Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

FORTSCHRITTLICHE NETZE: FUNDAMENT FÜR ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

Jens Fromm, Carsten Schmoll, Jens Tiemann, Mike Weber

Kompetenzzentrum Öffentliche IT

IMPRESSUM

Autoren:
Jens Fromm, Carsten Schmoll, Jens Tiemann, Mike Weber

Grafik:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3436-7173
Telefax: +49-30-3436-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage August 2013

VORWORT

Netze zur Übertragung von Sprache, Daten, Dokumenten und Multimedia-Inhalten begleiten uns heutzutage im privaten und im beruflichen Umfeld tagtäglich. In vielen Lebenslagen sind diese Kommunikationsnetze für den Nutzer unsichtbar. Oft sind wir uns der Technik im Hintergrund gar nicht bewusst, weil das genutzte Endgerät per Funkschnittstelle auf Netze zugreift oder wir uns an viele Anwendungen gewöhnt haben.

Gleichzeitig steigt die Bedeutung der Netze. Immer mehr Vorgänge sind von reibungsloser Kommunikation abhängig. Damit werden Netze zu kritischen Infrastrukturen, von deren Funktionieren die Wirtschaft, die Zivilgesellschaft und die öffentliche Hand abhängig sind. Netze dienen sowohl als Zugang wie auch als Basis für die Schaffung und Neugestaltung öffentlicher Räume. Sie bilden das Fundament der öffentlichen IT.

Verlässlichkeit, Verfügbarkeit und Sicherheit sind essenziell für Infrastrukturen und gewinnen durch den Bedarf an IT in vielen Domänen rasant an Bedeutung. Dabei muss die richtige Balance zwischen diesen Eigenschaften immer wieder neu definiert werden: Einerseits sollen Netze überall verfügbar sein, andererseits müssen Sicherheitsfragen angemessen berücksichtigt werden.

Der verstärkte Einsatz von IT in Bereichen wie Verwaltung, Gesundheit, Verkehr und Energie bedingt somit neue Herausforderungen für alle Akteure. Die Nutzung des Internets hat eine Dynamik entwickelt, die faktisch seine Weiterentwicklung durch die Technik bestimmt. Gesellschaftliche Implikationen können oft erst im Nachhinein diskutiert werden. Durch das Konzept der öffentlichen IT wird in einem ganzheitlichen Ansatz versucht, die bestehenden Herausforderungen offen und transparent anzugehen. Dazu bedarf es eines grundlegenden Verständnisses für die Funktionsweise und das Entwicklungspotenzial von Netzen.

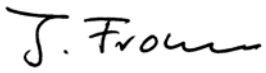
Der öffentlichen Hand als Akteurin im öffentlichen Raum fallen mindestens zwei Aufgaben zu: Neben der vorbildhaften Beteiligung am Austausch von Informationen im öffentlichen Raum obliegt ihr auch die Gestaltung und Sicherung dieser Räume. Dazu ist eine Diskussion über das Verständnis, die Prinzipien und die Entwicklung fortschrittlicher Netze unabdingbar. Diese fortwährende Diskussion muss die Weiterentwicklung der Netze im öffentlichen Raum prägen.

Die Ausgestaltung von Nutzungsszenarien öffentlicher IT macht eine strukturierte, planmäßige und kontinuierliche Modernisierung von Netzen und Netzzugängen notwendig. Im Zentrum sollte dabei eine dynamische, automatische Konfiguration der Netze stehen, sodass die weiter rapide wachsenden Anforderungen erfüllt werden können. Eine automatisierte Konfiguration wird besser in der Lage sein, Fehlkonfigurationen zu minimieren und damit die Sicherheit und Leistungsfähigkeit komplexer Netzstrukturen zu erhöhen. Die dafür notwendige, regelbasierte Netzinfrastruktur ermöglicht zugleich den gestalterischen Einfluss auf den Betrieb der Netze wie auch den Nachweis des ordnungsgemäßen Betriebs und sichert damit die Ausübung der Verantwortung, die der Staat bezüglich der Netze im öffentlichen Raum hat.

Der Umbau der Netze ist ein permanenter und langwieriger Prozess, da Erfahrungen für den Umgang mit neuen Mechanismen in Netzen aufgebaut werden müssen. Es wird ein Paradigmenwechsel stattfinden müssen, weg von starren Konzepten, die der Entfaltung vieler Potenziale neuer Anwendungen und Endgeräte entgegenstehen und trotzdem die Sicherheit von Infrastrukturen und Daten immer weniger gewährleisten können, hin zu Infrastrukturen – auf Basis von Standards –, die durch Strukturen, Berechtigungen und Kommunikationspfade überschaubarer und überprüfbarer werden.

Ich wünsche Ihnen eine anregende Lektüre und freue mich auf die Diskussion zu diesem grundlegenden Thema der öffentlichen IT.

Berlin im August 2013



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

1. NETZE – EINE EINFÜHRUNG

Das Internet durchdringt viele Lebensbereiche. Der Erfolg des Internets hat einen erheblichen Einfluss auf Kommunikation und Arbeitsprozesse. Die Anzahl der vernetzten Geräte steigt stetig und neue, mobile Endgeräte setzen die Vision einer allgegenwärtigen elektronischen Kommunikation um. Sie steigern damit auch die Zahl der Interaktionen, die über solche Kommunikationsnetze abgewickelt werden. Nicht zuletzt gehen dabei vom Internet starke Impulse auf die zwischenmenschliche Kommunikation aus. Arbeitsprozesse lassen sich einfacher, schneller und effizienter gestalten, neue Marketing- und Vertriebskanäle tun sich auf und neue, internetspezifische Wirtschaftszweige entstehen. Die entscheidende Entwicklung ist aber, dass Netze zunehmend nicht nur zur klassischen Automatisierung bekannter Prozesse eingesetzt werden, sondern sich auch ganz neue Modelle der Zusammenarbeit und des Zusammenlebens eröffnen, wie sie beispielhaft bei der Softwareentwicklung und im kulturellen Bereich bei der Komposition neuer Werke sichtbar werden.

Diese tief greifenden Veränderungen basieren auf Netzen, denen bereits heute bedeutende gesamtgesellschaftliche Potenziale zugeschrieben werden.[1] Netze bilden die Grundlage für technisch verstandene Kommunikationssysteme, die wiederum elektronische Kommunikation ermöglichen. Netze werden so zum wesentlichen Fundament für öffentliche IT und die durch sie geschaffenen öffentlichen Räume.[2]

Herausforderungen und Anforderungen an fortschrittliche Netze lassen sich in allen Gesellschaftsbereichen und Anwendungsdomänen in vergleichbarer Weise formulieren. Für die öffentliche Verwaltung ergeben sich Chancen und Pflichten, sich an dieser technologischen Entwicklung zu beteiligen. Beispielhafte Trends sind hier OpenData und OpenGovernment, aber eben auch die schon längst gestarteten Innovationen im E-Government, die aufgrund der dynamischen Entwicklung im Bereich der Netze und Anwendungen auf immer neue Geräte, Dienste, Anwendungen und Erwartungen treffen. Darüber hinaus müssen Netze der Verwaltung aber auch das Vorbild für ein Zusammenspiel von IT im öffentlichen Raum sein.

Dieses Papier stellt grundsätzliche Eigenschaften technischer Kommunikationsnetze (im Folgenden kurz: Netze) dar, um mögliche Weiterentwicklungen und sich daraus ergebende Konsequenzen für Aufbau und Betrieb fortschrittlicher Netze zu erläutern. Im Mittelpunkt stehen dabei der sichere und nahtlose Austausch von Informationen und sich daraus ergebende Bedingungen zur Förderung dieser Entwicklungen.

1.1 BEGRIFFE

Die fundamentale Bedeutung der Netze spiegelt sich in zahlreichen sprachlichen Analogien wider. Gesellschaftlich gefasste Begriffe wie Netz, Netzwerk und Kommunikationssystem finden ihr gleichnamiges Pendant in der Informationstechnologie.

Kommunikation im Sinne öffentlicher IT bezeichnet ganz allgemein den Austausch von Informationen, unabhängig vom genutzten Weg. Darunter fällt auch die in dieser Betrachtung im Mittelpunkt stehende elektronische Kommunikation über Kommunikationsnetze. Kommunikationsnetze sind komplexe technische Systeme, d. h. eine Gesamtheit von Komponenten, die im Zusammenspiel eine Aufgabe erfüllen und deshalb als Einheit angesehen werden können. Die Interaktion der einzelnen Komponenten oder Geräte wird bei den hier betrachteten technischen Kommunikationssystemen dadurch erschwert, dass sie häufig unter der Hoheit verschiedener Betreiber stehen.

Zur Verringerung der technischen Komplexität können Kommunikationssysteme in logische Einheiten zerlegt werden, die einzelne Dienste zur Erfüllung definierter Aufgaben erbringen. Grundlegende Dienste lassen sich dann wie bei einem Baukastensystem zu höherwertigen Diensten kombinieren, bspw. kann eine Übertragung um eine Verschlüsselung ergänzt werden. Eine Anwendung wird in diesem Zusammenhang als IT-Lösung verstanden, die direkt im Auftrag eines Benutzers agiert und dabei ggf. auf die Nutzung verschiedener Dienste zurückgreift. Die Begriffe Anwendung und Dienst werden aufgrund des geringen inhaltlichen Unterschieds im Folgenden synonym verwendet.

Im Zentrum der Betrachtungen von fortschrittlichen Netzen für die öffentliche IT stehen der Bereich um den Netzzugang zum Internet bzw. Mechanismen an der Schnittstelle zwischen dem Internet und den lokalen Netzen.[3] Die Ausgestaltung dieses Übergangs hat wesentlichen Einfluss auf die Gestaltung des beschriebenen öffentlichen Raums. Hier ist der möglichst einfache Zugang realisiert, der beispielsweise für Bürgerinnen und Bürger besonders wichtig ist. An dieser Schnittstelle werden auch die Angebote und Informationen bereitgestellt, aufgrund

Abbildung 1: Öffentlicher Raum zur Veranschaulichung öffentlicher IT

von Interessen der Akteure oder weil beispielsweise Organisationen dazu verpflichtet sind. Daneben gibt es selbstverständlich weite Bereiche der Nutzung von Netzen zur privaten oder vertraulichen Kommunikation. In diesem Bereich spielt öffentliche IT nur insoweit eine Rolle, als sie den Zugang zur elektronischen Kommunikation ermöglicht.

Der öffentliche Raum ist also keinesfalls mit dem Internet gleichzusetzen. Der öffentliche Raum entsteht auf Grundlage öffentlich verfügbarer IT-Dienste und Datenangebote. Er basiert auf dafür notwendiger Infrastruktur für Bereitstellung und Kommunikation, auch wenn sich diese in privater Hand befindet oder nicht direkt Teil des Internets ist.

»Der öffentliche Raum ist keinesfalls mit dem Internet gleichzusetzen.«

1.2 EIN NETZ FÜR ALLE(S)

Der Begriff »Internet« steht für zwei wesentliche Entwicklungen: einerseits als konkrete Kopplung von Netzen aller möglichen Betreiber oder Anwender und andererseits als eine Sammlung gemeinsamer Technologiestandards, der Internetprotokolle (auch bei Verwendung in lokalen, abgeschlossenen Netzen, im Intranet). Sowohl die Kopplung von Netzen als auch die Verwendung einheitlicher Protokolle führen zu großen Vorteilen für die Anwender, wie z. B. die durchgängige, einfache Erreichbarkeit anderer Anwender und die Verfügbarkeit von leistungsfähiger Hard- und Software. Daher kam und kommt es zu einem weiten Vordringen des Internets und von Internettechnologie in alle Lebens- und Technikbereiche, bspw. in die Telefonie, Mobilkommunikation und in die Steuerungstechnik der Industrie. Ein Schwerpunkt der folgenden Betrachtungen liegt dabei zunächst auf der Eigenschaft als Transportnetz, d. h., verschiedene Anwendungen nutzen eine gemeinsame Basisinfrastruktur und bieten darüber Dienste für verschiedene Anwendungsgebiete an. Dies bedeutet aber auch, dass sich das Internet als eine Basisinfrastruktur etabliert hat: Jeder braucht einen Zugang, und es besteht eine immer stärkere Abhängigkeit vom Funktionieren dieser Infrastruktur und seiner Mechanismen. Das Internet wird zu einer kritischen Infrastruktur.[4] Dies führt zu zwei wesentlichen Forderungen: Die Nutzung verschiedener, redundanter und/oder gesicherter Netzinfrastrukturen ist zwingend notwendig, und die Sicherheit der eingesetzten Mechanismen und Konfigurationen muss gewährleistet sein.

1.3 EVOLUTION IM NETZ, REVOLUTION IM ENDGERÄT

Die Internettechnologie basiert auf dem Ende-zu-Ende-Prinzip. Dabei erfolgt die Steuerung der Kommunikation über das Endgerät. Das Netz ist vergleichsweise einfach und robust gehalten, erst die Anwendungen auf dem Endgerät stellen dienstspezifische Kommunikationsfunktionen zur Verfügung, wie z. B. für Telefonie oder für die Übertragung von Webinhalten. Im Netz werden Nutz- und Steuerdaten über einen gemeinsamen Kommunikationskanal übertragen, was ein sehr einfaches und offenes Modell der digitalen Kommunikation ermöglicht. Ein Eingriff in diesen Kanal, beispielsweise durch Filterung oder Konvertierung von Daten, kann weitreichende technische Folgen haben, da dies grundlegende Annahmen über die Nutzung dieser Übertragungsstrecke verletzt und dazu führen kann, dass Anwendungen sich nicht wie geplant verhalten.

Das Internet ist also zunächst ein globales Transportnetz, und Kommunikationsvereinbarungen müssen durch die Endgeräte eingehalten werden. Einerseits macht dies es schwierig, neue Funktionen im Internet einzuführen. Andererseits bedeutet dieses Modell aber auch eine Stärke des Internets, sichtbar in all den Internet-Start-up-Unternehmen: Immer neue, bisher nicht

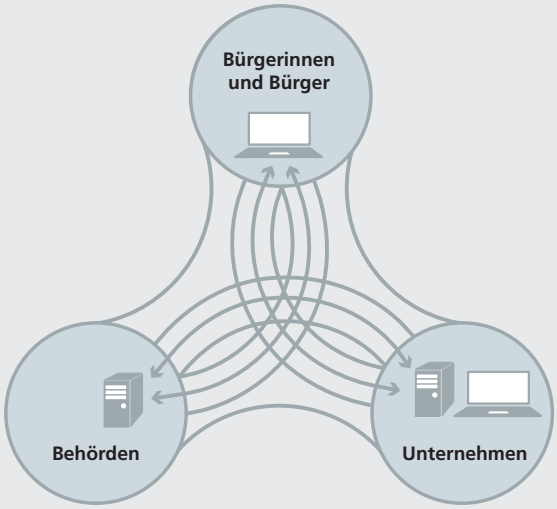


Abbildung 2: Die Analogie des öffentlichen Raums im Internet

2

gedachte Dienste und Anwendungen können über vergleichsweise einfache Datenübertragungsschnittstellen über das Internet realisiert werden. Ohne jede Vorbereitung im Netz sind schon zwei Endgeräte mit der gleichen Anwendung in der Lage, etwas Neues zu starten. Das Internet und seine Technologien stellen also eine verlässliche Basisinfrastruktur zur Verfügung, die sich nur langsam und evolutionär ändern kann. Damit bietet es auch Verlässlichkeit und universelle Verfügbarkeit, die Entwickler und Anbieter von Anwendungen und Endgeräten benötigen. Diese können sich darauf verlassen, dass ihre Entwicklungen überall von den Anwendern genutzt werden können.

Das Endgerät und die Anwendungen sind das, was der Benutzer vom Netz sieht, und hier findet die Differenzierung der Anbieter statt, auch in Bezug auf Design oder Image. Diese aus technischer Sicht ursprünglich sekundären Eigenschaften tragen mittlerweile erheblich zu Bedienbarkeit und Akzeptanz von technischen Geräten bei. Im Bereich der Mobilkommunikation und beim Erfolg der Tablets ist es augenfällig: Die Endsysteme sind der eigentliche Treiber für die Nutzung und Weiterentwicklung der Netze.

1.4 STANDARDS, STANDARDS, STANDARDS

Die Zeiten der »Browserkriege«[5] sind lange vorbei, heute setzen sich mehr und mehr Standards durch. In der ersten Phase der stürmischen Entwicklung der Internetnutzung war es schwierig, leistungsfähige Funktionen auf eher schwächerer Hardware zu implementieren. Immer neue, populäre Funktionen wurden und werden von Herstellern genutzt, um sich Vorteile am Markt zu sichern. Inkompatible Zusatzfunktionen spielten eine große Rolle, als noch keine leistungsfähigen Standards verfügbar waren, und verhinderten eine herstellerübergreifende Nutzung von eigentlich standardisierten oder standardisierbaren Produkten und Diensten.

In Zeiten schneller technischer Innovationen entwickelt sich die Standardisierung nicht immer äquivalent. Inzwischen haben sich jedoch leistungsfähige Konzepte etabliert und entsprechende Standards sind verfügbar. Dies geschah auch auf Druck von Kunden und Anwendern, die offene und interoperable Lösungen bevorzugen. Die Normung im Umfeld von Netzen und IT ist wesentlich diffuser aufgestellt als die klassische Normung durch formale Organisationen. Maßgeblich sind Gremien wie die Internet Engineering Task Force (IETF) oder das World Wide Web Consortium (W3C), aber auch Industriekonsortien und -standards spielen eine wichtige Rolle. Oft findet sich ein anderes Herangehen an die Neuentwicklung von Systemen: Die komplette, detaillierte Spezifikation bis ins letzte Detail wird weniger wichtig im Vergleich zu einer Kombination bestehender Standardkomponenten, einer Konfiguration im Hinblick auf »Best Practices« oder der kontinuierlichen Optimierung und Weiterentwicklung einzelner Systembestandteile. Nur so lassen sich bspw. komplexe Mobilfunksysteme mit immer neuen Funktionen und unter Einbeziehung neuester Funktechniken in kurzen Innovationszyklen entwickeln oder kurzfristig Sicherheitslücken in IT-Systemen effektiv und umfassend beheben. Die Gefahr einer Abhängigkeit von einzelnen Herstellern bzw. bestimmten Technologien und Komponenten muss dabei im Auge behalten werden.

[1] BITKOM und Fraunhofer ISI (Hrsg.), Gesamtwirtschaftliche Potenziale intelligenter Netze in Deutschland, Langfassung des Endberichts, 2012. http://www.bitkom.org/60376.aspx?url=Studie_Intelligente_Netze(2).pdf&mode=0&b=Publikationen&bc=Publikationen%7cStudien+%26+Grundsatzpapiere

[2] Jens Fromm, Petra Hoepner, Mike Weber und Christian Welzel, Öffentliche Informationstechnologie: Abgrenzung und Handlungsfelder, Juni 2013, ISBN: 978-3-9816025-0-0. http://www.oeffentliche-it.de/documents/18/80d3742e-2efe-43c3-9a78-9e3a6446b4da

[3] Nicht betrachtet werden in dieser Darstellung virtuelle Firmennetze über das Internet oder private Netze zwischen Standorten auf Basis von dedizierten Weitverkehrsverbindungen.

[4] Mehr Informationen und eine Definition des Begriffs kritische Infrastrukturen findet sich unter http://www.kritis.bund.de

[5] Internet Explorer gegen Netscape – als Folge wurden neutrale Standards vernachlässigt und Webseiten für die Betrachtung mit einer bestimmten Browsersoftware optimiert. http://de.wikipedia.org/wiki/Browserkrieg

2. HERAUSFORDERUNGEN

Im Zugangsbereich bewegen sich Netzinfrastrukturen im Wechselspiel von offenem und geschlossenem Betrieb. Für den offenen Betrieb stehen beispielhaft der freie Zugang zu Informationen eines Webservers oder die Bereitstellung eines temporären oder dauerhaften Internetzugangs für PCs und mobile Geräte. Im Gegensatz dazu steht der geschlossene Betrieb mit der verteilten Verarbeitung von vertraulichen Informationen. Netze müssen heute beiden Anforderungen genügen, gegebenenfalls sogar auf den gleichen Endgeräten, und zudem ihre Dienste dynamisch bereitstellen.

2.1 LOKALE NETZE ÖFFNEN SICH

Ein Leistungsmerkmal von Netzen (neben Bandbreite, Verzögerungszeit u. Ä.) ist die Flexibilität, mit der verschiedenste Dienste und Anwendungen unterstützt werden können. Die Einführung einer neuen Anwendung oder eine Änderung der Nutzung sollte möglichst einfach durch das Netz unterstützt und nahtlos umgesetzt werden können.

Ein grundlegendes Sicherheitskonzept für Netze ist die Aufteilung in verschiedene Sicherheitszonen.[6] Über den Einsatz von Paketfiltern (Firewalls) und Gateways wird der Zugriff zwischen diesen Zonen kontrolliert und gesteuert. Dabei ist die Balance zwischen der Flexibilität der Netze und den Sicherheitsanforderungen eine der wichtigsten Herausforderungen.

Der Schwerpunkt lokaler Netze verschiebt sich: Lange Zeit stand das lokale Netz als nicht-öffentliches Intranet im Mittelpunkt der Betrachtung, über dieses sind Arbeitsplätze mit Servern verbunden. Dabei ist das Internet oder ein Zugang zu anderen Weitverkehrsnetzen in diesem Modell wie ein Dienst eingebunden, d. h. »am Rande« des Intranets angesiedelt und mit fest umrissenen Aufgaben versehen (bspw. zur Nutzung weniger, wohlbekannter Dienste über statische und gesicherte Verbindungen). Mit dem Trend zum Outsourcing von IT-Diensten, der Einführung von IP-Telefonie sowie dem Einsatz von immer neuen Anwendungen und Endgeräten schiebt sich der Internetzugang bei der Betrachtung von Netzen immer mehr in den Mittelpunkt.

Auf flexible Weise müssen ganz unterschiedliche Anforderungen für die verschiedenen Nutzungsszenarien erfüllt werden. Mit dem Modell der zentralen Position des Internetzugangs wird die Grundlage dafür gelegt, dass eine wesentlich stärkere, funktionale Betrachtung möglich wird: Lokale, stationäre Arbeitsplätze und mobile Arbeitsplätze können in vielen Betrachtungen gleich behandelt werden. Der Unterschied zwischen dem Zugriff auf eine lokale Anwendung und eine Anwendung, die in ein Rechenzentrum ausgelagert ist, wird aufgehoben.

»Notwendig sind neue Sicherheitskonzepte: Schutz aller Teile der Netze trotz dynamischer Änderung der Kommunikation.«

Die Sicherheitskonzepte müssen an diese Entwicklung angepasst werden: Der Zugang zum Internet (oder zu anderen Netzen, z. B. Verwaltungsnetzen oder Netzen für geschlossene Nutzergruppen) ist breiter geworden und muss verschiedene Anwendungen und Protokolle nahtlos und parallel unterstützen. Die Verwendung von immer mehr Geräten und webbasierten Anwendungen, die Bereitstellung von Funktechnik im Intranet (Wireless LAN) und die Unterstützung von Mobil- und Gastsystemen erfordern außerdem eine Absicherung des lokalen Netzes und von Teilsystemen nach innen.

2.2 NETZWERKMANAGEMENT

Die Vielzahl von Geräten und Anforderungen an ein Netz wird immer schwieriger zu überblicken, insbesondere wenn sich Konfigurationen dynamisch ändern. Hierbei ist es wichtig, den Netzwerkadministrator von Routineaufgaben wie der Gerätekonfiguration zu entlasten. Vielmehr muss der Netzwerkadministrator dazu befähigt werden, die Übersicht über die Netze, die Kommunikationsbeziehungen und die Berechtigungen zu behalten.

Zur Verbesserung der Übersicht über die Netze gehört die Nutzung von Monitoring-Systemen, die sowohl zur Entdeckung aktueller Probleme (z. B. Fehlfunktionen, Sicherheitsprobleme) als auch zur Netzplanung (z. B. Analyse und Vorhersage der Nutzung von Ressourcen) herangezogen werden können.

Ein automatisiertes Management von Netzen kann die Leistungsfähigkeit des Netzes optimieren, und Fehlkonfiguration

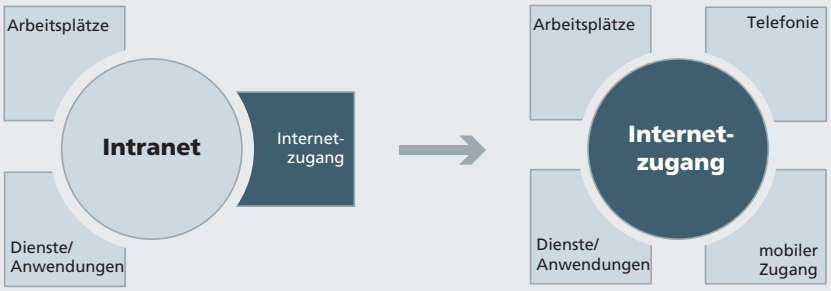


Abbildung 3: Die Öffnung lokaler Netze

3

verhindern, die Sicherheitsprobleme zur Folge hätten. Derartige Systeme werden schrittweise eingeführt, die verschiedenen Akteure im öffentlichen Raum sind hierbei unterschiedlich weit. Für Bürgerinnen und Bürger werden diese Aufgaben von den Betriebssystemen und den Internetzugangsanbietern in Form einer Grundversorgung mit übernommen. In der Wirtschaft spielen Kostenüberlegungen eine große Rolle. Deshalb werden derartige Netzwerkmanagementsysteme in einigen Unternehmen bewusst eingeführt, um die genannten Vorteile zu erzielen. In anderen Unternehmen ist die Netzinfrastruktur veraltet, aber aus Mangel an Fachwissen oder wegen fehlender finanzieller Mittel kann keine Abhilfe geschaffen werden.

Die Einführung derartiger Systeme bzw. die Weiterentwicklung der Netzwerkinfrastruktur erfordert allerdings einige Vorbereitung: Aufgrund der langfristigen Investitionszyklen bei Infrastrukturkomponenten dauert es eine lange Zeit, bis notwendige Funktionen im Netz vorhanden sind. Die Einführungsphase neuer Funktionen im Netz muss gleichzeitig dazu genutzt werden, Erfahrungen mit neuen Konzepten zum Netzwerkmanagement zu sammeln. Sichere Netze lassen sich nur betreiben, wenn das Verhalten der Netzkomponenten vorhersehbar und die Grenzen des Funktionsumfangs der einzelnen Komponenten bekannt sind. Gleichzeitig muss Vertrauen in die Funktionsfähigkeit dieser automatisierten Systeme vorhanden sein.

2.3 FLEXIBILISIERUNG VON INFRASTRUKTUREN

Gerade bei der Nutzung externer Dienste (z. B. bei Cloud-basierten Diensten), und im Bereich der mobilen Zugangsnetze ist weiterhin eine dynamische Entwicklung festzustellen. Die Auslagerung von Diensten verspricht große Potenziale zur Senkung von Kosten oder Erhöhung der Leistungsfähigkeit, aber noch sind nicht alle rechtlichen und politischen Konsequenzen absehbar.[7]

Es besteht ein erhebliches Risiko, dass die Bewertung der Nutzung dieser Technologien sich nach einem möglichen Datenschutz-Skandal erheblich wandelt. Ganz im Sinne des Cloud-Ansatzes sollte darauf geachtet werden, externe Dienste in standardisierter Weise anzusprechen und einzukaufen. Entsprechend den aktuellen Rahmenbedingungen können diese Dienste dann intern oder extern betrieben und vergleichsweise leicht verschoben werden, auch zwischen verschiedenen externen Anbietern.

Es ist davon auszugehen, dass es zu weiteren wirtschaftlichen Umwälzungen in der IT-Welt kommen wird. Internet- und Mobilfunkanbieter stehen vor Herausforderungen durch die steigenden Datenraten und den Kostendruck im Anschlussbereich, ohne bisher relevante neue Geschäftsmodelle entwickeln zu können (wie die geplante Einführung und Relativierung der Volumenbeschränkung beim DSL-Anschluss der Deutschen Telekom gezeigt hat[8]). Zusammen mit dem starken Wachstum einzelner Internetfirmen zeigt dies, dass man nicht von langfristig stabilen Verhältnissen ausgehen kann. Gleichzeitig muss aber das Vertrauen in extern genutzte Basisdienste im öffentlichen Raum für Zivilgesellschaft, Wirtschaft und Verwaltung gegeben sein.

»Flexible Infrastrukturen minimieren das Nutzerrisiko, das durch volatile Geschäftsmodelle rund um das Internet entsteht.«

Das schnelle Wachstum von Netzen und Anwendungen führt in einigen Bereichen auch immer wieder zu einer Vielzahl an Lösungen und Konfigurationen, wodurch es schwer wird, alle Seiteneffekte im Netz zu überblicken. Auch die Planung der Netze ging oft von viel geringeren Anforderungen aus und kann so den aktuellen Erwartungen nicht standhalten. Notwendig werdende Ad-hoc-Lösungen zur schnellen Einführung eines

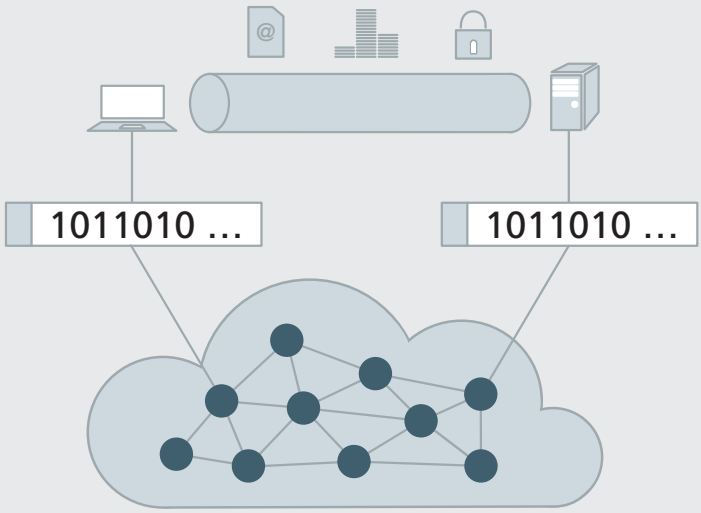


Abbildung 4: Schematische Darstellung des Ende-zu-Ende-Prinzips

4

Dienstes können neue Probleme schaffen. Eine planmäßige und strukturierte Einführung neuer Dienste und Komponenten sowie ein strategischer Netzausbau können dazu beitragen, gewachsene Infrastrukturen zu konsolidieren und im Sinne der Kosteneffizienz und Sicherheit zu optimieren.

2.4 INTEROPERABILITÄT

Die zunehmende Vernetzung verlangt auch eine zunehmende Interoperabilität zwischen Bürgern, Wirtschaft und öffentlicher Verwaltung. Im Hinblick auf die öffentliche IT ist u. a. die (Weiter-)Entwicklung höherwertiger Funktionen der Kommunikation, wie bspw. Verschlüsselung prioritär. Jedoch steigt der Aufwand für die Sicherstellung von Interoperabilität mit der Komplexität der Funktionen. Interoperabilität ist technisch nicht allein von der Einhaltung der Standards abhängig, sondern beinhaltet in der Praxis auch abgestimmte Konfigurationen. Für eine erfolgreiche, gesicherte Kommunikation ist also nicht nur das gleiche Verschlüsselungsverfahren auf beiden Seiten eine Voraussetzung, ebenso muss auch die Verwendung von Parametern wie der Schlüssellänge abgestimmt sein. Mit steigendem Datenaustausch gewinnen auch nicht-technische Aspekte der Interoperabilität an Bedeutung, bspw. rechtliche und organisatorische Fragestellungen.[9]

Ein wichtiger Aspekt für die technische Interoperabilität über Grenzen hinweg ist die Betrachtung der Kommunikation von Anfang bis Ende, gerade in der Zusammenarbeit zwischen unterschiedlichen Akteuren aus verschiedenen Domänen oder bei der Nutzung externer Dienste. Solange der Einsatz mehrerer Firewalls oder mehrfacher Verschlüsselung keinen zusätzlichen Sicherheitsgewinn bringt, wird lediglich die Leistungsfähigkeit der Übertragung und die Anwendung beeinträchtigt und ein nahtloses Zusammenwirken von IT erschwert. Alle beteiligten Kommunikationspartner sollten daher die Anforderungen und Risiken einer Kommunikationsbeziehung bewerten und darauf abgestimmte Sicherheitsmechanismen einsetzen. Schutzbedarfsanalysen gewinnen zunehmend an Bedeutung, auch wenn sie gegenwärtig eher eine Momentaufnahme darstellen und noch nicht die Dynamik der Entwicklung im Bereich von Netzen unterstützen. Es geht nicht in erster Linie darum, alles gleich stark zu schützen, sondern genau zu evaluieren, welche Sicherheitsniveaus für welche Dienste notwendig sind. Eine Möglichkeit der effizienteren Abstimmung ist hier der verstärkte Einsatz von Referenzarchitekturen, die praktische Richtlinien für den Aufbau von Netzen vorgeben. So kann eine Vergleichbarkeit von Infrastrukturen ermöglicht und die Interoperabilität zwischen den Systemen verbessert werden.

Durch die Förderung von Nutzungsszenarien, Referenzarchitekturen und Leitlinien kann der Staat gestaltend auf die Rahmenbedingungen zur Weiterentwicklung von Netzinfrastrukturen im öffentlichen Raum einwirken.

»Interoperabilität muss die Kommunikation von Anfang bis Ende betrachten.«

[6] Bundesamt für Sichheit in der Informationstechnik (BSI), Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA). https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/ISi-Reihe/ISi-LANA/lana_node.html

[7] Directorate-General for Internal Policies of the Union, Policy Department C: Citizens' Rights and Constitutional Affairs (Hrsg.), Fighting cyber crime and protecting privacy in the cloud, European Parliament, October 2012. http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

[8] Bericht der Bundesnetzagentur vom 14. Juni 2013 zur Tarifänderung der Deutschen Telekom AG für Internetzugänge vom 02. Mai 2013. http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Verbraucher/Breitband/Netzneutralitaet/Bericht_Bundesnetzagentur_14_Juni_2013.pdf?__blob=publicationFile&v=1

[9] »In Anlehnung an das European Interoperability Framework der Europäischen Kommission kann Interoperabilität als Fähigkeit von IKT-Systemen und deren unterstützender Geschäftsprozesse verstanden werden, Daten auszutauschen und das Teilen von Informationen und Wissen zu ermöglichen.« Fraunhofer FOKUS, Zentrum für Interoperabilität. https://www.interoperability-center.com/de/interoperabilitaet

3. LÖSUNGSANSÄTZE

Ausgangspunkt für alle Lösungsansätze sind die dargestellten Überlegungen, wie sich die Aufgaben von Netzen in den nächsten Jahren entwickeln werden. Attraktive Endgeräte treiben die Entwicklung an und führen zu Forderungen der Nutzer an die Netzbetreiber. Die tägliche Nutzung von praktischen, leicht bedienbaren Anwendungen führt zu steigenden Erwartungen an die Verfügbarkeit von Netzen und an die Bereitstellung von Diensten und Anwendungen. Über Funknetze und eingebettete Geräte wird elektronische Kommunikation allgegenwärtig sein, auch in mehr als einem Netz und über mehrere Endgeräte gleichzeitig.

Die Konfiguration und Kontrolle der Vielzahl derartiger Systeme kann zukünftig nur noch automatisiert erfolgen. Die Richtung der Kommunikationsbeziehungen wird auch im Normalfall vielfältiger, weg vom klassischen Download bei der Nutzung von Web-Anwendungen hin zu vielen Datenquellen, verteilt über eine Reihe von Teilnetzen. Beispiele dafür sind die Einführung von IP-Telefonie, Machine-to-Machine-Kommunikation und der verstärkte Einsatz von vernetzten Sensoren. Grundlage für die Konfiguration und Kontrolle muss immer eine Sicherheitsbetrachtung sein. Das Sicherheitskonzept muss in der Lage sein, alle Anforderungen an das Netz abzubilden und dafür den entsprechenden Einsatz von detaillierten technischen Sicherheitsfunktionen darzustellen.

3.1 REGELBASIERTE NETZE

Die Einführung von Regeln und Regelwerken (engl. network policies) für große, komplexe IT-Netze ermöglicht es, Eigenschaften der Netze auf einer höheren Abstraktionsebene zu definieren, als das z. B. durch die Konfigurationseinstellungen einzelner Geräte im Netz geleistet wird. Dies geht nur Hand in Hand mit Netzwerkmanagementsystemen, welche solche Regeln verstehen und in Konfigurationen für Geräte umsetzen können. Dadurch wird der Betrieb des Netzes in weiten Teilen automatisiert, der Netzwerk-Administrator behält die Übersicht und kann sich stärker um die Planung, den Ausbau und die Sicherheit der Netze kümmern. Die Nutzung von Netzwerkregeln anstatt starrer Konfigurationen auf den Geräten bedarf eines initialen Aufwands zum Entwurf eines sicheren und leistungsfähigen Netzes und seiner angebotenen Dienste. Anschließend sorgt die Automatisierung dafür, Widersprüche in Konfigurationen und ungewöhnliche Nutzungsmuster zu entdecken, die auf eine fehlerhafte oder missbräuchliche Nutzung der Infrastruktur hindeuten.

Die Nutzung abstrakter Regelsätze ist der Einstieg zu einem leistungsfähigeren Management von Netzen: Selbstorganisierende Komponenten können immer größere Teile des technischen Managements übernehmen und werden durch wenige, aber verbindliche Vorgaben aus dem jeweiligen Zuständigkeitsbereich gesteuert. Das ermöglicht auch die direkte Einbindung einer Regulierung, die als eine Instanz zur Steuerung des Netzes Vorgaben machen kann. Das Netz wiederum weist nach, dass es entsprechend dieser Vorgaben arbeitet, und alarmiert in Echtzeit, wenn es aufgrund von Störungen zu einer Verletzung dieser Vorgaben kommt.

3.2 EINSATZ VON VIRTUALISIERUNGSTECHNIKEN

Die Leistungsfähigkeit und Flexibilität heutiger Hardware ermöglicht die Nutzung von Virtualisierungstechniken. Dabei werden virtuelle Laufzeitumgebungen für Anwendungen, Computer und auch Netze erzeugt, um die Ressourcen realer Hardware besser ausnutzen zu können. Vorhandene Ressourcen können aufgeteilt werden, um diese gleichzeitig für verschiedene Aufgaben nutzen und dabei trotzdem eine sichere Trennung vornehmen zu können. Für den Einsatz von Virtualisierungstechniken müssen Netze eine ausreichende Bandbreite und eine sehr gute Verfügbarkeit bereitstellen.

Virtualisierungstechniken sind in der IT- und Netzwerktechnik schon lange bekannt. Vergleichsweise neu sind die dynamische Verwendung dieser Technologien und das Vordringen in alle Leistungsklassen von Geräten. Virtualisierungstechniken bieten einen Ansatz für die Realisierung von feingranular steuerbaren Systemen, wie sie als regelbasierte Netze zuvor beschrieben wurden.

Auch die Forschung im Bereich Future Internet[10] beschäftigt sich intensiv mit den beschriebenen Ansätzen. Mithilfe intelligenter, autonom entscheidender Systeme sollen Dienste und Netzwerkfunktionen bereitgestellt werden. Virtualisierungstechniken werden auch dazu vorgesehen, die Migration der umfangreich bestehenden Infrastrukturen in zu entwickelnde, neue Netze zu ermöglichen.

IPV6 BASIERT AUF DEN BEKANNTEN UND BISHER SEHR ERFOLGREICHEN INTERNET-DESIGNIDEEN UND MACHT DIESE ZUKUNFTSSICHER

3.3 STANDARDS IN EINEM DYNAMISCHEN UMFELD

Die Aufgaben von Netzen werden vielfältiger und umfassen komplexere Funktionen. Investitionen in Anwendungen müssen über lange Laufzeiten geschützt werden. Bei der fortschreitenden Auslagerung von Diensten muss die nötige Flexibilität gegeben sein, diese von verschiedenen Anbietern oder auch in Eigenregie bereitzustellen. Aufgrund all dieser Anforderungen ist die Nutzung und die strategische Auswahl von Standards unerlässlich.

»Standardisierung ist die Grundlage für Innovationen und Dynamik.«

Das dynamische Umfeld der Netze ist traditionell ein Gebiet mit gut verfügbaren und wirksamen Standards. Wie beschrieben spielen Foren und Konsortien mit Teilnahme von Industrie und Anbietern im Bereich der IT-Standardisierung eine wichtige Rolle. In verschiedenen Anwendungsgebieten haben sich führende Konsortien herausgebildet, die auf bestehende Standards aufsetzen und diese weiterentwickeln. Für die Sicherstellung der Interoperabilität zwischen verschiedenen Produkten im Bereich der Netze reichen Standards allein nicht aus, da konkrete Konfigurationen im dynamischen Netzumfeld nicht hinreichend berücksichtigt werden können. Daher spielen Best Practices und Leitlinien eine wichtige Rolle. Insofern muss die Standardisierung inklusive Umfeld beobachtet werden, um technologische Entwicklungen abzuschätzen und deren führende bzw. relevante Standards und Standardisierungsgremien zu identifizieren. Entscheidend dafür sind auch offene Standards, die für alle Marktteilnehmer besonders leicht zugänglich, einsetzbar und weiterentwickelbar sind.

Nutzergruppen der verschiedenen Anwendungsbereiche sollten auf eine ständig aktualisierte Auswahl relevanter Standards setzen und diese als Grundlage ihrer Arbeit nutzen. Gerade der Erfolg der Internetprotokolle und von Web-Anwendungen hat gezeigt, dass sich zukunftssichere Standards dadurch auszeichnen, dass sie wie Bausteine immer wieder für andere oder neue Anwendungen eingesetzt werden können. Sind diese Bausteine identifiziert, kann man Hersteller und Dienstanbieter finden, die zukunftssichere und offene Lösungen auf ihrer Basis anbieten oder erstellen.

In den Bereichen Anwendung von Standards und Best Practices, die in der sich schnell wandelnden technologischen Entwicklung fast die gleiche Bedeutung wie die Standards selbst haben, ist es vergleichsweise einfach, eigene Erfahrungen für verschiedene Anwendungsszenarien aufzubauen und sie Technologiepartnern und der eigenen Nutzergruppe oder der Öffentlichkeit bereitzustellen. Dabei werden typische und relevante Szenarien erstellt, die dann von verschiedenen Seiten diskutiert werden können und dadurch auch die Anbieter von Systemen bei der Weiterentwicklung ihrer Angebote unterstützen.

In diesem Sinne sollten Standards auch als Instrument für den Dialog zwischen Anbieter und Nutzer gesehen werden. Die Berücksichtigung der vielfältigen Interessen (z. B. Datenschutz und diskriminierungsfreier Zugang) bei Aufbau und Nutzung von IT-Systemen im öffentlichen Raum ermöglicht eine Vorbildfunktion. Darüber hinaus lassen sich hierdurch Partnerschaften für den Bereich der kritischen Infrastrukturen aufbauen, die durch transparente Anforderungen und Roadmaps Planungssicherheit für beide Seiten geben.

3.4 KONSEQUENTE EINFÜHRUNG VON IPV6

Ein entscheidender Standard für die Zukunft des Internets ist das Internetprotokoll Version 6 (IPv6). Nach mehr als 20 Jahren Entwicklung und Vorbereitung ist der Zeitpunkt gekommen, jetzt zügig mit der Migration von der alten Version 4 (IPv4) zu IPv6 zu beginnen.

Zum Empfang und Versenden von Nachrichten benötigt jedes Endgerät eine eindeutige und zumindest zeitweise stabile IP-Adresse. Spätestens nachdem im Februar 2012 in Europa die letzten Reserven an freien IPv4-Adressbereichen angebrochen wurden, ist die Situation der Adressknappheit bei IPv4 für alle offensichtlich geworden. Die gegenwärtig eingesetzten Hilfsmechanismen bei der Verwendung von IPv4 können noch die Funktionsfähigkeit der Netze und die Kommunikation gewährleisten, stellen aber keine dauerhafte Lösung dar. Nur die Einführung von IPv6 kann einerseits das ungebremste Wachstum des Internets sowie der Zahl der angeschlossenen Geräte unterstützen und andererseits die weltweite, nahtlose Kommunikation auf Dauer sicherstellen. Dabei gilt der Gewährleistung der Interoperabilität ein besonderes Augenmerk.

Da die Einführung von IPv6 ein länger andauernder Prozess über mehrere Jahre hinweg ist,[11] muss jetzt mit dem Umstieg begonnen werden, auch um die notwendigen Erfahrungen mit der Nutzung des neuen Protokolls zu sammeln. In Deutschland ist das Thema IPv6 durchaus bekannt, es hat allerdings noch nicht zur gewünschten Verbreitung der Technologie im praktischen Einsatz geführt.[12]

IPv6 basiert auf den bekannten und bisher sehr erfolgreichen Internet-Designideen und macht diese zukunftssicher. IPv6 ist allerdings viel mehr als nur „IPv4 mit langen Adressen". Wesentliche Designentscheidungen für IPv6 waren die Einführung der automatischen Konfiguration von Endgeräten, ein einfaches, modulares und erweiterbares Protokolldesign, die Vereinfachung von Netzstrukturen sowie die Berücksichtigung von Sicherheitsaspekten. Dies schafft eine Grundlage zur Unterstützung von neuartigen Anwendungen und damit die Voraussetzung für weitere Innovationen auf Basis des Internets. IPv6 ermöglicht aber auch neue Ansätze für den Betrieb und das Management der Netze selbst, hin zu einer dynamischeren Konfiguration und mehr Sicherheit.

Kritisch anzumerken ist, dass IPv6 noch nicht in allen Bereichen ausgereifte Sicherheitskonzepte anbietet. Die Entwicklung von IPv6 begann zu einer Zeit, als der Erfolg des Internets absehbar, die Sicherheitsprobleme aber noch nicht so offensichtlich waren wie heute. Umso wichtiger sind die konkrete Auseinandersetzung mit IPv6 und die Erarbeitung von Best Practices mit genügend Vorlaufzeit. Aufgrund des modularen Designs von IPv6 und der Kreativität der Protokollentwickler kann bei korrekter Nutzung davon ausgegangen werden, dass IPv6 jetzt und in Zukunft ein deutlich besseres Sicherheitsniveau als IPv4 ermöglichen wird.

»IPv6 ist mehr als „IPv4 mit langen Adressen" – es ist ein moderner System-Baukasten für Netze.«

[10] Richard Sietmann, In den Startlöchern - Wie sich die Netzarchitekten die Zukunft des Internet vorstellen, S. 80-87 in: c't Heft 21/09. http://www.heise.de/ct/artikel/In-den-Startloechern-973293.html

[11] Benedikt Stockebrand, Ende der Durststrecke - Chancen und Risiken von IPv6; S. 44-47 in: iX 7/2011.

[12] IPv6 Dashboard des Deutschen IPv6-Rats: http://www.ipv6council.de/ipv6day/ipv6_dashboard/
Dargestellt wird die IPv6-Erreichbarkeit der Haupt-Webseiten von bedeutenden Unternehmen. Zumindest bis Juni 2013 waren die DAX-Konzerne nicht über IPv6-erreichbar (Ausnahme: Deutsche Telekom unter T-Online).

Abrufdatum aller Internetquellen: 26.07 2013

4. THESEN

Netze sind das Fundament für öffentliche IT.

Die Allgegenwärtigkeit von IT führt dazu, dass der Zugang zu Infrastrukturen und Informationen für alle Bürgerinnen und Bürger in hinreichender Qualität sichergestellt werden muss. Dies gilt umso mehr, da immer mehr Netze und Kommunikationskomponenten zu kritischen Infrastrukturen werden – für Wirtschaft, Zivilgesellschaft und die öffentliche Hand. Der öffentlichen Hand kommt beim Aufbau und Betrieb von Netzen eine Vorbildfunktion zu.

Die Entwicklung der Netze wird derzeit von den Endgeräten getrieben.

Für jede Lebenslage steht ein passendes Gerät zur Verfügung. Die Anwendungen bilden die Motivation für den Netzzugang. Die Attraktivität der Anwendungen und die Benutzerfreundlichkeit des Endgeräts entscheiden über Art und Intensität der Nutzung von Netzen und Angeboten. Ein breiter Zugang muss gewährleistet werden. Als dienstneutrales Transportnetz ermöglicht und begünstigt das Internet die Einführung neuer, innovativer Dienste und Anwendungen.

Sicherheitsbetrachtungen müssen dem neuen Paradigma permanenter Anpassung folgen.

Bei der Betrachtung von Sicherheit muss ein auf weiterer Forschung basierender Paradigmenwechsel stattfinden, weg von einem starren Konzept mit wenigen Ausnahmen hin zur permanenten Anpassung auf Basis der dynamischen Konfiguration von Netzelementen und der Nutzung von Virtualisierungstechniken. Sicherheitskonzepte müssen das Endgerät miteinbeziehen und Kommunikationspfade ganzheitlich betrachten. Schutzbedarfsanalysen gewinnen an Bedeutung.

Standardisierung ist die Grundlage für Innovation und Dynamik.

Standards, insbesondere IPv6, und ihre übergreifende Anwendung stellen die Grundlage von interoperablen herstellerneutralen Infrastrukturen dar. Der Netzwerkbereich verfügt traditionell über ein gut funktionierendes System von Standards, das sich über die Verbreitung der Web-Technologien positiv auf die Dienst- und Anwendungsdomäne auswirkt. Die Dynamik der Netz- und Infrastrukturentwicklung beschleunigt den Bedarf an Normung und erfordert die Nutzung von Industriestandards und die Entwicklung von Best Practices. Hier muss sich die öffentliche Hand stärker an den verschiedenen Standardisierungsprozessen beteiligen, will sie gesamtgesellschaftliche und eigene Interessen vertreten wissen.

Netze benötigen ein dynamisches, automatisiertes Netzwerkmanagement.

Zunehmende Kommunikationsrelationen und eine Vielzahl von Endgeräten und Anwendungen erfordern ein automatisiertes und dynamisches Netzwerkmanagement. Die Automatisierung erhöht die Leistungsfähigkeit von Netzen und verhindert Fehler in komplexen Konfigurationen. Das Ziel ist die Steuerung komplexer Netze über allgemein verständliche, überschaubare Regeln, die auch den Nachweis eines korrekten Betriebs ermöglichen.

Ein regelbasiertes Netzwerkmanagement schafft gesellschaftspolitische Gestaltungsmöglichkeiten.

Nicht nur Fehlervermeidung und Dynamik, auch die gesellschaftspolitische Steuerbarkeit wird durch ein regelbasiertes Netzwerkmanagement forciert. Gesellschaftspolitische Vorgaben können vergleichsweise einfach in technische Netzwerk-Policys überführt und ihre Einhaltung damit überprüft werden. Für die Akzeptanz dieser unerlässlichen Interventions- und Gestaltungsmöglichkeiten ist es existenziell, dass nur in minimalem Umfang und in transparenter Weise von ihnen Gebrauch gemacht wird.

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

kre | 1308 (Fotos: Matthias Heyde / Fraunhofer FOKUS)