Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

VERNETZUNG ALS INFRASTRUKTUR – EIN INTERNET-MODELL

Jens Tiemann, Gabriele Goldacker

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Jens Tiemann, Gabriele Goldacker

Gestaltung:
Reiko Kammer

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

1. Auflage Oktober 2015

VORWORT

Das Internet war vor nicht allzu langer Zeit noch ein neues, eigenständiges Medium, genutzt zum Austausch von Informationen, zum Lesen von Nachrichten oder als zusätzliche Vertriebsweg für einzelne Produkte. Inzwischen hat sich das Bild grundlegend gewandelt: Das Internet ist zu einer technischen Basis-Infrastruktur geworden, auf der eine Reihe von ganz verschiedenen Diensten angeboten wird und von der aufgrund einer immer engeren Kopplung zwischen physischer und informationstechnischer Welt immer mehr abhängt.

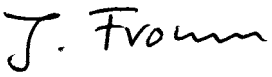
Während Teile der Wirtschaft – auch in Deutschland – früh die Chancen neuer Geschäftsmodelle und zunehmend auch die Möglichkeit zur Neuorganisation von ganzen Wirtschaftszweigen erkannt haben, ist die gesellschaftliche Diskussion der Internetentwicklung gespalten: Einerseits haben Internetpioniere auch die gesellschaftliche Bedeutung des Internets früh erfasst und daran gearbeitet, ihre Visionen umzusetzen. Andererseits haben aber politische Entscheidungsträger oftmals erst spät den Zugang zur Thematik gefunden und zunächst oberflächlich Phänomene reflektiert, ohne die grundlegenden Mechanismen der neuen Technik und daraus resultierende Konsequenzen zu berücksichtigen. Auch deshalb sorgen Schlagworte wie Netzneutralität, Kinder- und Jugend-Medienschutz oder Schengen-Routing nach wie vor für mediale Aufmerksamkeit.

Wenn man etwas verstehen und gestalten möchte, muss man es zunächst beschreiben können. Aber was ist eigentlich »das Internet«?

Eine kurze Übersicht der gegenwärtigen Internetnutzung macht schnell klar, dass das Internet aus sehr vielen Systemen zusammengesetzt ist, die von einer großen Zahl ganz unterschiedlicher Betreiber verwaltet wird. Diese heterogene und internationale Struktur führt zu langwierigen Prozessen bei der Gestaltung des Internets. Typische Anwendungsszenarien zeigen die Breite der Internetnutzung sowie verschiedene Anforderungen, die letztlich auch in Konkurrenz zueinander stehen können und bei einer Gestaltung des Internets miteinander verbunden werden müssen.

Schon diese beiden Aspekte verdeutlichen die Komplexität des Themas, wie man sie auch in öffentlichen Diskussionen über die Digitalisierung sehen kann. Wir möchten daher die informierte Diskussion fördern und präsentieren zunächst aus einer technischen Perspektive ein vereinfachtes Internet-Modell und einzelne technische Fakten, an denen man bei einer Diskussion über das Internet nicht vorbeikommt.

Jens Fromm



Leiter Kompetenzzentrum Öffentliche IT

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

INHALTSVERZEICHNIS

1. THESEN

Das Internet ist zu einer kritischen Basis-Infrastruktur geworden

Dienste auf Basis des Internets, wie E-Mail und IP-Telefonie, ersetzen zunehmend herkömmliche Dienste (z. B. Briefpost bzw. ISDN-Telefonie), die auf separaten Infrastrukturen angeboten werden. Die internetgestützten Anwendungen sowie die Effizienz und Leistungsfähigkeit des Internets nehmen weiterhin zu. Durch die Verknüpfung der physischen Umwelt mit Informationstechnologie erweitert sich der digitale Raum und damit die Abhängigkeit vom Internet. Die dadurch entstehende Monopolstellung des Internets macht dieses zur kritischen Ressource.

Die Gestaltung des Internets ist von einer rein technischen zu einer gesellschaftlichen Aufgabe geworden

Das Internet ist als eigenständiges Medium in einem technisch orientierten Umfeld gewachsen. Die Veränderungen des Internets durch fragwürdige Geschäftsmodelle, durch missbräuchliche Nutzung oder Überwachung führten zu Enttäuschungen bei langjährigen Gestaltern und Nutzern des Internets. Die Gestaltung des Internets, als Zugang und Grundlage des digitalen öffentlichen Raums, ist nicht länger eine nur technische, sondern mehr und mehr eine gesellschaftliche Aufgabe.

Zur Gestaltung des Internets und der Internetnutzung ist ein technisches Modell erforderlich

Es werden teilweise widersprüchliche Eigenschaften von der Infrastruktur Internet erwartet, wie Offenheit zur problemlosen Erreichbarkeit aller Teilnehmer und Sicherheit gegen Cyberangriffe. Diese Widersprüche können zum Teil aufgelöst werden, wenn die verschiedenen Bestandteile des Internets getrennt betrachtet und technisch fundierte Entscheidungen bei der Gestaltung von Netzen und der Internetnutzung getroffen werden.

Sicherheit und Gestaltung des Internets benötigen klare technische Schnittstellen zwischen Teilen des Internet-(modell)s

Teilsysteme der Internetkommunikation sind miteinander über technische Schnittstellen verbunden. Diese Aufteilung des Gesamtsystems erlaubt die Verankerung von Sicherheit, bspw. durch die Abschottung und Stabilisierung von Teilsystemen. Gleichzeitig bieten Schnittstellen bereits vorhandene Ansatzpunkte zur Gestaltung des Internets als Infrastruktur bzw. zur Durchsetzung von Regeln.

Der Begriff »Internet« muss in verschiedenen Facetten verstanden werden

Der Begriff »Internet« steht für die globale Verknüpfung von Netzen, für die Verbindung von Nutzern mit entfernten Dienstleistungsangeboten und auch für eine leistungsfähige und wirtschaftliche Technologie. Im öffentlichen Internet sind vielfältige Daten abrufbar oder Kommunikationsteilnehmer erreichbar. Auf verschiedenen Ebenen ist aber auch der Betrieb geschlossener Strukturen (z. B. privater Netze) möglich. Übergänge zwischen offenen und geschlossenen Strukturen sowie Abhängigkeiten zwischen Infrastrukturebenen müssen besonders beachtet werden.

Offenheit, Einfachheit, Dezentralität und Robustheit sind die Erfolgsfaktoren der Internetkommunikation

Teilnehmer sind über die Internetinfrastruktur prinzipiell weltweit direkt erreichbar. Dies kann über vielfältige Zugänge und Anbieter erfolgen. Die Internetinfrastruktur ist vor allem durch ihre Einfachheit und Robustheit geschützt. Daher kann das Internet durch neue Teilnehmer sowie durch neue Anwendungen oder Geräte weiterhin stark wachsen

Datenverarbeitung kann nicht mehr auf elektronische Datenkommunikation verzichten

Chancen und Risiken der Informationsgesellschaft beruhen auf leistungsfähigen und vernetzten Computern. Informationserfassung, -übertragung, -verarbeitung und als Folge zunehmend auch die automatisierte Ausführung von Aktionen bilden eine Einheit. Die dynamische Nutzung von Vernetzung ist dabei integraler Bestandteil und das Internet eine primäre Ressource.

2. EINLEITUNG

Die fortschreitende Digitalisierung aller Lebens- und Wirtschaftsbereiche führt zu einer immer stärkeren Bedeutung des Internets. Das Internet ist zu einer Basis-Infrastruktur geworden, die von ganz verschiedenen Diensten genutzt wird. Mehr noch: Das Internet entwickelt sich zu einer Meta-Infrastruktur – einer Infrastruktur, die für den Betrieb anderer Infrastrukturen (Strom, Wasser, Verkehr …) unverzichtbar wird und die physische Welt mit der informationstechnischen Welt immer stärker verbindet.

Mit dem Bedeutungszuwachs des Internets entwickeln sich neue Anforderungen an diese Infrastruktur, hervorgebracht von einer größer werdenden Zahl von Interessengruppen. Aufgrund des breiten Anwendungsgebietes und der vielfältigen Interessen bleibt es nicht aus, dass auch immer mehr widersprüchliche Anforderungen an Aufbau, Betrieb und Weiterentwicklung des Internets gestellt werden. Damit wird aber die Entwicklung des Internets nicht mehr nur von den technischen Möglichkeiten getrieben. Es muss sich einer breiteren, reflektierenden gesellschaftlichen Diskussion stellen, in der immer mehr wirtschaftliche und politische Argumente an Bedeutung gewinnen. Diese gesellschaftliche und politische Diskussion kann deutlich zielgerichteter geführt werden, wenn sie auf einem technischen Verständnis des Internets fußt.

In diesem Whitepaper erläutern wir technische Strukturen und Komponenten des Internets, um dabei zu helfen, aktuelle Schlagworte und Themen einzuordnen und deren Machbarkeit realistisch einzuschätzen. Dazu entwickeln wir ein Modell des Internets, das von den technischen Details stark abstrahiert, zugleich aber geeignet ist, aktuelle Begriffe der digitalen Debatte differenziert zu betrachten. Anschließend bilden wir beispielhaft zwei Handlungsfelder der Diskussion um das Internet auf das Modell ab, um dessen Anwendung zu demonstrieren. Aus der Entwicklung des Internet-Modells lassen sich erste, generelle Handlungsempfehlungen ableiten, die wir abschließend darstellen.

Das Whitepaper wendet sich an Menschen[1], die sich qualifiziert und zielführend an Diskussionen zu aktuellen Themen rund um das Internet beteiligen oder diese Diskussionen einfach besser verstehen und bewerten können wollen. Es richtet sich besonders an Entscheider in Politik, Verwaltung und Wirtschaft, die das zukünftige Internet entscheidend prägen können. Aber auch wer »nur« wissen will, wie bestimmte Dinge gehen und warum Anderes nicht geht, soll hier fündig werden.

Nicht behandelt sind Fragen zu Organisation und Aufsicht über das Internet, um die aktuell auch gerungen wird.

2.1 DAS INTERNET IN ZAHLEN

Um zu verstehen, warum die Umsetzung vermeintlich einfacher technischer Weiterentwicklungen, Qualitätssteigerungen oder Schutzmaßnahmen komplex und aufwändig sein kann, hilft es, sich einige Zahlen[2] zum Internet zu vergegenwärtigen:

- Für rund 40 Mio. der 40,7 Mio. bundesdeutschen Haushalte wird bereits heute eine Festnetz-Breitbandversorgung (mind. 1 Mbit/s Download) bereitgehalten. Diese wird von rund 30 Mio. Haushalten auch tatsächlich genutzt.
- Die Dienstleistung »Internetzugang« wird in Deutschland von rund 250 Anbietern vertrieben.
- Das weltweit jährlich anfallende Breitbandvolumen beträgt rund 8 Mrd. Gigabytes, das entspricht 22 Gigabytes pro Monat und angeschlossenem Haushalt.
- Hinzu kommt ein jährliches Gesamtvolumen von rund 200 Mio. Gigabytes, das über Mobilfunkanschlüsse übertragen wird.
- Das Internet besteht aus rund 50.000 unabhängig voneinander verwalteten und miteinander verbundenen Teilnetzen, sogenannten Autonomen Systemen. Davon befinden sich etwa 1500 in Deutschland.

[1] Wenn wir in diesem Whitepaper von Menschen als Nutzern, Bürgern Verbrauchern … sprechen, sind damit stets Personen jedweden Geschlechts gemeint.

[2] Quellen:
Bundesnetzagentur: »Tätigkeitsbericht Telekommunikation 2012/2013«, Stand: Dezember 2013
Michael Antrag: »Die Internetanbieter Deutschlands«: http://internetanbieter-deutschland.de/alle-anbieter/
N. Pohlmann, I. Siromaschenko, M. Sparenberg: »Das Schengen-Routing zu Ende gedacht – Direktvermittlung«, iX – Magazin für professionelle Informationstechnik, Heise-Verlag, 02/2014, s. a. https://www.eco.de/wp-content/blogs.dir/deutschland-routing-02_03_14.pdf
»CIDR Report«: http://www.cidr-report.org/as2.0/
Wikipedia: »Internet-Knoten«: http://de.wikipedia.org/wiki/Internet-Knoten
Packet Clearing House : »INTERNET EXCHANGE DIRECTORY«: https://prefix.pch.net/applications/ixpdir/?show_active_only=0&sort=participants&order=desc
DE-CIX: »Traffic Statistics«: http://www.de-cix.net/about/statistics/

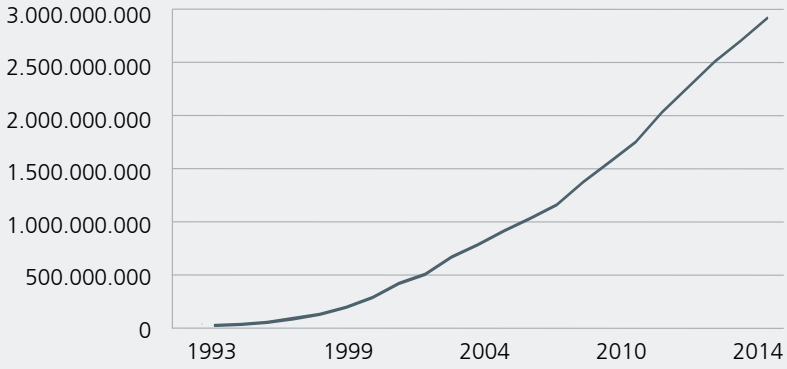


Abb. 1: Weltweite Internetnutzer, Quelle: Internet Live Stats (basiert auf Daten der International Telecommunication Union (ITU))

– Zwischen den Autonomen Systemen gibt es bereits rund 500.000 Verbindungen, die die Erreichbarkeit aller Teilnehmer im Internet ermöglichen.
– Autonome Systeme werden über eine direkte Leitung (1-zu-1) oder über Verkehrsknotenpunkte, sogenannte Internetknoten (IXPs: Internet Exchange Points) miteinander verbunden. Weltweit gibt es etwa 340 IXPs, davon 165 in Europa.
– Der IXP mit dem weltweit größten Durchsatz ist der DE-CIX in Frankfurt. Der aktuelle mittlere Durchsatz liegt bei etwa 2,2 Terabit/s. Der DE-CIX Frankfurt verbindet mehr als 600 Autonome Systeme miteinander.
  AMS-IX (in Amsterdam), der IXP mit den meisten angeschlossenen Autonomen Systemen, verbindet fast 700 derartige Systeme miteinander.
– Nur rund 50 Prozent der Kommunikationsbeziehungen im Internet finden zwischen Teilnehmern im selben Staat statt.

2.2 DAS INTERNET AUS NUTZERSICHT

Basis-Infrastrukturen, wie Verkehrswege oder das Internet, zeichnen sich dadurch aus, dass sie eine Grundlage für verschiedenartige und individuelle Nutzungsmöglichkeiten bilden. Entscheidende Kriterien zur Analyse derartiger Infrastrukturen sind Zugang, Qualität, Sicherheit und Kosten. Treten beim Ausfall einer Infrastruktur dramatische Folgen auf, wie bspw. Versorgungsengpässe oder eine Störung der öffentlichen Sicherheit, so spricht man von einer kritischen Infrastruktur.[3]

Unzweifelhaft ist das Internet eine sehr wichtige Infrastruktur geworden. Die Anforderungen sind vielfältig, wie aus folgenden beispielhaften Nutzungsszenarien hervorgeht.

Wirtschaft und Industrie

Anbieter aus der Wirtschaft nutzen das Internet als weiteren Vertriebsweg für traditionelle Angebote oder für neue, internetspezifische Dienste. Zunehmend dient es als Plattform für die Bereitstellung immaterieller Waren – Video und Audio, Spiele, Navigationsdaten, aktuelle Informationen und ganz allgemein »Wissen«. Die Nutzer zahlen dafür inhaltsbezogen, indirekt über Werbung oder indem sie eigene Daten zur Verfügung stellen. Im Vordergrund stehen für die Anbieter Zugang und Verfügbarkeit, um eine große Anzahl von Nutzern auf wirtschaftliche Weise zu erreichen.

Auch innerhalb von Wirtschaftsprozessen spielt das Internet eine immer stärkere Rolle. Bei rein informationstechnischen Prozessen wurden bereits deutliche Effizienzsteigerungen durch Vernetzung erreicht. Aktuell werden die Schnittstellen zwischen Informationstechnik und »realer«, physischer Welt ausgebaut und letztere damit direkt an das Internet herangeführt. Das reicht bis zu den vielschichtigen, verteilten Fertigungsprozessen, die eine wirtschaftliche Fertigung komplexer Produkte selbst in kleinsten Stückzahlen ermöglichen (Stichwort: Industrie 4.0). Voraussetzung für die Verknüpfung von physischer und virtueller Welt sind die Vernetzung einer Vielzahl von Sensoren, Robotern, Steuerungscomputern und Datenbanken sowie die flächendeckende Verfügbarkeit der erforderlichen Dienstqualität, beispielsweise garantierte Datenraten. Für störungsfreie Produktionsprozesse ist darüber hinaus eine hohe Angriffssicherheit der über das Internet transportierten oder im Internet aufbewahrten Daten notwendig.

Öffentlicher Sektor

Probleme bei der Energieversorgung oder der Verkehrsinfrastruktur sollen nicht weiter nur durch ein Mehr an direkten Ressourcen – mehr Kraftwerke, mehr Straßen … – gelöst werden. Effizientere Verfahren sind notwendig, die sich auch mithilfe von Informationstechnik realisieren lassen. Stichworte sind hier

[3] Bundesministerium des Innern: »Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)«, Stand: Juni 2009, http://www.kritis.bund.de/

TRETEN BEIM AUSFALL EINER INFRASTRUKTUR DRAMATISCHE FOLGEN AUF, SO SPRICHT MAN VON EINER KRITISCHEN INFRASTRUKTUR.

Intelligente Vernetzung[4] und Smart Cities. Verschiedenste Prozesse und Informationen müssen verknüpft werden, wobei das Internet eine wichtige Basis für den dazu notwendigen Datentransport bildet. Der Staat hat die Aufgabe, den Rahmen für diese Entwicklung vorzugeben, die dafür notwendige Kommunikationsinfrastruktur (vergleichbar z. B. zur Verkehrs- oder Strominfrastruktur) zu gestalten und deren Betrieb sicherzustellen.

Die öffentliche Verwaltung kann durch informationstechnisch gestützte, medienbruchfreie und damit auch weitgehend papierlose Prozesse erheblich effizienter werden. Optimalerweise werden die entsprechenden Prozesse bis zu den betroffenen Bürgern und Unternehmen ausgedehnt. Dabei fallen oft schutzbedürftige personenbezogene oder Wirtschaftsdaten an, die sicher transportiert und aufbewahrt werden müssen. Für eine direkte Kommunikation mit Wirtschaft und Bürgern muss auch die Verwaltung das Internet nutzen, wobei auch hier ein hohes Schutzniveau erwartet wird.

Private Haushalte

Ein wesentlicher Teil der Internetnutzung ist der direkte Austausch mit Anderen per E-Mail, Online-Kommunikation oder über soziale Netzwerke. Viele Nutzer möchten, als Privatperson oder im Berufsleben, an beliebigen Orten, auch mit mobilen Endgeräten, das Internet nutzen können. Neben der Verfügbarkeit sind auch die Kosten der Internetnutzung ein relevanter Faktor, um die Beteiligung aller Bürger an den internetbasierten sozialen oder wirtschaftlichen Prozessen zu ermöglichen.

Verbraucher nutzen zunehmend Internetangebote der Wirtschaft, wie die oben geschilderten Inhalte oder Bestellungen für Konsumgüter. Hinzu kommen in steigendem Maße Sensoren für den persönlichen Bedarf, sei es zur Steuerung des Haushalts oder zur Überwachung der Gesundheit.

Im Kontext des Internets sind für die Bürger neben der Verfügbarkeit und dem inhaltlichen Angebot auch Verbraucherschutz, Datenschutz und der Schutz der Privatsphäre wichtig. Durch die Nutzung einer weltweit zugänglichen Kommunikationsinfrastruktur öffnen Bürger den Zugang zu Informationen über viele ihrer Lebensbereiche, sodass sie ggf. die Kontrolle darüber verlieren, was mit ihren Inhalts-[5] und Metadaten[6] geschieht. Zudem können aus der Verknüpfung verschiedener Daten, evtl. auch über verschiedene Kommunikationsbeziehungen hinweg, Informationen gewonnen werden, deren Entstehung und Auswirkung für die Nutzer nicht unbedingt vorhersehbar ist.

Angesichts der steigenden Komplexität des Internetzugangs und des heimischen lokalen Netzes benötigen gerade private Nutzer einfache Bedien-, Installations- und Sicherheitskonzepte bzw. Unterstützung beispielsweise durch sinnvolle Voreinstellungen von Geräten.

[4] Intelligente Vernetzung bezeichnet die IT-Nutzung in Infrastrukturbereichen wie Energieversorgung, s. a. http://www.bmwi.de/DE/Themen/Digitale-Welt/Digitale-Wirtschaft/intelligente-vernetzung.html

[5] Inhaltsdaten: Daten, die ein Nutzer über das Internet versendet oder empfängt, um einen Bedarf oder ein Interesse zu befriedigen: E-Mail-Inhalte, Suchanfragen und -ergebnisse, Videos …

[6] Metadaten: Bestands- und Nutzungsdaten (bspw. Gesprächsdauer, Adresse des Gesprächspartners)

3. INTERNET-MODELL

Das Internet ist ein weltweiter Verbund öffentlich erreichbarer Netze. Die Netze werden unabhängig voneinander betrieben, nutzen aber einen gemeinsamen Adressraum und standardisierte gemeinsame »Sprachen«, sogenannte Übertragungsprotokolle, um die gegenseitige Erreichbarkeit sicherzustellen. Insbesondere das Internet Protocol (Internetprotokoll, kurz IP) hat eine zentrale Rolle. Das Internet ermöglicht den Transport beliebiger Daten. An das Internet angeschlossene Computer stellen Dienste und Anwendungen zur Verfügung (wie Web, E-Mail), die öffentlich oder für geschlossene Benutzergruppen verfügbar sind.

Hier werden einige technische Grundlagen des Internets zum Verständnis des Hintergrundes kurz vorgestellt, um daraus ein technisch orientiertes Modell des Internets zu entwickeln.

3.1 SCHICHTENMODELL

Mit einem Schichtenmodell (siehe Abildung 2) werden die verschiedenen Funktionen, die für eine Datenübertragung in Kommunikationsnetzen notwendig sind, hierarchisch gegliedert. Auf der untersten Schicht wird beschrieben, wie die Daten ganz konkret über eine Leitung oder die Luft übertragen und welche (elektrischen) Signale dabei verwendet werden. Auf einer mittleren Schicht wird bspw. die wichtige Funktion beschrieben, wie verschiedene Teilnehmer adressiert werden und damit überhaupt am Datenaustausch teilnehmen können. Auf höheren Schichten stehen Funktionen zur Gestaltung und zum Betreiben von Anwendungen, bspw. für den Aufruf von Webseiten, zur Verfügung.

Jede Schicht verbirgt die konkrete Art und Weise, wie sie ihre Funktion erbringt, vor den anderen Schichten. Logisch zusammengehörende Funktionen einer Schicht werden den jeweiligen Nutzern als sogenannter Dienst zur Verfügung gestellt. Durch die eindeutige Schichtenzuordnung können unterschiedliche Realisierungen mit geringem Aufwand gegeneinander ausgetauscht werden, ohne die unbeteiligten Schichten zu beeinträchtigen. Bspw. kann eine Übertragung über Glasfaser oder Funk, in Klartext oder verschlüsselt erfolgen. Das Schichtenmodell trägt aber auch zur Vereinfachung bei, indem es von der konkreten Realisierung abstrahiert und von jeder Realisierung stattdessen die Bereitstellung eines genau beschriebenen Dienstes erwartet. Dieses Prinzip wird bspw. sichtbar in immer leistungsfähigeren Webanwendungen. Wurden zunächst nur statische Webseiten mit Text und Bildern angeboten, stellen moderne, auf Webtechnologien basierende Plattformen viele Funktionen zur Verfügung, die es Anbietern leicht machen, leistungsfähige und nutzerfreundliche Anwendungen zu erstellen.

Durch die Nutzung der Dienste einer unteren Schicht »erbt« die höhere Schicht zunächst die Eigenschaften dieser unteren Schicht. Wenn bspw. die drahtlose Übertragung unzuverlässig ist, dann muss das in einer höheren Schicht berücksichtigt und dafür Sorge getragen werden, dass sich die unzuverlässige Übertragung nicht auswirkt bzw. unerwünschte Eigenschaften durch eine geeignete Funktion kompensiert werden. Ein weiteres Beispiel: Enthält eine Schicht vertrauenswürdige Verschlüsselung, kann zur Sicherheit von Anwendungen beitragen, ohne dass bei deren Entwicklung entsprechendes Spezialwissen vorhanden sein muss.

3.2 ZONENMODELL

Entsprechend der räumlichen Ausdehnung und den Aufgaben kann man verschiedene Typen von Netzen ausmachen: Großflächige IP-basierte Netze (IP-Transportnetze) ermöglichen die Kommunikation über große Entfernungen; ihr Zusammenschluss über direkte Verbindungen oder Internetknoten stellt damit den Kernbereich des Internets dar. Demgegenüber sind lokale Netze dafür zuständig, die verschiedenen IT-Komponenten einer Organisation oder eines Haushalts miteinander zu verknüpfen und mit dem Internetanschluss zu verbinden. Dazwischen verdienen die Zugangsnetze von Festnetz-, Kabelnetz- und Mobilfunkbetreibern eine besondere Beachtung, da sie für die Internetversorgung von Wirtschaft und Privathaushalten zuständig sind. Siehe dazu auch Abbildung 3.

Technisch und administrativ unterscheiden sich diese Netztypen sehr stark. Auf den unteren Schichten (siehe Kapitel 3.1) werden verschiedene Übertragungsverfahren eingesetzt. Das ist darin begründet, dass diese Netze unterschiedliche Aufgaben erfüllen müssen. Im Zugangsbereich besteht bspw. die Anforderung, zugleich leistungsfähige und wirtschaftliche Internetanschlüsse flächendeckend zur Verfügung zu stellen. Je nach Besiedelungsdichte und bereits vorhandenen Infrastrukturen kann dies zu ganz unterschiedlichen Lösungen führen. In den IP-Transportnetzen steht die Verwaltung der Netzressourcen im

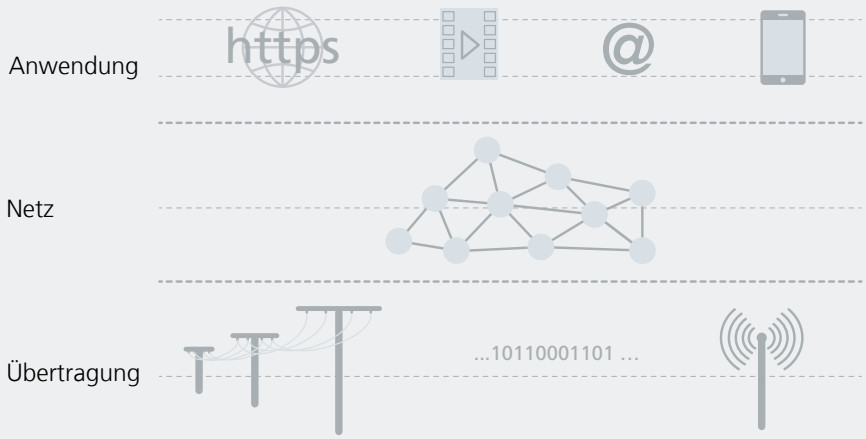


Abb. 2: Das Schichtenmodell zur Einordnung von Kommunikationsfunktionen

Vordergrund. Auf unterliegenden, vorwiegend Glasfaser-basierten Infrastrukturen werden nicht nur die Datenströme des Internets transportiert, sondern gleichzeitig auch davon völlig getrennte, geschlossene Infrastrukturen realisiert, wie Firmen- oder Verwaltungsnetze.

Neben Funktionen und Technik unterscheiden sich die Netztypen auch darin, wer die Hoheit darüber hat: Im lokalen Netz ist es der jeweilige Nutzer und im Zugangsnetz der Betreiber. Im Kernbereich sind es die Betreiber der IP-Transportnetze und der IXPs (s. Kapitel 2.1).

Aufgrund dieser Unterschiede bietet es sich an, ein an den Übergängen zwischen den Netztypen orientiertes Zonenmodell zu verwenden.

3.3 MODELL DES INTERNETS ALS INFRASTRUKTUR

Ein wichtiger Aspekt (technischer) Modelle ist die Reduktion von Komplexität. Für betrachtungsrelevante Eigenschaften eines Systems, die Auswirkungen auf die Umgebung haben, verfügt das Modell über einen ausreichend realitätsnahen Detailgrad, der z. B. die Verortung der Eigenschaften in konkreten Komponenten ermöglicht. Teile, die für die Betrachtung weniger relevant sind, werden nur grob dargestellt. Die Auswirkungen können diskutiert werden, die genaue Realisierung spielt zunächst keine Rolle.

Ein detailliertes Schichtenmodell, wie es für die Standardisierung und Implementierung von Kommunikationssystemen vorteilhaft ist, ist im Kontext dieses Whitepapers zu komplex.

In unserem Internet-Modell unterscheiden wir daher lediglich drei Ebenen:

- Anwendung: Anwendungen und Dienste, die über das Internet Protocol realisiert oder im Internet bereitgestellt werden, sowie die dazu erforderlichen anwendungsorientierten Protokolle (z. B. HTTP(S) oder RTP)
- Netz: die zentralen Vermittlungs- und Transportprotokolle Internet Protocol und TCP/UDP
- Übertragung: die verschiedenen Übertragungstechniken, über die das Internet Protocol genutzt wird

Im Modell nimmt das Internet Protocol auf der Netzebene eine besondere Stellung ein: Es ist der gemeinsame Nenner von weiten Teilen der Kommunikation. Das Internet Protocol kann über vielfältige Übertragungstechniken genutzt werden und stellt wiederum selbst die alleinige Basis für eine Vielzahl von Anwendungsprotokollen und Diensten dar. Die Verwendung dieses einen, zentralen Kommunikationsprotokolls ermöglicht die weltweite Erreichbarkeit über öffentliche Kommunikationsnetze sowie die Herstellung preisgünstiger und leistungsfähiger Geräte und Komponenten, auch für private Netze.

Im ursprünglichen Sinn bezieht sich der Internetbegriff nur auf die Netzebene unseres Modells: Die an der Internetkommunikation beteiligten Geräte – Endgeräte (z. B. Server und PCs) und Vermittlungssysteme (Router) – »reden« in der Netzebene miteinander. Sie benutzen dazu das Internet Protocol als »Sprache« und die Signalübertragung der Übertragungsstrecken (z. B. Glasfaser oder Funk). Diese Endgeräte, Router und Übertragungsstrecken bilden gemeinsam das Internet.

Das Internet Protocol gibt es in zwei Versionen, das ältere IPv4 und IPv6, das sich derzeit mehr und mehr durchsetzt. Beide Protokollvarianten sind nicht direkt miteinander kompatibel. Die

[7] Informationen zu IPv6 und aktuelle Statistiken zur Verbreitung finden sich unter http://www.google.de/ipv6

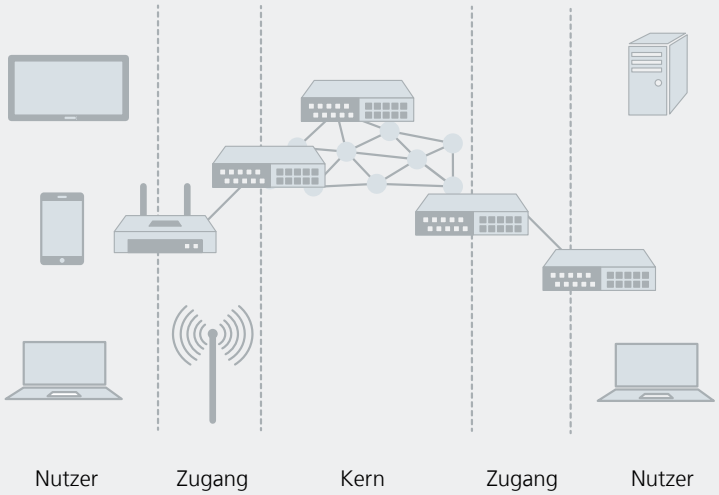


Abb. 3: Das Zonenmodell zur Einordnung von Netztypen

zentrale Rolle des Internet Protocol macht die weltweite IPv6-Einführung zu einem seit Jahren andauernden, langwierigen Prozess.[7]

Für eine ganzheitliche Betrachtung aller Aspekte der Internetkommunikation muss der komplette Weg über die verschiedenen Netze zwischen den beteiligten Kommunikationspartnern betrachtet werden. Ausgehend von einem Computer im privaten Netz eines Teilnehmers läuft der Weg über ein Zugangsnetz, über möglichweise mehrere IP-Transportnetze, über ein weiteres Zugangsnetz zum privaten Netz oder direkt zum Computer des Kommunikationspartners. Grundsätzlich ist diese Betrachtung für das Internet symmetrisch, d. h. die Kommunikation kann von beiden Kommunikationsteilnehmern ausgehen bzw. alle Kommunikationsteilnehmer können Informationen anbieten. Bekannt ist dieser Aspekt im Zusammenhang mit Peer-to-Peer-Anwendungen, bei denen Daten direkt zwischen den Teilnehmern ausgetauscht werden. In der Praxis ist das Modell für die Mehrzahl der Internetnutzer asymmetrisch geworden: Ohne eigene Angebote zu machen, greifen sie über einen Browser oder andere Software auf zentrale Angebote – Inhalte und Anwendungen – zu, die über Rechenzentren angeboten werden. Entsprechend unterschiedlich sind die Zugänge zum Internet.

In unserem Internet-Modell unterscheiden wir daher drei Netzzonen:

- Nutzer: Das private Netz des Nutzers bzw. einzelne Hard- und Softwarekomponenten
- Zugang: Zugangsnetze, typischerweise realisiert von Festnetz- oder Kabelnetzbetreibern bzw. von Mobilfunkanbietern
- Kern: IP-Transportnetze und Internetknoten auf der Netzebene, die die weltweite Kommunikation realisieren, sowie öffentlich zugängliche Dienste großer Anbieter auf der Anwendungsebene

Das Modell stellt also ggf. nur eine Hälfte der Ende-zu-Ende-Kommunikation direkt dar, bspw. bei der Betrachtung von Internettelefonie zwischen zwei Teilnehmern oder dem Zugriff eines Nutzers auf eine Anwendung in einem Rechenzentrum eines Unternehmens. Für einige Betrachtungen muss daher das Modell zweimal durchlaufen bzw. gespiegelt werden.

Die Felder, Ebenen und Zonen des Modells nutzen wir im Folgenden, um die Zuordnung von Funktionen zu verdeutlichen.

3.4 INTERNET UND INTERNET-TECHNOLOGIE

Das Internet als globaler Zusammenschluss unterschiedlicher Netze besteht nach dem obigen Modell aus den Kernnetzen und den Zugangsnetzen und reicht zumindest bis zu den öffentlich ansprechbaren Rechnern bei den Nutzern.

Der Begriff der Internettechnologie und der Internetprotokolle wird häufig wesentlich weiter gefasst und umfasst insbesondere eine ganze Reihe von Anwendungen und Anwendungsprotokollen, wie bspw. HTTP zur Übertragung von Webinhalten. Die Internettechnologie hat sich weitgehend durchgesetzt und wird auch in den privaten Netzen der Nutzer und in nichtöffentlichen Transportnetzen angewendet. Selbst da, wo sie aus historischen oder technischen Gründen nicht direkt angewendet wird (bspw. bei Steuerungen oder in Sensornetzen mit niedriger Datenrate), stehen Techniken zur Ankopplung an das Internet bereit, oder es wird bei Neuentwicklungen auf eine enge Abstimmung mit den bestehenden Funktionen aus der Internetwelt geachtet.

3.5 ERWEITERTER INTERNET-BEGRIFF

Der in Kapitel 3.3 eingeführte Internetbegriff – die Menge aller Geräte, die durch das gemeinsame Internet Protocol miteinander kommunizieren können – befindet sich im Wandel.

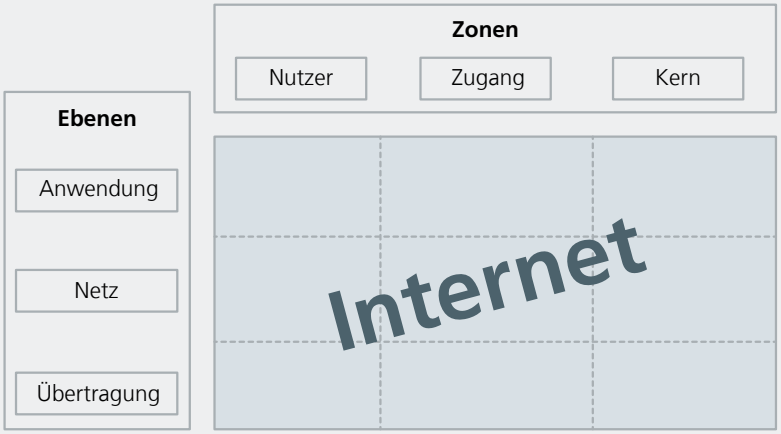


Abb. 4: Das Internet-Modell zur Diskussion von Handlungsfeldern

Inzwischen werden häufig nur die Endgeräte, Router und Übertragungsstrecke zum Internet gezählt, die zur allgemein nutzbaren Infrastruktur gehören, also zwar z. B. öffentlich erreichbare Webserver, nicht aber die nur innerhalb eines privaten oder Firmen-(W)LANs erreichbaren Geräte. Ein solches nicht öffentliches (W)LAN wird als Intranet bezeichnet.

Die Abgrenzung zwischen dem Internet und hier nicht betrachteten privaten Netzen oder privaten Anwendungen findet sich im Modell in der Nutzerzone und in der Anwendungsebene. Der Übergang ist allerdings fließend und hängt von den betrachteten Aspekten ab: Bspw. verbinden Firmen ihre privaten lokalen Netze über Sicherheitsgeräte mit dem Internetzugang und kontrollieren damit die durchgehenden Kommunikationsverbindungen. Ein privater Nutzer kann dagegen darauf angewiesen sein, dass sein Router teilweise vom Internetanbieter ferngesteuert wird, sodass er nicht die volle administrative Kontrolle über sein heimisches lokales Netz hat.

Außerdem umfasst der Internetbegriff vielfach nicht nur den reinen Datentransport in der Netzebene, sondern auch die von z. B. Web- oder E-Mailservern öffentlich bereitgestellte Dienstleistung. Solche in großem Umfang und weltweit genutzten Dienste werden nicht auf einzelnen Servern betrieben, sondern auf einem Verbund von Servern, die miteinander über das Internet (im engeren Sinn) oder geschlossene Infrastrukturen kommunizieren. Ebenso gibt es Anwendungen, die verschiedene Dienste (eines oder mehrerer Anbieter) nutzen und so höherwertige Ergebnisse produzieren, die wiederum im Internet verfügbar gemacht werden. Derartige komplexe Strukturen werden auch als Dienste-Plattformen bezeichnet.

Im Zusammenhang mit dem erweiterten Internetbegriff sind daher auch die Plattformen und Anwendungen großer, öffentlicher Anbieter wie Google oder Facebook zu nennen, die für viele Nutzer eine zentrale Anlaufstelle im Internet mit täglich genutzten Diensten bilden. Im engeren Sinne stellen sie »nur« Dienste auf Basis des Internets bereit.

Ein spezielles Beispiel sind Verteilplattformen wie Content Delivery Networks (CDN). Zur effizienten Bereitstellung bspw. von Multimediainhalten werden bei vielen globalen Diensten Anfragen nicht von einem zentralen Server beantwortet, sondern von einem beliebigen geeigneten Server der Verteilplattform. Ein CDN besteht aus geografisch verteilten Servern, die aus verschiedenen Regionen der Welt gut erreicht werden können. Die Inhalte werden innerhalb des CDN repliziert und verteilt, damit der Zugriff vom Benutzer effizienter und schneller über kürzere Wege erfolgen kann.

Im Bereich der IT-Dienstleistungen spielen Cloud-Infrastrukturen eine wichtige Rolle. Sie erlauben Unternehmen das Speichern und Bearbeiten ihrer Daten in skalierbarer und wirtschaftlicher Weise auf Servern im Internet. Auch hier lässt sich feststellen, dass Datenverarbeitung und Kommunikation immer stärker zusammenwachsen, insbesondere, wenn die Datenverarbeitung geografisch entfernt oder verteilt erfolgt.

Die hier beschriebenen Dienstleistungsangebote befinden sich in unserem Internet-Modell in der Kernzone.

Eine weitere Ausweitung des Internetbegriffs entwickelt sich einerseits aus der gemeinsamen Nutzung des (Privatkunden-) Netzanschlusses für Internetzugang und Telefonie sowie zunehmend auch für Rundfunk- und Fernsehverteildienste und andererseits aus der wachsenden Nutzung von IP-Telefonie. Für die Kunden verschwimmt die Kenntnis, welche der am Anschluss verfügbaren Dienste über das Internet abgewickelt werden und welche lediglich in der Zugangszone aus anderen Netzinfrastrukturen hinzugefügt werden.

4. INTERNETMECHANISMEN IM DETAIL

Die Kommunikation in der Netzebene erfolgt paketvermittelt, d. h., die Daten der Anwendungsebene werden in Einheiten – sogenannte Pakete – strukturiert, die sich gut für die Übertragung eignen. Diese Pakete werden mit notwendigen Zusatzinformationen versehen, hauptsächlich mit Absender- und Zieladresse. Das Internet Protocol regelt die Übertragung der entstehenden IP-Pakete unabhängig voneinander und jeweils nur zu der (bzw. einer) nächsten Vermittlungsstelle (Router). Diese Art der Übertragung heißt »verbindungslos«, weil der (vollständige) Übertragungsweg im Voraus nicht festgelegt ist und sich von Paket zu Paket ändern kann. Es gibt keine Garantie, dass alle IP-Pakete einer Anwendung gleichartig behandelt werden, bspw. dieselben Übertragungsstrecken benutzen und einander nicht überholen.

Für viele Protokolle und Anwendungen gilt das Ende-zu-Ende-Prinzip. Dabei erfolgt die Steuerung der Kommunikation durch die Endgeräte. Das dazwischen liegende Netz kann vergleichsweise einfach aufgebaut sein.

Die Endgeräte enthalten auch die anwendungsspezifischen Funktionen, d. h., sie verfügen über sehr ähnliche Internetanschlüsse, unterstützen aber so unterschiedliche Anwendungen wie Webzugriff oder IP-Telefonie. Die Technik der Netzebene ist anwendungsunabhängig, daher können neue Anwendungen sehr schnell und unabhängig von der bestehenden Infrastruktur eingeführt werden, z. B. eine neue App auf dem Smartphone. Sollen aber neue Mechanismen eingeführt werden, die ein geändertes Verhalten der Router (oder anderer Komponenten im Netz) erfordern, so ist das bei der internationalen Struktur des Internets nur sehr langsam bzw. evolutionär möglich.

Die Steuerung der Kommunikation erfolgt über die gleichen Wege wie die Übertragung der Inhaltsdaten. Daher kann ein erfolgreicher Angreifer des Kommunikationspfades stets auch die Steuerung der Kommunikation angreifen, die aus diesem Grund besonders geschützt werden muss.

4.1 ROUTING (WEGEWAHL)

Im Internet gibt es keine zentrale Steuerung von Netzen oder Kommunikationspfaden. Wenn Teilnehmer bzw. deren Autonome Systeme nicht direkt an dasselbe Netz angeschlossen sind, werden die IP-Pakete in Richtung des Adressaten in andere Netze weitergeleitet. Dabei wird die im IP-Paket enthaltene Zieladresse genutzt; die ebenfalls enthaltene Absenderadresse ermöglicht die Übertragung der Antwort des Kommunikationspartners. An Netzübergängen nehmen Router die Wegewahl vor. In Routingtabellen ist festgehalten, welche Netze bzw. Netzbereiche über welchen Pfad erreicht werden können.

Zum Aufbau der Routingtabellen tauschen Router Daten über die Erreichbarkeit von Netzen bzw. Netzbereichen aus. Auf Änderungen, wie bspw. den Ausfall einzelner Übertragungstrecken, kann so dynamisch reagiert werden. Dies und das individuelle Routing pro IP-Paket machen das Internet robust und skalierbar. Da das Internet Protocol verbindungslos funktioniert, werden IP-Pakete ohne Gewissheit weitergeleitet, dass der Adressat in der gewählten Richtung erreichbar ist. Es muss also nicht unbedingt eine »Gegenstelle« erreichbar sein, um eine Routingentscheidung zu treffen.

Der Zusammenschluss von Netzen der Kernzone als Grundlage für das Internet und das oben beschriebene Routing erfolgt in zwei Varianten: Zwei Netze werden direkt miteinander verbunden oder an Internetknoten (bspw. dem DE-CIX) wird eine größere Anzahl von Netzen zusammengeschlossen.

Die großen, überregional oder weltweit verfügbaren Netzinfrastrukturen bilden das Rückgrat (Backbone) des Internets. Betreiber großer, weltweiter Netzinfrastrukturen tauschen mit anderen großen Netzbetreibern direkt Daten aus und treten daneben als Internet Service Provider für mittlere und kleinere, nur regional präsente Netzbetreiber auf, die wiederum darüber einen Zugang zum Internet für ihre Kunden bereitstellen. Bei ausgeglichenen Interessen, meist zwischen größeren Providern, findet der Austausch ohne Berechnung statt; kleinere Provider müssen für ihren Zugang zu den Backbones des Internets bezahlen. Ausgehend von Europa hat sich das Konzept der Internetknoten entwickelt, an denen mehrere mittlere und kleinere Provider ihre Daten untereinander austauschen und so den Austausch mit den großen Providern verringern. Ein zentraler Internetknoten ermöglicht kurze Übertragungswege zwischen den Netzen der angeschlossenen Teilnehmer, was sich in kurzen Verzögerungszeiten für den Internetverkehr der Kunden positiv bemerkbar macht.

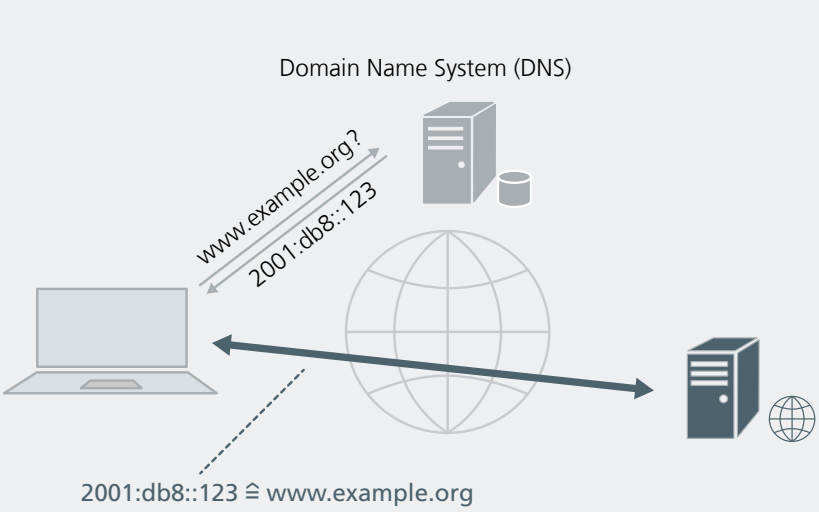


Abb. 5: Funktionsweise einer Namensabfrage über DNS

4.2 DOMAIN NAME SYSTEM (DNS)

Das Routing basiert auf den in den IP-Paketen enthaltenen Zieladressen (z. B. 192.0.2.123 für IPv4 oder 2001:db8::123 für IPv6). Da diese technischen Adressen für Menschen schwer nutzbar sind, wurde das Domain Name System (DNS) eingeführt, eine Art Telefonbuch für das Internet, das auf hierarchischen Namensbestandteilen beruht (z. B. »www.example.org«).

DNS basiert auf einer Baumstruktur, in der die Namen von rechts nach links aufgelöst werden. Im obigen Beispiel ist »org« die höchstrangige Domäne (Top Level Domain), innerhalb derer die Domäne »example« festgelegt ist. Komplettiert wird die Adresse eines Internetendgeräts (Hosts) hier durch den domänenspezifischen Hostnamen »www«, der wiederum innerhalb der Domäne mit dem niedrigsten Rang festgelegt ist. Dem vollständigen Hostnamen, hier: www.example.org, ist (mindestens) eine IP-Adresse zugeordnet.

Die Verwaltung der Domänen unterliegt sogenannten Registraren, für die Top Level Domain »de« ist das bspw. die DENIC eG.[8] Die reine Datenübertragung im Internet funktioniert auch ohne das DNS, allerdings wären dann Endgeräte und damit Dienste nicht oder nur schwer auffindbar. Technisch erfolgt der Zugang zu einem sogenannten Nameserver, der Host- und Domänennamen in IP-Adressen »übersetzt«, meist über den Internet Service Provider. Daneben existieren verschiedene unabhängige DNS-Strukturen, die aber vergleichsweise wenig genutzt werden. Sie sind meist politisch motiviert, bspw. mit dem Anspruch, Zensurmaßnahmen zu umgehen oder der (früher stärkeren) US-Dominanz beim Betrieb des DNS entgegenzuwirken.

Mittels des DNS kann zudem die Zuordnung zwischen Hostnamen und IP-Adressen flexibilisiert werden. Ein Endgerät kann verschiedene Namen bekommen, die auf dieselbe IP-Adresse abgebildet werden (z. B. können Funktionsnamen vergeben werden, wie »www« oder »mail«). Oder der gleiche DNS-Name kann auf verschiedene konkrete Endgeräte verweisen (z. B. zur Lastverteilung: Angesprochen wird immer »www.example.org«, aber je nach Region oder Auslastung werden verschiedene konkrete Server adressiert).

Die Adressierung über feste Namen kann auch eine Rolle spielen, wenn sich die IP-Adresse eines Dienstes gelegentlich ändert, wie es bei privaten Internetzugängen oder bei Nutzung von Mobilfunk der Fall sein kann. Sollen Dienste über einen derartigen Anschluss erreicht werden (bspw. im Anwendungsbereich Smart Home), so können diese dynamischen Adressänderungen im DNS über spezielle Dienstleister vorgenommen werden.[9]

Das Funktionieren des DNS und korrekte DNS-Zuordnungen sind notwendig für die übliche, typische Nutzung des Internets. Deshalb wird die Kommunikation mit und zwischen Nameservern zunehmend abgesichert (z. B. durch DNSSEC, das die Authentizität und Integrität von DNS-Nachrichten sicherstellt und damit verschiedene Angriffe auf das Internet über das DNS unterbindet).

Es ist zu erwarten, dass das DNS in der sich stetig weiterentwickelnden Architektur des Internets als einer der wenigen zentralen Mechanismen zukünftig eine noch wichtigere Rolle bei Sicherheitsfunktionen spielen wird. Bspw. zur Verteilung von Zertifikaten oder Schlüsseln stünden in den DNS-Nachrichten und -Servern geeignete Felder bereits zur Verfügung.

[8] http://www.denic.de/

[9] Eine weiter verbreite Alternative dazu ist, dass sich der Dienst unter seiner neuen Adresse bei einer dienstspezifischen Plattform anmeldet, womit der Betrieb dieses Dienstes dann aber möglicherweise von einer geschlossenen Plattform abhängig wird oder verschiedene Dienste unterschiedliche Plattformen benötigen.

IM INTERNET ERFOLGT DIE STEUERUNG DER KOMMUNIKATION ÜBER DIE GLEICHEN WEGE WIE DIE ÜBERTRAGUNG DER INHALTSDATEN, DAHER MUSS DIE STEUERUNG BESONDERS GESCHÜTZT WERDEN.

4.3 DIENSTQUALITÄT

Verschiedene Anwendungen haben unterschiedliche Anforderungen an die Datenübertragung: Beim Surfen im Web sollen sich Webseiten schnell aufbauen, auch wenn sie Bilder oder aus externen Quellen eingebettete Elemente (z. B. Video, Werbung) enthalten. Danach ist eine Lesepause, in der keine Übertragung stattfindet. Video und Audio erzeugen einen gleichmäßigen Datenstrom mit mehr oder weniger Übertragungsrate. Für ein angenehmes Gespräch zwischen Menschen sind geringe Antwortzeiten notwendig. Softwareupdates haben teilweise eine erstaunliche Größe, können aber zeitlich eher unkritisch im Hintergrund nebenbei geladen werden. Derartige Anforderungen an die Datenübertragung bzw. entsprechende Leistungsversprechen oder Messwerte werden als Dienstqualität bezeichnet.

Für jede Kommunikation müssen entsprechende Ressourcen zur Verfügung stehen. Früher wurden bei Telefonaten die maximal notwendigen Ressourcen vor Beginn des Gesprächs auf dem gesamten Kommunikationspfad und für die gesamte Dauer des Gesprächs reserviert. Bei Nutzung der Internettechnologie wird pro IP-Paket und nur jeweils für die Leitung oder den Funkkanal zum nächsten Router bzw. zum Adressaten entschieden, wann das IP-Paket diese Ressource benutzen darf.

Ressourcenvergabe ist in allen drei Zonen des Internet-Modells erforderlich, sie findet lokal auf der Netzebene in enger Abstimmung mit der jeweils lokalen Übertragungsebene statt.

Prinzipiell kann für jedes IP-Paket in jedem benutzten Router eine Konkurrenzsituation auftreten. Dies kann zu einer Überlastung führen, wobei der Router zunächst IP-Pakete zwischenspeichert und diese bei anhaltender Überlastung schlimmstenfalls wegwirft. Da normalerweise auf den Inhalt verworfener IP-Pakete nicht verzichtet werden kann, müssen sie vom Absender erneut geschickt werden. Dies bleibt den Nutzern in der Regel verborgen, kann sich aber durch größere Antwortzeiten bemerkbar machen.

Im einfachsten Fall werden die IP-Pakete unabhängig vom Inhalt in der Reihenfolge ihres Eingangs beim Router bearbeitet. Aber auch eine dienstklassenspezifische Behandlung ist möglich. Dabei können z. B. zeitkritische Pakete (die Sprache, Audio oder Video enthalten) bevorzugt werden.

Derzeit funktionieren Sprach-, Audio- und Videoübertragung über das Internet in der Regel erstaunlich gut, weil in allen drei Zonen meist mehr Ressourcen als Nachfrage vorhanden sind. Da sich jedoch mit insgesamt steigender Nachfrage und immer anspruchsvolleren Anwendungen Engpässe abzeichnen, wird über die Priorisierung von Datenströmen gegen höhere Gebühren diskutiert. Dies könnte kleine Unternehmen und Bürger gegenüber großen Konzernen benachteiligen, deshalb wird über die sogenannte Netzneutralität kontrovers diskutiert.

4.4 VERSCHLÜSSELUNG UND ANONYMISIERUNG

Verschlüsselung und Anonymisierung dienen dem Schutz gegen Ausspähung und damit einem Grundbedürfnis des Menschen.

Verschlüsselung

Verschlüsselung wird benutzt, um vertrauliche Daten sicher zu speichern und/oder über nicht vertrauenswürdige Kommunikationspfade zu transportieren. Im Internet bestehen diese Pfade aus Leitungen, Routern und Funkkanälen, die mit mehr oder weniger Aufwand und Expertenwissen abgehört werden können.

Verschlüsselung basiert stets auf einem Geheimnis, das nur dem Adressaten oder – abhängig vom Verschlüsselungsverfahren – Absender und Adressat bekannt ist.

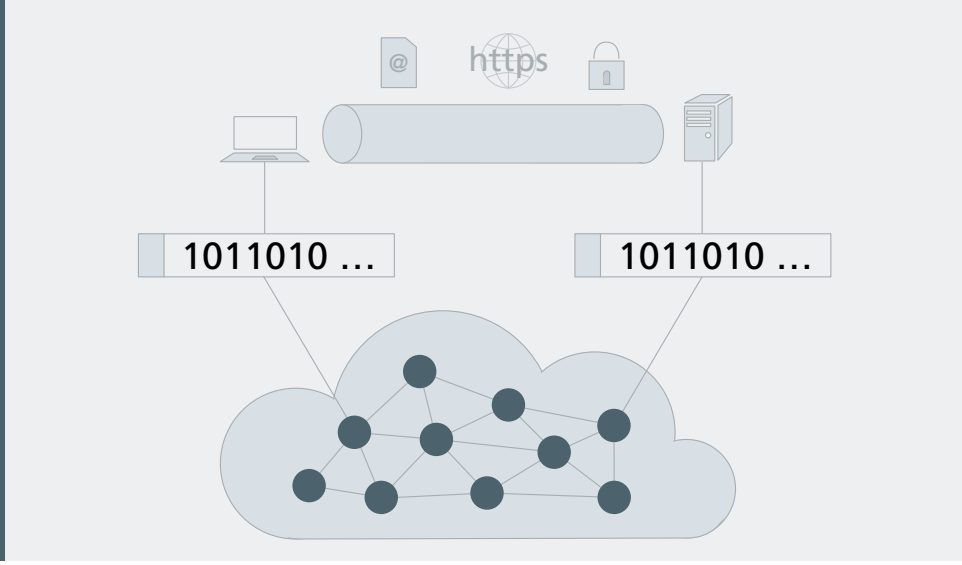


Abb. 6: Schematische Darstellung des Ende-zu-Ende-Prinzips (siehe ÖFIT-Whitepaper »Fortschrittliche Netze«)

Eine Nachricht, z. B. der Inhalt einer E-Mail, kann durch den Absender (bzw. ein entsprechendes Computerprogramm) verschlüsselt, anschließend übertragen und vom Adressaten entschlüsselt werden. Dies findet auf der Anwendungsebene statt und man spricht von Ende-zu-Ende-Verschlüsselung. E-Mail-Anhänge können auch bereits außerhalb des Modells verschlüsselt werden, beispielsweise, wenn sie schon auf dem Computersystem des Absenders geschützt werden müssen.

Es ist außerdem möglich, eine verschlüsselte virtuelle Verbindung der Netzebene zu nutzen. Dabei verschlüsselt die Netzebene alle Daten, die über eine solche Verbindung transportiert werden. Da, wie in Kapitel 4 beschrieben, Verbindungen nicht dauerhaft etabliert werden, ist eine virtuelle Verbindung der Netzebene durch ein konkretes Paar aus Absender- und Zieladresse gekennzeichnet.

Befinden sich zwischen Absender und Adressat Sicherheitsgeräte, die abgehende oder ankommende Datenströme filtern, um beispielsweise den Versand vertraulichen Materials an Unbefugte oder Angriffe auf die lokale IT-Infrastruktur zu verhindern, müssen diese Geräte ebenfalls die erforderlichen, geheimen Schlüssel besitzen, um die Daten analysieren zu können. Werden dabei Teile der Daten verändert, müssen ggf. auch die Schlüssel zur erneuten Verschlüsselung vorhanden sein. Dies gilt für Verschlüsselung in der Anwendungs- wie auch in der Netzebene.

Darüber hinaus ist Verschlüsselung in der Übertragungsebene möglich. Diese findet regelmäßig nur auf einzelnen Übertragungsstrecken, also beispielsweise auf der Funkstrecke zwischen mobilem Endgerät und Mobilfunk-Basisstation bzw. WLAN-Hotspot statt. Auf allen Übertragungsabschnitten kann unabhängig voneinander verschlüsselt oder unverschlüsselt übertragen werden. Eine abschnittsweise Verschlüsselung (unabhängig von der Ebene) dient der lokalen Absicherung der Kommunikation; ein Nutzer kann dabei nicht auf Ende-zu-Ende-Abhörsicherheit vertrauen.

Die Verschlüsselung der Daten in der Übertragungsebene der Kernzone verlangt aufgrund der großen Datenraten der dortigen Übertragungsstrecken eine hohe Rechenleistung in den Routern an beiden Enden. Sie ist dennoch sinnvoll: Sie bietet einen Basisschutz und verhindert einige Möglichkeiten des Abhörens.

Auf deutschen Mobilfunkstrecken ist Verschlüsselung generell üblich, auch WLAN-Verkehr ist häufig verschlüsselt. In beiden Fällen sind in der Vergangenheit gravierende Schwachstellen aufgetreten, weil beispielsweise die Daten zu leicht entschlüsselt werden konnten oder Schlüssel leichtfertig an nicht ausreichend authentifizierte Dritte weitergegeben wurden. Derartige Schwachstellen werden allerdings in der Regel zügig beseitigt.

Eine wichtige Rolle bei der sicheren Kommunikation über das Internet spielen auch sogenannte VPNs (Virtual Private Networks). Oberhalb der Netzebene werden virtuelle Verbindungen geschaffen, die sich gegenüber den Anwendungen wie eine abhörgeschützte Netzebene verhalten. Gleichzeitig bleibt geheim, welche Dienste konkret genutzt werden. Netzbetreiber bieten Geschäftskunden i. d. R. auch sogenannte MPLS[10]-Lösungen an, die in der Netzebene vom öffentlich zugänglichen Internet getrennt sind und den Kunden geschützte Kommunikationspfade zu vorkonfigurierten Partnern bereitstellen.

Anonymisierung

Absender- und Zieladresse jedes IP-Paketes sind auch bei Verschlüsselung des Paketinhaltes stets unverschlüsselt, da sie von den Routern auf dem Kommunikationspfad ausgewertet werden müssen. Sind die Adressen bzw. Adressbereiche Teilnehmern fest zugeordnet, lässt sich ausspähen, wer mit wem kommuniziert.

[10] MultiProtocol Label Switching

DIE ANALYSE UND FILTERUNG VON DATENSTRÖMEN IST EINE WICHTIGE GRUNDLAGE FÜR SICHERE INTERNETKOMMUNIKATION.

Anonymisierungsdienste bieten an, die Beziehung zwischen Absender- und Zieladresse zu verschleiern. Die Nutzer des Dienstes verpacken ihre IP-Pakete einschließlich Absender- und Zieladresse in IP-Pakete an den Dienstleister (so, wie man einen Brief samt Umschlag in einen weiteren Umschlag stecken kann) und verschicken diese. Dabei wird das ursprüngliche IP-Paket oder die virtuelle Verbindung zum Dienstleister verschlüsselt. Ein unerwünschter Beobachter kann nur feststellen, dass der Nutzer mit dem Dienstleister kommuniziert. Der Dienstleister packt die ursprünglichen IP-Pakete aus und wertet die Zieladresse aus. In der Regel ersetzt er die Absenderadresse durch seine eigene und sendet das Ergebnis an die Zieladresse. Etwaige Antworten landen damit ebenfalls beim Dienstleister, der sie wiederum verpackt an den Nutzer des Dienstes weiterleitet. So wird die eigentliche Kommunikationsbeziehung verschleiert. Allerdings muss die Nutzer dem Dienstleister vertrauen, da dieser die gesamte Kommunikation verfolgen kann.

Beim Tor-Netzwerk[11] wird das geschilderte Verfahren erweitert: Die Nutzer schicken ihre Pakete mehrfach verschlüsselt über einen Kommunikationspfad, der über drei vom Nutzer ausgewählte Anonymisierungsserver führt. Jeder Anonymisierungsserver entfernt eine Entschlüsselungsschicht und erhält so ein Datenpaket, das er an den nächsten Server bzw. am Ende an den Adressaten weiterleiten kann. Jeder der Server kennt so nur seinen Vorgänger und seinen Nachfolger. Auf dem Rückweg erfolgt dieser Vorgang umgekehrt. Durch den dynamischen Wechsel von Pfaden innerhalb des Anonymisierungsnetzwerks und das begrenzte Wissen eines Servers über die Kommunikationsbeziehungen wird die Anonymisierung ohne zentrale Mechanismen hergestellt. Der Nutzer muss nicht mehr einem Dienstleister vertrauen, er hat einen inhärent wirksamen Mechanismus zur Verfügung. Allerdings kann auch ein derartiges Anonymisierungsnetzwerk mit einigem Aufwand angegriffen werden, bspw. mittels Analysen verteilter Datenströme oder der Kontrolle über wesentliche Teile des Netzwerks.

4.5 ANALYSE, FILTERUNG UND DROSSELUNG

Analyse und Filterung von Datenströmen des Internets wird meist zuerst mit Überwachung und Zensur assoziiert, beides bildet aber auch eine entscheidende Grundlage für das Funktionieren des Internets und die Sicherheit dabei. Einzelne Informationen, wie Absender- und Zieladresse, müssen zur Wegewahl von Routern analysiert werden. Und gerade aufgrund der offenen Struktur des Internets ist es notwendig, an Übergängen zu privaten Netzen und zu geschlossenen Infrastrukturen bestimmte Teile der ankommenden Kommunikation zu analysieren und ggf. nicht oder nur verändert zuzulassen, um Gefahren wie Viren oder Denial-of-Service-Angriffe[12] abzuwehren.

Analysierende und ggf. filternde Sicherheitsgeräte sind ein notwendiges Mittel zum Schutz privater Netze und geschlossener Infrastrukturen. Neben der Abwehr von Angriffen aus dem Internet können sie auch die Aufgabe haben, das ungewollte Abfließen vertraulicher Daten aus den geschützten Strukturen zu verhindern. Dazu ist eine Analyse und ggf. Filterung abgehender Daten notwendig.

Die Filterung in der Netzebene findet meist an Übergängen zu Firmen- oder heimischen Netzen statt. Dabei kommen Firewalls (Paketfilter) zum Einsatz, die über die Filterung der Datenströme des Internetzugangs bspw. nur erwünschte Kommunikationsbeziehungen zulassen, die durch bekannte Internetadressen gekennzeichnet sind.

In der Zugangszone werden von den Netzbetreibern vereinzelt Filter eingesetzt, um einzelne Dienste zu unterbinden, bspw. Internettelefonie, wenn dadurch Einnahmeeinbußen beim klas-

[11] https://www.torproject.org/;
vgl. auch ÖFIT-Trendschau, Trendthema 30: »Darknet«, Stand: Juni 2015

[12] Z. B. Überflutung mit Nachrichten, die den ordnungsgemäßen Betrieb eines Dienstangebotes oder eines ganzen Firmennetzes lahmlegen würden.

ZUR SICHERSTELLUNG DER DIENSTQUALITÄT IST DER EINBLICK IN INHALTSDATEN NICHT NOTWENDIG – ENTHALTEN IP-PAKETE STANDARDISIERTE QUALITÄTSANFORDERUNGEN, KANN DIE NETZEBENE EINE ENTSPRECHENDE PRIORISIERUNG VORNEHMEN.

sischen Telefondienst drohen. Internetanbieter drosseln auf bestimmten Anschlüssen das Volumen, wenn das vertraglich vereinbarte maximale Verkehrsvolumen überschritten ist.[13]

Für bestimmte Anwendungen mit Nutzung festgelegter Dienste (bspw. bei Kommunikation von Maschinen oder Sensoren) ist es vorstellbar, dass entsprechend eingeschränkte Internetzugänge in Zukunft eine größere Rolle spielen. Dabei werden die komplexen Sicherheitsfunktionen von Spezialisten als Dienstleistung in der Zugangszone übernommen.

Filter in der Anwendungsebene oder für Inhaltsdaten schützen bspw. gegen die Verbreitung von Schadsoftware durch Webseiten oder Spam-E-Mails. Sie werden bei einem Dienstleister, über den der Nutzer seine entsprechende Kommunikation leitet, oder direkt im Netz des Nutzers eingesetzt.

Verschlüsselte Daten können nicht analysiert werden, siehe Kapitel 4.4. Da es aber aus Sicherheitsgründen notwendig sein kann, Teile eines Datenstroms zu analysieren, stehen mehrstufige Verschlüsselungsmechanismen zur Verfügung. Nur die spezifischen Daten notwendiger Schichten werden entschlüsselt und ausgewertet. Insbesondere die Inhaltsdaten können durch Verschlüsselung Ende-zu-Ende geschützt werden. In der Netzebene werden bspw. Internetadressen ausgewertet, die Notwendigkeit zur Analyse von Daten der darüber liegenden Anwendungsebene oder gar der Inhaltsdaten besteht in vielen Fällen nicht. Auch zur Sicherstellung der Dienstqualität ist der Einblick in die Anwendungsebene nicht notwendig. Enthalten die IP-Pakete standardisierte Qualitätsanforderungen, kann die Netzebene eine entsprechende Priorisierung vornehmen.

[13] Eine Testseite zur Ermittlung des Dienstqualität von Internetzugängen im Auftrag der Bundesnetzagentur findet man unter http://www.initiative-netzqualitaet.de

5. BEISPIELE ZUR ANWENDUNG DES MODELLS

Die Anwendung des beschriebenen Internet-Modells wird anhand von zwei Beispielen erläutert. Wir konzentrieren uns dabei entsprechend dem Modell auf die technische Dimension und zeigen erste Verbindungen zwischen verschiedenen Themen auf. Eine umfangreiche Darstellung der Themen und die Bewertung von mehreren, alternativ denkbaren Lösungsmöglichkeiten würden hier den Rahmen sprengen.

5.1 KINDER- UND JUGENDSCHUTZ

Der Schutz von Kindern und Jugendlichen gegen ungeeignete audiovisuelle Medien erhält eine umso höhere Bedeutung, je mehr solcher Medien im Internet genutzt oder aus diesem zur Offline-Nutzung heruntergeladen werden. Nach einer aktuellen Studie[14] nutzen mehr als 98 Prozent der Jugendlichen (älter als 12 Jahre) das Internet, im Schnitt mehr als eine Stunde täglich. Mehr als 75 Prozent davon schauen Videos, rund 55 Prozent spielen Online-Spiele. Eine weitere Studie kommt zu ähnlichen Zahlen.[15]

Nutzerseitig können Eltern und Betreuer in allen drei Ebenen unseres Internet-Modells Filter- und Blockierungsmaßnahmen einsetzen. Um den gewünschten Schutz zu erreichen, ohne gleichzeitig die akzeptierte Internetnutzung für die Kinder und Jugendlichen zu beschränken, sind abgestimmte Maßnahmen notwendig. Zu berücksichtigen sind dabei auch andere Personen, die dieselben Endgeräte oder denselben Zugang benutzen.

In der Anwendungsebene – bei den Inhalten und bei den sie beschreibenden Daten – stehen hauptsächlich die Titel der Medien, die Titel der Webseiten, die Webadressen und von den Anbietern bereitgestellte Beschreibungen zur Verfügung. Die beschreibenden Daten können z. B. sogenannte Labels (age-label.de, ICRA[16], PICS[17]) oder Inhaltsbeschreibungen der Medien sein.

In der Netzebene kann der Zugang zu Hostnamen bzw. IP-Adressen und zu Diensttypen (E-Mail, Webzugriff …) eingeschränkt werden. Hier zeigen sich verschiedene Probleme: Ändert ein Dienstanbieter seinen Hostnamen oder seine IP-Adresse, wird er von Suchdiensten bzw. dem DNS (s. Kapitel 4.2) nach kurzer Zeit wieder gefunden, eine statisch eingestellte Zugangsbeschränkung hat ihre Wirkung verloren. Ebenso ist der Zugang über verschiedene Wege oder Dienste möglich, wobei einzelne Einschränkungen dann ins Leere laufen können. Beispielsweise kann auf E-Mails häufig sowohl über E-Mail-Programme als auch über eine Webseite zugegriffen werden.

In der Übertragungsebene werden zeitweilige Nutzungsverbote, z. B. bei Abwesenheit der Erziehenden, technisch unterstützt.

Für private lokale Netze gibt es Kinder- und Jugendschutz-Software, die im heimischen Router installiert und konfiguriert wird und über das heimische Netz die Konsistenz der Nutzungsregeln in allen Geräten sicherstellt. Alle den Kindern/Jugendlichen verfügbaren Geräte, die einen weiteren Internetzugang nutzen (bspw. Smartphones), müssen separat konfiguriert werden. Diese Mechanismen sind in der Nutzerzone angesiedelt.

Von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) indizierte Inhalte dürfen in Deutschland nur in geschlossenen Benutzergruppen angeboten werden, für die eine Altersüberprüfung und eine individuelle Authentifizierung (z. B. über Benutzername und Passwort) erforderlich ist. Allerdings kann das nicht den Zugriff auf ausländische Angebote verhindern. Mehrere bedeutende Suchmaschinenbeteiber haben sich verpflichtet, Webseiten mit indizierten Inhalten – soweit dies für den Suchmaschinenbeteiber erkennbar ist – nicht in ihren Trefferlisten anzuzeigen. Nach unserem Internet-Modell findet diese Filterung und Blockierung in der Anwendungsebene der Kernzone statt.

[14] BITKOM: »Jung und vernetzt – Kinder und Jugendliche in der digitalen Gesellschaft«, 11.01.2015, http://www.bitkom.org/files/documents/BITKOM_Studie_Jung_und_vernetzt_2014.pdf
[15] D21-»Digital-Index 2014 - Die Entwicklung der digitalen Gesellschaft in Deutschland«, Befragungszeitraum: Juni bis Juli 2014, http://www.initiatived21.de/portfolio/nonliner-atlas/
[16] https://www.fosi.org/icra/
[17] http://www.w3.org/TR/REC-PICS-services-961031

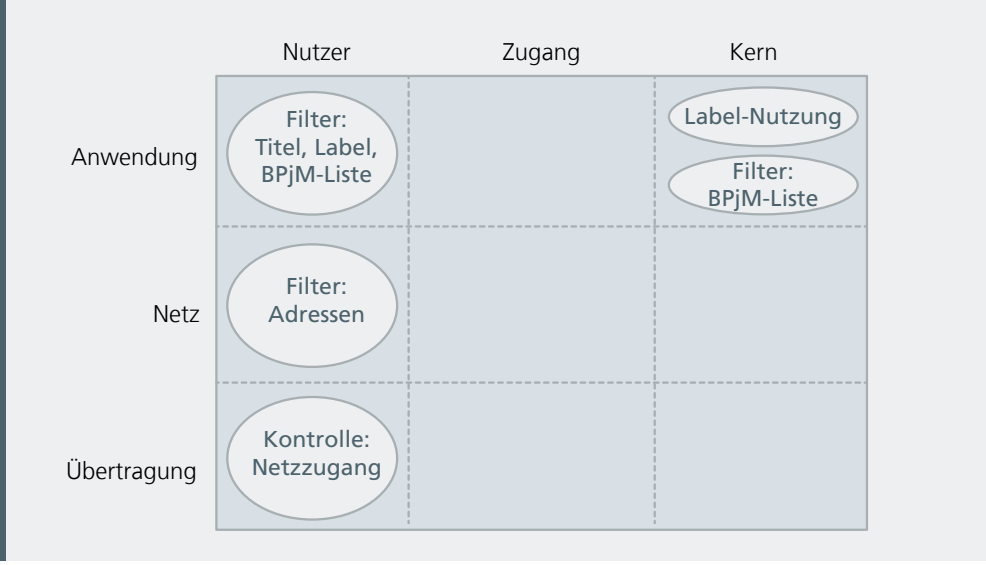


Abb. 7: Die Handlungsfelder für Kinder- und Jugendschutz im Internet-Modell

5.2 NATIONALISIERUNG VON ROUTING UND CLOUD-DIENSTEN

Nach den Enthüllungen zu Möglichkeiten und Ausmaß der Überwachung des Internets durch Geheimdienste wurden verschiedene Gegenmaßnahmen diskutiert. Als eine mögliche Maßnahme wurde eine stärkere regionale Abgrenzung des Internetverkehrs vorgeschlagen, bekannt geworden unter dem Stichwort »Schengen-Routing«. Bei der Idee geht es darum, dass der Datenverkehr zwischen einem Absender und einem Adressaten in Deutschland oder im Schengen-Raum auch nur innerhalb dieses Raums übertragen wird. So sollen die Möglichkeiten zum Abhören von Kommunikation erschwert, aber auch Wirtschaft und Zivilgesellschaft gegen Cyberkriminalität geschützt werden.[18]

Beim Routing in der Kernzone stehen normalerweise verschiedene Wege zur Auswahl, die konkrete Entscheidung wird aufgrund von Wirtschaftlichkeit oder Verfügbarkeit von Kapazitäten getroffen. Dabei kann es dazu kommen, dass Internetverkehr, der eigentlich in einer politischen Region (Deutschland, Schengen-Raum) verbleiben könnte, über andere Regionen sein Ziel erreicht. In der Topologie des Internets kann dieser Weg durchaus »naheliegend« sein.

Es ist nachvollziehbar, dass ein nationales Routing als Lösung gegen die Ausspähung gesehen wird. Diese Sichtweise greift allerdings zu kurz: Für fremde Geheimdienste ist es möglicherweise schwieriger, in Deutschland statt im Heimatland zu agieren. Sie haben jedoch mit hoher Wahrscheinlichkeit auch Mittel, Inhalte in Deutschland auf anderen Wegen auszuspähen, z. B. direkt auf Servern, falls diese nicht zeitgemäße und angemessene Sicherheitsmaßnahmen nutzen. Voneinander abweichende Rechtssysteme und die tlw. unterschiedliche Behandlung eigener und fremder Bürger können das Handeln fremder Geheimdienste in Deutschland bzw. dem Schengen-Raum sogar rechtlich erleichtern. Ein regionales Routing ist zudem naturgemäß nur möglich, wenn sich beide Enden der Kommunikationsbeziehung in derselben Region befinden. Viele attraktive Dienste werden aus wirtschaftlichen oder gesetzlichen Gründen gerade nicht regional betrieben. Darüber hinaus ist es für die Nutzer nicht unbedingt auf Anhieb erkennbar, ob sie einen regional betriebenen Dienst nutzen.

Aus technischer Sicht sind die verschiedenen Pfade und eine hohe Zahl von Übergängen zwischen verschiedenen Netzen ein wesentlicher Grund für die Robustheit des Internets. Ein Ausbau des Internets innerhalb einer Region stärkt das Internet. Wenn alle bisherigen Übergänge zwischen den Netzen erhalten bleiben, spricht also nichts gegen den Ausbau des regionalen Austauschs.

Zunehmend werden auch schutzbedürftige Inhalte, die bisher auf firmeneigenen bzw. privaten Computern vorgehalten wurden, »in die Cloud« verlagert. Nach unserem Modell handelt sich dabei um Inhaltsdaten der Anwendungsebene, die vom Nutzer auf eine Plattform verlagert werden. Damit befinden sie sich dann auf Servern, die von Dienstleistern betrieben werden und auf die über das Internet zugegriffen wird. Im Gegensatz zu den für den Nutzer nicht erkennbaren Kommunikationspfaden ist der Dienstleister bei der Speicherung und Verarbeitung von Daten klar erkennbar und es besteht zwischen beiden mindestens über die AGBs[19] des Dienstleisters ein Vertragsverhältnis. Nationale bzw. regionale Anbieter können das Vertrauen der Nutzer durch rechtliche und kulturelle Aspekte in den Verträgen bzw. den AGBs (bspw. beim Verständnis von Datenschutz) fördern und sich so Alleinstellungsmerkmale erarbeiten.

[18] Obermann, René: Die vergiftete Freiheit, http://www.faz.net/aktuell/politik/inland/nsa-debatte-die-vergiftete-freiheit-12661522.html
[19] Allgemeine Geschäftsbedingungen

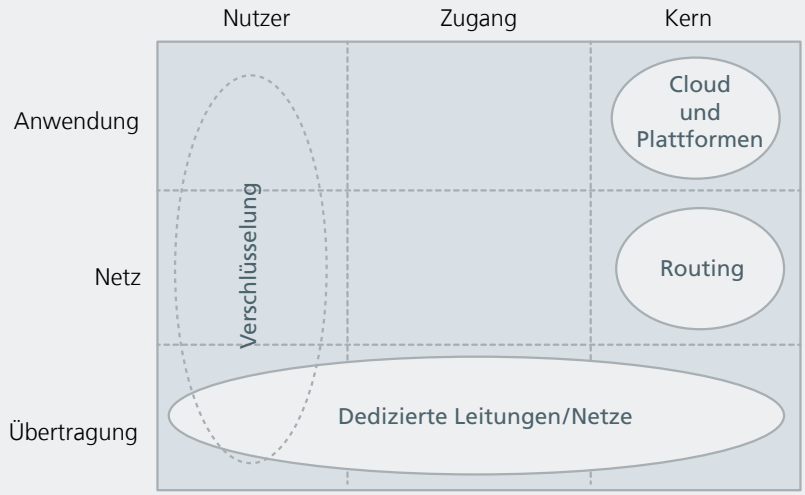


Abb. 8: Die Handlungsfelder der Nationalisierung von IT im Internet-Modell

Ein wirksamerer Schutz der Daten ist allerdings Verschlüsselung, s. Kapitel 4.4. Erfolgt die Verschlüsselung unter der Hoheit der Nutzer (d. h., die Schlüssel verbleiben ausschließlich bei ihn), dann kann ein Dienstleister gegenüber Kunden und Dritten glaubhaft versichern, dass er keinen Zugriff auf die Daten hat.

Für große Unternehmen oder große Teilbereiche der öffentlichen Verwaltung kann auch eine direkte Anbindung an eine Cloud über dedizierte physische oder virtuelle Leitungen – in der Übertragungsebene des Internet-Modells – angemessen sein, um das Risiko einer Ausspähung beim Transport zu reduzieren.

Auch wenn der Nutzen einer Nationalisierung des Internets begrenzt ist, gibt es dennoch Maßnahmen, die sinnvoll staatlich unterstützt werden sollten. Dazu gehören z. B. Maßnahmen zur Erhaltung (bzw. Wiedererlangung) nationaler technischer Souveränität: Geeignete Verschlüsselungsverfahren und deren Umsetzungen in Produkte können nur von Spezialisten bewertet werden; eine Bewertung bspw. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)[20] und durch unabhängige Wissenschaftler kann eine sichere und transparente Grundlage schaffen. Der praktische Einsatz von Verschlüsselung beruht u. a. auf Infrastrukturen zur Verteilung von Schlüsseln und der Ausgabe von vertrauenswürdigen Zertifikaten.[21] In diesem Bereich können Wirtschaft und Zivilgesellschaft unterstützt bzw. das für die Sicherheit notwendige Vertrauen verankert werden.

[20] Bspw. mit der Technischen Richtlinie »BSI TR-02102-1 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen« oder mit Empfehlungen über das Portal »BSI für Bürger«, https://www.bsi-fuer-buerger.de/
[21] Elektronischen Identitätsbelegen

6. HANDLUNGSEMPFEHLUNGEN

In diesem Dokument haben wir ein einfaches Internet-Modell sowie Eigenschaften und Mechanismen des Internets vorgestellt, um eine fundierte Diskussion von Netzfragen zu unterstützen. Das technisch orientierte Modell ermöglicht es, die Beziehungen zwischen verschiedenen Bereichen des Internets im Blick zu behalten. Aus unseren Betrachtungen lassen sich allgemeine Handlungsempfehlungen ableiten:

Entwicklungstempo von Internetanwendungen und deren wirtschaftliche und gesellschaftliche Auswirkungen nicht unterschätzen

Motor und Richtungsgeber der Internetentwicklung sind jene Anwendungen, die als nützlich empfunden werden, sich – z. B. über mobile Endgeräte – schnell auf dem Markt etablieren und potenziell einen großen Einfluss auf den Alltag haben. Beispiele sind Musikdownloads und Online-Versandhandel, aber auch Internet-Videotelefonie und -Dateispeicherungssysteme. Die Entwicklungszyklen in traditionellen Branchen (vgl. Industrieautomatisierung) mögen noch langsam sein, geraten aber durch die Informations- und Kommunikationstechnik ebenfalls unter Druck. Dabei darf man nicht nur auf die direkte Konkurrenz schauen, es können auch schlagartig ganze Anwendungsfelder oder gar Branchen infrage gestellt werden, wie die Beispiele Videothek vs. Streaming oder SMS vs. Instant Messaging zeigen.

Offene Schnittstellen im Internet beibehalten

Im Zuge der Entwicklung von Netz und Anwendungen muss darauf geachtet werden, dass funktional unterschiedliche Teile weiterhin voneinander trennbar und damit einzeln austauschbar bleiben, um alternative Lösungen und Wettbewerb zu erlauben. Das Internet-Modell beschreibt in vereinfachter Weise Schnittstellen zwischen den verschiedenen Teilbereichen des Internets. Finanzkräftige Anbieter internetbasierter Dienste oder kundenstarke Internetanbieter dürfen nicht den kompletten Pfad durch das Netz bedingungslos kontrollieren. Auf der Anwendungsebene muss die Existenz konkurrierender Dienstleistungen und Anwendungen gefördert werden bzw. monopolartige Angebote müssen besonderen Verpflichtungen unterliegen.

Internetanschluss und Internet offen, einfach und durchlässig halten

Die offene und einfache technische Struktur des Internets und des Internetzugangs müssen erhalten bleiben, um zukünftige Innovationen zu ermöglichen. Ohne Änderungen an der einfachen physischen Struktur können komplexe Anwendungen mit höheren technischen Anforderungen realisiert werden, bspw. durch die Kombination bestehender Elemente. Widersprüchliche Anforderungen nach Sicherheit, Leistungsfähigkeit und Wirtschaftlichkeit können dazu führen, dass sich verschiedene Anschlusstypen weiter ausdifferenzieren und der Internetzugang zusätzliche Funktionen für den Nutzer oder angeschlossene Geräte übernimmt. Der Internetzugang, bspw. für private Haushalte und Maschinen, muss den steigenden Anforderungen genügen und gleichzeitig so einfach und transparent wie möglich bleiben.

Die grundlegende Internationalität des Internets bei politischen Entscheidungen mitdenken

Das Internet ist in seiner technischen Struktur zunächst unabhängig von politischen Strukturen, z. B. Staaten oder Bundesländern, und bildet einen eigenen, virtuellen Raum. Darüber angebotene Dienste sind grundlegend international angelegt und werden weltweit nachgefragt. Kommunikationspfade orientieren sich beispielsweise nur an Staatsgrenzen, wenn dies explizit verlangt wird. Angebotene Dienste können prinzipiell von jedem Zugangspunkt des Internets genutzt werden, es sei denn, dies wird durch Filterung aktiv verhindert. Überlegungen und Regelungen zur gezielten Wahl von Kommunikationspfaden zum Schutz der Nutzer und ihrer Daten usw. sollten diese Internationalität stets im Blick behalten. Sonst wird evtl. zwar national eine angemessene Regelung gefunden, diese bleibt aber durch die Internationalität des Internets wirkungslos oder stellt sogar für deutsche Unternehmen einen Wettbewerbsnachteil dar. Beispielsweise wird eine Blockierung fragwürdiger Inhalte aus deutschen Quellen zu einer vermehrten Nutzung ausländischer Quellen derselben Inhalte führen.

Angemessene Versorgung fördern

Das Internet als Basis-Infrastruktur wird vielfach bereits als Teil der Grundversorgung angesehen und müsste in der Konsequenz für private Haushalte und Unternehmen in angemessenem Maß zugänglich und nutzbar sein. Die Angemessenheit wandelt sich in Bezug auf das Internet noch rasant und muss in kurzen Zyklen neu festgelegt werden. Grundlage dafür sind bekannte Kriterien wie die Gleichwertigkeit von Lebensverhältnissen und die Teilhabe am gesellschaftlichen Leben. Dazu muss auch einkommensschwachen Haushalten und Unternehmen in

DAS VORGESTELLTE, TECHNISCH ORIENTIERTE INTERNET-MODELL UNTERSTÜTZT EINE FUNDIERTE DISKUSSION VON NETZFRAGEN.

strukturschwachen Gebieten die zeitgemäße Internetnutzung ermöglicht werden.

Der Netzausbau als Ganzes und speziell die Versorgung schwach besiedelter Gebiete bedarf besonderer Beachtung: Erfolg versprechende technische Lösungen müssen erforscht und gefördert werden, ggf. müssen die Netzbetreiber durch regulative und/oder Anreizmaßnahmen veranlasst werden, auch wirtschaftlich weniger attraktive Lösungen zum gesamtgesellschaftlichen oder gesamtwirtschaftlichen Nutzen zu realisieren.

Öffentlich geförderte WLAN-Hotspots oder die Mitnutzung fremder privater WLANs können zur Verbesserung der Situation beitragen. Dazu muss gesetzlich sichergestellt werden, dass der Bereitsteller eines derartigen Zugangs nicht für ein Fehlverhalten der Nutzer verantwortlich gemacht werden kann. Eine staatliche Unterstützung könnte beispielsweise auch durch Aufstellungs-, Montage- und Betriebserlaubnisse erfolgen.

Regelmäßig einen Bericht zum Zustand des Internets veröffentlichen

Große Dienstleister auf Netz- und Anwendungsebene erfassen viele Daten über den aktuellen Zustand des Internets und dessen Nutzung (bspw. Erreichbarkeit anderer Netze, Qualität von Verbindungen, Auslastung von Ressourcen), die teilweise als Geschäftsgeheimnis eingestuft und nur zu einem Teil veröffentlicht werden. Von Forschungseinrichtungen und Einrichtungen wie Internet-Registraren werden weitere Daten zum Zustand des Internets veröffentlicht. Die hohe Bedeutung des Internets als technische Basis-Infrastruktur erfordert eine systematische Auswertung vorhandener Daten und die verständliche Darstellung von Entwicklungen und Problemen in einem periodischen Bericht. Die Diskussion über zusätzliche Metriken und deren ggf. resultierende Erfassung sollten entsprechend der Internetkultur bevorzugt in einer offenen, internationalen Kooperation erfolgen.

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Jens Tiemann
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

kre | 1510 (Fotos: Fraunhofer FOKUS)