Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

ZUKUNFT DES INTERNETS UND DER VERWALTUNGSVERNETZUNG

Gabriele Goldacker, Jens Tiemann

Fraunhofer
FOKUS

IMPRESSUM

Autoren:
Gabriele Goldacker, Jens Tiemann

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

ISBN: 978-3-9816025-8-6

1. Auflage Januar 2017

Bildnachweise:
Seite 1: PolarityFlow
Seite 6: WikiImages
Seite 12: SpaceX-Imagery
Seite 18-19: 12019
Seite: 22: WikiImages
Seite 26: Mariss
Seite 29: manolofranco
Seite 30: 12019
Seite 34: Comfreak

VORWORT

Das Internet wird oft als homogene Infrastruktur gesehen, die sich in einem technischen und vor allem auch wirtschaftlichen Konkurrenzkampf durchgesetzt hat und als die alleinige technische Infrastruktur für die Kommunikation übrig geblieben ist. Aus dieser scheinbaren Alternativlosigkeit des Internets folgt eine gelegentlich schizophren anmutende Haltung, dass einerseits alles vernetzt und über das Internet erreichbar sein soll, andererseits nach IT-Sicherheitsvorfällen die technische Entwicklung oder gar die Digitalisierung insgesamt kritisch gesehen wird. Zugunsten unserer Bequemlichkeiten fordern wir eine umfassende Verfügbarkeit von Informationen und Diensten im Netz, klar ist aber auch, dass wir Kernkraftwerke, Industrieanlagen und vielleicht auch unser Smart Home oder vernetztes Auto nicht dem beliebigen Zugriffsversuch von außen aussetzen wollen.

Leicht übersehen wird dabei, dass die derzeitigen Netzstrukturen weit differenzierter sind: Auch wenn sich das Internet-Protokoll bzw. die Internet-Technik in fast allen Netzen durchgesetzt hat, so bedeutet das keinesfalls, dass alle vernetzten Systeme erreichbar sind. Und selbst bei der alltäglichen Nutzung des öffentlichen Internets kommen inzwischen Komponenten zum Einsatz, die in der »Reinform« des Internets nicht vorgesehen waren. Mehr noch: Bei zahlreichen Anwendungen, die wir heute nutzen, verschwimmt die Grenze zwischen lokalem Computer und Kommunikation immer mehr. Wissen wir noch, wo die Route unseres Navigationssystems berechnet wird – im Fahrzeug oder irgendwo im Internet?

Durch die steigenden Anforderungen an die Netzinfrastrukturen müssen fortlaufend neue Techniken entwickelt werden, von der Erhöhung der Datenraten im Mobilfunk bis zur Optimierung der Auslieferung von Multimediainhalten. Welche Möglichkeiten zur Steigerung der Leistungsfähigkeit des Internets gibt es? Dazu wird zunächst betrachtet, was das Internet ausmacht. Welche Ansätze für eine gänzlich neue Architektur des Internets kommen aus der Future-Internet-Forschung? Und welche Weiterentwicklungen des Internets sind aufgrund der steigenden wirtschaftlichen Bedeutung notwendig geworden? Fest steht, dass Vernetzung inzwischen unverzichtbar ist und das Internet die wesentliche Basisinfrastruktur darstellt, die sich entsprechend den steigenden Anforderungen weiterentwickeln muss. Worauf muss sich dabei die öffentliche Verwaltung – ähnlich wie jedes Unternehmen mit mehreren vernetzten Standorten – bei ihren Infrastrukturen einstellen?

Ihr Kompetenzzentrum Öffentliche IT

DAS KOMPETENZZENTRUM ÖFFENTLICHE IT ERFORSCHT PRAXISRELEVANTE KONZEPTE UND ENTWICKELT ANWENDUNGEN FÜR DIE BEREICHSÜBERGREIFENDE ZUSAMMENARBEIT ZWISCHEN ÖFFENTLICHER VERWALTUNG, ZIVILGESELLSCHAFT UND WIRTSCHAFT.

INHALTSVERZEICHNIS

1. THESEN

Vernetzung basiert zunehmend auf Internet-Technik
Bisher mit spezifischer Technik realisierte Kommunikation wird immer mehr zu Internet-Technik migriert. So befindet sich Telefonie im rasanten Übergang zur Nutzung von Internet-Technik in der Regelversorgung. Fernsehen und Radio werden mehr und mehr über diese Technik konsumiert. Diese Vereinheitlichung ermöglicht mehr Wirtschaftlichkeit und Innovation durch sinkende Stückkosten und mehr Durchlässigkeit zwischen Diensten.

Zukünftig wird es nicht nur das eine, offene Internet geben
Die Nutzer haben steigende Qualitätserwartungen und Sicherheitsanforderungen, die das heutige Internet nicht immer und überall erfüllen kann. Dies bedingt divergierende, vom Anwendungsfall abhängige technische und organisatorische Ausprägungen. Gleichzeitig fordern Politik und Wirtschaft mehr Einfluss auf die Gestaltung und Nutzung des Internets. In der Folge werden Fragmentierung und Segmentierung des Internets zunehmen.

Vom heutigen Internet sind keine umfassenden Qualitätssteigerungen zu erwarten
Die Einfachheit und Flexibilität der Internet-Technik und die Offenheit des Internets sind Basis für Innovation und Wettbewerb in der Anwendungs- und der Übertragungsebene. Aber neue Funktionen der Netzebene, wie die Sicherstellung von Videoqualität über große Entfernungen, sind weltweit nur schwer bis unmöglich einzuführen. Eine grundsätzliche Änderung der Internet-Architektur ist nicht abzusehen. Der Erfolg des Internets lähmt die Weiterentwicklung dieser zentralen Ebene.

Mehr Übertragungsqualität ist notwendig
Vernetzung ist unverzichtbar, digitale Netze sind in Teilen eine kritische Infrastruktur. Bei der Nutzung neuer, hochwertiger Anwendungen sind eine garantierte Übertragungsqualität und ein besonderes Schutzniveau notwendig. Die Grundlage für Qualität und Schutz der Datenübertragung ist eine zuverlässige und leistungsfähige Infrastruktur.

Hochwertige und sichere Kommunikation braucht mehrere parallele Infrastrukturansätze
Die vielfältigen Anforderungen an Netze sind teilweise widersprüchlich, wie die Forderung nach weltweiter Erreichbarkeit bei gleichzeitigem Schutz gegen Angriffe. Das heutige Internet kann das nicht alles leisten. Ein Ansatz zur Steigerung der Qualität der Vernetzung beruht auf der Nutzung verschiedener, jeweils optimierter Infrastrukturen. Das reicht von Mobilfunk- oder WLAN-Nutzung eines Smartphones unter wechselnden Bedingungen bis zur Anbindung eines Rechenzentrums (bspw. der Verwaltung) an Netze unterschiedlicher Sicherheitsniveaus.

Die Verwaltung nutzt zukunftsorientierte Ansätze
Mit eigenständigen, getrennten Verwaltungsnetzen, dem übergreifenden Verbindungsnetz und dem öffentlichen Internet, die alle durchgängig auf Internet-Technik basieren, sowie mit der zunehmenden Nutzung zentraler Rechenzentren stehen die Bausteine einer leistungsfähigen und flexiblen Verwaltungsinfrastruktur bereit. Bei Diensten zur sicheren und vertrauenswürdigen Kommunikation mit Wirtschaft und Bürgern über das Internet besteht allerdings Nachholbedarf.

2. STOCKENDES ERFOLGSMODELL INTERNET

Die Nutzer erwarten angesichts des Erfolges des Internets in der jüngeren Vergangenheit auch für die nahe und mittlere Zukunft beträchtliche Innovationsschübe. Es soll mehr Leistung bringen, als Basisinfrastruktur für vielfältige Dienste aus immer unterschiedlicheren Bereichen dienen und dabei höchsten Qualitäts- und Sicherheitsanforderungen genügen. Schätzungen gehen davon aus, dass sich das Internetvolumen in den kommenden vier Jahren mehr als verdoppeln wird.[1] Allerdings gerät das Internet (s. Abschnitt 2.1) an seine Grenzen. Der bisherige Erfolg steht der Umsetzung neuer Paradigmen im Weg (s. Abschnitt 2.2). Um aktuelle Entwicklungen bewerten zu können, bedarf es vor diesem Hintergrund zunächst einer vertieften Betrachtung der aktuellen Herausforderungen durch die allgegenwärtige Vernetzung (s. Abschnitt 2.3) sowie eines Blicks auf die Organisation abgestufter Offenheit im Netz (s. Abschnitt 2.4).

2.1 DAS ERFOLGSREZEPT DES HEUTIGEN INTERNETS

Seit rund 30 Jahren ist das Internet ein Erfolgsmodell, das eine erstaunliche Anpassungsfähigkeit gezeigt hat. Sieben Zutaten machen diesen Erfolg aus:

Offene Konnektivität und weltweite Erreichbarkeit
Die technischen Grundlagen des Internets ermöglichen die spontane Kommunikation zwischen beliebigen, technisch kompatiblen Systemen unabhängig von deren Standorten. Allerdings fordern Politik und Wirtschaft mehr Einfluss auf das Internet, wodurch seine Fragmentierung[2] zunehmen kann.

Modulare Struktur
Das Internet lässt sich durch ein einfaches Modell aus drei Ebenen mit klaren Schnittstellen beschreiben (s. Abbildung 1). Dies ermöglicht bedarfsgerechte Kombinationen aus Übertragungstechnik und Anwendungen, ohne jeweils die Lösung komplett neu entwickeln zu müssen.

Einheitliche Internettechnik
Anwendungen und Übertragungstechniken werden einheitlich über das Internet-Protokoll (IP) und Managementmechanismen der Netzebene angebunden. Anpassungen müssen also regelmäßig nur an diesen Schnittstellen vorgenommen werden.

Das Ende-zu-Ende-Prinzip
Die Übertragung im Internet erfolgt möglichst einfach, die Funktionen im Netz sind auf das notwendige Minimum beschränkt. Es gilt das Ende-zu-Ende-Prinzip, nach dem die übertragenen Inhalts- und Steuerungsdaten weitgehend unverändert vom Absender zum Adressaten gelangen. Zusätzliche Funktionen, wie z. B. Bestätigung des Empfangs, müssen von den angeschlossenen Endgeräten erbracht werden.

Offene Protokolle[3] und kooperative Protokollentwicklung
Die notwendigen Protokolle sind offengelegt und lizenzkostenfrei nutzbar. Neue Protokolle werden in einem frei zugänglichen, konsensorientierten Verfahren entwickelt.

Weitgehende Unabhängigkeit der Teilnetzbetreiber
Auf- und Ausbau des Internets erfolgen durch vielfältige Betreiber mit unterschiedlichsten Geschäftsmodellen ohne zentrale organisatorische oder technische Steuerung. Notwendige Abstimmungen erfolgen durch offene, kooperative Gremien wie die Multi-Stakeholder-Institution ICANN (Internet Corporation for Assigned Names and Numbers) bzw. durch bi- oder multilaterale Vereinbarungen zwischen benachbarten Betreibern.

Strukturierter Adressraum
Die geografisch ausgerichtete, hierarchische Adressstruktur des Internets ermöglicht eine weitgehende Dezentralisierung der Adressverwaltung[4] und eine effiziente Bündelung jener Datenströme, die über große Entfernungen transportiert werden müssen.

[1] http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

[2] http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

[3] Protokoll: Syntax- und Semantikregeln, die eine elektronische Kommunikation ermöglichen

[4] https://www.eco.de/2016/pressemeldungen/iana-stewardship-transition-erfolgreich.html und http://www.faz.net/aktuell/feuilleton/debatten/widerstand-der-republikaner-gegen-iana-transition-14448104.html

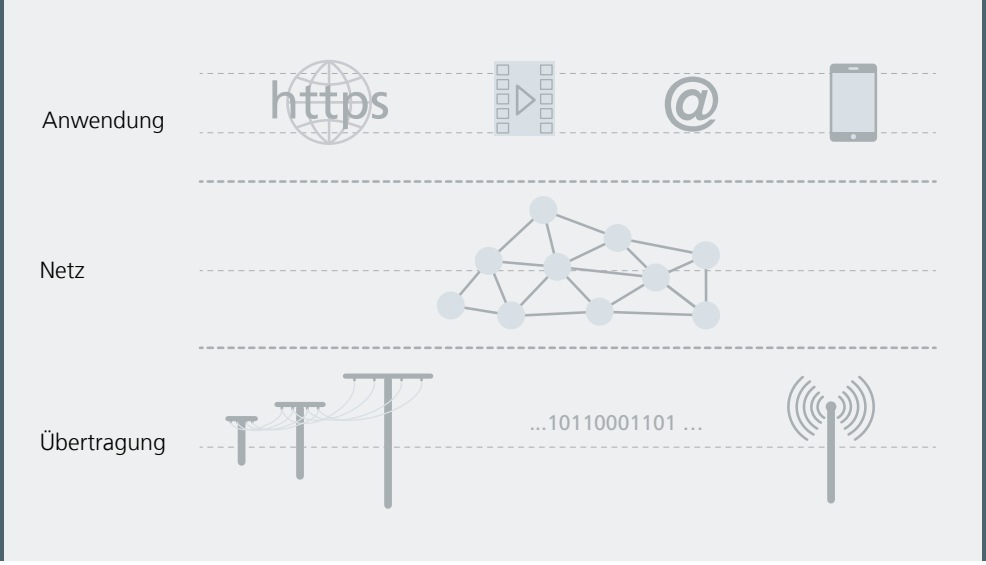

Abb. 1: Die Ebenen des Internet-Modells

2.2 DIE ABSEHBARE VERLANGSAMUNG DER INTERNETREVOLUTION

Bereits die enormen Nutzer- und Durchsatzzahlen sowie die Konkurrenzlosigkeit als leistungsfähige und weltumspannende Kommunikationsinfrastruktur zeigen die gegenwärtige Bedeutung des Internets. Zudem sind viele kritische Infrastrukturen wie Energie, Wasserversorgung, Bankensektor und nicht zuletzt die öffentliche Verwaltung auf die Verfügbarkeit der Internetkommunikation angewiesen. Das Internet ist zu einer übergreifenden kritischen Infrastruktur ohne gleichwertige technische Alternativen geworden.

Der Erfolg des Internets beruht also auf dem Zusammenspiel kooperativer Strukturen auf Netzebene und einem so ermöglichten Innovationswettbewerb auf der Übertragungs- und der Anwendungsebene. Die kooperativen Strukturen stellen dabei sicher, dass eine einheitliche Technologie auf der Netzebene eingesetzt wird, die auf offenen, akzeptierten Protokollen und Schnittstellen beruht, und dass die technischen Regelungen auf das Notwendigste beschränkt bleiben. Wegen dieser einheitlichen Schnittstellen können die Ideen für die Ausgestaltung von Anwendungen und Übertragungstechnologien jeweils miteinander in den Wettbewerb treten, was zu einer enormen Innovationsdynamik geführt hat. Während Übertragungstechnologien und Anwendungen dadurch leicht anpassbar sind, lässt sich die Internetsprache auf der Netzebene ungleich schwerer verändern. Der Erfolg des Internets steht Innovationsprüngen auf der Netzebene, die angesichts aktueller Herausforderungen unerlässlich wären, entgegen.

Änderungen an den auf der Netzebene verwendeten Protokollen und Konventionen würden in vielen Fällen ein abgestimmtes, gemeinsames Vorgehen aller beteiligten Akteure innerhalb eines relativ kurzen Zeitrahmens erfordern. Die Anwendungsebene müsste an die neue Sprache des Internets adaptiert werden. Bleibt dies aus, wären die betroffenen Nutzer und Dienstanbieter völlig von der Nutzung abgeschnitten, sich verweigernde Netzbetreiber könnten zudem Überlastsituationen in anderen Bereichen des globalen Internets, Qualitätseinbußen und schwer erkennbare Sicherheitslücken verursachen. Dies sind Risiken, die angesichts der Bedeutung des Internets kaum mehr tragbar sind.

In der Folge bleiben viele Nutzungsmöglichkeiten ungenutzt, für die standardisierte Internetmechanismen vorliegen. Die Realisierung gleichmäßiger Datenströme auch über große Entfernungen (Priorisierung von Video/Audio/Sprache bspw. mittels der Mechanismen IntServ oder DiffServ) ist hier ebenso zu nennen wie das effiziente Übertragen und Verteilen von Daten an mehrere Adressaten (Multicast).

Besonders deutlich ist das Dilemma bei der unumgänglichen Einführung von IPv6 (Internet Protocol version 6) zu beobachten: Bei der Spezifikation von IPv6 wurden die Architektur und wesentliche Prinzipien von IPv4 übernommen, allerdings bewusst ein anderes, mit dem bestehenden nicht kompatibles Adressformat gewählt. Über 20 Jahre nach der Standardisierung des IPv6-Protokolls bleibt die Verbreitung weit hinter den Erwartungen zurück, obwohl schon bei der Entwicklung des Protokolls auf Mechanismen zur Migration Wert gelegt wurde.

2.3 HERAUSFORDERUNGEN DURCH ZUNEHMENDE VERNETZUNG

Angesichts der beobachtbaren Innovationshemmnisse auf der Netzebene stellt sich die Frage, wie den Herausforderungen durch die zunehmende Vernetzung begegnet werden kann. Viel diskutierte Anwendungsszenarien – wie etwa ortsverteiltes, kollaboratives Arbeiten, Maschinensteuerung über Distanz, Fernwirken mit haptischem Feedback und hoch vertrauliche Kommunikation – sollen gleichermaßen unterstützt werden.

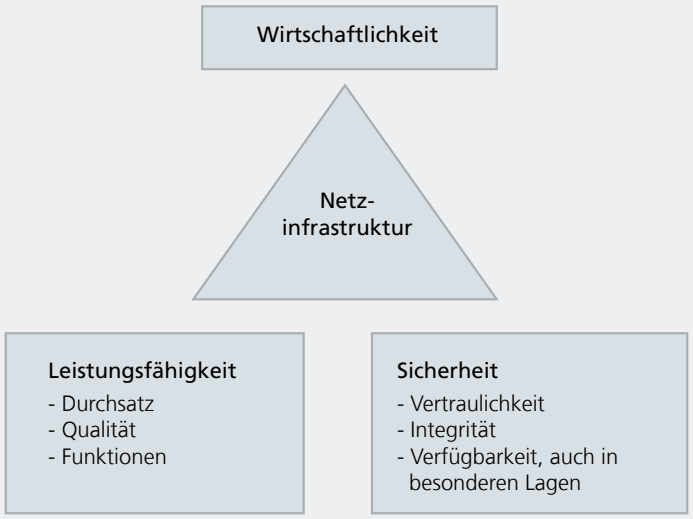

Abb. 2: Netzinfrastruktur im Spannungsfeld divergierender Anforderungsdimensionen

Im Detail werden von der Vernetzung ganz unterschiedliche Eigenschaften erwartet. Dessen ungeachtet lassen sich drei generelle Anforderungsdimensionen identifizieren, denen sich die Entwicklung der Netzinfrastruktur schon immer stellen musste, die durch zukünftige Anwendungsszenarien jedoch auf eine neue Stufe gehoben werden: Leistungsfähigkeit, Wirtschaftlichkeit und Sicherheit (vgl. Abbildung 2).

Die Leistungsfähigkeit berücksichtigt vornehmlich Aspekte wie Datendurchsatz (die »Schnelligkeit« der Kommunikation) oder die Qualität der Datenübertragung. Diese aus der Nutzerperspektive besonders wichtige Anforderungsdimension wird durch zukünftige Anwendungen vor immer höhere technische Herausforderungen gestellt. Hochauflösendes Videostreaming erfordert beispielsweise einen stabilen Datendurchsatz von mehreren Mbit/s, der sich mit jeder Erhöhung der Auflösung weiter erhöht. Während Telefonie noch mit Datenlaufzeiten von 100 ms als akzeptabel empfunden wird, erlauben sicherheitskritische Maschinensteuerungen nur noch 1 ms. Bei medizinischen Eingriffen über Distanz können Datenverluste nicht durch erneute Übertragung kompensiert werden und sind daher intolerabel.

Dabei steigen zugleich die Anforderungen an die Sicherheit der Übertragung. Anwendungen wie Maschinensteuerung oder Telechirurgie erlauben keine Instabilitäten des Netzes. Auch vertrauliche Kommunikation stellt eine besondere Herausforderung dar, weil es auch bei verschlüsselter Kommunikation über das öffentliche Internet technisch nicht möglich ist, die Adressen von Sender und Empfänger und den für die Kommunikation benutzten Weg komplett zu verbergen. (S. a. Abschnitt 2.4.)

Durchsetzen werden sich Innovationen auf der Netz- und Übertragungsebene nur, wenn sie die Wirtschaftlichkeit des Netzbetriebes erhöhen. Für die Netzbetreiber heißt dies konkret, dass sie entweder Einsparungen oder monetarisierbare Mehrwerte für ihre Kunden realisieren können.

Idealerweise müsste ein Netz alle drei Anforderungsdimensionen gleichermaßen berücksichtigen. Technisch und wirtschaftlich zeigt sich jedoch ein mehrfaches Spannungsverhältnis: Hohe Sicherheit kostet Geld und steht noch nicht für die breite Nutzung durch kleinste, leistungsschwache Endgeräte zur Verfügung. Ebenso rechnet sich eine hohe Leistungsfähigkeit des Netzes nicht, die auf keinen entsprechenden Bedarf trifft und deshalb von Kunden nicht nachgefragt wird. Sicherheitsfeatures können wiederum die Leistungsfähigkeit beeinträchtigen, wenn hierfür zusätzliche Rechenleistung oder zusätzlicher Kommunikationsaufwand benötigt wird.

Faktisch kann eine Netzinfrastruktur also nicht allen Anforderungsdimensionen in gleicher Weise gerecht werden. Für die Bewertung von Innovationen sind daher nicht nur Fragen nach der Verortung in den Netzebenen und der Einfachheit ihrer Diffusion wesentlich, sondern auch danach, welche Anforderungsdimensionen stärker und welche schwächer adressiert werden.

Viele Herausforderungen sind bekannt und werden sowohl in der Forschung als auch der Wirtschaft adressiert (s. Abschnitte 3 und 4), wobei unterschiedliche Lösungsansätze entstehen. Eine wichtige und häufig genutzte Lösung für bestimmte Leistungs- und Sicherheitsaspekte in Netzen ist »abgestufte Offenheit«, die in Kombination mit verschiedenen der vorgestellten Lösungsansätze zum Einsatz kommt und deshalb hier kurz vorgestellt wird.

2.4 ABGESTUFTE OFFENHEIT IM NETZ

Neben technischen Alternativen bei der Vernetzung wie z. B. Mobilfunk oder Glasfasertechnik lassen sich bestimmte Anforderungen auch alternativ oder ergänzend durch organisatorische Maßnahmen erfüllen. Diese zielen darauf ab, bestimmte Kommunikationspartner oder Kommunikation mit bestimmten

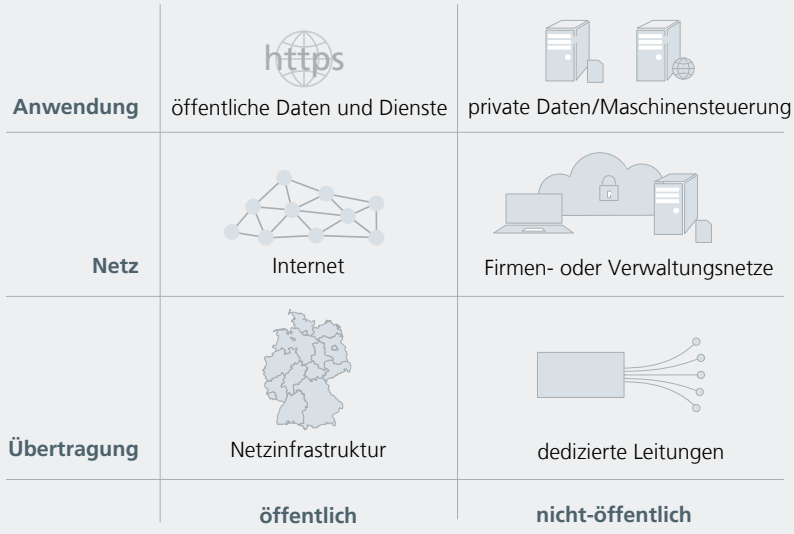

Abb. 3: Öffentliche und nicht-öffentliche Ausprägungen auf den drei Ebenen des Internet-Modells

Eigenschaften auszuschließen und so die Qualität, Verfügbarkeit oder weitere Sicherheitsaspekte der verbleibenden Kommunikation zu verbessern.

Auf allen drei Ebenen des Internet-Modells sind organisatorisch öffentliche und nicht-öffentliche Ausprägungen möglich, die entsprechend den jeweiligen Anforderungen kombiniert werden können. »Öffentlich« bezeichnet dabei die prinzipielle Offenheit für jedermann[5], wobei die Nutzer – i. d. R. auf Basis kommerzieller Nutzungsverträge – Kommunikationspartner, Zeitpunkt, Dauer und Inhalte der Kommunikation sowie die auf ihrer Seite eingesetzte Hard- und Software frei wählen können. Demgegenüber ist bei »nicht-öffentlichen« Lösungen der potenzielle Nutzerkreis vorbestimmt und die Netzadministration kann vielfältigen Einfluss auf die Kommunikationsparameter nehmen.

Abbildung 3 zeigt Beispiele für öffentliche und nicht-öffentliche Ausprägungen. Sie illustriert wesentliche Unterschiede, in der Realität sind die Übergänge teilweise fließend, aber auch wesentlich stärker ausdifferenzierte Angebote sind anzutreffen.

Übertragungsebene

Auf der Ebene der Übertragung lassen sich die öffentlichen Transportnetze der Netzbetreiber und dedizierte (Glasfaser-)Leitungen unterscheiden. Öffentliche Transportnetze sind Infrastrukturen, auf denen verschiedene Kunden (insbesondere Internet Service Provider, s. Netzebene) parallel ihre standortübergreifenden, das Internet-Protokoll benutzenden Netze betreiben können. Der Betrieb eines Transportnetzes und die Isolation der Kundennetze untereinander werden durch den Netzbetreiber sichergestellt, dieser garantiert auch Netzeigenschaften (im Rahmen von Service Level Agreements). Vorteile öffentlicher Transportnetze sind die Abdeckung in der Fläche und die Wirtschaftlichkeit des Betriebs. Im Kontrast dazu kann eine nicht-öffentliche Transportinfrastruktur auf Basis dedizierter Leitungen aufgebaut werden, die komplett unabhängig von anderen Netzen ist.[6] Dies kann bei hohen Anforderungen an Vertraulichkeit oder Verfügbarkeit geboten sein.

Netzebene

Auf der Netzebene werden typischerweise Zugänge zum öffentlichen Internet benutzt, die von Internet Service Providern (ISPs) kommerziell angeboten werden. Allerdings besteht in öffentlichen Netzen ein erhöhtes Risiko, von unerwünschter Seite kontaktiert zu werden oder unerwünschte Inhalte zugestellt zu bekommen. Für öffentliche Netze gilt das Gebot der Netzneutralität, wie es in den BEREC Guidelines[7] zu EU-Verordnung 2015/2120[8] konkretisiert ist: keine netzseitige Beschränkung des Zugangs zu beliebigen anderen Netznutzern, keine Bevorzugung einzelner Dienste oder Netznutzer ohne technische Notwendigkeit.

Nicht-öffentliche (Weitverkehrs-)Netze ermöglichen die Durchsetzung einer erhöhten Kontrolle über die Kommunikation. Bspw. können unerwünschte Kommunikationsbeziehungen blockiert und unerwünschte Inhalte ausgefiltert werden. Nicht-öffentliche Netze können auch so gestaltet werden, dass stets ausreichend Datenrate für den Bedarf einzelner Anwendungen bereitgestellt werden kann, ggf. auch auf Kosten weniger wichtiger Kommunikation. Diese Firmen- oder Verwaltungs-

[5] Protokoll: Syntax- und Semantikregeln, die eine elektronische Kommunikation ermöglichen

[6] In dieser vereinfachten Darstellung wird nicht zwischen einzelnen physischen Leitungen und den Möglichkeiten des Wellenlängen-Multiplexing (WDM) unterschieden, bei denen verschiedenen Kunden eine Wellenlänge auf einer gemeinsam genutzten Glasfaser zugeordnet ist.

[7] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, August 2016

[8] Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union

FÜR ÖFFENTLICHE NETZE GILT
DAS GEBOT DER NETZNEUTRALITÄT.

Intranetze können auf einem beliebigen Mix aus den Transportinfrastrukturen und dedizierten Leitungen basieren. Von nicht-öffentlichen Netzen aus kann bei Bedarf ein Übergang in das öffentliche Internet hergestellt werden, der sorgfältig überwacht werden muss, um das Qualitäts- bzw. Sicherheitsniveau des nicht-öffentlichen Netzes nicht zu gefährden.

Anwendungsebene
Ein sehr offenes Netz ist das WWW, das für ein breites Spektrum an Inhalten und Angeboten steht und für dessen Nutzung keine weiteren Vorbedingungen existieren.

Telefonie und Video-/Fernsehverteilung sind Beispiele für Anwendungen öffentlicher Netze, für die eine Mindestqualität erforderlich ist. Dies kann durch ausreichende Netzressourcen (»Overprovisioning«) erreicht werden. Eine Qualitätsgarantie erfordert aber die Steuerung der Datenströme, bspw. durch die Priorisierung von Audio und Video gegenüber zeitunkritischen Daten.

Bei nicht-öffentlichen Diensten, die nur bestimmten externen Nutzern zugänglich sind, müssen Zugang und Nutzung ausreichend abgesichert sein. Bei einer Anbindung über das Internet kann bspw. die Vertraulichkeit der Daten durch Authentisierung der Kommunikationspartner und verschlüsselte Kommunikation sichergestellt werden.[9] Alternativ können sie über nicht-öffentliche Netze, die bereits für den erforderlichen Schutz sorgen, genutzt werden, wenn alle Nutzer Zugang zu diesen Netzen haben.

Anmerkung: Eine Besonderheit stellen Plattformen mit Marktplatzcharakter dar. Aufgrund des Netzwerkeffekts entstehen oft monopolartige Strukturen, weil die Plattformen besonders nützlich sind, wenn sich möglichst viele potenzielle Kommunikationspartner oder Angebote auf einer einzigen Plattform befinden. Die wenigen, schnell gewachsenen Plattformen sind allerdings keine feststehenden Infrastrukturen, die eine rechtlich abgesicherte Basis für Angebote von Nutzern bieten. Vielmehr handelt es sich um teilweise sehr spezialisierte Dienste mit selbst festgelegten Regeln und Geschäftsbedingungen, weshalb über die Notwendigkeit einer Regulierung diskutiert wird.

[9] Die Verfügbarkeit kann so jedoch nicht sichergestellt werden. Sie kann etwa mithilfe von Denial-of-Service-Angriffen beeinträchtigt werden; Ende September 2016 machten Angriffe mit enormen Datenmengen von bis zu 1 Tbit/s Schlagzeilen, die auch Anbieter spezieller Hosting-Lösungen vor Probleme stellten (s. https://www.heise.de/security/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html)


SPACEX

3. DIE FORSCHUNG ALS TREIBER

Nach der Erkenntnis, dass »weiter so wie bisher« beim Internet keine Option sein kann, soll zunächst dargestellt werden, welche Lösungen aus der Forschung kommen. Unter dem Begriff »Future Internet« werden im Bereich der Forschung vor allem Ansätze für eine neue Architektur des Internets verstanden. Wie schon beim Übergang von Leitungs- zu Paketvermittlung löst man sich ganz grundsätzlich von bestehenden Architekturmustern und entwickelt einen zeitgemäßen Ansatz der Vernetzung vor dem Hintergrund aktueller technischer Möglichkeiten.

Als Forschungsthema wurde Future Internet vor allem im 7. Forschungsrahmenprogramm der EU (FP7) ab dem Jahr 2008 mit zahlreichen Projekten gefördert.[10] Entsprechende Forschungsprogramme gab es zeitgleich auch in den USA, Japan und China.[11] Die damaligen FP7-Forschungsprojekte fokussierten sich auf Forschung zu Internetarchitektur und -protokollen, zu Funkübertragung und Nutzung des Funkspektrums sowie zu optischen Netzen. Spätere Forschungsprojekte der EU adressieren nicht mehr die Übertragungs- und Netztechniken, sondern stellen Plattformen und Anwendungen in den Mittelpunkt.[12] Im Herbst 2016 wurde die Next Generation Internet Initiative gestartet, zu der bis 09.01.2017 eine Konsultation durchgeführt wurde und für die aktuell die Ermittlung der Forschungsthemen und die Programmerstellung ausgeschrieben sind.[13]

Grob lassen sich zwei Future-Internet-Forschungsbereiche unterscheiden: Die Weiterentwicklung der Netze auf Basis bestehender Architekturen bzw. Protokolle und die Einführung eines radikal neuen Ansatzes, der mit den bestehenden Netzwerk-Prinzipien bewusst bricht, um erkannte Einschränkungen grundsätzlich zu überwinden und noch einmal neu anzufangen (»Clean Slate Design«). Da das Forschungsthema sehr umfangreich ist, können nur einzelne neue Ansätze vorgestellt werden. Im Mittelpunkt steht dabei die praktische Bedeutung, auch unabhängig von einer komplett neuen Internetarchitektur. Die Forschung zum Future Internet bietet teilweise ungewohnte Sichtweisen auf Netze oder die Übertragung von Information bzw. allgemeiner auf die Informationsverarbeitung. Bestimmte Aufgaben können ganz anders gelöst werden und ein Teil der Probleme heutiger Netze entfällt einfach.

Ein neuer Ansatz muss sich an der Leistungsfähigkeit des heutigen Internets sowie seinen Weiterentwicklungen messen lassen und einen Migrationspfad bereitstellen. Die Forschung im Bereich Future Internet bezieht daher sehr stark Experimentalplattformen ein, in denen einerseits neue Mechanismen, Protokolle und Anwendungen in der verteilten Umgebung eines möglichst realistischen Netzes ausprobiert werden können, die sich andererseits aber auch als Ausgangspunkt für die spätere Einführung dieser neuen Ansätze eignen können.

Derzeit ist ein grundlegend neuer Ansatz für die Architektur des Internets nicht erkennbar, obgleich viele der Forschungserkenntnisse zur Weiterentwicklung des Internets beitragen, etwa zur Entwicklung neuer Protokollmechanismen oder leistungsfähiger Softwarewerkzeuge und Netzwerkkomponenten.

3.1 ADRESSIERUNG UND MOBILITÄT

Eine Herausforderung ist die zunehmende Mobilität bei der Nutzung von Netzen, da die Adressen, Netze und das Routing[14] hierarchisch aufgebaut sind. Im heutigen Internet wird einem vernetzten Gerät eine IP-Adresse aus einem (i. d. R. geografisch zusammenhängenden) Teilnetz des Internets zugewiesen. Über die hierarchisch aufgebaute Adresse kann das Endgerät effizient erreicht werden. Wird das Endgerät in ein anderes Teilnetz überführt und bekommt dort eine neue IP-Adresse, so kann es zur unterbrechungsfreien Kommunikation notwendig sein, weiterhin unter der ursprünglichen Adresse erreichbar zu bleiben. Einfache Ansätze lösen dieses Problem mithilfe des »Nachsendens« von Paketen vom ursprünglichen in das aktuelle Teilnetz. Allerdings verlängert sich dadurch die Paketlaufzeit und es

[10] Peter Stuckmann, Rainer Zimmermann: European Research on Future Internet Design, Pre-print version of article published in IEEE Wireless Communications Magazine, October 2009, online http://cordis.europa.eu/fp7/ict/future-networks/eu-research-future-internet-design.pdf

[11] J. Pan, S. Paul, R. Jain, »A Survey of Research on Future Internet Architectures,« IEEE Communications Magazine, Vol. 49, No. 7, July 2011, pp. 26-36., online http://www.cs.umsl.edu/~pan/papers/5.internet--commag-2011.pdf

[12] Ein Beispiel ist FIWARE (https://www.fiware.org/), eine von der EU geförderte Plattform zur Entwicklung und Bereitstellung von Anwendungen des Future Internet, bspw. für den Bereich Smart City. Durch die Förderung soll eine unabhängige, offene Gemeinschaft entstehen, die ein nachhaltiges Ökosystem auf Basis von offenen Standards und Schnittstellen schafft.

[13] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative

[14] Routing: Festlegung des Weges der Datenpakete in einem Netz vom Absender zum Adressaten.

Abb. 4: Erwartungen an das Internet der Zukunft[15]

entsteht zusätzlicher Verkehr im Internet. Nimmt der Aspekt Mobilität bei der IT-Nutzung weiter zu (mobile Endgeräte, aber auch flexible Cloud-Lösungen oder Wechsel des Internet Service Providers), so lohnt sich die Suche nach neuen Ansätzen.

Eine Internetadresse hat zwei Aufgaben: Einerseits stellt sie die Identität eines Endsystems als Teilnehmer dar (»Identifier«), andererseits verweist sie auch auf den Ort dieses Systems im Internet im Sinne des aktuellen Netzzugangspunktes (»Locator«). Bei einem mobilen System muss diese Verbindung zwischen Identität und Ort aufgelöst werden (»Locator Identifier Split«). Ändert sich die IP-Adresse (bspw. Zugang zum Internet über ein anderes WLAN), dann ist dieses Gerät nicht mehr unter der bisher bekannten IP-Adresse erreichbar, obwohl sich die Identität nicht ändert.[16]

Lösungsvorschläge beruhen darauf, einen notwendigen Wechsel der IP-Adresse auf der Netzebene (aufgrund eines Ortswechsels) vor der Anwendungsebene zu verbergen, damit die Anwendungen wie gewohnt davon ausgehen können, über stabile Adressen (hier: Identitäten) zu verfügen und über diese Identitäten auch erreichbar zu sein. Zur Wahrung des Ende-zu-Ende-Prinzips und zur Vermeidung der Weiterleitung von Daten sind neue Funktionen (Beispiel: Host Identity Protocol, HIP) oder auch der Aufbau eines neuen Verzeichnisses zur aktuellen Zuordnung von Ort und Identität (Beispiel: Locator/ID Separation Protocol, LISP) notwendig.

[15] Basiert auf Kurzbeschreibungen der FI-Projekte des 7. EU-Forschungsrahmenprogramms, Quelle: http://www.future-internet.eu/activities/fp7-projects.html

[16] Die Ausführungen beziehen sich auf vollwertige IP-Endsysteme, die auch als Server fungieren können. Bei einer Beschränkung auf die Rolle als Klient hat der IP-Adresswechsel ggf. keine Auswirkung (Web-Browser im WLAN) oder kann über anwendungsspezifische Infrastruktur abgefangen werden (IP-Telefonie, generell Nutzung von Plattformen).

Mobilität ist dabei nicht nur für Nutzer-Endgeräte wie Notebooks und Smartphones wichtig, sondern kann auch im Rechenzentrum helfen: In flexiblen Cloud-Umgebungen kann es nützlich sein, Anwendungen bzw. (virtualisierte) Server während des Betriebes und für die Nutzer unterbrechungsfrei innerhalb eines Rechenzentrums oder sogar zwischen Rechenzentren zu verschieben, bspw. zur Lastverteilung oder um Hardwarekomponenten warten zu können.

3.2 INFORMATIONSZENTRISCHE NETZE

Die gegenwärtige Internetarchitektur ist Geräte-zentriert, d. h., die Kommunikation erfolgt zwischen zwei explizit adressierten Geräten. Zwischen diesen Geräten wird eine Kommunikationsbeziehung aufgebaut, um Informationen zu übertragen, von denen bekannt ist, dass sie sich auf einem der Geräte befinden.

Bei informationszentrischen Netzen steht die Information im Mittelpunkt, es werden also Informationen oder allgemein Inhalte direkt adressiert und übertragen (»Information/Content Centric Networking«). Ein Beispiel für derartige Forschungsaktivitäten ist das »Named Data Networking (NDN)«-Projekt.[17] Bei dieser Art von Kommunikation verliert die direkte Verbindung zwischen Geräten an Bedeutung, wichtig ist nur die Bereitstellung der gewünschten Informationen. Informationsquelle und -nutzer müssen nicht direkt miteinander in Beziehung stehen.

Die Information kann auf dem Weg durch das Netz bearbeitet oder zwischengespeichert werden. Dadurch kann die Übertragung zwischen Nutzer und Quelle auch zeitlich entkoppelt werden. Weitere Empfänger können die gleiche Information bekommen, ohne dass die Quelle der Information zusätzlich belastet werden muss. Diese Art der Übertragung ist insbeson-

[17] https://named-data.net/project/

BEI INFORMATIONSZENTRISCHEN NETZEN WERDEN INHALTE ORTSUNABHÄNGIG ADRESSIERT.

dere für den Abruf von Medien und anderen häufig verwendeten Informationen vorteilhaft. Zwischenspeicher können die Last der Auslieferung untereinander aufteilen und ggf. zusätzliche Aufgaben wie die Anpassung der Information an verschiedene Endgerätetypen übernehmen.

In ähnlicher Weise wird das Internet genutzt, wenn beispielsweise über das Portal einer Medienplattform ein Film anhand des Titels ausgewählt und dieser anschließend von irgendeinem geeigneten Server der Plattform ausgeliefert wird.

Ebenfalls aus diesem Ansatz resultiert das Publish-Subscribe-Kommunikationsmuster, bei dem eine Datenquelle bekannt gibt, welche Informationen sie zur Verfügung stellen kann. Bei diesem für das Internet der Dinge[18] wichtigen Kommunikationsansatz abonnieren Interessenten gezielt bestimmte Informationen, die ihnen bei Aktualisierung automatisch zugestellt werden (bspw. neue Werte von Sensoren).

3.3 SICHERHEIT

Ein wichtiger Aspekt bei allen Forschungsansätzen ist die Sicherheit. Aus Forschungsnetzen der Frühzeit der Datenkommunikation entwickelt, ist die ursprüngliche Internetarchitektur von einem kooperativen Ansatz geprägt, der bei räumlicher Ausdehnung der Netze und Nutzung durch vielfältige Gruppen an seine Grenzen gestoßen ist. Aktuelle Forschung und Weiterentwicklungen werden sich daher immer mit Aspekten der Sicherheit beschäftigen müssen. Zudem wandeln sich die Schwerpunkte von Sicherheit entsprechend den aktuellen Herausforderungen, wie die gestiegene Bedeutung vertraulicher Kommunikation in den letzten Jahren gezeigt hat.

Zwei Beispiele illustrieren die Beschäftigung mit dem Thema Sicherheit in der Future-Internet-Forschung:

- Die Datensicherheit kann mit den Informationsobjekten selbst verbunden werden (Dateiverschlüsselung, signierte E-Mails …), während die heutige Nutzung von Transportsicherheit (TLS, SSL, HTTPS …) eine zusätzliche, von der zu schützenden Information unabhängige Funktion darstellt. Hier gilt es nach wie vor, verbesserte Verfahren zu entwickeln, aber auch die Benutzbarkeit zu erleichtern.
- Eine andere interessante Möglichkeit ist die Absicherung der Adressierung mittels kryptografischer Funktionen. Da sich im heutigen Internet die Absenderadressen leicht fälschen lassen, sind darauf basierende Angriffsszenarien entwickelt worden, die tagtäglich eingesetzt werden. Angriffe dieser Art können nicht einfach an jeder Stelle im offenen, aus vielen Teilnetzen zusammengesetzten Internet erkannt werden und sind daher nur schwer zu bekämpfen. Auch ein informationszentrischer Ansatz würde das Problem von Denial-of-Service-Angriffen[19] auf gezielt ausgewählte Geräte stark reduzieren, da der Nutzerdatenverkehr nicht mehr auf Geräteadressen referenzieren würde.

3.4 SELBSTSTÄNDIGE OPTIMIERUNG

Die Architektur der Internet-Protokollfamilie beruht auf geschichteten, aufeinander aufbauenden Protokollen. Dabei nutzt jede Schicht zur Erfüllung ihrer Aufgaben die Funktionen der darunterliegenden Schicht. Eine Stärke dieses Ansatzes liegt in der Abstraktion, was meint, dass jede Protokollschicht in Richtung der höheren Schichten und letztlich zu der Anwendung genau definierte Dienste anbietet, deren konkrete Realisierung

[18] Vielfältige Alltagsgegenstände (Haushaltsgeräte, Maschinen, Fahrzeuge …), die mittels integrierter Kommunikationskomponenten über das Internet mit klassischen IT-Komponenten, miteinander und damit mittelbar mit Menschen interagieren können.

[19] Denial-of-Service-Angriffe: Überlasten von Geräten durch übermäßig viele, unseriöse Kommunikationsaufforderungen

DIE VIRTUALISIERUNG REALISIERT Z.B. ROUTERFUNKTIONEN DURCH DAS ZUSAMMENSPIEL UNIVERSELLERER GERÄTE.

aber verbirgt. So kann man sich bei einigen Protokollen bspw. darauf verlassen, dass Daten fehlerfrei übertragen oder ggf. korrigiert werden. Dieser Ansatz erlaubt eine sehr einfache Kombination verschiedener Protokolle entsprechend den Anforderungen der Anwendungen und den Umständen bei der Nutzung. Ändern sich allerdings die Umstände der Nutzung dynamisch, bspw. durch den Wechsel von einer festen zu einer mobilen Internetanbindung, kann das dazu führen, dass nicht in allen Schichten optimal aufeinander abgestimmte Protokolle genutzt werden. Ein einfaches Beispiel: Da bei der Telefonie keine Zeit für die Wiederholung einer fehlerhaften Übertragung ist, werden von vornherein zusätzlich Korrekturdaten übertragen. Je nach Qualität des Transports können diese überflüssig sein. Die übergreifende Sicht auf den Protokollstapel und die gegenwärtigen Umstände der Datenübertragung bietet daher evtl. Möglichkeiten der Optimierung (»Cross Layer Optimization«). Ein weiteres Beispiel ist, dass ein Video je nach Displaygröße in der optimalen Auflösung ausgeliefert wird.

Neben der selbstständigen Optimierung der Protokoll- und Parameterauswahl spielt auch die Automatisierung im Netz selbst eine wichtige Rolle. Eine Aufgabe des Netzwerkmanagements ist die optimale Verteilung des Datenverkehrs auf die vorhandenen Ressourcen (Leitungen, Router …, ggf. auch Sicherheitsgeräte und Zwischenspeicher), wobei eine manuelle Konfiguration von Netzen in weiten Teilen nicht mehr praktikabel ist.

3.5 VIRTUALISIERUNG UND SOFTWARE-DEFINED NETWORKING

Die für die Internetforschung notwendigen Experimentalnetze werden auf bestehende Infrastrukturen aufgesetzt. Das Internet mit seinen physischen Eigenschaften, z. B. verfügbare Datenraten und Laufzeiten, dient dabei als Transportinfrastruktur, auf der die neuen Techniken implementiert und ausprobiert werden können, bspw. eine neue Form der Adressierung oder die Nutzung neuer Dienste (Dienste der Netzebene, aber auch zur Informationsverteilung und -verarbeitung) eines zukünftigen Netzes. Dieses Vorgehen bildet gleichzeitig einen möglichen Migrationspfad vom derzeitigen Internet zu einem Future Internet, da auf diese Weise Netze nach herkömmlichen Standards und neue Netze parallel genutzt werden können und somit ein schrittweiser Übergang zwischen verschiedenen Ansätzen möglich ist. Beim Aufbau der Experimentalnetze kommt das Prinzip der Virtualisierung zum Einsatz.

Die Netzwerkvirtualisierung realisiert klassische Funktionen spezifischer physischer Geräte durch das Zusammenspiel verschiedener, oft allgemeiner einsetzbarer Geräte. Anwendungen bemerken davon nichts. Generell erlaubt die Virtualisierung die Entkopplung zwischen den physischen Gegebenheiten und der tatsächlichen Nutzung. Es werden also bestehende Basisdienste (wie der Transport von Daten) genutzt, um neue, erweiterte Funktionen anzubieten (bspw. parallele Transportnetze mit unterschiedlicher Übertragungsqualität). Dieses Vorgehen kann dazu beitragen, die vorhandenen Ressourcen einfacher zu verwalten oder Komplexität zu verdecken. Aber auch in Sicherheitskonzepten spielt die Virtualisierung eine wichtige Rolle: Verschiedene logische Verbindungen auf dem gleichen physischen Übertragungsmedium können vollständig voneinander getrennt werden, sodass ein Übergang zwischen den verschiedenen entstehenden virtuellen Netzen nicht möglich ist.

Einen Schritt weiter geht das Konzept des Software-defined Networking (SDN), bei dem die beiden wesentlichen Funktionen von Netzwerkkomponenten getrennt werden: die Weiterleitung der Datenpakete (»Data Plane«) und die Steuerung dieser Weiterleitung (»Control Plane«). In einem klassischen Router sind beide Funktionen in einem Gerät vereint, das ankommende Datenpaket wird innerhalb des Routers untersucht und entsprechend einer lokalen Entscheidung weitergeleitet. Mithilfe des SDN-Konzepts kann die Weiterleitung der Pakete von ver-

	Leistungsfähigkeit	Sicherheit	Wirtschaftlichkeit
Adressierung	+		
Informationszentrische Netze	+	+	+
Selbstständige Optimierung	+	(+)	+
Virtualisierung und SDN	+	+	+

Tabelle 1: Zuordnung der Forschungsansätze zu den Anforderungsdimensionen

gleichsweise einfachen und leistungsfähigen Switches[20] vorgenommen werden, die geräteübergreifend gemeinsam gesteuert werden. Diese zentrale Steuerung bietet aufgrund der vorhandenen Informationen über das Netz Möglichkeiten zur Automatisierung und Optimierung. Dadurch, dass die Kommunikationsbeziehungen an zentraler Stelle bekannt sind, können notwendige Netzwerkressourcen nach Bedarf zugeordnet und die entsprechende Konfiguration der Geräte automatisiert vorgenommen werden. Software-defined Networking erhöht somit die Flexibilität und Skalierbarkeit von Netzen und unterstützt damit insbesondere die bessere Nutzung von Ressourcen und die Automatisierung des Netzwerkmanagements.

3.6 FAZIT

Aus dem Bereich der Future-Internet-Forschung gibt es eine Reihe von neuen, disruptiven Ansätzen, die insbesondere die Sichtweise auf Funktionen des Netzes erweitern und dadurch interessante Impulse auch für die schrittweise Weiterentwicklung des Internets geben.

Im Mittelpunkt der Forschung steht die Verbesserung der Leistungsfähigkeit von Netzen, entweder in Form neuer Funktionen oder als Anpassung an veränderte Nutzungsgewohnheiten. Ein Faktor der Leistungsfähigkeit, der wesentlichen Einfluss auf die Wirtschaftlichkeit beim Betrieb von Netzen hat, ist die Automatisierung des Netzwerkmanagements. Bei allen Entwicklungen ist Sicherheit ein Aspekt, der aufgrund gesammelter Erfahrungen von vornherein beim Entwurf neuer Mechanismen berücksichtigt wird. (S. a. Tabelle 1.)

Die Forschung im Bereich Future Internet zeigt folgende Möglichkeiten auf:

- Trennung von Orts- und Identitätsbezug einer Internetadresse zur Unterstützung von Mobilität und Portabilität, sowohl von Endgeräten einschließlich Servern als auch von ganzen Netzen[21];
- Entkopplung von Informationsquelle und -nutzung durch informationszentrische Netze, wobei sich notwendige Sicherheitsmechanismen stärker auf die zu schützende Information als auf beteiligte Geräte beziehen;
- übergreifende Optimierung von Protokollmechanismen entsprechend dem konkreten Einsatzgebiet der Kommunikation; positive Auswirkungen auf die Wirtschaftlichkeit stammen hauptsächlich aus der Vereinfachung des Netzwerkmanagements und weniger aus der eigentlichen Datenübertragung;
- Netzwerkvirtualisierung und Software-defined Networking erlauben – ausreichende Ressourcen in Form von Übertragungskapazität und Rechenleistung vorausgesetzt – einen flexiblen und automatisierten Betrieb von Netzen. Im Idealfall erlaubt die dadurch mögliche feingranulare Steuerung von Netzen eine Optimierung von Leistungsfähigkeit, Sicherheit und Wirtschaftlichkeit für unterschiedliche Nutzungsszenarien auf einer gemeinsamen Basisinfrastruktur.

[20] Switches entscheiden nicht bei jedem Paket erneut anhand von Paketparametern und Netzzustand über den nächsten Streckenabschnitt, sondern benutzen für dessen Ermittlung eine einfache, vorkonfigurierte Abbildungstabelle.

[21] Das schließt auch die Nutzung eigener, weltweit erreichbarer IP-Adressbereiche ein, die von einer Organisation selbst verwaltet werden, im Gegensatz zu der herkömmlichen Nutzung eines IP-Adressbereichs des Internet Service Providers (ISP).


United States

4. DER MARKT ALS TREIBER

Eine globale Einigung über eine neue Art der Vernetzung, wie sie in der Future-Internet-Forschung angestrebt wird, ist nur schwer vorstellbar. Das Internet ist inzwischen wirtschaftlich so wichtig geworden, dass selbst eine mittelfristige Umstellung aller Dienste und Angebote unmöglich erscheint. Trotzdem gibt es insbesondere aus wirtschaftlicher Sicht den Druck zur Weiterentwicklung des Internets, wie bereits in Abschnitt 2.3 angesprochen.

Leichter umzusetzen als internetweite netzinterne Protokolländerungen sind sukzessive Anpassungen des Internets, wie

- Strukturveränderungen, nach denen Daten an anderen Orten als bisher aufbewahrt und somit über andere (meist kürzere) Wege im Internet transportiert werden;
- die qualitative Diversifizierung von Übertragungswegen, soweit sie individuell von einzelnen bzw. bilateral kooperierenden Netzbetreibern oder auf der Basis von Vorkonfiguration angeboten werden kann.

4.1 VERTEILTE INHALTE

Die interne Struktur des Internets verändert sich derzeit vor allem aufgrund von zwei Entwicklungslinien:

- Hochauflösendes Videostreaming über das Internet, sei es für das unmittelbare Betrachten von Filmen oder Live-Fernsehen, für qualitativ ansprechende Videokonferenzen oder für anspruchsvolle Online-Spiele
- Verlagerung nicht-öffentlicher Daten und zunehmend auch der Verarbeitung »in die Cloud« (d. h. auf Server, mit denen über das Internet interagiert wird), sei es eine kommerzielle Drittanbieter-Cloud oder ein kommunales Rechenzentrum

Will man sich Videoströme unmittelbar ansehen, benötigt man neben der erforderlichen Datenrate einen gleichmäßigen Datenstrom und eine geringe Fehlerrate zwischen Server und Endgerät. Da das Internet nicht durchgängig die benötigte Qualität garantiert, müssen die Dienstanbieter, also z. B. Videoportale oder Fernsehsender, mit ihren Daten möglichst nahe an die Kunden heranrücken, um die Unwägbarkeiten des Internets zu reduzieren. Unterstützt beispielsweise der Anschlussbetreiber des Kunden in seinem Zuständigkeitsbereich die besonderen Ansprüche von Videostreaming, kann es für einen Streaminganbieter vorteilhaft sein, den verwendeten Server ebenfalls im Zuständigkeitsbereich des Anschlussbetreibers stehen zu haben.

Ähnlich verhält es sich, wenn interaktive Dienste auf Daten oder Verarbeitung »im Internet« angewiesen sind. Hier wird die Verfügbarkeit des Dienstes vor allem durch ein angemessenes Antwortverhalten bestimmt. Wenn bisher offline oder lediglich innerhalb eines lokalen Netzwerkes genutzte Dienste in eine Cloud bzw. ein (entferntes) Rechenzentrum verlagert werden, erwarten die Benutzer, dass sich das Antwortverhalten dadurch nicht negativ verändert.

Überregionale Dienstanbieter verteilen ihre Dienstangebote bzw. die Daten nach Gesichtspunkten der Wirtschaftlichkeit: Wenn es finanziell günstiger ist, Dienste oder Daten geografisch verteilt mehrfach vorzuhalten, weil durch die kürzeren Wege zum Kunden geringere Zahlungen an Netzbetreiber anfallen, wird ein sogenanntes Content-Delivery-Netz aus mehreren Servern genutzt.

Große Streaming- und Cloudanbieter müssen die Datenbestände von vornherein, z. B. wegen der Leistungsfähigkeit der Server oder der Datenrate am Serveranschluss, auf mehrere Server verteilen. Damit sind sie für den Aufbau eines geografisch verteilten Servernetzes besser vorbereitet als kleine und kleinste Anbieter, für deren Angebot prinzipiell ein einzelner Server ausreichen würde.

Für kleine und kleinste Anbieter, wozu im relevanten Maßstab auch Kommunen gehören können, lohnt sich der Betrieb eines eigenen, geografisch verteilten Servernetzes nicht. Für sie bietet es sich an, die Dienste eines – vertrauenswürdigen – Content-Delivery-Network-Betreibers zu nutzen. Dieser stellt auf seinen Servern die Daten mehrerer Kunden nutzernah bereit.

Livestream-Anbieter können ihre Daten nicht »auf Vorrat« auf ein Servernetz verteilen. Große Anbieter wie Fernsehsender verfügen jedoch typischerweise über ein vom Internet unabhängiges Backbone-Verteilnetz[22] (z. B. zu regionalen Antennen) und können an den entsprechenden Endpunkten einen kundennahen Übergang in das Internet realisieren.

[22] Backbone-Verteilnetz: Geografisch weiträumiges Verteilnetz mit Anschlusspunkten zur regionalen/lokalen Weiterverteilung

DIE REICHWEITE VON FUNKLÖSUNGEN BEEINFLUSST DIE NOTWENDIGE ROUTER- UND SERVERDICHTE.

4.2 REDUZIERUNG DER REAKTIONSZEIT

Eine weitere Internet-Entwicklungslinie entsteht gerade: Im Kontext von Industrie 4.0[23], kooperativem Fahren oder im Zusammenhang mit dem Begriff »Taktiles Internet«[24] ist die Rede von z. T. extrem kurzen Antwort- bzw. Reaktionszeiten im Bereich einer Millisekunde – und das bei gleichzeitig sehr geringer Fehler- und Verlustrate[25]. Bereits wenn man die stets notwendigen Bearbeitungszeiten bei Sender und Empfänger außer Acht lässt, begrenzt hier die Signalgeschwindigkeit von rund 2 * 108 m/s auf typischen Leitungen die Entfernung zwischen den Kommunikationspartnern auf etwa 100 km.

Die reine Übertragungszeit stellt zwar kein Problem dar, wenn z. B. Fahrzeuge in geringem Umkreis direkt miteinander kommunizieren. Ist aber ein zentraler, geografisch entfernter Server beteiligt, kann die Datenübertragung zu lange dauern. In diesen Fällen wird also ein ausreichend dichtes Netz von Servern erforderlich sein, die nicht nur Daten zum Abruf bereithalten, sondern komplexe Berechnungen auf Basis vieler Einzeldaten durchführen können.

Bei vielen Nutzungsszenarien von Industrie 4.0 oder des Internets der Dinge ist allerdings die Rechtzeitigkeit durchaus entfernungsabhängig: Informationen über Störungen einer örtlich direkt nachgelagerten Produktionsstrecke oder über einen wenige Straßenkreuzungen entfernten Stau benötigt man »sofort«, während Störungsmeldungen von einem 20 km entfernten Zulieferer oder Meldungen über einen 100 km entfernten Unfall meist auch nach Minuten noch rechtzeitig sind, um angemessene Aktionen durchführen zu können.

Es ist nicht zu erwarten, dass das Internet der Dinge oder Industrie 4.0 in absehbarer Zeit massive Auswirkungen auf die Kernzone des Internets haben werden, weil auch zukünftig Maschinen, Sensoren/Aktuatoren oder Fahrzeuge nicht in großem Maßstab über weite Entfernungen direkt miteinander (jeder mit vielen) interagieren werden.

Für Fahrzeug-zu-Fahrzeug- oder Fahrzeug-zu-Infrastruktur-Kommunikation und für die öffentliche Vernetzung mobiler »Dinge« werden am Zugang in der Übertragungsebene vornehmlich Nahbereichs-Funktechniken ohne Reservierung eingesetzt, d. h. es gibt keine Zugangseinschränkungen und nur eine kollaborative Benutzungssteuerung. Hier muss die Zukunft zeigen, ob die entstehende Konkurrenzsituation lokale oder generelle Benutzungseinschränkungen erfordert, die sich auf die Struktur des öffentlichen Internets auswirken. Denkbar wären hier z. B. Reichweiten- oder Aktivitätseinschränkungen, die Einfluss auf die notwendige Router- und Serverdichte haben können.

Eine reduzierte Reaktionszeit ist auch oft Anlass für den Aufbau oder begrüßter Nebeneffekt eines Content-Delivery-Netzes (s. Abschnitt 4.1).

4.3 MOBILE NUTZUNG

Während in der Anfangszeit die Internetnutzung auf leitungsgebundene Festnetzkommunikation beschränkt war, hat inzwischen die Nutzung von mobilfunkbasierten Zugangsnetzen einen hohen Anteil erreicht. Mehr und mehr erfolgt die mobile Nutzung auch über öffentlich zugängliche lokale Netze, vornehmlich WLANs.

---

[23] Umfassende Vernetzung von Produktionsanlagen, Betriebssteuerung usw. bis hin zu Vorprodukten und Werkzeugen, auch unternehmensübergreifend, um individuelle Produkte effizient und just in time industriell herstellen zu können.

[24] Taktiles Internet: die (fast) unmittelbare Rückkopplung komplexer haptischer, visueller oder anderer Sinneseindrücke

[25] http://www.elektroniknet.de/elektronikfertigung/strategien-trends/artikel/106806/ und http://www.stiftungaktuell.de/wp-content/uploads/2014/07/Positionspapier_Das_Taktile_Internet_final.pdf

Aus diesen Verschiebungen ergeben sich Konsequenzen für die Struktur des öffentlichen Internets: Server für bestimmte qualitäts- oder zeitkritische Dienste müssen auch an die Mobilfunk-Zugangsnetze, möglicherweise zukünftig sogar an zentrale WLAN-Hotspots heranrücken (s. dazu die Abschnitte 4.1 und 4.2). Diese Angebote müssen wegen der Mobilität der Nutzer an noch mehr Orten vorgehalten werden. Mobilfunktechnik kann in Bezug auf Mobilitätsanforderungen aber auch dazu beitragen, die herkömmliche, einfache Struktur des Internets zu bewahren und gleichzeitig die Leistungsfähigkeit zu erhöhen: Bei der Nutzung von Mobilfunk kommt die Netzebene günstigstenfalls ohne Mobilitätsmechanismen aus.

Die Ergänzung bzw. der Austausch von mobil genutzten Offline-Programmen durch Online-Funktionen und -Dienste der bisherigen oder neuer Anbieter ist ebenfalls ein Trend. Selbst dann, wenn es dabei um hochaktuelle Daten, z. B. zum Verkehrsgeschehen, geht, stellt dies das Internet im engeren Sinne nur vor geringe Herausforderungen, da die erforderlichen Datenraten und akzeptable Übertragungszeiten mit dem vorhandenen Internetausbau i. d. R. erreicht werden. In speziellen Situationen, beispielsweise bei einem großen Stau oder bei Massenveranstaltungen, kann es jedoch zu lokalen Engpässen in den betroffenen mobilfunkbasierten Zugangsnetzen (in der Übertragungsebene des Internet-Modells) kommen.

Eine spezielle Form der mobilen Nutzung könnte zukünftig das kooperative Fahren darstellen: Die beteiligten Fahrzeuge teilen ihrer Umgebung ihre eigenen Daten (Richtung, Geschwindigkeit, Beschleunigung/Verzögerung usw.) mit und reagieren auf die Daten anderer Fahrzeuge und spezifischer Infrastrukturkomponenten, ohne dass eine gezielte Kommunikation zwischen bestimmten Fahrzeugen bzw. Komponenten stattfindet.

Für die sicherheitsrelevante, zeitkritische Fahrzeug-zu-X-Kommunikation[26] wird versucht, mit regulativen Maßnahmen – z. B. Reservierung eines Frequenzbereiches für diese Kommunikation – ausreichende Kommunikationsqualität zu ermöglichen. Somit kommt auch hier eine qualitative Diversifizierung (auf die in Abschnitt 4.6 näher eingegangen wird) zum Tragen.

Die vielfältigen Dinge im öffentlichen Raum kommunizieren häufig per Nahbereichsfunk. Selbst die, die nicht mobil sind, benötigen in diesem Fall nahe gelegene Router oder Server, über die bzw. mit denen sie Daten austauschen können.

4.4 ZUSAMMENWACHSEN VON NETZEN

Aus der Perspektive der Nutzer wird es schon jetzt immer schwieriger, »reine« Internetnutzung – also Kommunikation, die zwischen allen beteiligten Parteien ausschließlich auf Übertragungsstrecken, Komponenten und Protokollen des öffentlichen Internets beruht – von verschiedenen gebräuchlichen Mischkonfigurationen zu unterscheiden:

- Selbst wenn im lokalen Netz des Nutzers und mit dem Anschlussbetreiber bereits IP-Telefonie benutzt wird (All-IP-Anschluss), erfolgt jenseits des Anschlusses häufig ein Übergang auf ein separates Netz.
- Fernseh- und Rundfunkanlieferung erfolgen beim Nutzer über denselben Festnetzanschluss wie die Internetkommunikation. Dass dabei die Signale erst kurz zuvor zusammengeführt werden, entzieht sich dem Nutzer.
- Viele Angebote, z. B. Fernsehen und Rundfunk, stehen sowohl über klassische Wege als auch über das Internet zur Verfügung. Multifunktionsendgeräte (Smart-TVs) und entsprechende Bedienmechanismen (Widgets/Apps) lassen mehr und mehr verblassen, auf welchem Weg die Daten in das Gerät gelangt sind.

[26] Fahrzeug-zu-X: Fahrzeug-zu-Fahrzeug, Fahrzeug-zu-Infrastruktur.

DURCH ANWENDUNGSPLATTFORMEN ENTSTEHEN NEUE DATENSTRÖME ODER EXISTIERENDE WERDEN GEBÜNDELT.

– Zukünftig werden beispielsweise durch Fahrzeug-zu-Infrastruktur-Kommunikation oder durch die Vernetzung von »Dingen« im öffentlichen Raum weitere öffentliche Netze mit dem Internet verbunden oder Teil desselben.

4.5 (ANWENDUNGS-)PLATTFORMEN UND ÖKOSYSTEME

Ursprünglich bildete das Internet lediglich eine Kommunikationsplattform, über die beliebige Anwendungskomponenten Daten austauschen und (Anwendungs-)Dienste realisieren konnten.

Bereits heutzutage ist zu beobachten, dass mehr und mehr Anwendungsplattformen auf Internetbasis entstehen: Dienstleister bieten Komponenten und Blaupausen an, mit denen Dritte ihre komplexen Anwendungen umsetzen können: Als Beispiele können so unterschiedliche Dinge wie Online-Marktplätze – auf denen viele Anbieter nach einheitlichen Regeln ihre eigenen Shops »aufstellen« können – oder Hardware-as-a-Service – entfernte, nach Nutzerbedürfnissen konfigurierte virtuelle Computer – genannt werden. Durch die Etablierung derartiger Anwendungsplattformen entstehen neue Internetdatenströme oder bestehende werden gebündelt. Große Plattformen stehen damit in enger Wechselwirkung mit der Kommunikationsinfrastruktur, da sie je nach Ausprägung viele oder hochratige Datenströme unterstützen müssen und die dafür erforderlichen Internetressourcen benötigen.

Während die Benutzung von Plattformen besonders kleinen und mittleren Unternehmen bereits oft als wirtschaftlich unverzichtbar erscheint, kann sich daraus auch die Gefahr einer Monopolisierung oder eines Vendor Lock-in (unerwünschte Bindung an einen Anbieter wegen hoher Umstiegskosten) ergeben, wenn die Schnittstellen zur Plattform nicht standardisiert sind und nicht von mehreren Anbietern unterstützt werden.

Ein im ersten Schritt zu Content-Delivery-Netzen (s. Abschnitte 4.1 und 4.2) gegenläufiger Effekt – eine verstärkte Konzentration – tritt auf, weil viele Dienstanbieter ihr Portfolio verbreitern und die Nutzer häufig, z. B. aus Bequemlichkeitsgründen, zur Nutzung der Dienste eines einzigen Anbieters übergehen. Exemplarisch für solche Ökosysteme sind Social-Network-Dienste, die wie selbstverständlich inzwischen mit individuellen E-Mail-Diensten oder mit über das soziale Netzwerk hinausgehenden Suchfunktionen verbunden sind.

Bei einigen Plattform- und Ökosystembetreibern ist bereits eine Verbreiterung des Geschäftsmodells auf für sie relevante Teile der Internet-Kommunikationsinfrastruktur zu beobachten, z. B. durch den Betrieb von dedizierten Übertragungsstrecken zu ihren Servern oder die Bereitstellung von (alternativen) Zugangsnetzen. In anderer Hinsicht verbreitern sich Ökosysteme, indem nicht nur die anwendungsbezogenen Dienste aus einer Hand kommen, sondern auch das Betriebssystem und entsprechend vorkonfigurierte Endgeräte angeboten werden.

Ökosysteme können sich für den Nutzer besonders komfortabel darstellen, z. B. durch eine übersichtliche Navigationsstruktur und ein einheitliches Look-and-feel, und dadurch mittelbar sogar die Sicherheit wegen geringerer Gefahr der Fehlbedienung erhöhen. Zugleich bergen sie die erhöhte Gefahr, sich einer Beeinflussung auszusetzen, da dem Anbieter nutzerspezifische Informationen anwendungsübergreifend zur Verfügung stehen, die dieser für die gezielte Auswahl und Sortierung angezeigter Inhalte und Werbung nutzen kann.

4.6 QUALITATIVE DIVERSIFIZIERUNG DES INTERNETS

Neben den Strukturveränderungen im bzw. am öffentlichen Internet wird es zukünftig verstärkt weitere Übertragungsangebote geben, die zwar ebenfalls im Wesentlichen Internettechnik einsetzen, aber beispielsweise vom öffentlichen Internet

NETWORK SLICING ERLAUBT, INNERHALB EINES NETZES VERSCHIEDENE ÜBERTRAGUNGSDIENSTE ANZUBIETEN.

unabhängige physische Übertragungsstrecken oder reservierte Kontingente auf gemeinsamen Übertragungsstrecken nutzen.

Für Datenströme, die sich aufgrund ihrer inkompatiblen Qualitäts- oder Sicherheitsanforderungen in einem gemeinsamen System aus Leitungen und Routern gegenseitig negativ beeinflussen könnten, ist der Transport auf separaten Übertragungssystemen möglich. Dies ist jedoch oft nicht wirtschaftlich, weil alle Systeme mit nur selten benötigter, hoher Leistungsfähigkeit vorgehalten werden müssten.

Eine heute genutzte Variante ist das MPLS-Verfahren[27]. Mittels MPLS werden Datenströme speziell gekennzeichnet (»Labeling«) und in Routern auf vorkonfigurierte Art und Weise weitergeleitet. Dies erspart die beim Einsatz der Internettechnik sonst üblichen, zeitaufwändigen Routingentscheidungen pro Nachricht. Zusätzlich können auf den Übertragungsstrecken Kontingente für bestimmte Labels reserviert werden. Ein MPLS-Pfad über mehrere Router hinweg kann so günstigstenfalls ähnlich geringe Laufzeiten erreichen wie eine durchgehende Übertragungsstrecke zwischen den Endpunkten des Pfades. MPLS ermöglicht damit die Nutzung gemeinsamer Router und gemeinsamer Übertragungsstrecken für Datenströme mit unterschiedlichen Qualitätsanforderungen. MPLS-Pfade mit reservierter Kapazität sind zudem gegen Überlastangriffe durch Dritte geschützt, da in diese Pfade nur an den konfigurierten Endpunkten Daten eingespeist werden können.

[27] MPLS: Multiprotocol Label Switching, ein verbindungsorientiertes Übertragungsverfahren unterhalb der Netzebene

Bislang werden MPLS-Pfade üblicherweise nur innerhalb des Zuständigkeitsbereiches eines einzelnen Netzbetreibers angeboten. Vielfach sind sie langfristig konfiguriert und können nicht kurzfristig bei Bedarf angefordert werden.

Zukünftig werden zudem verstärkt Virtualisierungstechniken eingesetzt. Ein Beispiel ist Network Slicing[28], das bei der kommenden 5. Mobilfunkgeneration (5G) zum Einsatz kommt und es erlaubt, innerhalb eines Netzes verschiedene, anwendungsspezifische Übertragungsdienste anzubieten. Treiber für die Diversifizierung sind Anforderungen an die Dienstqualität, wie Laufzeit und Laufzeitschwankungen der Daten, Fehler- und Verlustcharakteristika. Für bestimmte, wichtige Anwendungen, z. B. Telefonie, ist die Verfügbarkeit (mit einer Mindestqualität) sogar ein Sicherheitsmerkmal.

Über solche alternativen Übertragungswege sind nicht mehr alle Internetnutzer erreichbar, sondern nur die jeweils organisatorisch angeschlossenen Nutzer. Je nach Abschottung gegenüber dem allgemeinen Internet können so nicht-öffentliche Segmente entstehen. Allerdings sind auch Übergänge zwischen den alternativen Wegen und dem allgemeinen Internet möglich. So könnte z. B. Videoconferencing am Netzzugang ausgekoppelt und unabhängig von sonstigem Internetverkehr übertragen werden.

Ein gern vorgebrachtes Beispiel für die Möglichkeiten eines taktilen Internets ist die entfernte Durchführung chirurgischer Eingriffe. Diese Rückkopplung muss unabhängig von der Entfernung in sehr kurzer Zeit erfolgen. Es wird leicht klar, dass vereinzeltes Ruckeln – das Halten eines alten Bildes bis zum Eintreffen eines fehlerfreien Bildes nach einer Störung – nicht nur unkomfortabel, sondern lebensgefährlich sein kann. Die Signal-

[28] 5G Systems, Ericsson White Paper, Januar 2017, https://www.ericsson.com/res/docs/whitepapers/wp-5g-systems.pdf und ÖFIT Trend und Themensammlung zu 5G unter http://www.oeffentliche-it.de/-/5g

	Leistungsfähigkeit	Sicherheit	Wirtschaftlichkeit
verteilte Inhalte	+	+	+
Reaktionszeit	+	(+)	
mobile Nutzung	+	(+)	
Netzvereinheitlichung			+
Plattformen/Ökosysteme		+	+
Qualitative Diversifizierung	+	++	

Tabelle 2: Zuordnung der Weiterentwicklungen zu den Anforderungsdimensionen

laufzeiten und die Fehler- und Verlustcharakteristika auf den Übertragungstrecken setzen hier physikalische Grenzen. Allerdings lassen sich diese ausreizen, indem möglichst wenige Übertragungsstrecken benutzt werden, die zudem sehr geringe Fehler- und Verlustraten aufweisen. Zwischen den einzelnen Übertragungsstrecken sollte der Weg bevorzugt über – geringere Verzögerungen verursachende – vorkonfigurierte Router, z. B. unter Verwendung des MPLS-Verfahrens, geführt werden.

Im Bereich Industrie 4.0 kann es ähnliche Situationen wie bei medizinischen Operationen geben, wenn industrielle Prozesse aus der Ferne überwacht werden sollen und ggf. ein unverzügliches Eingreifen notwendig ist, um Verletzungen von Mitarbeitern oder Schäden an Maschinen oder Werkstücken zu verhindern. Auch hier werden dedizierte Übertragungswege mit erhöhter Qualität gegenüber dem öffentlichen Internet notwendig sein. Ziel ist es allerdings auch, derartige Überwachungs- und Notfallreaktionsfunktionen vor Ort zu automatisieren.

4.7 FAZIT

Die unter Marktgesichtspunkten stattfindenden, schrittweisen Weiterentwicklungen des Internets sind stets eine Reaktion auf mindestens eine der in Abschnitt 2.3 betrachteten Anforderungsdimensionen, s. Tabelle 2.

Insgesamt führt die zunehmende Vernetzung dazu, dass

- Daten und Dienste auf von vielen Orten aus zugreifbare, logisch zentrale Server (z. B. »in die Cloud«) verlagert werden
- Server, auf denen Daten, Dienste oder Verarbeitungskapazität verteilt bereitgehalten werden, räumlich nah an den Endnutzern installiert werden, bspw. um trotz verteilten Zugangs die Reaktionszeiten zu verkürzen,
- Server auch an Mobilfunkzugangsnetze oder sogar an WLAN-Hotspots heranrücken, um den Anforderungen der verstärkten mobilen Nutzung gerecht zu werden,
- weitere öffentliche Netze mit dem Internet verbunden werden und mehr und mehr Dienste Internettechnik durchgängig nutzen (IP-Telefonie, Fernsehen usw.),
- Plattformen und Ökosysteme entstehen, die teils bereits ihre eigenen Übertragungsstrecken und Zugangsnetze betreiben und für ihre Nutzer zum »Pförtner« für das Internet werden, z. B. ausgehend von Suchmaschinen oder sozialen Netzwerken,
- nicht-öffentlich genutzte Übertragungsstrecken und reservierte Kontingente auf gemischt genutzten Leitungen zunehmen, z. B. unter Einsatz von MPLS-Technik oder Network Slicing.


ВОСТОК

5. VOM HEUTIGEN INTERNET ZUR VERNETZUNG MITTELS INTERNET-TECHNIK

Können die Nutzeranforderungen bei Verwendung des öffentlichen Internets und der dafür eingesetzten Übertragungsstrecken nicht erfüllt werden, entstehen alternative bzw. zusätzliche Angebote und Strukturen. Je nach Art der Anforderungen sind aus Nutzersicht dafür separate physische Anschlüsse (Zugänge), zusätzliche Geräte am Anschluss (in der Zuständigkeit des Nutzers oder des Netzbetreibers) oder lediglich spezielle Software (beim Nutzer und/oder beim Netzbetreiber) erforderlich. Über die Nutzersicht hinaus finden zusätzlich Strukturveränderungen im oder am Internet statt.

Entstehende Angebote und Strukturen können dabei Teil des zukünftigen öffentlichen Internets sein – d. h. der gegenseitigen Erreichbarkeit beliebiger Teilnehmer dienen – oder nur einem geschlossenen Kreis von Teilnehmern vorbehalten sein. Gegen Denial-of-Service-Angriffe kann beispielsweise ein separater Anschluss helfen, der nur Kommunikation mit einem eingeschränkten (vertrauenswürdigen) Teilnehmerkreis ermöglicht. Ein solcher Anschluss schafft – auch wenn Internettechnik eingesetzt wird – allerdings keinen Zugang zum öffentlichen Internet, sondern nur zu einem (virtuellen) nicht-öffentlichen Netz des speziellen Teilnehmerkreises.

Die Erweiterung des Funktionsumfangs des Internets selbst ist ein schwieriger und langwieriger Prozess, der vor allem auch die Komplexität des Systems »Internet« ansteigen lassen kann. Um einerseits der Dynamik bei der Entwicklung neuer Vernetzungsszenarien und andererseits der eher langfristigen Weiterentwicklung des öffentlichen Internets Rechnung zu tragen, ist die gleichzeitige Nutzung verschiedener Netze derzeit die beste Option. Entsprechend den jeweiligen Anforderungen können separate Netze ausgeprägter in Bezug auf ihre jeweiligen Haupteigenschaften optimiert werden.

Nun könnte man einwenden, dass es genau das ja schon gab – für die verschiedenen Kommunikationsarten wurden in der Vergangenheit unterschiedliche Netze genutzt. Der entscheidende Unterschied ist die durchgängige Verwendung des Internet-Protokolls bzw. von Internettechnik. Das ermöglicht die Nutzung der gleichen standardisierten Hard- und Software-Komponenten, was sich positiv auf die Verfügbarkeit leistungsfähiger und preiswerter Komponenten auswirkt, zudem ist viel Erfahrung für die Erstellung und Nutzung dieser Komponenten vorhanden. Hinzu kommt die Durchlässigkeit für Innovationen. Neue vernetzte Anwendungen können mit vergleichsweise geringem Aufwand zur Nutzung über das Internet entwickelt werden und dann beliebigen Personengruppen und mit geringen technischen Vorbedingungen angeboten werden. Setzt sich eine neue Idee oder Realisierung durch, so kann sie einfach auch in nicht-öffentlichen Netzen oder spezialisierten Anwendungsfällen genutzt werden. An diesem Vorgehen zeigt sich die Wichtigkeit des öffentlichen Internets für Innovation und Wettbewerb. Das Ziel ist die netzseitige Unterstützung von spezifischen Anforderungen, bspw. nach einem aus Sicherheitsgründen eingeschränkten Kreis an potentiellen Kommunikationspartnern oder nach einer ausreichenden Datenrate.

Die Vernetzung wird zukünftig aus einer Vielzahl von (virtuellen) Netzen bestehen, die Internettechnik verwenden und zwischen denen unterschiedlich offene Übergänge existieren. Speziell bei nicht-öffentlichen Netzen mit mehreren Teilnehmerorganisationen – z. B. Netze, die Behörden oder Unternehmen miteinander verbinden – und (eingeschränkten) Übergängen in das öffentliche Internet verschwimmt dabei zumindest aus Nutzersicht die Grenze zwischen dem nicht-öffentlichen Netz und dem öffentlichen Internet. Virtuelle nicht-öffentliche Netze können zudem durchaus gemeinsame Ressourcen mit dem öffentlichen Internet nutzen. Eine Reservierung von Ressourcen für bestimmte Zwecke garantiert beispielsweise, dass zugesicherte Durchsatz-, Qualitäts- oder Sicherheitsanforderungen eingehalten werden.

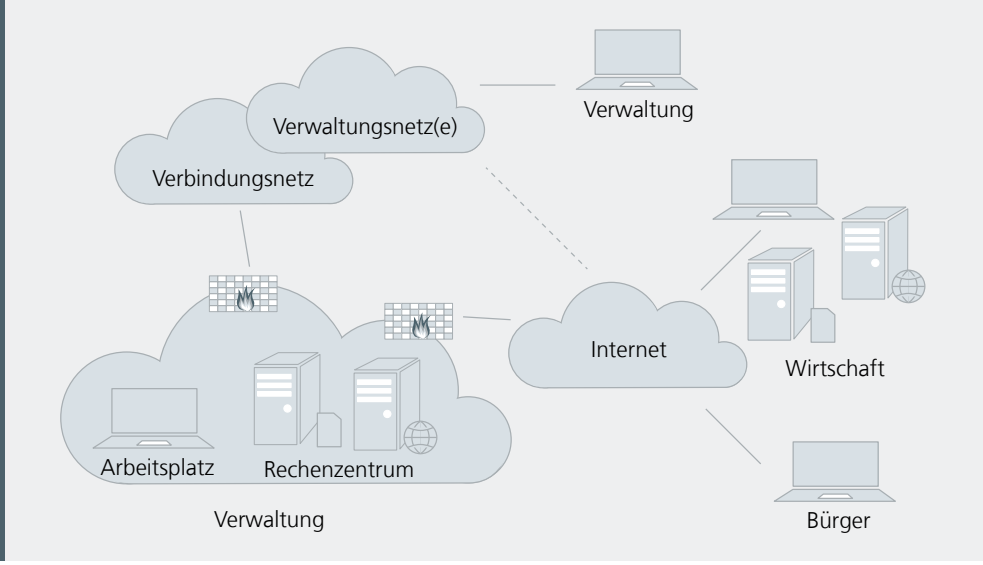

Abb. 5: Vernetzung der öffentlichen Verwaltung

6. PERSPEKTIVE DES ÖFFENTLICHEN SEKTORS

Die in Abschnitt 2.4 beschriebenen öffentlichen bzw. nicht-öffentlichen Vernetzungsalternativen lassen sich gut am Beispiel der öffentlichen Verwaltung illustrieren. Ausgehend von einem Arbeitsplatz der Verwaltung zeigt Abbildung 5 beispielhaft verschiedene Kommunikationsbeziehungen mit anderen Partnern.

Verwaltungen erreichen einander über nicht-öffentliche Verwaltungsnetze, z. B. Landesnetze, von denen bei Bedarf auch mehrere durchquert werden. Dies unterscheidet sich technisch nicht von der Vernetzung mehrerer Firmenstandorte. Die Länder und der Bund kommunizieren über das Verbindungsnetz, ein spezielles Verwaltungsnetz, miteinander.[29] Die Verwaltungsnetze können aufgabenbezogen optimiert werden und erlauben eine effektive Kontrolle der Kommunikationsbeziehungen, wodurch hohe Leistungsfähigkeit und Sicherheit erreichbar sind. Auch der gemeinsame IPv6-Adressraum der Verwaltung trägt durch die leichte Unterscheidbarkeit zwischen interner und externer Kommunikation zur Sicherheit bei.

In vielen Fällen wird die Verwaltung aber auch über das Internet mit Bürgern oder der Wirtschaft kommunizieren müssen: Einerseits stellt die Verwaltung über Rechenzentren öffentlich Informationen bereit, andererseits nutzt die Verwaltung übliche Kommunikationsdienste wie E-Mail. Eine sorgfältige Absicherung des Internetzugangs der Verwaltung bzw. von deren Rechenzentren realisiert eine Trennung zwischen dem öffentlichen Internet und den nicht-öffentlichen Infrastrukturen der Verwaltung. Die Herausforderung dabei ist die Anpassung der Verwaltung an die sich wandelnden bevorzugten Kommunikationsarten ihrer Kommunikationspartner.

Zunehmend muss die Verwaltung auch komplexere Dienste oder einen automatisierten Informationsaustausch mit Wirtschaft und Bürgern anbieten. Die Kommunikation wird dabei stets teilweise über das öffentliche Internet abgewickelt werden müssen. Hierbei kommt es in besonderem Maße auf den Einsatz von sicheren und leistungsfähigen Konfigurationen allgemein genutzter Dienste (bspw. E-Mail) oder die Nutzung von spezialisierten Protokollen (bspw. OSCI-Transport) an.

Im derzeit diskutierten Vernetzungsszenario »Smart City/Smart Region« ist die Verwaltung ein Hauptakteur. Im Mittelpunkt stehen generelle öffentliche Aufgaben wie nachhaltige Energieversorgung oder Ressourcen schonende Mobilität. Eine konkrete Realisierung könnte bspw. die Steuerung von Verkehrsflüssen auf Basis einer Vielzahl von Sensoren zur Erfassung von Umweltdaten, Fahrzeugen, freien Parkplätzen oder öffentlichen Verkehrsmitteln sein. Generell sollen technische Lösungen in Form von Informationssystemen und übergreifender Datennutzung Optimierungen und neue Anwendungen ermöglichen – man kann vom Internet der Dinge im öffentlichen Raum sprechen.[30]

Insbesondere im Bereich der Sensoren und Daten umfasst das Szenario alle möglichen Kommunikationsarten und damit Infrastrukturansätze: Sensordaten müssen zunächst sicher über nicht-öffentliche Kommunikationsbeziehungen erfasst werden, auch wenn die erfassten Daten später zur Information von Bürgern (oder zum Aufbau neuartiger Anwendungen Dritter) bspw. über Open-Data-Portale öffentlich zur Verfügung gestellt werden. Sensoren reagieren dabei allenfalls auf Anfragen ihnen bekannter Komponenten oder senden ihre Daten ausschließlich initiativ an bekannte oder unbekannte Adressaten, Letzteres beispielsweise als ungerichteter, regional begrenzter Broadcast.

[29] Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – vom 10. August 2009 (BGBl. I S. 2702, 2706)

[30] Fraunhofer FOKUS: Public IoT – Das Internet der Dinge im öffentlichen Raum, Mai 2015, https://cdn2.scrvt.com/fokus/36c5e4909a46af02/982714594f78/WP_Public_Internet_of_Things_web.pdf


esa
esa

7. HANDLUNGSEMPFEHLUNGEN

Aus den dargestellten Entwicklungen ergeben sich Handlungsnotwendigkeiten für Politik und Verwaltung sowohl bei der Ausgestaltung der öffentlichen Vernetzung und der Regulierung des Internets als auch bei Behördennetzen und -diensten.

7.1 PLANUNG & STRATEGIE

Nutzung öffentlicher und nicht-öffentlicher Vernetzung strategisch planen und zeitnah anpassen
Verfügbarkeit, Vertraulichkeit und Qualität der Behördenkommunikation, ob untereinander oder mit Bürgern und Unternehmen, müssen dem jeweiligen Anlass entsprechen. Angesichts steigender Nutzererwartungen und der anhaltenden technischen Entwicklung ist eine kontinuierliche, vorausschauende Planung und Anpassung der Infrastrukturen notwendig, um Sicherheits- und Qualitätsmängel zu vermeiden.

Auf Nutzungstrends frühzeitig und angemessen reagieren
Ob mobiles Arbeiten oder die Online-Schulung mittels videounterstütztem Webinar, ob Internet der Dinge oder Smart-City – die Verwaltung ist als Nutzer oder Anbieter dieser neuen Szenarien gefordert. Unabdingbar sind, je nach Szenario, nicht nur geeignet ausgebaute Netzinfrastrukturen, sondern auch entsprechend ausgestattete Endgeräte und notwendige Softwarekomponenten, die alle gemeinsam das erforderliche Sicherheitsniveau einhalten. Behörden benötigen aus rechtlichen oder organisatorischen Gründen hierfür einen deutlichen Vorlauf und müssen umso früher Trends erkennen und die Konsequenzen einplanen. Neben Beurteilungskompetenz sind konkrete Planung und Umsetzung unerlässlich, die über aktuelle Aspekte hinaus zukünftige Dienste und Verknüpfungen mitbetrachten.

Komplexität in Behördennetzen reduzieren
Auch bei leistungsfähigen Netzen ist es notwendig, die Komplexität der Kommunikationsinfrastruktur innerhalb von Behördennetzen möglichst gering zu halten. Eine schlankere Infrastruktur erleichtert zudem die Bewertung der Wirksamkeit von Sicherheitsmechanismen.

Zur Reduktion der großen Zahl intermediärer Systeme wie Switches, Router, Gateways, Firewalls usw. sind die Entwicklung, Umsetzung und regelmäßige Aktualisierung eines Topologiekonzeptes erforderlich, das die oft historisch gewachsenen Strukturen zukunftsfest vereinfacht. Dabei gilt es auch, die Durchlaufzeiten kritischer Datenströme zu optimieren, ohne die Sicherheitsziele zu kompromittieren. Vielfach kann dies durch ein Zusammenfassen von Geräten gleichen Sicherheitsbedarfs in einem gemeinsamen Netzsegment erreicht werden. Findet ein Umstieg von IPv4 auf IPv6 statt, sollte zunächst eine Idealtopologie entworfen und anschließend möglichst weitgehend umgesetzt werden. Dabei gilt es vor allem, intermediäre Systeme zu entfernen, deren Notwendigkeit sich lediglich aus Grenzen des IPv4-Protokolls (z. B. maximale Anzahl von IP-Adressen pro Subnetz) ergeben hatte.

Durch den Einsatz von Virtualisierung bei Servern und Arbeitsplatzrechnern entfallen Geräte, Verkabelung und die Konfiguration der überflüssigen physischen Komponenten. Auf der Netzebene kann Software-Defined Networking (SDN) einen Beitrag leisten. Indem SDN von den konkreten Komponenten abstrahiert, ermöglicht es eine weitaus komfortablere und einfachere Konfiguration des Netzes sowie der Weiterleitungs- und Filterregeln.

7.2 SICHERHEIT

Vielfalt der Sicherheitsansätze gezielt nutzen
Für eine sichere und gleichzeitig komfortable Kommunikation ist es notwendig, den Schutzbedarf zu bestimmen, das Risiko zu analysieren und daraufhin gezielt geeignete Sicherheitsmechanismen auszuwählen, einzusetzen und modular wiederzuverwenden.

Auf der Netz- und der Übertragungsebene können insbesondere drei Maßnahmen gezielt ansetzen: Zunächst gilt es, (hoch) sichere nicht-öffentliche Netze im lokalen wie im Weitverkehrsbereich, z. B. das Verbindungsnetz, bedarfsgerecht auszubauen und zu nutzen. Soweit erforderlich, sollten in allen Netzen Datenströme nach Qualitäts- und Sicherheitsanforderungen frühzeitig und konsequent, aber erst auf höchstmöglicher Ebene getrennt werden (s. a. MPLS, Abschnitt 4.6). Ferner muss das Nebeneinander von kontrollierten Behördengeräten und fremden, z. B. privaten Endgeräten angemessen berücksichtigt werden, etwa durch ein separates Gäste-WLAN mit ausschließlichem Internetzugang.

EXPERTEN NEHMEN FÜR DIE STANDARDISIERUNG VORGESCHLAGENE SICHERHEITSLÖSUNGEN UNTER DIE LUPE.

Auf der Anwendungsebene lassen sich zwei Fälle unterscheiden: Reicht das Sicherheitsniveau allgemein gängiger Sicherheitsmechanismen aus, so sollten standardkonforme, geprüfte bzw. zertifizierte Implementierungen entsprechender Funktionen eingesetzt werden. Anderenfalls sollten anwendungsbezogene Sicherheitslösungen der öffentlichen Hand – z. B. OSCI – genutzt werden, etwar wenn die Kommunikation über das öffentliche Internet stattfinden muss.

Darüber hinaus können Komponenten für den Krisenfall – Fallback- und Reservekomponenten – im Regelbetrieb zur Qualitätsverbesserung mitgenutzt werden.

Informationsaustausch im Bereich IT-Sicherheit ausbauen
Ein ebenen- und ressortübergreifender, zeitnaher und enger Austausch über Sicherheitsvorfälle und Gegenmaßnahmen zwischen den Behörden und eine sachgerechte Information der Öffentlichkeit helfen, ähnliche Vorfälle bei anderen Betroffenen schneller zu identifizieren, die Auswirkungen zu minimieren und ggf. ganz zu vermeiden. Deshalb sollte mit Sicherheitsvorfällen in Behörden möglichst offen umgegangen werden. In diesem Kontext ist zu prüfen, ob Advisories des CERT-Bund auch der Öffentlichkeit bzw. zumindest Landes- und Kommunalbehörden und deren Rechenzentrums-Dienstleistern ganz oder in Teilen zur Verfügung gestellt werden können, ohne die Sicherheit von Bundesbehörden zu schwächen.

Sicherheitslösungen offenlegen und in die Standardisierung einbringen
Offengelegte und für die Standardisierung vorgeschlagene Lösungen werden von Experten unter die Lupe genommen, die in der Regel erkannte Schwachstellen wiederum offenlegen und so eine zeitnahe Behebung ermöglichen. Die Resultate sind damit besser als die Ausgangslösung. Hingegen können nur im wenig realistischen Idealfall vollständiger und fehlerfreier Spezifikation, Implementierung, Installation und Parametrisierung geheim gehaltene, individuelle Lösungen optimale Sicherheit gewährleisten.

Sicherheitslösungen sollten daher von vornherein so konzipiert werden, dass sie auch bei vollständiger Offenlegung das beabsichtigte Schutzziel erreichen. Entwickelte Lösungen sollten für beliebige Experten überprüfbar sein und zur Entwicklung allgemein verfügbarer Lösungen in die Standardisierung eingebracht werden. Da die öffentliche Hand vom Einsatz standardisierter Sicherheitslösungen profitieren kann, sollte sie sich verstärkt selbst an der Standardisierung beteiligen und kleinere und mittlere Unternehmen umfassender dabei unterstützen.

7.3 BEREITSTELLEN VON SOFTWARE & ERFAHRUNGEN

Vernetzungssoftware der öffentlichen Hand breit zur Verfügung stellen
Die öffentliche Hand entwickelt für den Eigenbedarf zahlreiche fachunabhängige Softwarekomponenten (bspw. SW-Bibliotheken für sicheren Datentransport), die hohe Qualitätsanforderungen erfüllen müssen. Diese Komponenten können auch für Bürger, Unternehmen und andere Behörden nützlich sein und sollten ihnen kostenlos oder zu den möglicherweise durch die Bereitstellung entstehenden Mehrkosten zur Verfügung gestellt werden. Ebenso sollte angestrebt werden, dass im Auftrag der öffentlichen Hand von Dritten entwickelte Komponenten in gleicher Weise weitergegeben werden können.

Anwendungserfahrungen dokumentieren und veröffentlichen
Anwendungserfahrungen, z. B. bezüglich Bedienung, Parametrisierung (Profilierung), Einführung oder Regelbetrieb, sollten dokumentiert und veröffentlicht werden. Dies hilft Dritten – insbesondere auch anderen Behörden – Fehler und Missverständnisse zu vermeiden und vorteilhafte Vorgehensweisen nicht erst durch zeitaufwändiges Ausprobieren herauszufinden. Ebenso tragen solche Best Practices dazu bei, zukünftige Softwareversionen, Spezifikationen und Standards zu optimieren.

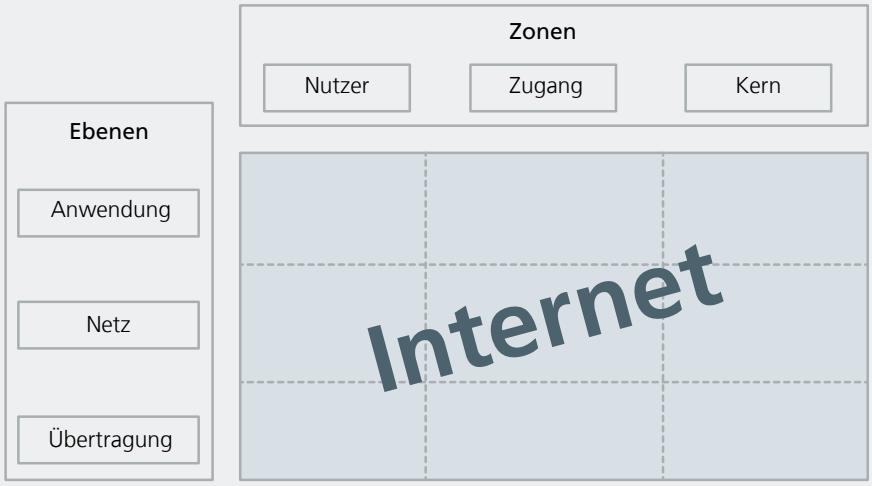

Abb. 6: Internet-Modell

7.4 BEWERTEN & GESTALTEN

Zustand des öffentlichen Internets regelmäßig beobachten und bewerten

Das öffentliche Internet ist zum Informationsaustausch und für Innovationen unverzichtbar – für Sozialkontakte, für vielfach genutzte Unterhaltungsangebote, für den Handel und zunehmend auch für die Interaktion zwischen Bürgern, Unternehmen und der öffentlichen Verwaltung. Der Staat ist daher in der Mitverantwortung für einen fairen und gesellschaftlich angemessenen Zugang aller Beteiligten zum öffentlichen Internet. Dazu muss er sich regelmäßig ein unabhängiges Bild der sich ständig und schnell verändernden Verhältnisse und Konditionen im Internet machen, diese bewerten und bei drohenden Ungleichgewichten rechtzeitig eingreifen. Die Diskussionen um Netzneutralität (s. Abschnitt 2.4) und die Meldepflichten im Rahmen des IT-Sicherheitsgesetzes bieten hier anschauliche Beispiele, wobei Letzteres einen wichtigen Beitrag zur Beobachtung des technisch komplexen Systems leistet.

Schnittstellen zum und im Internet offen halten

Wesentliche Entwicklungen des Internets und der Internetnutzung wurden nur dadurch möglich, dass zwischen allen Internetkomponenten sowohl horizontal – zwischen verschiedenen Beteiligten – als auch vertikal – zwischen den unterschiedlichen technischen Funktionsebenen – stabile technische Schnittstellen standardisiert sind, die von jedem Entwickler frei genutzt werden können.

Diese Innovationsbasis muss gegenüber Tendenzen zur Etablierung alternativer, proprietärer Schnittstellen und monolithischer Blöcke geschützt werden. Dabei gilt es, mit umfassendem Sachverstand technische Notwendigkeiten von strategischen Behinderungen des Marktzutritts zu unterscheiden. Zudem sollte die Einhaltung der etablierten Schnittstellen durch entsprechende Einkaufspraxis der Verwaltung als substanziellem IT-Kunden gestützt, die Standardisierung erforderlicher weiterer Schnittstellen gefördert und ggf. regulierend eingegriffen werden.

Monopolistischen Tendenzen entgegenwirken

Monopolistische Tendenzen können im Zusammenhang mit dem Internet in mehreren Bereichen entstehen. Ein Beispiel sind die Teilnehmeranschlüsse, wo steigende Nutzungs- und Qualitätsanforderungen Ausbau-, technischen Umstrukturierungs- und Konzentrationsdruck erzeugen. Ein anderes Beispiel sind Plattformen, deren Nutzen mit der Konzentration der Nutzer steigt.

Während im Bereich der Netzanbieter und Internet Service Provider die Bundesnetzagentur regulierend tätig ist, gestaltet sich in anderen Bereichen eine Steuerung weitaus schwieriger. Auch das Kartellrecht greift zu kurz, wenn Marktmacht durch die Entscheidung der Nutzer entsteht, vom Netzwerkeffekt zu profitieren. Ein Ansatzpunkt ist auch hier die Forderung nach der Einhaltung offener, standardisierter Schnittstellen, die zumindest Interoperabilität zwischen verschiedenen Anbietern ermöglichen und einen Wechsel erleichtern.

Forschung gezielt und bedarfsgerecht fördern

Die spezifischen Entwicklungen rund um das Internet in all seinen Facetten offenbaren neben den großen Themen, wie Sicherheit oder effizientere Nutzung von Netzressourcen, speziellen technischen Forschungsbedarf. Beispiele sind die effiziente Transportkodierung von Videostreaming-Inhalten, speziell bei mobiler Nutzung oder kleinen Wiedergabeflächen wie Smartphone-Bildschirmen, oder die effiziente Verschlüsselung kleiner Dateneinheiten durch und für leistungsschwache Geräte, seien es Messdaten und Steuerbefehle in Smart-City- und Industrie-4.0-Kontexten oder Echtzeit-Audio- und Sprachdaten.

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Gabriele Goldacker, Jens Tiemann
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

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

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

ISBN: 978-3-9816025-8-6

kre | 1701 (Fotos: https://pixabay.com)