

DIGITALE MOBILITÄT – DYNAMIK IM ÖFFENTLICHEN RAUM

Carsten Schmoll, Jens Tiemann, Christian Welzel



IMPRESSUM

Autoren:

Carsten Schmoll, Jens Tiemann, Christian Welzel

Gestaltung:

Reiko Kammer

Herausgeber:

Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Januar 2014

Dieses Werk steht unter einer Creative Commons
Namensnennung 3.0 Unported (CC BY 3.0) Lizenz.
Es ist erlaubt, das Werk bzw. den Inhalt zu vervielfältigen,
zu verbreiten und öffentlich zugänglich zu machen,
Abwandlungen und Bearbeitungen des Werkes bzw.
Inhaltes anzufertigen sowie das Werk kommerziell zu nutzen.
Bedingung für die Nutzung ist die Angabe der
Namen der Autoren sowie des Herausgebers.

VORWORT

Ob mit dem Smartphone im Zug, dem Tablet daheim oder mit einem Latte macchiato im hippen Café – physische und digitale Mobilität bestimmt immer mehr das Leben der Menschen und treibt in nahezu allen Handlungsfeldern wichtige Innovationen und Fortschritte voran. Ungeachtet dieser Entwicklung bestimmen häufig noch stationäre und immobile Szenarien unser Handeln sowie auch viele Forschungs- und Entwicklungsvorhaben im IT-Bereich. Die Mobilität der Bürgerinnen und Bürger muss beim Ausbau und der Sicherung öffentlicher Räume und der damit verbundenen öffentlichen IT konsequent mitgedacht und bei Neuentwicklungen von Anfang an mit berücksichtigt werden. Dies schließt auch die Probleme und Erwartungslagen auf Seiten der Nutzer mit ein.

Um dem gerecht zu werden, wird ein Konzept von öffentlicher IT benötigt, das die Bürger als Individuen begreift, welche jederzeit und überall auf unterschiedliche Dienste öffentlicher IT zugreifen möchten. Trends wie mobiler Arbeitsplatz, mobile Endgeräte oder die Nutzung von privaten Geräten im beruflichen Umfeld weisen den Weg in die Zukunft. Um diese digitale Mobilität zu ermöglichen, müssen vier grundlegende Voraussetzungen durch die öffentliche IT erfüllt sein: zuverlässiger Netzzugang, mobile Endgeräte, daran angepasste Anwendungen und Beachtung von Datenschutz und -sicherheit. Dabei ist eine Vielzahl unterschiedlicher Einzelfragen zu betrachten, für die es zukünftig geeigneter Lösungen bedarf. Dazu zählen der sichere mobile Datenzugriff, die Bereitstellung der IT-Infrastruktur, die Verfügbarkeit, aber auch Regelungen für den Netzzugang sowie die Verarbeitung und der Schutz von Daten.

Mit der Ausweitung der (mobilen) Datennetze steigt aber auch die Erwartungshaltung der Bürgerinnen und Bürger, elektronische Dienste der Unternehmen und Verwaltungen auf einfache Art jederzeit mobil nutzen zu können. So entstehen zugleich neue Herausforderungen, u. a. die steigende Komplexität der Anwendungsentwicklung aufgrund der Vielfalt der Endgeräte, die Integration bestehender Anwendungen und Dienste sowie die Beschränkungen der Ökosysteme der Geräteanbieter. Technologien dafür sind verfügbar und vielfach erprobt. Internationale und nationale Standards sind vorhanden und bieten eine hohe Investitionssicherheit. Es bedarf einer gesamtheitlichen Strategie der Firmen und Unternehmen, die auf einer geräteunabhängigen Dienstplattform basiert. Strategien und Masterpläne müssen diese Entwicklung berücksichtigen und dabei die Bürgerinnen und Bürger in den Mittelpunkt stellen.

Mit diesem Whitepaper wollen wir Ihnen das Thema digitale Mobilität aus dem Blickwinkel der öffentlichen IT näher bringen, die unterschiedlichen Diskussionsfelder aufzeigen und Anknüpfungspunkte für weitere Debatten darlegen. Provokante Thesen am Anfang des Whitepapers machen die Bedeutung des Themas und seine Konsequenzen deutlich. Ich wünsche Ihnen eine anregende Lektüre und freue mich auf die Diskussion zu diesem, die öffentliche IT in vielen Bereichen durchdringenden Thema.

Berlin im Januar 2014



Jens Fromm

UNTER ÖFFENTLICHER IT VERSTEHT MAN
INFORMATIONSTECHNOLOGIEN, DIE IN EINEM ÖFFENTLICHEN
RAUM DURCH DIE GESAMTGESELLSCHAFTLICHE
RELEVANZ UNTER BESONDERER BERÜCKSICHTIGUNG
DER STAATLICHEN VERANTWORTUNG STEHEN.

INHALTSVERZEICHNIS

	Vorwort	3
	Inhaltsverzeichnis	4
1.	Thesen	5
2.	Dynamik im öffentlichen Raum	6
2.1	Motivation	6
2.2	Digitale Mobilität	6
2.3	Eingrenzung	7
3.	Handlungsfelder digitaler Mobilität	8
3.1	Netzzugang	8
3.2	Mobile Endgeräte	9
3.3	Anwendungen	10
3.4	Datenschutz und Sicherheit	11
3.5	Medienkompetenz und Technikakzeptanz	13
3.6	Ausblick	14

1. THESEN

1. Die mobile Nutzung von IT wird zum Normalfall.

Mobilität ist ein Grundbedürfnis des Menschen. Mit den aktuellen Möglichkeiten der mobilen Nutzung von Diensten und Anwendungen können die Bürger nahezu immer vernetzt und online sein. Digitale Mobilität entwickelt sich zu einem Leitbild der Gesellschaft, die uneingeschränkte Kommunikation fordert und jederzeit überall auf Informationen zugreifen will. Dies bedeutet, dass alle notwendigen Infrastrukturkomponenten (Endgeräte, Netzzugänge, Netze) und die Anwendungen die mobile Nutzung sinnvoll unterstützen müssen. Nur in ihrer Kombination schaffen sie die Möglichkeit für digitale Mobilität.

2. Der freie Zugang zum Internet muss immer und überall möglich sein.

Der Internetzugang – auch der mobile – muss aufgrund seiner Bedeutung für private wie kommerzielle Nutzer als kritische Infrastruktur wahrgenommen werden. Dies bedeutet, dass vermehrt auch der Netzzugang redundant verfügbar und durchlässig sein muss. Dafür müssen technische, organisatorische und rechtliche Konzepte weiterentwickelt werden. Einen schnellen, mobilen Internetzugang ausschließlich in Ballungsgebieten anzubieten, behindert nicht nur die digitale Mobilität, sondern widerspricht auch dem Grundgedanken der Gleichwertigkeit der Lebensverhältnisse.

3. Anwendungen müssen vorrangig an den Mobilitätsbedürfnissen der Nutzer ausgerichtet sein.

Die mobile Nutzung von Diensten und Daten wird zunehmend zum Standardfall und erfordert damit eine kontext- und situationsabhängige, dynamische Anpassung der Anwendungen. Die Anwender erwarten ein stets optimales Nutzungserlebnis entsprechend dem eingesetzten Endgerät (Tablet, Smartphone, aber auch am PC) und ihrer aktuellen Situation. Aufgrund dieser weitgehenden Anpassung gibt es im Idealfall nur noch barrierefreie Angebote. Die digitale Mobilität verstärkt wesentlich die Durchdringung aller Lebensbereiche mit IT.

4. Die mobile Nutzung von IT verändert grundlegend die Qualität der angebotenen Dienste.

Neben der Ausweitung der Nutzung von IT ergeben sich auch qualitative Veränderungen: Die enge Bindung von Nutzer und

Mobilgerät ermöglicht zunehmend spontane oder automatisierte Transaktionen in immer mehr Situationen. Die Angebote erfahren dadurch eine Dynamisierung und Individualisierung, die weit über die reine Präsentation des Angebots hinaus reichen. Die Personalisierung der Endgeräte ermöglicht wiederum die Gestaltung neuer personalisierter Anwendungen, es kommt zu Rückkopplungen zwischen Nutzung und Dienst.

5. Die zunehmende digitale Mobilität erfordert ein Umdenken in der IT-Sicherheit.

Aufgrund der besonderen Eigenschaften, die sich aus einer mobilen Nutzung von Diensten sowie der starken Kopplung zwischen Nutzerkonto und Endgerät ergeben, sind zusätzliche, neue Verfahrensweisen im technischen und im organisatorischen Bereich zum Schutz der Nutzer und ihrer Daten notwendig, sowohl auf dem Endgerät als auch auf Seiten der Diensteanbieter.

6. Die Medienkompetenz der Bürger muss gesteigert werden.

Die breite Nutzung von IT verändert nachhaltig die Lebensgewohnheiten der Bürgerinnen und Bürger. Hierfür müssen Nutzer aller Altersgruppen in die Lage versetzt werden, selbstständig entscheiden zu können, welche Auswirkungen ihr Handeln im digitalen Raum hat. Sie müssen verstehen, welche Prozesse ablaufen und welche Konsequenzen diese haben können. Hierzu ist in erster Linie der Staat gefordert, entsprechende Bildungsmöglichkeiten anzubieten.

7. Es muss ein situationsbezogener Kompromiss zwischen Sicherheit und Komfort gefunden werden.

Ein Mehr an Sicherheit bedeutet zumeist Einbußen beim Nutzungskomfort und umgekehrt. Dazu muss für jeden Anwendungsfall ein angemessener Kompromiss zwischen Sicherheit und Nutzungskomfort gefunden werden. Förderlich hierfür sind ein offen geführter Diskurs und die Entwicklung eines gemeinsamen kulturellen Verständnisses für die sichere Nutzung von Diensten im Internet.

2. DYNAMIK IM ÖFFENTLICHEN RAUM

2.1 MOTIVATION

Mobilität ist ein Grundbedürfnis des Menschen. Seit Jahrtausenden ermöglicht sie den Menschen Zugriff auf räumlich verteilte Ressourcen und soziale Teilhabe. Im Zuge der Forschung zu Mobilität und Verkehr sind die Grundlagen und Motivationen von Mobilität in den letzten Jahrzehnten vielfältig untersucht worden. Ergebnisse dieser Arbeiten können als Ausgangspunkt für die vorliegende Betrachtung dienen.¹ Dabei wird vor allem die enorme Bedeutung von Mobilität für unsere Gesellschaft deutlich. In modernen Gesellschaften korreliert der Wohlstand mit der Verkehrsleistung.² Dies zeigt sich in der seit Jahren breit geführten gesellschaftlichen Diskussion zu Chancen und Auswirkungen des Themas »Mobilität und Verkehr«.³

Informationstechnologie trägt zu dieser Diskussion zwei wichtige Ansätze bei: die Unterstützung physischer Mobilität, also die Bewegung im realen Raum, und die Ermöglichung von virtueller Mobilität, welche die Bewegung in digitalen, also virtuellen, Räumen meint. Während virtuelle Mobilität aufgrund der Nutzung von speziellen Anwendungen bisher noch als eine individuelle Angelegenheit angesehen werden kann, ist die Unterstützung der mobilen Nutzung von IT unzweifelhaft zu einer öffentlichen Infrastrukturaufgabe geworden.

»Digitale Mobilität geht weit über die mobile Smartphone-Nutzung hinaus.«

Grundlegend für die hohe Bedeutung sind die Universalität und der Grad der Einbettung mobiler Endgeräte. Diese sind eben nicht nur portable Geräte, die eine Mediennutzung herkömmlicher Art an verschiedenen Orten erlauben. Es treffen sich heute Bedürfnisse von Menschen und technologische Möglichkeiten in einer Art und Weise, die eine sehr enge Bindung von Nutzer und mobilem Endgerät sowie eine weitgehende Einbettung von IT-Systemen in reale Objekte erlauben. Daraus folgt eine quantitative und qualitative Ausweitung der IT-Nutzung, die neue Aspekte öffentlicher IT aufwirft und im Folgenden diskutiert wird.

Grundsätzlich muss Mobilität als individuelle Option verstanden werden – Mobilität bezeichnet die Möglichkeit zur Bewegung,

nicht in erster Linie die Bewegung selbst. Ein Beispiel verdeutlicht dies: Für eine geschäftliche Besprechung kann oftmals eine Telefon- oder Videokonferenz als wirtschaftlichere Lösung genutzt werden, trotzdem finden immer noch viele Dienstreisen statt. Unterwegs werden dann wiederum Mobilgeräte genutzt, um auf Ressourcen der eigenen Organisation zuzugreifen oder per E-Mail weiterhin an aktuellen Prozessen beteiligt zu sein. Der Aspekt der Teilhabe wird dabei stets nach individuellen Kriterien situationsbezogen beurteilt. Mobilität erweitert den eigenen Handlungsspielraum, auch wenn nicht jede Möglichkeit tatsächlich genutzt wird.

2.2 DIGITALE MOBILITÄT

In verschiedenen Fachgebieten wird der Begriff Mobilität unterschiedlich und teilweise diffus verwendet.⁴ In technischen Zusammenhängen steht der Begriff zunächst für die physische Mobilität, zumeist des Menschen, also die konkrete Raumüberwindung.⁵ Im Zeitalter der rapide wachsenden Internetnutzung in allen Lebensbereichen und -situationen steigt damit der Bedarf nach Geräten und Diensten, die ihre Nutzer in Phasen der physischen Mobilität unterstützen. Diese Unterstützung ist z. B. im Bereich multimodaler Mobilität, also der kombinierten, effizienten Nutzung verschiedener Mobilitätsangebote (Auto, Fahrrad, Bus, Bahn, Leihfahrzeug), essenziell. Im Gegensatz zur physischen Mobilität wird bei der virtuellen Mobilität die physische Raumbewegung durch den elektronischen Austausch von

¹ Canzler, Weert/Knie, Andreas (2000): »'New Mobility?' Mobilität und Verkehr als soziale Praxis«, in: Aus Politik und Zeitgeschichte. Beilage zur Wochenzeitung Das Parlament, B 45-46/2000, S. 29-38. online unter: <http://www.bpb.de/apuz/25355/new-mobility-mobilitaet-und-verkehr-als-soziale-praxis>

² VZ Magazin, Ausgabe 3, Peter Phleps: »Mobilität: Zukunftsmarkt oder Ende des Wachstums?«, online unter http://www.verantwortungzukunft.com/sites/verantwortungzukunft.de/files/images/VZ_Magazin_Ausgabe_3_2013_Titelstory.pdf

³ Detlef Frank, Mobilität Grundbedürfnis des Menschen, Spektrum der Wissenschaft 6/1997, Seite 34.

⁴ Dennis Krannich: Mobile Usability-Testing, Dissertation, 2010, online unter <http://issuu.com/krannich/docs/mut>

⁵ Peter Zoche, Simone Kimpeler, Markus Joepgen: »Virtuelle Mobilität: Ein Phänomen mit physischen Konsequenzen?«, 2001.

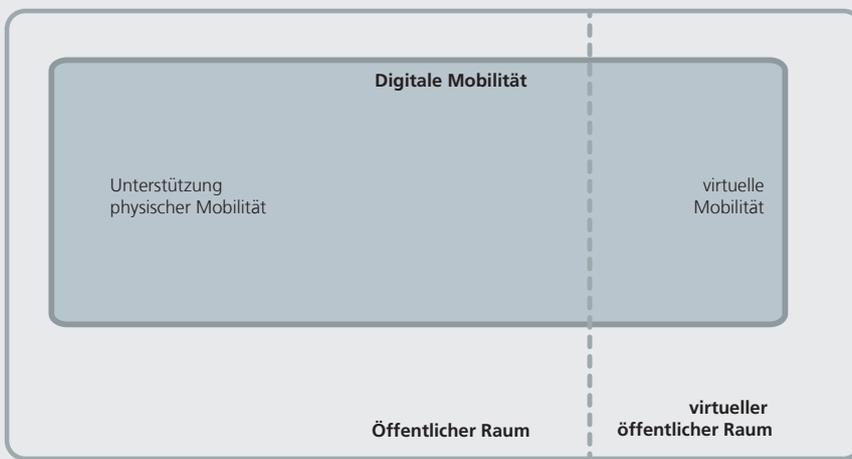


Abbildung 1: Digitale Mobilität ist die durch Technik unterstützte Bewegung in physischen und virtuellen Räumen.

Informationen ersetzt. Die digitale Mobilität ist die durch Technik unterstützte Bewegung in physischen und virtuellen Räumen. Sie unterstützt und erweitert die Möglichkeiten der Menschen mobil zu sein, indem sie eine höhere Flexibilität und mehr Bewegungsfreiheit für die Nutzer ermöglicht. Dies schließt auch die mobile Nutzung von Anwendungen und Diensten ein, deren Ziel nicht direkt die Unterstützung von Mobilität ist.

Um digitale Mobilität zu ermöglichen, bedarf es aus technischer Sicht mobiler Endgeräte und Zugangsnetze hierfür sowie Anwendungen, welche mobil genutzt werden können. Neben den technischen Aspekten bedarf es dazu leistungsfähiger Systeme auf allen Gebieten sowie angemessener Sicherheits- und Datenschutzmechanismen. Erst wenn diese Grundvoraussetzungen erfüllt sind, ist eine digitale Mobilität gegeben. Der Grad der digitalen Mobilität hängt dabei vom Grad der Umsetzung der jeweiligen Grundvoraussetzungen ab.

»Die mobile Nutzung von IT wird zum Normalfall.«

2.3 EINGRENZUNG

In diesem Whitepaper werden insbesondere Aspekte digitaler Mobilität im Kontext öffentlicher IT erörtert. Dabei handelt es sich um die physische Mobilität unterstützende oder ersetzende Kommunikation über öffentliche IT-Infrastrukturen. Ausgehend von dem Bedürfnis nach und dem Trend zu mehr Mobilität werden Fragen der öffentlichen IT behandelt, die sich durch den Zuwachs an digitaler Mobilität und ihrer Ausprägungen in der digitalen Welt ergeben. Technische Fragen physischer Mobilität (Verkehr, Logistik etc.) bleiben in diesem Papier unberücksichtigt. Das Whitepaper konzentriert sich auf die digitale Unterstützung physischer Mobilität im öffentlichen Raum.

3. HANDLUNGSFELDER DIGITALER MOBILITÄT

Ausgehend von dem Bedürfnis nach digitaler Mobilität ergeben sich eine Reihe von Herausforderungen für die öffentliche IT. Digitale Mobilität ermöglicht nicht nur neue Nutzungsszenarien, sie stellt durch ihre neue Flexibilität auch einen entscheidenden gesellschaftlichen Entwicklungsschritt und Wettbewerbsvorteil für die Wirtschaft dar, indem Geschäfts- oder Verwaltungsprozesse effizienter gestaltet werden können.

Der Trend zur digitalen Mobilität stellt technische, organisatorische und rechtliche Anforderungen an die öffentliche IT:

- Dazu zählt die Gewährleistung mobiler Zugangsnetze im Sinne einer Grundversorgung und der Sicherstellung der Gleichwertigkeit von Lebensverhältnissen.
- Des Weiteren ist eine breite Unterstützung mobiler Endgeräte notwendig. Dies erfordert gemeinsame technische Standards, die definiert und weiterentwickelt werden müssen.
- Darüber hinaus müssen die herkömmlichen Anwendungen und Prozesse an die Anforderungen der digitalen Mobilität angepasst werden. Dazu zählen Daten, aber auch Dienste, die bspw. Ortsinformationen der Nutzer berücksichtigen müssen.
- Aspekte der Sicherheit und des Datenschutzes spielen eine wichtige Rolle. Dazu ist ein ganzheitlicher Ansatz erforderlich, der Sicherheit und Datenschutz als integralen Bestandteil bereits bei der Konzeption der technischen Systeme betrachtet.

Darüber hinaus bestimmen weitere Faktoren die digitale Mobilität. Insbesondere die Aspekte Medienkompetenz der Bürgerinnen und Bürger und allgemeine Technikakzeptanz in der Gesellschaft seien hier genannt.

Die Möglichkeiten auf allen Ebenen – in allen denkbaren Kombinationen – führen zu einer hohen Dynamik bei der IT-Nutzung. Die erweiterte Verfügbarkeit von Anwendungen macht diese vielfältiger und in den verschiedensten Situationen nutzbar. Die Anwendungen werden über verschiedene Netze und Endgeräte genutzt und passen sich dabei wechselnden Bedingungen und Situationen an.

3.1 NETZZUGANG

Die alltägliche Nutzung des Internets unterwegs, sowohl für den privaten wie auch für den geschäftlichen Bereich, führt zu einer kontinuierlich steigenden Abhängigkeit von der Verfügbarkeit schneller, mobiler Internetzugänge. Eine flächendeckende Bereitstellung schneller, mobiler Zugangsnetze schafft einen Ausgleich zwischen konkurrierenden Regionen und vermindert Abwanderungstendenzen von Bürgern und Unternehmen. Der Faktor mobiler Netzzugang ist damit ein entscheidender Standortfaktor für die Wirtschaft aber auch für die Bürgerinnen und Bürger, insbesondere in ländlichen Regionen. Für die mobile Nutzung digitaler Dienste sind zur Verfügung stehende Bandbreite und Datenvolumen die entscheidenden Faktoren. Breitbandverbindungen⁶ von mindestens 2 Mbit/s ermöglichen aktuell auch für anspruchsvolle Dienste eine sehr gute Nutzbarkeit und damit ein gutes Anwendererlebnis.

»Der freie Zugang zum mobilen Internet ist Grundvoraussetzung für die effektive Nutzung digitaler Mobilität.«

Die stetig steigende Nachfrage nach drahtloser Kommunikation erfordert eine andauernde Optimierung der Ausnutzung des nur begrenzt verfügbaren Frequenzspektrums. Diese Aufgabe betrifft in gleicher Weise Forschung, Standardisierung und Regulierung im Bereich kognitiver Funkssysteme und Frequenzmanagement. Für einzelne Übertragungsverfahren gibt es Entwicklungspotenzial bzgl. Robustheit und Redundanz, Zuverlässigkeit sowie der ständigen Verfügbarkeit hoher Bandbreiten. Begrenzungen basieren hauptsächlich auf physikalischen Eigenschaften von Funkübertragungstechniken. Trotz prinzipieller Einschränkungen (bspw. Frequenzspektrum als gemeinsam genutzte, stör anfällige Ressource) ermöglicht die Auswahl passender Frequenzbereiche eine Optimierung der Übertragung für den speziellen Einsatzbereich. Daher wird es auch in Zukunft verschiedene Übertragungstechnologien geben, die gleichzeitig von universellen Endgeräten genutzt werden.

⁶ vgl. Definition Breitband der ITU, <http://www.itu.int/osg/spu/publications/birthofbroadband/faq.html>



Abbildung 2: Digitale Mobilität stellt technische, organisatorische und rechtliche Anforderungen an die öffentliche IT.

2

Mit dem Einsatz derzeitiger Mobilfunk-Technologien (GSM, UMTS, LTE) kann die topografische Netzabdeckung weiter ausgebaut werden. Mittels Regulierung werden freie Frequenzbereiche aus der Abschaltung des analogen Fernsehens («digitale Dividende») bevorzugt zum Ausbau der Breitbandversorgung⁷ in der Fläche genutzt. In Ballungsgebieten werden auch die erweiterten Frequenzbereiche des Mobilfunks nicht ausreichen, daher müssen die Mobilfunknetze um Basisstationen mit geringer Reichweite (Piko-/Femtozellen) erweitert oder der nahtlose Übergang zu WLAN-Netzen genutzt werden. Der Aspekt der (Mistörer-)Haftung hindert Betreiber in vielen Bereichen derzeit noch daran, freie Netzzugänge zur Verfügung zu stellen.⁸

Netzzugänge werden ihrer Aufgabe als öffentliche Infrastruktur nur gerecht, wenn sie einen uneingeschränkten, diskriminierungsfreien Zugang für die Nutzer und die Dienstanbieter bieten. Als eine Grundvoraussetzung für digitale Mobilität muss die Erlangung eines solchen Zugangs für die Nutzer möglichst unkompliziert sein.

Empfehlungen zur Gestaltung:

- Förderung der anwendungsnahen Forschung zur optimierten Nutzung des begrenzten Frequenzspektrums. Technologisch sich abzeichnende oder bereits verfügbare Verfahren bedürfen internationaler Abstimmung, lokaler Infrastrukturen und eines adäquaten Ordnungsrahmens.
- Neben dem Breitbandausbau wird die Verfügbarkeit freier Zugangsnetze immer wichtiger. Für Betreiber freier Zugangsnetze, bspw. freier WLANs, muss Rechtssicherheit hergestellt werden, indem Haftungsfragen klar geregelt werden.
- Freigabe von Frequenzspektrum ohne Bindung an einen Kommunikationsanbieter für die lokale Nutzung durch freie Kommunikationsdienste unter Verwaltung einer kommunalen Institution. Dieses »Smart City«-Frequenzspektrum könnte zur Unterstützung kommunaler Aufgaben genutzt werden, von der Steuerung der Infrastruktur (in Ballungsgebieten) bis zur Verbesserung der Internetinfrastruktur (in ländlichen Räumen).

Empfehlungen zur Nutzung:

- Bereitstellung von freien Netzzugängen als gemeinsame Infrastruktur für interne und externe Nutzer, auch zur Trennung und angemessenen Behandlung von privater und geschäftlicher Kommunikation im Sinne von Datenschutz und Datensicherheit.

3.2. MOBILE ENDGERÄTE

Die globale Verbreitung mobiler Endgeräte (Smartphones, Tablets etc.) mit Internetzugang hat den Trend der digitalen Mobilität in den letzten Jahren maßgeblich vorangetrieben. Die funktionale Heterogenität der Endgeräte bietet ein großes Innovationspotenzial für die Wirtschaft und sollte weiter gefördert werden. Die stetig steigende Leistungsfähigkeit der Endgeräte und deren Ausstattung mit immer neuen Funktionen und vielfältigen Sensoren eröffnen unzählige neue Anwendungsszenarien.

Das Smartphone entwickelt sich zu einem ständigen Begleiter, der sowohl die private als auch die berufliche Lebenswelt abbildet. In dieser universellen Rolle wird es zukünftig nicht nur als Kommunikationszentrale dienen, sondern bspw. auch als Zahlungsmittel oder Türöffner. Die Interaktion mit der Umgebung und mit vernetzten Objekten wird künftig ebenfalls maßgeblich über ein mobiles Endgerät gesteuert werden. Die damit verbundenen Abhängigkeiten stellen eine Herausforderung für die Nutzer und die Dienstanbieter oder sogar für die Arbeitgeber dar.

⁷ vgl. Breitbandatlas der Bundesregierung, <http://www.zukunft-breitband.de/DE/breitbandatlas.html>

⁸ vgl. Länderinitiativen zu freiem WLAN: »Entscheidung des Bundesrates zur Beschränkung des Haftungsrisikos für Betreiber drahtloser lokaler Netzwerke (WLANs) unter http://www.bundesrat.de/clin_227/SharedDocs/Drucksachen/2012/0501-600/545-12,templateId=raw,property=publicationFile.pdf/545-12.pdf

**DIE BREITE MOBILE NUTZUNG
VON IT VERÄNDERT NACHHALTIG
DIE LEBENSGEWOHNHEITEN DER
BÜRGERINNEN UND BÜRGER.**

Zu beobachten ist eine steigende Abhängigkeit von den Geräteherstellern. Anwendungen sind oftmals nur über die herstellereigenen Quellen (»App-Store«) zu beziehen. Auch die Steuerung und Konfiguration der Endgeräte liegt zunehmend in der Hoheit der Gerätehersteller. Damit entscheiden nicht nur die Anwendungsentwickler, sondern vor allem auch die Gerätehersteller und Plattformanbieter darüber, welche Anwendungen den Nutzern unter welchen Bedingungen zur Verfügung stehen.

Mobile Endgeräte haben zunehmend auch Komfortfunktionen, die eine dauerhafte Aktivierung von Mikrofon, Kamera oder anderen Sensoren bedingen. Durch ihre gleichzeitige, ständige Online-Verbindung ergeben sich hier zahlreiche Herausforderungen bzgl. Sicherheit und Privatsphäre, die nicht nur den Inhaber, sondern auch seine unmittelbare Umgebung betreffen.

Die technische Entwicklung im Bereich mobiler Endgeräte ermöglicht nicht nur eine Unterstützung der physischen Mobilität, sondern schafft auch Mischformen zwischen physischen und virtuellen öffentlichen Räumen. Mit einer Datenbrille oder modernen Smartphones beispielsweise kann eine reale Umgebung durch eine zusätzliche virtuelle Sicht erweitert werden, man spricht hierbei von erweiterter Realität bzw. Augmented Reality.

Empfehlungen zur Gestaltung:

- Aufgrund der engen Bindung zwischen mobilen Endgeräten und Nutzern muss darauf geachtet werden, dass die Nutzer weiterhin zumindest die Möglichkeit haben, diese Bindung zu durchbrechen, ohne dabei eine Einschränkung im Funktionsumfang hinnehmen zu müssen.
- Gerade vor dem Hintergrund der starken Bindung der Nutzer an mobile Endgeräte und der damit verbundenen, einfachen Profilbildung muss die Hoheit der Nutzer gestärkt werden, beispielsweise, indem das Surfen im Internet nicht zwingend die Aktivierung eines persönlichen Nutzerkontos voraussetzt.

- Kommunikationsfunktionen werden in immer mehr Klassen von – bisher nicht vernetzten – technischen Systemen eingebaut (z.B. in Fahrzeuge). Entscheidend ist dabei nicht die Ausgestaltung der Endgeräte, sondern die Möglichkeit zur Interaktion mit ihnen und der Grad ihrer Einbettung. Dies bedeutet, dass der Begriff »mobiles Endgerät« auf eine Vielfalt von Geräteklassen angewendet werden muss, die weit über Smartphones und Tablet-Computer hinausgeht.

Empfehlungen zur Nutzung:

- Aus Sicht der öffentlichen IT sind Mindestanforderungen an mobile Endgeräte notwendig, die vor allem über internationale Standardisierungsgremien realisiert werden müssen. Diese Mindestanforderungen sollten für Beschaffungen verbindlich definiert werden.
- Durch die ständige Aktivierung der vielfältigen Sensoren mobiler Endgeräte tragen die Nutzer auch eine Verantwortung für die Umgebung, in der sie diese einsetzen. Sie müssen sich dieser technischen Möglichkeiten bewusst sein und ihr Handeln in der Gemeinschaft entsprechend anpassen.

3.3 ANWENDUNGEN

Immer mehr digitale Anwendungen nutzen aktive Internetverbindungen oder funktionieren ausschließlich online. Dadurch können sich signifikant der Komfort und die Nutzerfreundlichkeit erhöhen. Dies gilt nicht zuletzt, weil die bereitgestellten Dienste in der öffentlichen IT den Nutzern – Netzzugang vorausgesetzt – »immer und überall« und mit aktuellen Daten zur Verfügung stehen.

Für zukunftssichere Dienste und Webseiten muss aktuell und in Zukunft der Zugriff durch mobile Endgeräte als der Standardfall angesehen werden, welcher über Geräteklassen hinweg in gewohnter Nutzungsqualität unterstützt werden muss. Dies gilt sowohl für die Internetpräsenzen der Privatwirtschaft als auch



für die digitalen Bürgerdienste der öffentlichen Hand, welche tendenziell eine physikalische Mobilität teilweise ersetzen können.

Jedoch sind nicht alle über das Internet verfügbaren Dienste auch problemlos mobil nutzbar, sei es aufgrund eines nicht flexiblen Layouts, unangepasster Schriftgrößen oder im Einzelnen nicht erfüllbarer Anforderungen an die Performance oder die Funktionalität eines Endgerätes. Hierin liegt eine große Herausforderung für die Anwendungsentwickler, mit den beschränkten Ressourcen der verschiedenen Endgeräte ihre Dienste möglichst optimal zur Verfügung zu stellen. Hinzu kommt die Erwartungshaltung der Nutzer, neue technische Möglichkeiten auch innerhalb der Anwendungen nutzen zu können.

Die Vielzahl der Endgeräte, die sich signifikant in ihren Eigenschaften (Display, Leistungsfähigkeit, Laufzeit, Anbindung) unterscheiden, erfordert eine flexible Anpassung der Anwendungen an die aktuelle Umgebung der Nutzer. Diese Heterogenität der Endgeräte stellt jedoch für Anwendungsentwickler derzeit einen nicht zu unterschätzenden Aufwand dar. Sie müssen ihre Anwendungen oftmals parallel für eine breite Palette an Endgeräten entwickeln.

Mobile Endgeräte begleiten die Nutzer rund um die Uhr. Dies birgt eine Reihe von Herausforderungen und Gefahren (siehe Datenschutz und Sicherheit), ermöglicht aber auch eine qualitative individuelle Ausgestaltung von Anwendungen. Durch die Rückkopplung von Informationen können sich Dienste und Anwendungen situationsabhängig verhalten.

Empfehlungen zur Gestaltung:

- Internationale offene Standards, die die Interoperabilität fördern (beispielsweise HTML5), müssen aktiv unterstützt werden, u.a. um die Abhängigkeit von Geräteherstellern und Plattformanbietern zu verringern.

- Eine individuelle und situationsabhängige Ausgestaltung von Anwendungen und Diensten ermöglicht neue Formen der Barrierefreiheit. Diese wird von einer aufgesetzten zu einer integrierten Eigenschaft.

Empfehlungen zur Nutzung:

- Für mobile Anwendungen und Dienste sind Mindeststandards hinsichtlich ihrer Sicherheit und Nutzbarkeit erforderlich. Diese können durchaus branchenspezifisch vorangetrieben werden.

3.4 DATENSCHUTZ UND SICHERHEIT

Aktuelle Mobilgeräte und deren Nutzung bedingen zumeist eine starke Personalisierung des Gerätes, d.h. eine enge Bindung zwischen Person und eigenem Mobilgerät. Diese Bindung ermöglicht ein hohes Maß an Komfort, erfordert aber gleichzeitig einen besonders gut funktionierenden Schutz der Daten. Die Tatsache, dass diese Geräte nur selten komplett ausgeschaltet werden, mit vielen persönlichen Nutzerdaten arbeiten und in der Lage sind, detaillierte Bewegungsprofile zu erstellen, ermöglicht eine Qualität der personalisierten Profilbildung wie bei keiner Geräteklasse je zuvor. Dies weckt Begehrlichkeiten durch Dritte auch jenseits der legalen Verwendung dieser Daten.

Neue Endgeräte, Anwendungen und Funktionen bieten immer auch neue Angriffsvektoren. Gerade für Smartphones als Universalgeräte stellt diese Tatsache eine zunehmende Herausforderung dar. Trends wie mobiler Arbeitsplatz oder »bring your own device« (BYOD) verstärken hier den Bedarf nach neuen, effizienten Sicherheitskonzepten.

⁹ Was Vorratsdaten über uns verraten <http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz>

Ferner bieten mobile Anwendungen und Endgeräte problematische neue Angriffsflächen durch die mobile (Funk-)Datenübertragung, ihre vielfältigen Datenschnittstellen und ihre weite Verbreitung. Die Möglichkeit, durch die ständige Verbindung der Geräte über Mobilfunk oder WLAN-Hotspots unbemerkt Angriffe durchzuführen und z.B. Schadcodes zu installieren und auf dem Smartphone/Tablet auszuführen, verquickt mit der Menge persönlicher Daten auf diesen Geräten, lassen sie zu wertvollen Zielen für Angreifer werden. Sinnvolle, technische Verfahren zur Erhöhung der Sicherheit sind u. a. die Nutzung von Passwort/PIN, Fern-Sperrung, Datenverschlüsselung oder auch die E-Mail-Signierung. Klassische Sicherheitskonzepte können als Ausgangspunkt dienen, stoßen aber zunehmend an ihre Grenzen. Zukünftig wird es darauf ankommen, Vertrauensanker zu etablieren, die eine abgesicherte Kommunikation auch in einer unsicheren Umgebung ermöglichen.

Neben den Aspekten der Datensicherheit gilt auch dem Datenschutz ein besonderes Augenmerk. Bei der Nutzung von Internetdiensten im Allgemeinen und mobilen, digitalen Diensten im Besonderen sollten die Nutzer sich bewusst darüber sein, welche ihrer Daten von Ihnen wo (in welchem Land/in welcher Institution) durch welchen Dienst übertragen und gespeichert werden. Damit dies überhaupt möglich ist, muss hierfür eine Transparenz bzgl. der Kommunikationswege und der Lokation der Dienste und Daten geschaffen werden. Dies muss in einer Art geschehen, welche für die Nutzer auch nachvollziehbar und einfach anwendbar ist. Anbieter mobiler Anwendungen sind hier gefordert, durch klare Informationen Vertrauen zu schaffen.

Die Analyse des Nutzerverhaltens ist gerade für die Werbewirtschaft von großem Interesse. Neben herkömmlichen Analyseverfahren wie Browser-Cookies sind bei mobilen Endgeräten auch neuere Verfahren denkbar wie beispielsweise Browser-Fingerprinting oder Hardware-Tracking.¹⁰ Diese Entwicklungen müssen beobachtet werden. Bei Bedarf muss diesen entgegen gewirkt werden, um sicherzustellen, dass die Datenschutzrechte der Nutzer gewahrt bleiben.

Weitere Herausforderungen ergeben sich durch die zunehmende Vermischung privater und beruflicher Daten auf einem mobilen Endgerät. Ein Konzept, welches die sichere Nutzung mobiler Anwendungen unterstützt, ist die konsequente Nutzung von verschiedenen, getrennten Rollen auf mobilen Endgeräten. Dies muss sowohl technisch unterstützt, als auch aktiv durch die Nutzer gelebt werden. In Bezug auf die Unterstützung vertrauenswürdiger Kommunikation mit verifizierbaren Absendern und Adressaten erlauben Mobilgeräte idealerweise die Nutzung von Geräte- und Personenzertifikaten, mit denen z. B. E-Mails signiert werden können.

Neben der technischen Unterstützung auf den Geräten bedarf dies einer effizienten Kopplung von Endgeräten bzw. Personenprofilen mit elektronischen Identitäten (eID). Dies könnte zum einen eine technische Kopplung mit einem Träger solch einer eID, wie dem neuen Personalausweis (nPA), oder zum anderen die Installation von elektronischen Zertifikaten auf dem Endgerät selbst sein. Seitens der Infrastruktur bedarf es dazu in beiden Fällen sicherer, vertrauenswürdiger Zertifizierungsstellen für diese eIDs.

Eine effektive Datensicherheit bei digitaler Mobilität lässt sich daher nur durch eine parallele Nutzung mehrerer, komplementärer Verfahren wirkungsvoll erreichen, inklusive der Aufklärung der Nutzer und ggf. der Anpassung des eigenen Verhaltens.

Empfehlungen zur Gestaltung:

- Konsequente Entwicklung und Nutzung einfacher anzuwendender und langfristig sicherer Verschlüsselungsverfahren für den allgemeinen Datentransport und auf Anwendungsebene.

¹⁰ siehe: <http://www.zeit.de/digital/datenschutz/2013-10/cookies-browser-fingerprint-hardware-tracking>

- Einführung und Nutzung neuer, an Objekte gebundener Sicherheitsmodelle (als Ergänzung zu klassischen, zonenbasierten Sicherheitskonzepten).
- Für vertrauenswürdige Kommunikation sollten mobile Endgeräte die Nutzung von Geräte- und Personenzertifikaten unterstützen. Dazu bedarf es einer nutzerfreundlichen Koppelung mit sicheren elektronischen Identitäten (eID).

Empfehlungen zur Nutzung:

- Konsequente Umsetzung von Rollenmodellen (z. B. Trennung privater und dienstlicher Bereiche auf allen genutzten Endgeräten – oder strikte Trennung durch Nutzung verschiedener Endgeräte).
- Verstärkte Nutzung von Ansätzen des Risikomanagements (angepasste Sicherheit, Abschätzung von Risiko und Konsequenzen, je nach Kritikalität der genutzten Daten).
- Nutzer von mobilen Endgeräten müssen sich mit den sicherheitstechnischen Möglichkeiten ihrer Geräte vertraut machen.
- Darüber hinaus sind Verfahren zu entwickeln, die Nutzungsbedingungen und Datenschutzbestimmungen in einer standardisierten und verständlichen Art und Weise darstellen. Außerdem sollten Verbraucherrechte regelmäßig an neue technische Entwicklungen der öffentlichen IT angepasst werden.

3.5 MEDIENKOMPETENZ UND TECHNIKAKZEPTANZ

Viele Herausforderungen sind nicht allein durch technische Mittel lösbar. Voraussetzung für die kompetente und verantwortungsvolle Nutzung mobiler, digitaler Dienste ist die Medienkompetenz der einzelnen Nutzer und die Technikakzeptanz in der Gesellschaft. Das umfasst die Fähigkeit der Nutzer zur sicheren Kommunikation im privaten und beruflichen Umfeld unter Einbeziehung der Aspekte des Datenschutzes. Medien-

kompetenz und Technikakzeptanz sind zwei Aspekte zur ausgewogenen Nutzung der Vorteile digitaler Mobilität. Eine informierte und reflektierte Nutzung neuer, innovativer Dienste unterstützt nachhaltig die Förderung und Anwendung neuer Technologien.

Medienkompetenz wird zunehmend auch zu einem Wirtschaftsfaktor und hat Einfluss auf die gesellschaftliche Entwicklung. Viele Unternehmen erwarten heute bereits, dass Arbeitnehmer ein gewisses Grundverständnis für den Umgang mit Informationstechnologien haben. Durch die beschriebenen qualitativen Veränderungen von Diensten und Anwendungen hat der Einsatz allgegenwärtiger IT-Komponenten weitergehende Konsequenzen als nur die zusätzlich mobile Nutzung bekannter Anwendungen. Die Fähigkeit des Einzelnen zur gezielten Informationsbewertung wird immer wichtiger, ebenso wie eine gesellschaftliche Auseinandersetzung über die Erzeugung, Verarbeitung und Nutzung von Daten, die alle Lebensbereiche durchdringen.

Bei der Nutzung von personalisierten digitalen Diensten gehen Internetnutzer seit jeher Kompromisse zwischen Komfort und Datensicherheit ein. Im Zeitalter mobiler Internetnutzung »immer und überall« sind daher sowohl die Datenspuren der Nutzer wie auch das – zumeist von nur einer Person in wechselnden Umgebungen verwendete – mobile Endgerät angreifbar. Beides, Datenspuren und Gerät, sind stark personalisiert und daher besonders schutzbedürftig.

Kommunikations- und Dienstleister können die sicherheitsbewusste Nutzung von Diensten unterstützen durch Einhaltung relevanter Best Practices, praktizierter Datensparsamkeit sowie transparenter Informationspolitik.

Mobile, digitale Dienste bedingen bei den Bürgern ein fundiertes Verständnis der Technik, um qualifizierte, persönliche Entscheidungen zu treffen. Hierbei ist auch der Staat in der Pflicht, sowohl durch entsprechende Vorgaben an die Anbieter als



auch durch Aufklärungs- und Bildungsangebote für die Bürger. Er muss ihnen ermöglichen, technische Hintergründe so weit zu verstehen, dass sie sich bewusst für oder gegen die Nutzung einer Anwendung oder eines Dienstes entscheiden können.

Das natürliche Interesse der Nutzer an technischen Neuerungen wird auch durch attraktive Angebote der Wirtschaft in Form von neuen Diensten und Geräten sowie deren Designs gefördert. Die Anbieter selbst sowie die Gesellschaft sollten darauf achten, dass diese grundsätzliche Technikakzeptanz nicht durch Frustrationen gefährdet wird, beispielsweise durch unvorhergesehene gesellschaftliche Fehlentwicklungen oder Datenschutzskandale.

Empfehlungen zur Gestaltung:

- Frühzeitige Förderung der Medienkompetenz ab dem Vorschulalter. Möglichkeiten zur kontinuierlichen Weiterbildung und Informationen zu Fragen aktueller technischer Entwicklungen bauen die Kompetenz der Nutzer weiter aus.
- Vorgaben und Rahmenbedingungen zur Vereinfachung der Sicherheitsfunktionen, insbesondere durch die Einbeziehung des branchenspezifischen Wissens, um eine Balance zwischen Komfort und Sicherheit zu erreichen.
- Intensivierung der Technikfolgenabschätzung im Bereich mobiler Endgeräte und Kommunikation. Beispielsweise haben drahtlose Körpersensoren und erweiterte Realität (Augmented Reality) das Potenzial, über längere Zeiträume entwickelte gesellschaftliche Normen tiefgreifend zu erschüttern.
- Förderung und Begleitung eines gesellschaftlichen Dialogs zu neuen Formen des digitalen Miteinanders. Dies reicht von Regeln zur Nutzung allgegenwärtiger und eingebetteter IT-Systeme bis zur umfassenden Weiterentwicklung des Themas Datenschutz.

3.6 AUSBLICK

Die Nutzung digitaler Mobilität ist im heutigen Alltag, ja in der derzeitigen Kultur, nicht mehr wegzudenken. Zu vielfältig, praktisch und allgegenwärtig sind ihre Anwendungen – und fast täglich kommen neue Dienste hinzu. Um diese effektiv nutzen zu können, müssen Voraussetzungen geschaffen werden, welche zentrale Bereiche wie den Netzzugang, die mobilen Endgeräte, die mobil nutzbaren Anwendungen sowie den Datenschutz und die Datensicherheit umfassen. Erst wenn Anforderungen aus all diesen Bereichen – und die Erwartungslagen der Nutzer – zufriedenstellend erfüllt sind, ist digitale Mobilität »immer und überall« effektiv und sicher durch die Nutzer einsetzbar. Hierfür sind Zivilgesellschaft, Wirtschaft und öffentliche Hand zum Spiegeln der Sinnhaftigkeit aktueller Entwicklungen gleichermaßen gefragt.

In Abhängigkeit von den oben aufgezeigten Handlungsfeldern digitaler Mobilität bestimmt sich der Grad der digitalen Mobilität. Eine der wichtigen gesamtgesellschaftlichen Aufgaben der kommenden Jahre wird es sein, diesen Grad der digitalen Mobilität so auszugestalten, dass er optimal auf die jeweiligen Bedürfnisse der Nutzer, die kollektiven Bedürfnisse der Wirtschaft und die umfassenden Bedürfnisse der Gesellschaft abgestimmt werden kann. Die beschriebenen Empfehlungen zeigen auf, welche technischen, organisatorischen und rechtlichen Voraussetzungen dafür erfüllt sein müssen.

Medienkompetenz und Technikakzeptanz sind die Schlüssel, um digitale Mobilität so nutzen zu können, dass neue innovative Dienste und echte Mehrwerte für die Gesellschaft entstehen.

»Anwendungen müssen sich situationsbedingt den Mobilitätsbedürfnissen der Benutzer anpassen.«

GEFÖRDERT VOM



Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
jens.fromm@fokus.fraunhofer.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

