ressource nicht nur durch rudimentäre „hat Zugriff“ oder „hat keinen Zugriff“ Entscheidungen geschützt werden. User des WLANs dürfen nur bestimmte Verbindungen zu den Dienstleistungsservern, speziell zum Content Share und Analyseserver, herstellen. *Abbildung 22* stellt eine mögliche Regelabfolge dar. Firewall-Regeln werden stets von oben nach unten betrachtet. WLAN-Teilnehmer dürfen auf das Netzwerkinterface der pfSense zugreifen, damit der darauf gebundene Webserver das HTML-Grundgerüst übermitteln kann. WLAN-User dürfen auf den Content Share und Analyseserver zugreifen, der Zugang zum Management-Netzwerk wird jedoch verwehrt. Zum Schluss dürfen und müssen die WLAN-Teilnehmer Informationen aus dem Internet abrufen können.





	States	Protocol	Source	Port	Destination
<input type="checkbox"/> 	321/14.96 MiB	IPv4 TCP/UDP	*	*	ITGSTANDORTE address
<input type="checkbox"/> 	76/881.83 MiB	IPv4 TCP/UDP	*	*	10.56.0.2
<input type="checkbox"/> 	0/92 KiB	IPv4 *	*	*	APMANAGEMENT net
<input type="checkbox"/> 	1/93.38 GiB	IPv4 *	*	*	*

Abbildung 22 Sicherheitsmanagement durch Firewall-Regeln

Quelle: vom Autor erstellt

(Nicoletti, 2013, S. e120) illustriert den Prozess zur Überprüfung und Fehlerbehandlung von Content-Filtering auf sehr detaillierter Ebene, schafft jedoch auch zugleich eine breite Betrachtung der Thematik. *Abbildung 23* zeigt diese Ablaufstruktur und verweist auf mögliche Maßnahmen zur Identifikation und Lösung von Problemen.

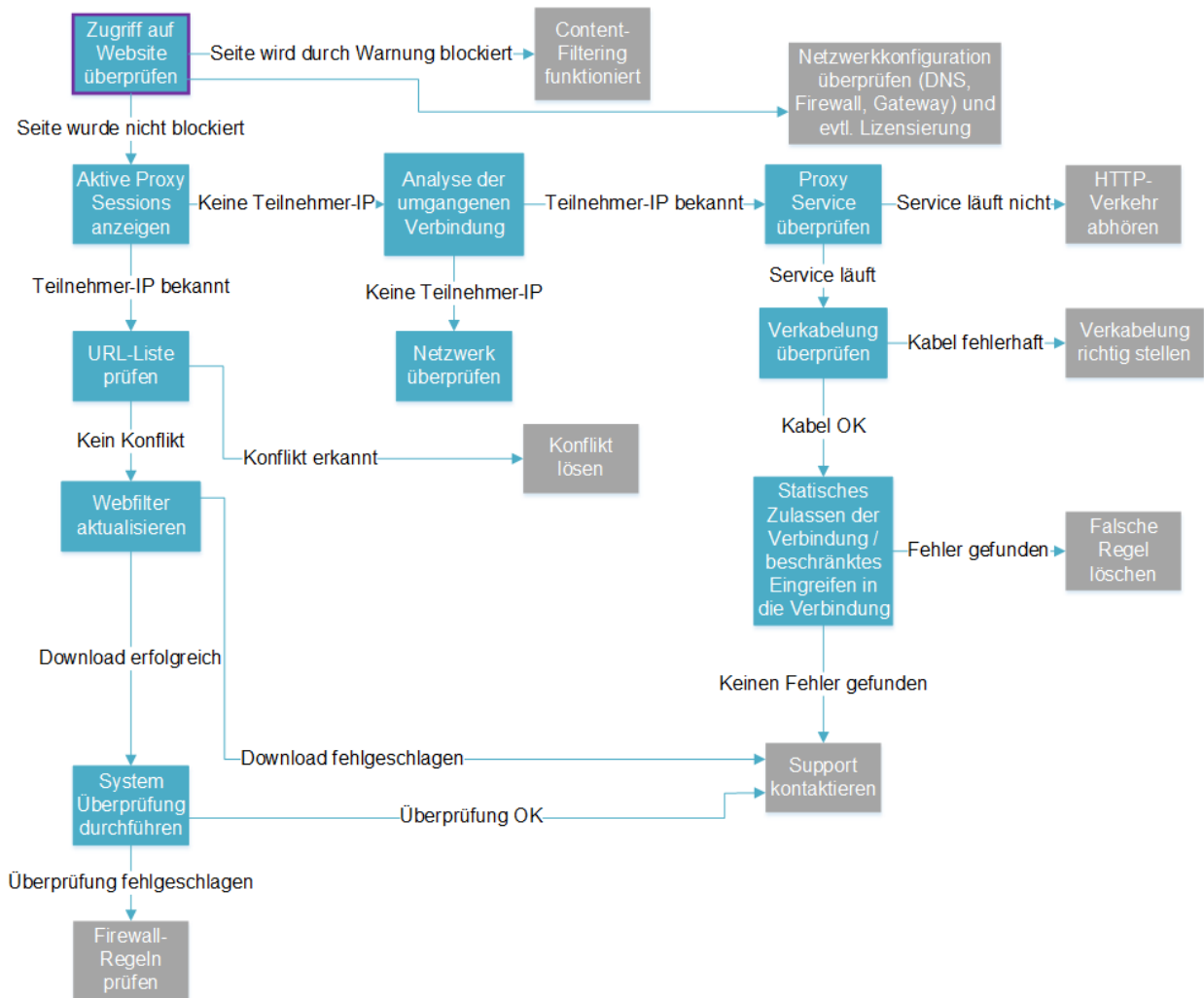


Abbildung 23 Sicherheitsmanagement durch Content-Filtering
 Quelle: eigene Darstellung nach (Nicoletti, 2013, S. e120)

5.3.2 Dienstleistungsüberwachung

Die Überwachung des Netzwerks ist obligatorisch, da sich potentielle Ressourcenengpässe störend auf den WLAN-User Auswirkungen können. Mögliche Engpässe sind beispielsweise Bandbreitenauslastungen oder zu klein dimensionierte Dienstleistungsserver. Die Erkennung solcher Probleme kann mittels SNMP-Abfragen erfolgen. Hierzu sammelt ein zentrales Überwachungssystem Informationen aller im Management-Netzwerk lokalisierten SNMP-fähigen Server und stellt diese graphisch dar. Access Points werden typischerweise durch einen WLAN-Controller überwacht. Sollte dies aus produkttechnischer Sicht nicht möglich sein, weil es keine zentrale Steuerung gibt, so kann ebenso SNMP verwendet werden. Durch den Einsatz von Monitoring-Software, wie beispielsweise CactiEZ¹⁷, werden Netzwerkausfälle klar ersichtlich. *Abbildung 24* stellt ein Netzwerkdiagramm zur Überwachung der Internetleitung dar.

¹⁷ <http://cactiez.cactiusers.org/> (abgerufen am 15. November 2016)

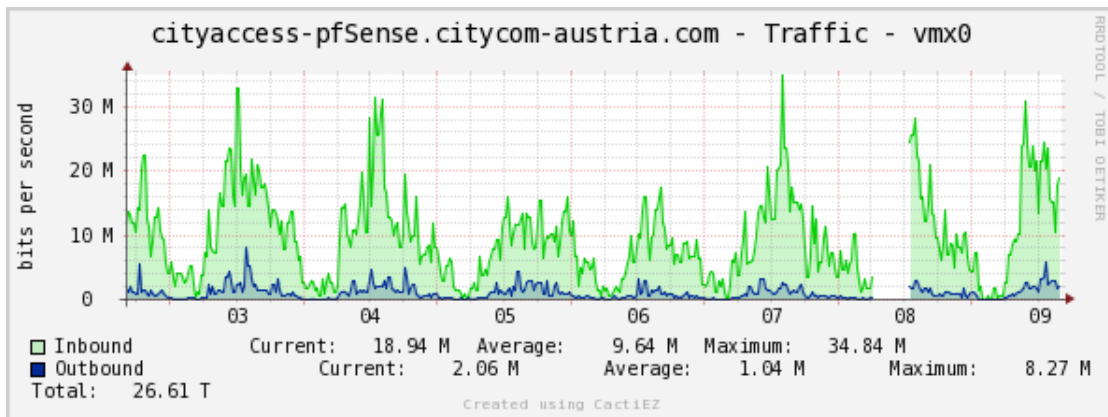


Abbildung 24 Erkannter Netzwerkausfall
Quelle: vom Autor erstellt

Die Open Source Firewall pfSense bietet zudem weitreichende Monitoring-Fähigkeiten zur effizienten Erkennung von Performance-Problemen in Echtzeit. In *Abbildung 25* ist die Netzwerkauslastungshistorie des Uplink-Interfaces dargestellt. Hier sieht man detailliert zu welchem Zeitpunkt wie viel Daten in Mbit/s übertragen wurden.

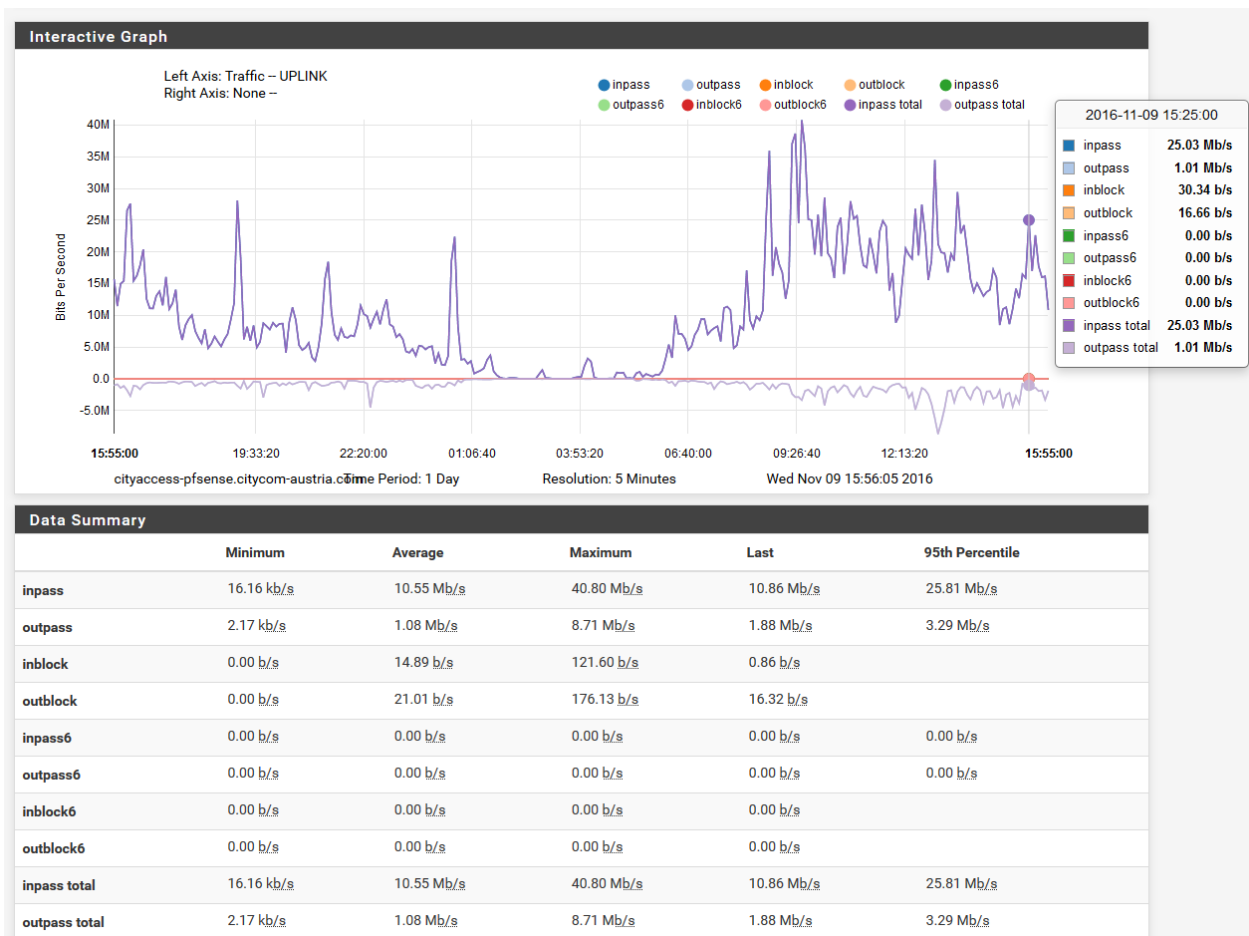


Abbildung 25 pfSense Netzwerkauslastung
Quelle: vom Autor erstellt

(Rech, 2012, S. 548) identifiziert Schwierigkeiten, die häufig im Zusammenhang mit kabellosen Verbindungen auftreten, denn ausgelastete Netzwerk-Interfaces sind nicht die einzigen potenziellen Störquellen. Roaming- und Sicherheitsprobleme, Funklöcher, überbuchte Frequenzbänder, Interoperabilität und Übertragungsfehler sind weitere erkennbare Herausforderungen. Durch die Analyse der übertragenen Frames und deren Inhalte erfolgt eine Identifikation dieser Probleme. (Rech, 2012, S. 549) beschreibt dieses Vorgehen als „Protokollanalyse“.

5.4 Resultat

Ziel ist die Illustrierung der Anforderungen und Lösungen zur Umsetzung eines urbanen WLAN-Netzwerks aus Betreibersicht. Zudem wird der Nutzen des eben konzipierten Netzwerks anhand des Value Proposition Canvas auf Basis von Personas verdeutlicht. Die Personas repräsentieren sowohl WLAN-Teilnehmer diverser Standorte, aber auch Stakeholder des Netzwerks wie beispielsweise Entscheidungsträger und IT-Techniker.

5.4.1 Graphische Modelldarstellung

Abbildung 26 zeigt den alternierenden Fluss, welcher die drei Bestandteile des Modells darstellt. Dieser beschreibt die drei wesentlichen Punkte zur technischen Erstellung eines urbanen WLAN-Netzwerks. Das Modell kann sowohl zur Neueinführung einer WLAN-Infrastruktur herangezogen werden, aber auch als Kontrollwerkzeug bestehender Dienstleistungen dienen.

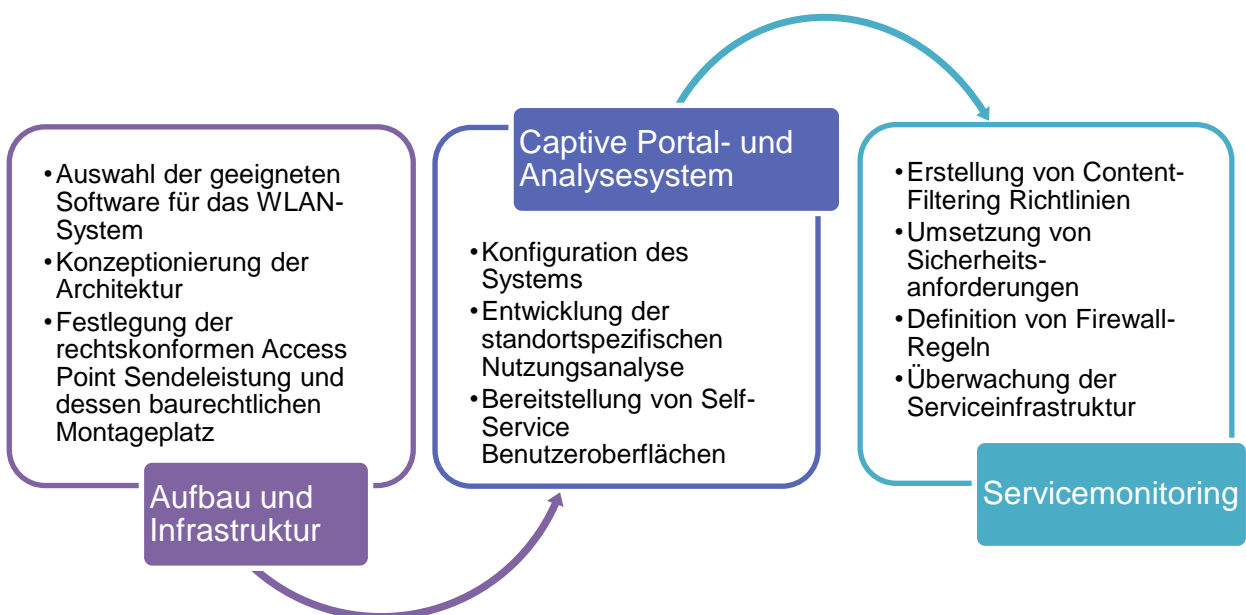


Abbildung 26 Modell eines urbanen WLAN-Netzwerks

Quelle: vom Autor erstellt

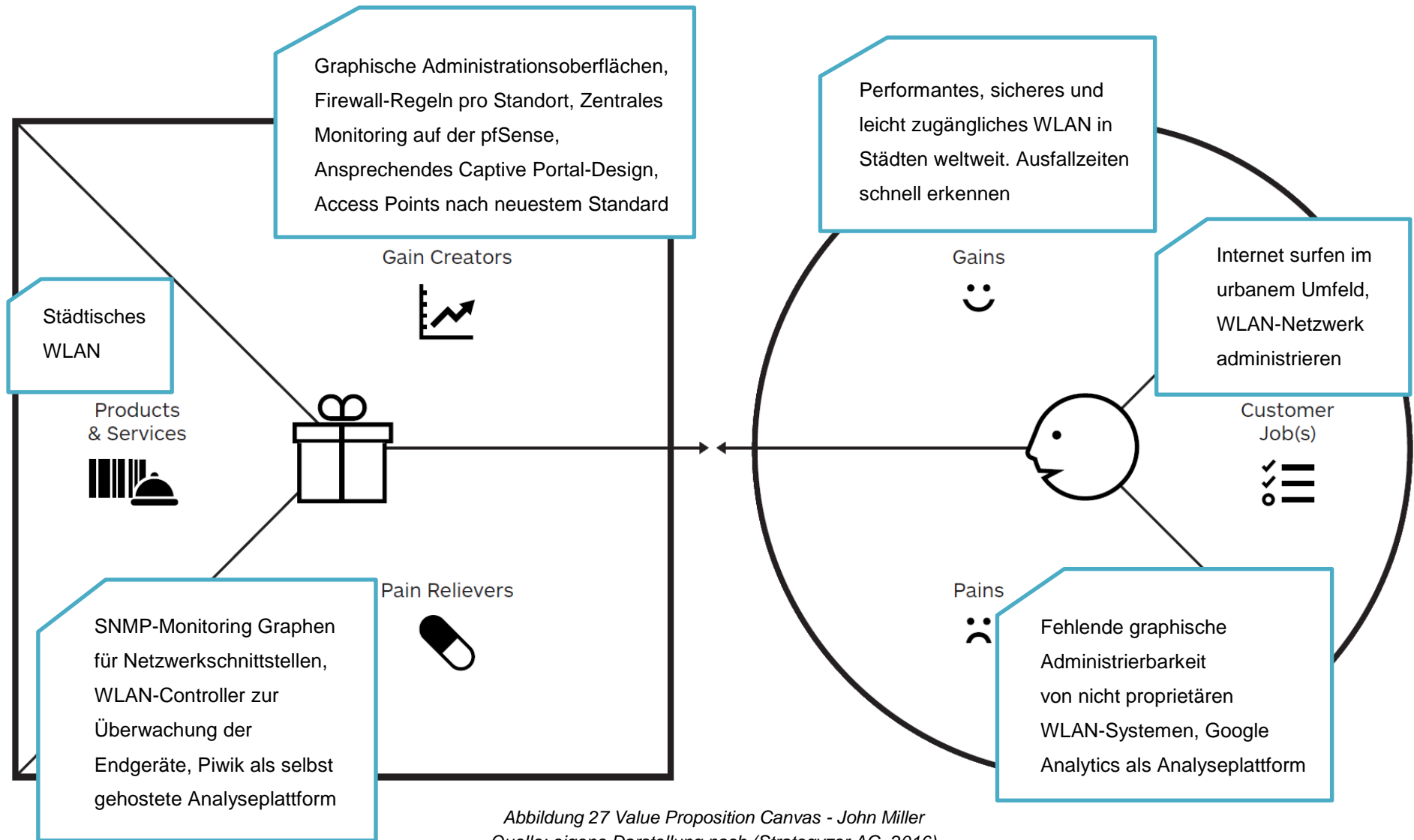
5.4.2 Modellvalidierung

Folgende Personas dienen als Grundlage für die Modellvalidierung durch den Value Proposition Canvas von Alexander Osterwalder¹⁸:

- John Miller (IT-Administrator)
- Andrea Brown (Entscheidungsträgerin)
- Sarah Baker (WLAN-Nutzerin)

Im *Anhang B* befinden sich detaillierte Personenbeschreibungen. Das Modell wird aus mehreren Blickwinkeln und unter Anbetracht verschiedener Expertisen und Erwartungen bewertet. Die Abbildungen 27, 28 und 29 illustrieren den Aufbau des Value Proposition Canvas, der für die drei beschriebenen Personas einzeln durchlaufen wird.

¹⁸ <http://alexosterwalder.com/> (abgerufen am 21. November 2016)



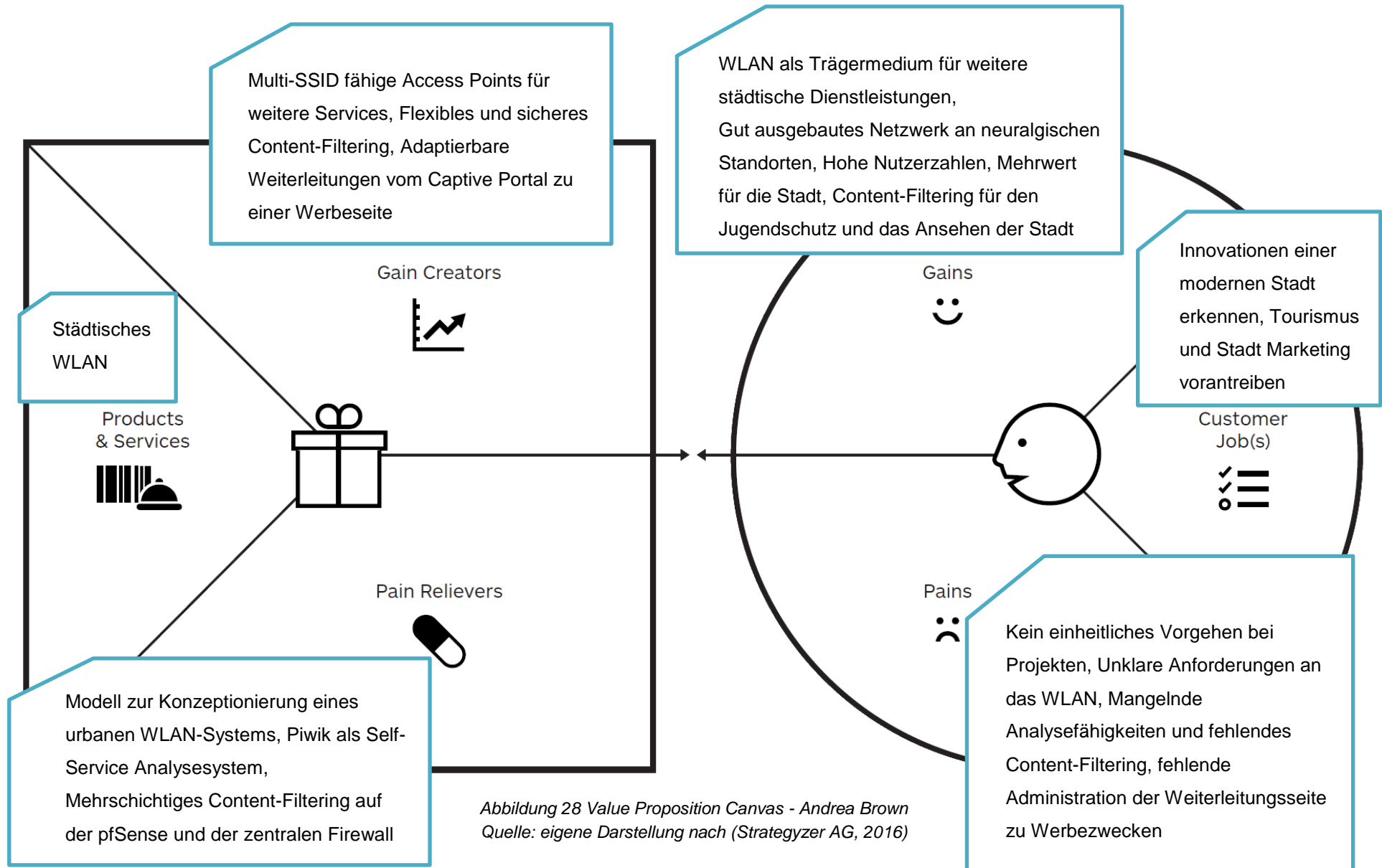


Abbildung 28 Value Proposition Canvas - Andrea Brown
 Quelle: eigene Darstellung nach (Strategyzer AG, 2016)

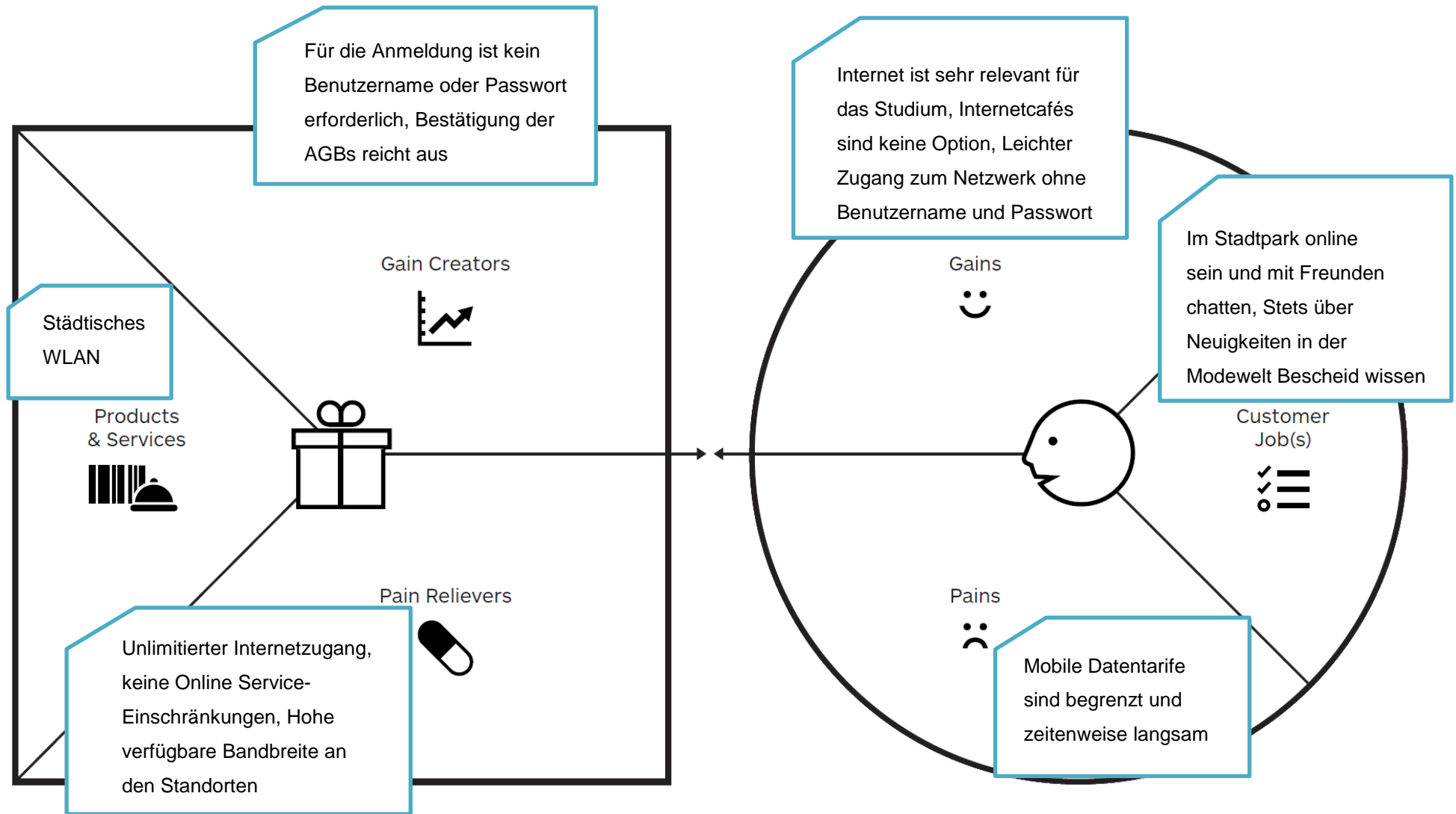


Abbildung 29 Value Proposition Canvas - Sarah Baker
 Quelle: eigene Darstellung nach (Strategyzer AG, 2016)

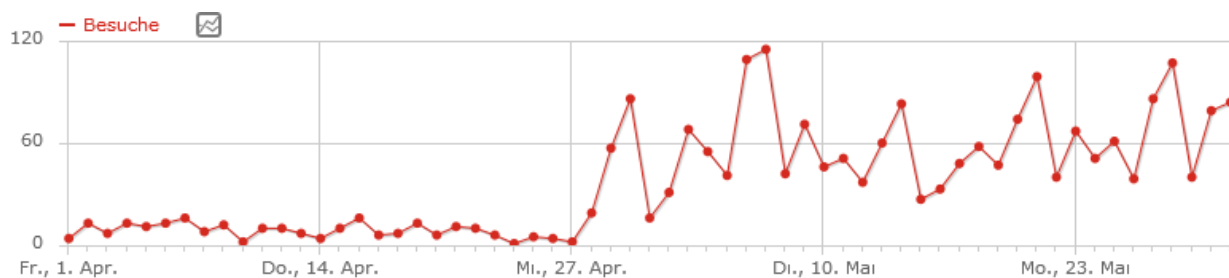
6 AUSBLICK UND FAZIT

Zusammenfassend ist festzustellen, dass erfolgreiches Anbieten von kabellosem Internet durchdachte Richtlinien und technische Voraussetzungen impliziert. Es muss klar sein, dass WLAN Luft als geteiltes Trägermedium verwendet, was zu Qualitätsschwankungen bei der Übertragung führen kann. Diese Arbeit gibt einen Überblick über den WLAN-Standard IEEE 802.11 und dessen neuen Derivate. Zusätzlich werden auftretende Interferenzen in kabellosen Umgebungen behandelt. Speziell im urbanen Umfeld häufen sich potentielle Störquellen, die den Service maßgeblich beeinträchtigen. Ein weiterer wichtiger Punkt ist der energieeffiziente Betrieb von WLAN-Umgebungen. Die in der Forschungsarbeit dargelegten Aktivierungsstrategien von Hotspots führen zu einer Verringerung des Stromverbrauchs eines WLAN-Systems. Sicherheit in kabellosen Netzwerken ist äußerst wichtig, da Personengruppen nicht an eine stationäre Schnittstelle gebunden sind, sondern sich in einem Bereich frei bewegen können. Sicherheitsmaßnahmen zum autorisierten Zugriff auf kabellose Netzwerke sind besonders im unternehmerischen Umfeld von essentieller Bedeutung, sodass Firmendaten nicht durch Dritte einsehbar oder kompromittierbar sind. Öffentliches WLAN hingegen wird einer breiten Nutzerbasis zur Verfügung gestellt. Hierbei ist der einfache Zugang im Vordergrund, wonach alternative Schutzmechanismen anzuwenden sind. Gerade im städtischen Bereich müssen Content-Filter-Maßnahmen gesetzt werden, um Personen vor ungeeignetem Material zu schützen.

Weiterführend gelten gesetzliche Regulierungen hinsichtlich Bau, Betrieb, IT und Sicherheit in Bezug auf WLAN im öffentlichen Raum. Betreiberunternehmen müssen die Gesetze beachten, um straffrei operieren zu können. Mögliche Fallstricke sind hier die Auswahl des erlaubten Frequenzbandes in Kombination mit der zulässigen Sendeleistung von Access Points. Was die übertragenen Inhalte im Netzwerk betrifft, besteht in Österreich Handlungsbedarf. Es müssen klare Richtlinien zur Haftung eines WLAN-Betreibers dargelegt werden. Ordentlich reguliert hingegen ist die Nutzungsanalyse der Internetuser. Anbieter müssen hier besonders auf die Hinweispflicht, die sich aus der Verwendung von Cookies ergibt, achten.

Die Analyse des öffentlichen WLAN der steirischen Landeshauptstadt Graz verschafft dieser Arbeit einen essentiellen Mehrwert. Die genauere Betrachtung und der Ausbau eines etablierten Netzwerks zeigen potentielle Fallstricke für weitere, in WLAN interessierte, Städte. Besonders die Ausrichtung der Dienstleistung am Markt und die Zusammenarbeit mit dem lokalen Tourismusverband stellen die organisatorischen Weichen für einen erfolgreichen Service. Ebenso muss der Standorterhebungs- und Umsetzungsprozess den rechtlichen und organisatorischen Gegebenheiten entsprechen. Aus technischer Sicht ergeben sich gerade im urbanen Umfeld erweiterte Anforderungen an ein WLAN-System. Hierzu wurde ein Modell zur Konzeptionierung einer urbanen WLAN-Lösung entwickelt. Die Modellentwicklung erfolgte auf Basis der in der Arbeit identifizierten Anforderungen an das System.

Die Darstellung zeichnet sich durch technische Detaillierung und Einführung von Self-Service Funktionalitäten aus. Ebenso bleibt das System für den Endbenutzer leicht zugänglich, da weder Benutzername noch Passwort für die Anmeldung erforderlich sind. *Abbildung 30* zeigt den Erfolg des Modells anhand des WLAN-Standorts Lendplatz in Graz. Der nutzenoptimierte Betrieb der WLAN-Lösung ist in der Darstellung klar erkennbar.



*Abbildung 30 Nutzungsstatistik 01. April bis 31. Mai 2016 am Lendplatz in Graz
Quelle: vom Autor erstellt*

Die Gesamtauslastung vor dem 27. April 2016 bewegte sich im unteren einstelligen Bereich. Nachdem das Modell zur Konzeptionierung eines urbanen WLAN-Systems angewandt wurde, vervielfachten sich die Nutzerzahlen, ohne das marketingtechnische Zusatzleistungen erbracht wurden.

Auf rechtlicher Ebene bleibt die Klärung der Haftung des WLAN-Betreibers offen, da es hier in Österreich noch keine eindeutige Rechtsprechung diesbezüglich gibt. Zudem muss der Begriff WLAN im steirischen Baurecht verankert werden, um hier klare Rahmenbedingungen zu schaffen. Andere akademische Arbeiten können diese Thematik als Grundlage zur Erstellung weiterer Forschungsfragen heranziehen.


ANHANG A - Beispiel für den WLAN-Analysecode

Die Datei zur standortspezifischen Analyse von WLAN-Teilnehmern könnte wie folgt aussehen:

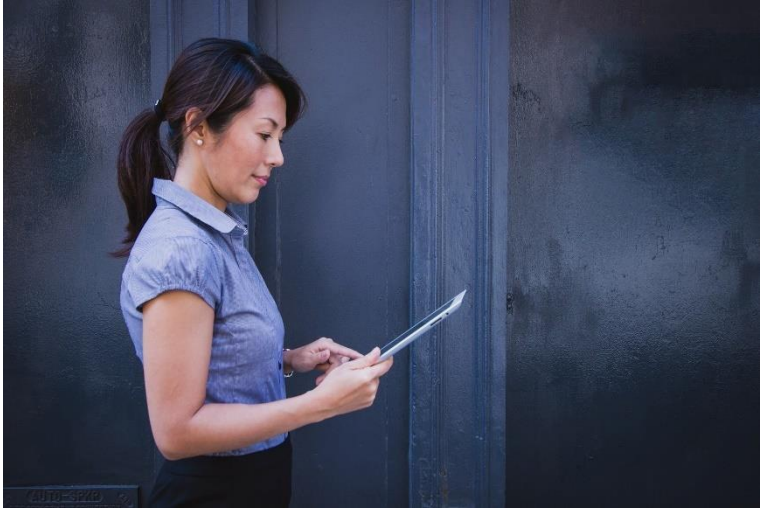
```
<?php
//Piwik ID Festlegung anhand des Standortnetzes
//Quelle: vom Autor selbst erstellt
$piwikHandler = getPiwikId();
function getPiwikId() {
    $net = array (
        '192.168.1.' => '2',          //Standort A
        '192.168.2.' => '3'          //Standort B
    );
    $clientIp = getenv('REMOTE_ADDR');
    foreach ($net as $netip => $page) {
        if (strstr($clientIp, $netip)) {
            $pageId = $page;
            break;
        }
    }
    if(!isset($pageId)){
        $pageId=1; //Fallback Seite im Fehlerfall
    }
    return $pageId;
}
?>

//Adaptierter, bereits bestehender Analysecode der Plattform Piwik
var _paq = _paq || [];
_paq.push(['trackPageView']);
_paq.push(['enableLinkTracking']);
(function() {
    var u="//piwikserver.domain.tld/piwik/";
    _paq.push(['setTrackerUrl', u+'piwik.php']);
    _paq.push(['setSiteId', <?php echo $piwikHandler; ?> ]);
    var d=document, g=d.createElement('script'),
s=d.getElementsByTagName('script')[0];
    g.type='text/javascript'; g.async=true; g.defer=true; g.src=u+'piwik.js';
s.parentNode.insertBefore(g,s);
})();
```


ANHANG B - Personas

<p>John Miller</p>	 <p>19</p>
<p>Soziodemographische Merkmale</p>	<p>Geschlecht: Männlich Alter: 31 Familienstand: ledig Beruf: IT-Administrator bei City-Verwaltung GmbH Hobbies: Laufen, Mountainbike fahren, Fotografieren, Reisen</p>
<p>Denken und fühlen</p>	<p>Freier und performanter Internetzugang, hohe Bandbreiten, Sicherheit</p>
<p>Sagen und machen</p>	<p>WLAN als Mehrwert für eine Stadt, identifiziert sich mit seiner Arbeit</p>
<p>Hören</p>	<p>Keine unlimitierten Mobilfunktarife, Foto-Upload langsam, teure Verbindungen im Ausland</p>
<p>Sehen</p>	<p>Menschen mit Smartphones an öffentlichen Plätzen, ausbaufähiges WLAN</p>
<p>Schmerzen und Ärgernisse</p>	<p>Fehlende graphische Administrierbarkeit von nicht proprietären WLAN-Systemen, Google Analytics als Analyseplattform</p>
<p>Wünsche und Erwartungen</p>	<p>Performantes, sicheres und leicht zugängliches WLAN in Städten weltweit. Ausfallzeiten schnell erkennen</p>

¹⁹ <http://freestocks.org/photo/people-tram-stop/> (abgerufen am 19. November 2016)

<p>Andrea Brown</p>	 <p>20</p>
<p>Soziodemographische Merkmale</p>	<p>Geschlecht: Weiblich Alter: 40 Familienstand: verheiratet Beruf: Vorstand bei City-Verwaltung GmbH Hobbies: Lesen, Reisen, Yoga</p>
<p>Denken und fühlen</p>	<p>Innovationen einer modernen Stadt erkennen, Tourismus und Stadt Marketing vorantreiben</p>
<p>Sagen und machen</p>	<p>WLAN als Trägermedium für weitere städtische Dienstleistungen, Internetsurfen an öffentlichen Plätzen</p>
<p>Hören</p>	<p>Viele Städte weltweit bieten öffentliches WLAN an, Mehrwert für Bürger und Touristen</p>
<p>Sehen</p>	<p>Aufwendige Bürokratie, hohe Projektumsetzungskosten, Fehlende Nutzungsauswertungen</p>
<p>Schmerzen und Ärgernisse</p>	<p>Kein einheitliches Vorgehen bei Projekten, Unklare Anforderungen an das WLAN, Mangelnde Analysefähigkeiten und fehlendes Content-Filtering, fehlende Administration der Weiterleitungsseite zu Werbezwecken</p>
<p>Wünsche und Erwartungen</p>	<p>Gut ausgebautes Netzwerk an neuralgischen Standorten, Hohe Nutzerzahlen, Mehrwert für die Stadt, Content-Filtering für den Jugendschutz und das Ansehen der Stadt</p>

²⁰ <https://pixabay.com/en/woman-person-business-professional-801872/> (abgerufen am 20. November 2016)

<p>Sarah Baker</p>	 <p style="text-align: right;">21</p>
<p>Soziodemographische Merkmale</p>	<p>Geschlecht: Weiblich Alter: 20 Familienstand: ledig Beruf: Studentin Hobbies: Chatten, Mode-Blog, Webdesign</p>
<p>Denken und fühlen</p>	<p>Im Stadtpark online sein und mit Freunden chatten, Stets über Neuigkeiten in der Modewelt Bescheid wissen</p>
<p>Sagen und machen</p>	<p>Leben verlagert sich zunehmend in die Onlinewelt, Videotelefonieren mit bekannten in Amerika</p>
<p>Hören</p>	<p>Städte bauen zunehmend öffentliches WLAN aus</p>
<p>Sehen</p>	<p>Internet ist sehr relevant für das Studium, Internetcafés sind keine Option</p>
<p>Schmerzen und Ärgernisse</p>	<p>Mobile Datentarife sind begrenzt und zeitenweise langsam</p>
<p>Wünsche und Erwartungen</p>	<p>Gut ausgebautes WLAN in Parkanlagen, Leichter Zugang zum Netzwerk ohne Benutzername und Passwort</p>

²¹ <https://static.pexels.com/photos/3566/woman-smartphone-girl-bus.jpg> (abgerufen am 20. November 2016)

ABKÜRZUNGSVERZEICHNIS

°C	Grad Celsius
ACI	Adjacent Channel Interference
ACK	Acknowledgment
AEG	Altstadterhaltungsgesetz
AGB	Allgemeine Geschäftsbedingungen
ANDSF	Network Discovery and Selection Function Server
AP	Access Point
ATS	App Transport Security
CACAO	Client-Assisted Channel Assignment Optimization
CAPWAP	Control and Provisioning of Wireless Access Points
CBIF	Content Based Image Filtering
CNAME	Canonical Name
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Carrier Sense
CSMA/CA	Carrier Sense Multiple Access Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access Collision Detection
CTS	Clear-to-Send
DFS	Dynamic Frequency Selection,
DIFS	Distributed Inter-Frame Spacing
DLP	Data Leakage Prevention
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECG	E-Commerce-Gesetz
EDUROAM	EDUcation ROAMing
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
ggü	gegenüber
GmbH	Gesellschaft mit beschränkter Haftung
GUI	Graphical User Interface
HEW	High efficient WLANs
HEW TG	high-efficiency WLAN Task Group

HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IASO	Interference-aware Self-optimizing
ICMP	Internet Control Message Protocol
ICNIRP	International Commission on Non-Ionizing Radiation Protection
ICT	Information and Communication Technology
ID	Identifikator
IDS	Intrusion-Detection-Systeme
IEEE	Institute of Electrical and Electronics Engineers
IFOM	IP Flow Mobility and Seamless Offload
IPS	Intrusion-Prevention-Systeme
iSd	im Sinne des
ISP	Internet Service Provider
kbit/s	Kilo Bit pro Sekunde
KVM	Kernel-based Virtual Machine
LCCS	Least Congested Channel Selection
LEAP	Lightweight Extensible Authentication Protocol
LWL	Lichtwellenleiter
MAC	Media Access Control
MGMT	Management
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MK	Master Key
MRTG	Multi Router Traffic Grapher
MSCHAP-V2	Microsoft Challenge Handshake Authentication-Protokoll Version 2
mW	Milliwatt
NGFW	Next-Generation Firewall
NREN PC	National Research and Educational Network Policy Committee
OSI	Open Systems Interconnection Model
PEAP	Protected Extensible Authentication Protocol
PFS	Perfect Forward Secrecy
PHP	PHP: Hypertext Preprocessor
PMK	Pairwise Master Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Code 4
RF	Radio Frequenz

RSA	Rivest, Shamir und Adleman
RSN	Robust Security Network
RSNA	Robust Security Network Association
RTS	Request-to-Send
SaaS	Software-as-a-Service
SAR	spezifische Absorptionsrate
SCENIHR	Scientific Committee on Emerging and Newly Identified Health Risks
SHA	Secure Hash Algorithm
SIFS	Short Inter-Frame Spacing
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
STA	Station (nach dem IEEE 802.11 Protokoll kompatibles Gerät)
TKG	Telekommunikationsgesetz
TKIP	Temporary Key Integrity Protocol
TPS	Transmit Power Control
UCI	Unified Command Interface
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTM	Unified Threat Management
VIP	Virtuelle IP-Adresse
VLAN	Virtual Local Area Network
VM	Virtuelle Maschine
W/kg	Watt pro Kilogramm
WEP	Wired Equivalent Privacy
WHO	World Health Organization
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTP	Wireless Termination Point

ABBILDUNGSVERZEICHNIS

Abbildung 1 Der in Österreich erzielte Umsatz mittels E-Paper pro Jahr (in Millionen Euro)	2
Abbildung 2 IEEE 802.11 CSMA/CA.....	8
Abbildung 3 Kollisionsvermeidung mittels RTS/CTS	9
Abbildung 4 Entlastung von LTE mittels WLAN	11
Abbildung 5 UniFi Enterprise Controller Dashboard	20
Abbildung 6 UniFi Enterprise Controller Nutzungsanalyse	21
Abbildung 7 UniFi Enterprise Controller WLAN Abdeckung	21
Abbildung 8 IEEE802.11i Authentifizierung.....	23
Abbildung 9 „eduroam“ RADIUS Authentifizierungsweg	24
Abbildung 10 Durchschnittliche Internetgeschwindigkeit in Österreich (in kbit/s)	32
Abbildung 11 WLAN in den 2,4 GHz-Spektren	35
Abbildung 12 WLAN in den 5 GHz-Spektren	35
Abbildung 13 Mobilfunk: Meinungen über den Effekt auf die Gesundheit	37
Abbildung 14 Verwendung von Cookies	40
Abbildung 15 Cookie-Steuerungspanel auf der Website der Firma Oracle	44
Abbildung 16 Öffentliches WLAN am Grazer Hasnerplatz.....	46
Abbildung 17 Öffentliches WLAN am Citybeach (Grazer Murbrücke)	54
Abbildung 18 Öffentliches WLAN am Grazer Jakominiplatz	55
Abbildung 19 WLAN-Architektur.....	61
Abbildung 20 Technischer Konfigurationsablauf eines WLAN-Standorts	63
Abbildung 21 Standortspezifische WLAN-Nutzungsanalyse.....	64
Abbildung 22 Sicherheitsmanagement durch Firewall-Regeln	65
Abbildung 23 Sicherheitsmanagement durch Content-Filtering.....	66
Abbildung 24 Erkannter Netzwerkausfall	67
Abbildung 25 pfSense Netzwerkauslastung.....	67
Abbildung 26 Modell eines urbanen WLAN-Netzwerks	68
Abbildung 27 Value Proposition Canvas - John Miller	70
Abbildung 28 Value Proposition Canvas - Andrea Brown.....	71
Abbildung 29 Value Proposition Canvas - Sarah Baker.....	72
Abbildung 30 Nutzungsstatistik 01. April bis 31. Mai 2016 am Lendplatz in Graz	74

TABELLENVERZEICHNIS

Tabelle 1 Von der Masse an Endgeräten unterstützte 802.11 Derivate	7
Tabelle 2 Ausblick kommender IEEE 802.11 Derivate	7
Tabelle 3 OpenCapwap Bestandteile.....	19
Tabelle 4 Arten von Cookies	41
Tabelle 5 Access Point-Spezifikationen	58

LITERATURVERZEICHNIS

- Akamai Technologies. (2016). *Durchschnittliche Verbindungsgeschwindigkeit der Internetanschlüsse in Österreich vom 3. Quartal 2007 bis zum 1. Quartal 2016 (in kbit/s)*. Abgerufen am 5. September 2016 von de.statista.com:
<http://de.statista.com/statistik/daten/studie/416669/umfrage/durchschnittliche-internetgeschwindigkeit-in-oesterreich/>
- ARGE DATEN - Österreichische Gesellschaft für Datenschutz (a). (kein Datum). *Wer trägt die Verantwortung für (öffentliche) WLAN Hotspots?* Abgerufen am 9. September 2016 von www.argedaten.at: http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=49722szz
- ARGE DATEN - Österreichische Gesellschaft für Datenschutz (b). (kein Datum). *Leitfaden zum datenschutzkonformen Cookie-Einsatz*. Abgerufen am 13. September 2016 von www.argedaten.at: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=51778ngg
- Artikel-29-Datenschutzgruppe. (2013). *Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies*. (J. Kohnstamm, Hrsg.) Abgerufen am 14. September 2016 von www.cnpd.public.lu: http://www.cnpd.public.lu/de/publications/groupe-art29/wp208_de.pdf
- Axnix, P. (15. September 2016). Der Standorterhebungs- und Umsetzungsprozess. 4. (W. Berger, Interviewer) Graz, Steiermark, Österreich.
- Ballard, L., & Cooper, S. (2016). *What's New in Security*. Abgerufen am 28. Juni 2016 von <http://devstreaming.apple.com>:
http://devstreaming.apple.com/videos/wwdc/2016/706sgjvzkvg6rrg9icw/706/706_whats_new_in_security.pdf
- Bellalta, B., Bononi, L., Bruno, R., & Kessler, A. (2015). Next generation IEEE 802.11 Wireless Local Area Networks: Current status, future directions and open challenges. *Computer Communications*, 75, S. 1-25.
- Bernaschi, M., Cacace, F., Davoli, A., Guerri, D., Latini, M., & Vollero, L. (2011). A CAPWAP-based solution for frequency planning in large scale networks of WiFi Hot-Spots. *Computer Communications*, 34(11), S. 1283–1293.
- Bundesministerium für Verkehr, Innovation und Technologie. (2010). *Information der Obersten Fernmeldebehörde. Drahtlose lokale Netzwerke (WAS, WLAN, RLAN)*. Abgerufen am 8.

- September 2016 von www.rtr.at: https://www.rtr.at/de/tk/Spektrum5GHz/1997_bmvit-info-052010de.pdf
- Cisco Systems, Inc. (2007). *20 Myths of Wi-Fi Interference: Dispel Myths to Gain High-Performing and Reliable Wireless*. Abgerufen am 16. Mai 2016 von http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd807395a9.pdf
- Droneberger, P. (19. Oktober 2016). Ausrichtung der Dienstleistung am Markt. 6. (W. Berger, Interviewer) Graz, Steiermark, Österreich.
- Europäische Kommission (a). (kein Datum). *Europa Analytics*. Abgerufen am 19. September 2016 von [ec.europa.eu: http://ec.europa.eu/info/europa-analytics_de](http://ec.europa.eu/info/europa-analytics_de)
- Europäische Kommission (b). (2010). *Wie stark beeinflussen Mobiltelefone Ihrer Ansicht nach die eigene Gesundheit?* (TNS Infratest) Abgerufen am 20. September 2016 von [de.statista.com: https://de.statista.com/statistik/daten/studie/159767/umfrage/meinung-zum-einfluss-von-mobilfunk-sendemasten-auf-die-eigene-gesundheit/](https://de.statista.com/statistik/daten/studie/159767/umfrage/meinung-zum-einfluss-von-mobilfunk-sendemasten-auf-die-eigene-gesundheit/)
- Extreme Networks. (2016). *ExtremeWireless™ Integration Guide*. Abgerufen am 24. August 2016 von [documentation.extremenetworks.com: http://documentation.extremenetworks.com/wireless/9034918_Wireless_Integration_Guide.pdf](http://documentation.extremenetworks.com/wireless/9034918_Wireless_Integration_Guide.pdf)
- Fahrnberger, H. (2014). Warum jede Tourismusregion gratis WLAN anbieten sollte. (Ö. Werbung, Hrsg.) *Marketing der Zukunft. Wie digitale Medien den Tourismus verändern*.
- FMK Forum Mobilkommunikation (a). (kein Datum). *Die Festlegung der Grenzwerte*. Abgerufen am 20. September 2016 von [www.fmk.at: http://www.fmk.at/gesundheitsumwelt/grenzwerte-who/die-festlegung-der-grenzwerte/](http://www.fmk.at/gesundheitsumwelt/grenzwerte-who/die-festlegung-der-grenzwerte/)
- FMK Forum Mobilkommunikation (b). (kein Datum). *Die Einhaltung der Grenzwerte*. Abgerufen am 20. September 2016 von [www.fmk.at: http://www.fmk.at/gesundheitsumwelt/grenzwerte-who/die-einhaltung-der-grenzwerte/](http://www.fmk.at/gesundheitsumwelt/grenzwerte-who/die-einhaltung-der-grenzwerte/)
- Ganjia, F., Budziska, Ł., Debeleb, F. G., Lli, N., Meo, M., Ricca, M., . . . Wolisz, A. (2014). Greening campus WLANs: energy-relevant usage and mobility patterns. *Computer Networks*, 78, S. 164-181.
- Google (a). (2016). *Google Chrome – Whitepaper zum Datenschutz. Aktueller Stand für Chrome 52.0.2743.82*. Abgerufen am 24. August 2016 von [www.google.com: https://www.google.com/chrome/browser/privacy/whitepaper.html](https://www.google.com/chrome/browser/privacy/whitepaper.html)
- Google (b). (2016). *SafeSearch aktivieren oder deaktivieren*. Abgerufen am 30. August 2016 von [support.google.com: https://support.google.com/websearch/answer/510](https://support.google.com/websearch/answer/510)

- Google (c). (2016). *Nicht jugendfreie Inhalte an Bildungseinrichtungen blockieren*. Abgerufen am 30. August 2016 von support.google.com: <https://support.google.com/websearch/answer/186669>
- Google (d). (2016). *Google Analytics Terms of Service*. Abgerufen am 14. September 2016 von www.google.com: <https://www.google.com/analytics/terms/us.html>
- Greiner, M. (12. Oktober 2016). Technische Konzeptionierung der Servicestandorte. 4. (W. Berger, Interviewer) Graz, Steiermark, Österreich.
- Hardt-Stremayr, D. (5. Oktober 2016). Öffentliches WLAN als Service für den Tourismus- und Wirtschaftsstandort Graz. 5. (W. Berger, Interviewer) Graz, Steiermark, Österreich.
- Huawei Technologies Co., Ltd. (2012). *WLAN Access Security Technical White Paper*. Abgerufen am 2016 von enterprise.huawei.com: http://enterprise.huawei.com/ilink/cnenterprise/download/HW_195860
- Huber, I. (28. September 2016). Urbanes WLAN in Graz. 4. (W. Berger, Interviewer) Graz, Steiermark, Österreich.
- Insight Intelligence. (2016). *Usage of cookies in Sweden in 2016*. Abgerufen am 19. September 2016 von www.statista.com: <https://www.statista.com/statistics/591804/usage-of-cookies-in-sweden/>
- Kurose, J. F., & Ross, K. W. (2012). *Computernetzwerke. Der Top-Down-Ansatz* (5. Ausg.). München, Deutschland: Pearson Deutschland GmbH.
- Kwon, M. Y., Choi, K., Kim, M., & Chung, Y. M. (2015). Distributed channel selection scheme based on the number of interfering stations in WLAN. *Ad Hoc Networks*, 39, S. 45-55.
doi:10.1016/j.adhoc.2015.12.005
- Lee, I.-G., & Kim, M. (2016). Interference-aware self-optimizing Wi-Fi for high efficiency internet of things in dense networks. *Computer Communications*(89-90), S. 60-74.
doi:10.1016/j.comcom.2016.03.008
- Liikanen, E. (2003). *Empfehlung der Kommission vom 20.März 2003 zur harmonisierten Gewährung des öffentlichen Funk-LAN-Zugangs zu öffentlichen elektronischen Kommunikationsnetzen und -diensten in der Gemeinschaft*. Abgerufen am 12. September 2016 von www.bmvit.gv.at: <http://www.bmvit.gv.at/telekommunikation/recht/europa/empfehlungen/downloads/em2003de203.pdf>
- Mekhazniaa, T., & Zidania, A. (2015). Wi-Fi security analysis. *Procedia Computer Science*, 73, S. 172-178.

- Meuser, M., & Nagel, U. (2009). *Das Experteninterview - konzeptionelle Grundlagen und methodische Anlage* (1. Aufl.). (S. Pickel, G. Pickel, H.-J. Lauth, & D. Jahn, Hrsg.) Wiesbaden: VS Verlag für Sozialwissenschaften | GWV Fachverlage GmbH.
- Milinović, M., Winter, S., Srce / CARNet, RESTENA, & SA3 T2 group. (26. Juni 2012). *eduroam.org*. Abgerufen am 22. 06 2016 von Eduroam Website: https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf
- Ney, A. (2015). *Welche Haftungsrisiken bestehen beim Betrieb eines offenen WLAN-Netzes?* Abgerufen am 27. Juli 2016 von www.wko.at: https://www.wko.at/Content.Node/branchen/oe/sparte_iuc/Telekommunikations--und-Rundfunkunternehmungen/Infos-fuer-Telekommunikationsunternehmen/Sonstige/Welche_Haftungsrisiken_bestehen_beim_Betrieb_eines_offenen_.html
- Nicoletti, P. (2013). Chapter e66 – Content Filtering. In J. R. Vacca (Hrsg.), *Computer and Information Security Handbook* (2. Aufl., S. e101–e122). Waltham, Massachusetts: Morgan Kaufmann.
- Ochang, P. A., Irving, P. J., & Ofem, P. O. (2016). Research on Wireless Network Security Awareness of Average Users. *I.J. Wireless and Microwave Technologies*, 2, S. 21-29.
- OnGuardOnline.gov. (2014). *Tips for Using Public Wi-Fi Networks*. Abgerufen am 28. Juni 2016 von www.onguardonline.gov: <https://www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks>
- Piwik PRO GmbH. (2016). *Piwik vs. Google Analytics. The Ultimate Guide to Choosing the Right Web-Analytics Tool*. Abgerufen am 14. September 2016 von www.piwikpro.de: https://piwikpro.de/wp-content/uploads/sites/2/2016/05/PIWIK_vs_Google_Analytics_Whitepaper.pdf
- Rech, J. (2012). *Wireless LANs. 802.11-WLAN-Technologie und praktische Umsetzung im Detail* (4. Aufl.). Hannover: Heise Zeitschriften Verlag GmbH & Co. KG.
- Ruckus Wireless, Inc. (2014). *What is airtime fairness and why do I need it?* Abgerufen am 24. August 2016 von support.ruckuswireless.com: <https://support.ruckuswireless.com/answers/000002008>
- Rundfunk und Telekom Regulierungs-GmbH. (2012). *5-GHz-Spektrum*. Abgerufen am 9. Juli 2016 von www.rtr.at: <https://www.rtr.at/de/tk/Spektrum5GHz>
- Rundfunk und Telekom Regulierungs-GmbH. (2013). *Spektrum 2400 MHz*. Abgerufen am 9. Juli 2016 von www.rtr.at: <https://www.rtr.at/de/tk/Spektrum2400MHz>
- Rundfunk und Telekom Regulierungs-GmbH. (kein Datum). *Allgemeingenehmigung*. Abgerufen am 12. September 2016 von www.rtr.at: <https://www.rtr.at/de/tk/Allgemeingenehmigung>

- SCENIHR Scientific Committee on Emerging and Newly Identified Health Risks. (2015). *Potential health effects of exposure to electromagnetic fields (EMF)*. Abgerufen am 20. September 2016 von ec.europa.eu: http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_041.pdf
- Schreiner, R. (2012). *Computer - Netzwerke. Von den Grundlagen zur Funktion und Anwendung* (4. Ausg.). München, Deutschland: Carl Hanser Verlag.
- Schumann, L., & Stock, W. G. (2015). *Acceptance and use of ubiquitous cities' information services*. Heinrich Heine University Düsseldorf, Department of Information Science. Düsseldorf, Deutschland: IOS Press. doi:10.3233/ISU-140759
- Shirazi, F. (2011). Free and Open Source Software versus Internet content filtering and censorship: A case study. *The Journal of Systems and Software*, 85(4), S. 920-931.
- Sotzek, R. (2012). *Beyond WEP - WLAN Security Revisited*. Fakultät für Informatik, Technische Universität München, Lehrstuhl Netzarchitekturen und Netzdienste, München.
- Statista GmbH. (2015). *Digital Market Outlook*. Abgerufen am 2016 von de.statista.com: <https://de.statista.com/outlook/215/128/epaper/oesterreich#>
- Strategyzer AG. (2016). *The Value Proposition Canvas*. Abgerufen am 20. November 2016 von www.strategyzer.com: <https://strategyzer.com/canvas/value-proposition-canvas>
- The pfSense Project. (2014). *Captive Portal Vouchers*. Abgerufen am 29. August 2016 von doc.pfsense.org: https://doc.pfsense.org/index.php/Captive_Portal_Vouchers
- Thiele, C. (2015). Haftung für die Nutzung von WLAN. (K. g. GmbH, Hrsg.) *ipCompetence*(14), S. 5-11.
- Ubiquiti Networks, Inc. (a). (2016). *UniFi AC 802.11ac Dual-Radio Access Points Datasheet*. Abgerufen am 4. Dezember 2016 von UBNT: https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf
- Ubiquiti Networks, Inc. (b). (2016). *Enterprise System Controller. User Guide*. Abgerufen am 9. Juni 2016 von UBNT: https://dl.ubnt.com/guides/UniFi/UniFi_Controller_V5_UG.pdf
- Wippersberg, J. (2016). *Informationsverhalten der Digital Natives. Informationsbeschaffung und Informationsnutzungsverhalten bei Jugendlichen und jungen Erwachsenen im digitalen Zeitalter*. Abgerufen am 2016 von www.rtr.at: https://www.rtr.at/de/ppf/Kurzbericht2015_20160503133012/KURZBERICHT_Forschungsprojekt_Digital_Natives.pdf
- World Health Organization. (2006). *Electromagnetic fields and public health*. Abgerufen am 20. September 2016 von www.who.int: <http://www.who.int/peh-emf/publications/facts/fs304/en/>