Bundesministerium
für Wirtschaft
und Technologie

WIRTSCHAFT.
WACHSTUM.
WOHLSTAND.

Das Internetprotokoll Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland

Abschlussbericht

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Technologie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Stand
Juni 2012

Druck
BMWi

Gestaltung und Produktion
PRpetuum GmbH, München

Redaktion
Bundesministerium für Wirtschaft
und Technologie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Das Bundesministerium für Wirtschaft und Technologie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Bundesministerium
für Wirtschaft
und Technologie

WIRTSCHAFT.
WACHSTUM.
WOHLSTAND.

Das Internetprotokoll Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland

Abschlussbericht

Inhaltsverzeichnis

Workshop „Das Internetprotokoll Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland“

Zusammenfassung der Ergebnisse

Mit dem Workshop „Das Internetprotokoll Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland“ ging es dem Bundesministerium für Wirtschaft und Technologie vor allem darum, gemeinsam mit den wichtigsten Akteuren aus Wirtschaft und Wissenschaft die Auswirkungen der laufenden Umstellung auf das neue Internetprotokoll für deutsche Wirtschaftsinteressen in ausgesuchten Handlungsfeldern zu erörtern und hieraus ggf. Handlungsempfehlungen abzuleiten. Zusammenfassung der wesentlichen Ergebnisse:

A. Grundsätzliches

- Nur zur Herstellung der Interoperabilität zwischen IPv4 und IPv6 bedarf es keiner besonderen Anstrengungen beim Umstieg auf das neue Internetprotokoll, denn die Einführung von IPv6 lässt sich mit bekannten technischen Hilfsmechanismen herbeiführen; erst durch eine konsequente Nutzung der neuen, technischen Funktionalitäten von IPv6 eröffnen sich im Internet neue Wachstumschancen. Empfehlung: Gerade die öffentlichen Hände müssen hier mit gutem Beispiel vorangehen und den nötigen „Zug“ entwickeln; insbesondere in der öffentlichen Beschaffung und bei netzbasierten F&E-Projekten sollte der Einsatz von IPv6 ein durchgängiges Thema sein.

- Das neue Internetprotokoll IPv6 stellt das sog. „Ende-zu-Ende-Paradigma“ bei der Architektur künftiger IKT-Netze wieder her; dabei wird die dynamische Entwicklung des Internets und seiner Anwendungen unterstützt; die Wertschöpfung und Innovation bzw. Funktionen und „Intelligenz“ werden weiter zunehmend von den Transportnetzen in die Endgeräte und Dienste verlagert.

- Von zentraler Bedeutung für eine wirtschaftspolitische Bewertung der jeweiligen Umstellungsinteressen ist die Unterscheidung zwischen den wirtschaftlichen Interessen von TK-Infrastruktur-/Zugangsanbietern und denen der Endgeräte-Hersteller und Dienst-Anbieter. Während der Umstieg für Erstere regelmäßig kurzfristig mit erheblichem Aufwand verbunden ist, dem kein unmittelbar messbarer Mehrwert gegenübersteht, können Letztere oft mit vergleichsweise geringem Einsatz die neuen Funktionen von IPv6 nutzen, hieraus innovative neue Geschäftsmodelle entwickeln und damit von der Umstellung der TK-Netze mittelbar profitieren. Während Erstere i. d. R. lokal gebunden sind, können Letztere global agieren. Für den Endnutzer ist diese Unterscheidung unwichtig; ihm kommt es alleine auf die Verfügbarkeit von IPv6-basierten Diensten und Endgeräten an. Allerdings könnte diese Konstellation den Konflikt zwischen den großen TK-Infrastrukturanbietern (Carrier) und den Diensteanbietern im Internet weiter verschärfen.

B. TK-Anbieter/TK-Ausrüster

- Die Umstellung bestehender TK-Netze ist komplex, aufwendig und kann schon bei kleinen Fehlern bzw. Nachlässigkeiten von der Verminderung der Leistungsfähigkeit bis zu Ausfällen kompletter Teil- bzw. Unternehmensnetze führen. Um solche Fehler zu vermeiden, bedarf es einer sorgfältigen Planung des konkreten Umstiegs sowie eines recht spezifischen IKT-Know-hows, das allerdings nach Meinung einiger Teilnehmer bei zahlreichen Systemadministratoren in Deutschland, vor allem von Unternehmensnetzen, anders als bei den großen TK-Anbietern nicht vorhanden sei. **Empfehlung:** Sensibilisierung der Betreiber von Unternehmensnetzen für das Thema sowie Vermittlung des notwendigen Umstellungs-Know-hows, z. B. durch Förderung eines übergreifenden Informationsaustauschs oder Veröffentlichung von Best-Practice-Beispielen. Förderung von Testbeds zur Überprüfung der sicheren Interoperabilität IPv6-fähiger Netzwerkkomponenten (insbesondere quelloffener Software für eingebettete Systeme), einschließlich Bereitstellung von Empfehlungen und entsprechender Zertifizierungen.

- Diese wachsende Komplexität und Fehleranfälligkeit der Netze ist vor allem Ergebnis des für einen Übergangszeitraum von – nach Teilnehmersicht – rd. 10 Jahren erforderlichen Parallelbetriebs beider Protokolle. Während dieser Übergangszeit ist auch

die Sicherheit der Netze durch neue Angriffsverfahren in erhöhtem Maße bedroht. **Zentrale Empfehlungen:** Systematische Sicherheitsuntersuchung von IPv6-Protokollstacks (vgl. BSI-Schwachstellenampel), Verbesserung der Informationsvermittlung über die Abwehr neuer IPv6-bezogener Angriffe.

→ Es steht zu erwarten, dass sich die Umstellung auf das neue Internetprotokoll für einen TK-Anbieter erst mittel- bis langfristig rentiert, da IPv6-basierte Netze deutlich wartungsärmer und weniger komplex sind als die bisherigen IPv4-Netze inklusive der teilweise notwendigen Hilfsmechanismen. Eine entsprechende Analyse ist stark einzelfallabhängig und insbesondere der Nutzen lässt sich nicht exakt beziffern; das macht eine Kosten-/Nutzenbewertung recht schwierig. Weitaus effizienter, als bestehende TK-Strukturen umzurüsten, ist es dagegen, neue TK-Infrastrukturen mit IPv6 neu aufzubauen. Dies könnte zu Kräfteverschiebungen im TK-Bereich, insbesondere mit Blick auf die Anbieter neuer Mobilfunknetze, führen.

C. Dienste-/Endgerätehersteller

→ Durch die enormen Adressräume von IPv6 wird es vor allem einen Schub für die weitere Entwicklung des „Internet der Dinge“ geben; betroffen hiervon sind nicht zuletzt auch die Hersteller „traditioneller“ Güter (z. B. „Weiße Ware“, Automobile), die sich für eine Einbindung in die „vernetzten Welten“ (z. B. „Smart Home“, Intelligente Transportsysteme) eignen. Die Zukunftsfähigkeit gerade dieser Hersteller hängt wesentlich davon ab, sich frühzeitig mit den Möglichkeiten von IPv6 auseinanderzusetzen. **Zentrale Empfehlungen:** Sensibilisierung der „traditionellen“, bislang oft „internetfernen“ Hersteller für die Thematik, einschließlich der Möglichkeit einer Einbindung ihrer Produkte in das „Internet der Dinge“.

→ Durch die direkte Adressierung bei IPv6 wird die unmittelbare Verwirklichung einer Geschäftsidee im Internet und damit die unternehmerische Existenzgründung erleichtert. Im Bereich „Smart Home“ und „Internet der Dinge“ ergeben sich ganz neue Anwendungs- und Geschäftsfelder in privaten oder sensiblen Bereichen. Erleichtert werden durch einen solchen Direktzugriff allerdings auch neue Angriffsformen und Missbräuche. **Zentrale Empfehlungen:** Schaffung von anerkannten „Standards“ und Zertifizierungen für den Zugriff durch vertrauenswürdige Diensteanbieter.

D. Datenschutz

→ Es ist bei IPv6 grundsätzlich möglich, eine dynamische Adresszuweisung vorzunehmen und dadurch Kollisionen mit dem Datenschutz zu vermeiden. Internet-Zugangsprovider sehen eine Neuvergabe einer IPv6-Adresse auf Kundenwunsch als „freiwilliges“ Angebot und erwarten hier durchaus Akzeptanzgewinne bei den Nutzern.

→ Für bestimmte Dienste (z. B. IP-Telefonie, insbesondere Notrufe) und das Angebot von eigenen Diensten ist die Unterbrechung durch eine dynamische Adresszuweisung allerdings kontraproduktiv, deshalb sollte der Verbraucher über die Art der Adressvergabe selbst entscheiden können. **Zentrale Empfehlung:** Entwicklung unterschiedlicher Datenschutzprofile für unterschiedliche Anwendungsszenarien durch TK-Anbieter und Datenschutzbeauftragte.

1. Einführung

Die letzten verfügbaren IPv4-Adressen sind von der Internet Assigned Numbers Authority (IANA) ausgegeben worden. Mit dem als Nachfolgeprotokoll zur Verfügung stehenden IPv6 kann das weitere Wachstum des Internets als weltweit wichtigstes Kommunikationsmedium gewährleistet werden. IPv6 wird in den nächsten Jahren schrittweise nach spezifischem Bedarf eingeführt. Um die Herausforderungen, die sich daraus ergeben, angemessen zu diskutieren, initiierte das Bundesministerium für Wirtschaft und Technologie (BMWi) einen Workshop zum Thema „Das Internetprotokoll Version 6 (IPv6) – Chancen und Herausforderungen für den Wirtschaftsstandort Deutschland“ am 26. Januar 2012 in Berlin. Dieser Bericht greift die diskutierten Themen und Thesen auf und bezieht sich zudem auf Positionen der Arbeitsgruppe 2, Sonderthemengruppe „Einführung von IPv6“ des Nationalen IT-Gipfels 2011 und des Deutschen IPv6-Rats. Zunächst werden „Spannungsfelder“, „Technologische“ und „Wirtschaftliche“ Themen erörtert und abschließend Handlungsempfehlungen formuliert.

Die Umstellung auf die neue Version des Internet-Protokolls (IPv6) wird sich tief greifend auf das Internet und die Kommunikationsnetze auswirken, insbesondere durch

- ein fast unerschöpfliches Reservoir zur Verfügung stehender Internet-Adressen,
- den Wegfall von bestimmten Infrastrukturkomponenten und Hilfsfunktionen, die bisher für den Einsatz von IPv4 unerlässlich waren,
- die Wiederherstellung des Ende-zu-Ende-Paradigmas in der Internetkommunikation,
- die Einführung von Funktionen zur automatischen Konfiguration von Netzkomponenten.

Mit der Nutzung von IPv6 wird erwartet, dass die Netze aufgrund der dargestellten Eigenschaften leistungsfähiger werden können und mit IPv6 eine verbesserte Basis für die Evolution des Internets und seiner Anwendungen bereitsteht. Bei der Entwicklung von IPv6 wurde allerdings ein Bruch mit IPv4 in Kauf genommen: Beide Protokolle sind nicht direkt interoperabel, lassen sich jedoch parallel betreiben. Dieser Umstand nimmt starken Einfluss auf die Einführung von IPv6 in bestehende Netze und Systeme. Weitere Ausführungen zu den technischen Eigenschaften von IPv6 finden sich im Abschnitt „3. Technik“.

Darüber hinaus eröffnet die technische Weiterentwicklung des Internets durch IPv6 ein enormes wirtschaftliches Potenzial. Von der Einführung werden vor allem Anwendungsfelder profitieren, die

- erheblichen Adressbedarf besitzen, wie etwa die Bereiche Logistik, Smart Home, Cloud Computing, Internet der Dinge/Internet der Services oder „Big Data”,
- auf einen unmittelbaren Zugang zum Internet angewiesen sind, wie Sensorik, Internet der Dinge, neue Netzzugänge sowie Anwendergruppen, wie etwa Gründer und Unternehmen mit neuen Geschäftsideen, neue Netz- oder Zugangsanbieter.

Darüber hinaus ergeben sich durch die IPv6-Einführung Verbesserungen in den Bereichen

- Netzdesign: Der große Adressraum und die direkte Adressierbarkeit ermöglichen den Netzaufbau entsprechend einer logischen Struktur, ohne zusätzliche Adressumsetzungen oder erzwungene Infrastrukturkomponenten zur Herstellung der Erreichbarkeit.
- Netzkonfiguration: Die automatische Konfiguration und vielfältige Adressierungsmöglichkeiten erlauben einen wirtschaftlichen Betrieb, bspw. von Sensornetzen.

Während auf der einen Seite Branchen und Unternehmen von der Umstellung profitieren werden, stehen auf der anderen Seite Geschäftsmodelle vor großen Anpassungen. Das betrifft Unternehmen, deren Produkte und Dienste auf der Nutzung von charakteristischen Funktionalitäten des IPv4-Standards basieren, aber auch Unternehmen, die ihre Produkte mit Kommunikationsfähigkeiten ausstatten.

Insgesamt stellt die Einführung des neuen Internetprotokolls gerade die deutsche Wirtschaftspolitik vor enorme Herausforderungen. Es gilt insbesondere sicherzustellen, dass

- die Anwender in Deutschland nicht von der Kommunikation mit IPv6-Netzen abgekoppelt werden und
- sich die Nutzung des neuen Internetprotokolls nicht ausschließlich auf die Herstellung von Interoperabilität beschränkt, sondern auch seine zusätzlichen Innovationspotenziale geprüft und eingesetzt werden.

Dabei muss vermieden werden, dass

- die Umstellung auf IPv6 in Deutschland durch die Nutzung von Hilfsmechanismen hinausgezögert wird. Eine unnötige Verlängerung der Übergangszeit bedeutet zusätzliche Risiken z. B. für die IT-Sicherheit aufgrund der erhöhten Komplexität.
- die Umstellung der IKT-Netze in Deutschland zwar auf den neuen Standard erfolgt, die neuen Dienste und Endgeräte aber ausschließlich von ausländischen Unternehmen angeboten werden.

Weitere Ausführungen zu den wirtschaftlichen Aspekten der IPv6-Einführung finden sich im Abschnitt „4. Wirtschaft“.

Auch wenn die Anforderungen an alle Beteiligten hoch sind, so hat doch der World IPv6 Day im Juni 2011 ein positives Bild vom Stand der IPv6-Einführung gezeichnet. An diesem Tag boten über 200 Anbieter ihre Dienste im Web neben IPv4 auch über IPv6 an, wobei die Webseiten über die gleiche symbolische Adresse (URL) verfügbar waren. Dieses sogenannte Dual-Stack-Verfahren ist ein wichtiger Mechanismus für die Migration, da Inhalte sowohl unter IPv4 als auch unter IPv6 zur Verfügung stehen und damit während der Migrationsphase von allen Nutzern des Internets abgerufen werden können. Im Bereich der Technik zeigte sich, dass es zu keinen nennenswerten Problemen bei der Nutzung von Dual-Stack-Angeboten kam, d. h. wenn IPv6-Nutzer diese Angebote nutzten, dann verfügten sie in der Regel über eine ausreichend moderne Version eines Betriebssystems und die Internet-Zugänge waren korrekt konfiguriert.

2. Spannungsfelder von IPv6

Die IPv6-Einführung in Deutschland erzeugt eine Reihe von Spannungsfeldern, die im Folgenden beschrieben werden.

2.1 Kurzfristige Kosten vs. langfristige Ertragschancen

Die weltweite Einführung von IPv6 hat begonnen. Es werden Erfahrungen und „Best Practices“ gesammelt, wie Netze am besten konfiguriert oder wie Protokollmechanismen am besten genutzt werden können. Dabei ist zu erwarten, dass die Migration zu IPv6 für einzelne Akteure, insbesondere die TK-Infrastrukturanbieter, kurzfristig zum Teil erhebliche Kosten verursachen kann. Zudem kann es zu Sicherheitsproblemen kommen. Ein Grund liegt insbesondere im Parallelbetrieb bestehender und neuer Infrastrukturen, der in der Migrationsphase nötig ist, um eine durchgehende Erreichbarkeit von Diensten und Geräten zu garantieren. Andererseits werden sich durch die Umstellung mittelfristig Kostenvorteile ergeben, da IPv6-Netze weniger komplex und dadurch leistungsfähiger sowie wartungsärmer sind.

2.2 Umstellungserfordernis vs. Umstellungsrisiken

Auch wenn die Notwendigkeit einer Umstellung der IKT-Netze auf das Nachfolgeprotokoll grundsätzlich nicht hinterfragt wird, bedarf diese Umstellung sorgfältiger Planung und Durchführung. Falsche Planungen können zum Ausfall von Teilnetzen führen. Wichtig ist, den richtigen Zeitpunkt für die Migration zu finden, da nur dann der Aufwand für die Einführung von IPv6 minimiert werden kann. Mit der Planung sollte möglichst früh begonnen werden, um Erfahrungen zu gewinnen und fundierte Entscheidungen für das weitere Vorgehen zu treffen. Die Migration muss sich auch an der Dynamik des Internet-Wachstums orientieren. So ist es empfehlenswert, dass Unternehmen bereits jetzt einen strukturierten IPv6-Adressplan aufbauen, der skalierbar ist und eine mögliche Umorganisation berücksichtigt.

2.3 Investition vs. Gewinnchancen

Bei der strategischen Betrachtung der IPv6-Migration muss dem Umstand Rechnung getragen werden, dass der Aufwand im Allgemeinen für die Kunden nicht direkt sichtbar ist und damit keinen unmittelbaren Vorteil für den Anbieter bringt. Andererseits müssen Anbieter ihre Produkte auf IPv6 umstellen, um wettbewerbsfähig zu bleiben. Einige Marktakteure wie etwa TK-Zugangsanbieter werden für die Umstellung ihrer Netze auf IPv6 erhebliche Investitionen tätigen müssen. Gleichzeitig schätzen sie die mit der Umstellung verbundenen unmittelbaren Gewinnchancen als gering ein.

Deutlich optimistischer werden diese Chancen hingegen von einzelnen Produzenten von Endgeräten bzw. den Entwicklern von IPv6-fähigen Diensten eingeschätzt, die jedoch weniger in die Umstellung ihrer Produkte/Dienste investieren müssen. Einzelne Anbieter von Endgeräten oder Diensten können über neue IPv6-Funktionen ihre Produkte für den Kunden sichtbar verbessern.

Auch eine umgekehrte Sichtweise gilt: Kommt es zu Fehlern bei Endgeräten oder im Netzzugang, wird der Kunde seinen Dienstanbieter im Internet dafür verantwortlich machen, obwohl dieser auf die Konfiguration am Endgerät des Kunden nur wenig Einfluss hat.

2.4 Parallelbetrieb vs. Komplettumstellung

Geht es einem Infrastrukturbetreiber nur darum, die Interoperabilität seiner IPv4-Netze zu IPv6-Netzen herzustellen, käme grundsätzlich der technisch mögliche Parallelbetrieb beider Protokolle oder Protokollumsetzung in Frage. Davon abgesehen werden sich manche Netze oder Dienste, unter wirtschaftlichen Gesichtspunkten betrachtet, nicht umstellen lassen bzw. wird es für einen längeren Übergangszeitraum einen Parallelbetrieb geben müssen. Zudem kann es zu erhöhten Betriebskosten sowie Sicherheitsproblemen kommen. Wichtig ist eine sorgfältige Planung, denn während zu Beginn der Aufwand durch das neu einzuführende IPv6-Protokoll entsteht, entwickelt sich gegen Ende der Migration der Weiterbetrieb des IPv4-Protokolls zu einer Altlast. Zu Beginn der Migration liegt der Schwerpunkt auf der Erreichbarkeit bestehender

Dienste auch über IPv6, am Ende geht es um die Relevanz verbliebener IPv4-Nutzer oder Dienste. Somit gibt es neben der individuellen Bestimmung des Zeitpunkts in den Einstieg der Migration auch den Bedarf an einer spezifischen Exit-Strategie, die verhindert, dass Doppelinfrastrukturen unnötig lange betrieben werden, mit allen Konsequenzen für die Leistungsfähigkeit und Sicherheit von Infrastrukturen und Produkten. Einen technischen und wirtschaftlichen Vorteil bieten hier neu aufgebaute Infrastrukturen, bei denen ein aufwendiger Parallelbetrieb nicht erforderlich ist und die unmittelbar mit IPv6 in Betrieb genommen werden können.

2.5 Datenschutz und Sicherheit

Auch bei der Nutzung von IPv6 muss zwischen unterschiedlichen Einsatz- und Nutzungsszenarien unterschieden werden (Unternehmenskommunikation, privater Internet-Anschluss, interne oder externe Teilnetze, Internet der Dinge und Sensornetze, Nutzung von Diensten und sozialen Netzwerken usw.). Für diese verschiedenen Szenarien gelten ganz unterschiedliche Anforderungen aus Sicht des Datenschutzes und der Sicherheit.

IPv6 bietet eine Chance, den Datenschutz gegenüber IPv4 zu verbessern. Zum Datenschutz sind bei IPv6 keine generellen Regelungen angedacht und ebenso nicht sinnvoll, da die Spannbreite des Einsatzes in den verschiedenen Szenarien sehr groß ist. Gute Ansätze für Endanwender sind Privacy Extensions für multifunktionale Geräte und eine Präfix-Kaskadierung in den Zugangsnetzen.

Zunächst ist wegen des erhöhten Aufwands beim Betrieb der Netze (IPv4 und IPv6) und neuer Implementierungen (IPv6) mit einem geringeren Sicherheitsniveau zu rechnen. Des Weiteren gibt es aufgrund des neuen Protokolldesigns neue Schwachstellen, deren Relevanz sich erst im Laufe der Zeit bei entsprechender Verbreitung des Nachfolgeprotokolls zeigen wird.

Für die Sicherheit und den Datenschutz ist es erforderlich, dass die Nutzer die technischen Möglichkeiten kennen und sie angemessen und bedacht einsetzen. Das neue Protokoll kann Netze verbessern – aber das geschieht eben nicht zwangsläufig.

2.6 Ende-zu-Ende-Kommunikation als Chance

IPv6 ermöglicht direkte Ende-zu-Ende-Kommunikation für die Nutzung neuer Anwendungen und Dienste und kann zur Absicherung der Kommunikation beitragen, d. h. vertrauliche und sensible Informationen können direkt zwischen Sender und Empfänger ausgetauscht werden, ohne dass es einer weiteren Instanz bedarf. Diesem positiven Einfluss durch die IPv6-Einführung stehen Bedenken in Bezug auf Datenschutz und Sicherheit gegenüber. Grundsätzlich ist mit der Entwicklung von IPv6 keine wesentliche Änderung im Kommunikationsmodell des Internets gegeben.

Beim Datenschutz hat man heute ein anderes Bewusstsein als zu Beginn der Nutzung des Internets. Zudem sind für die nachhaltige Entwicklung von neuen Geschäftsmodellen die Akzeptanz und das Vertrauen der Kunden sehr wichtig. Es gilt daher, die Möglichkeiten von IPv6 im Sinne des Datenschutzes einzusetzen.

Auch unter IPv6 muss es weiterhin interne Netze geben, die nicht aus dem Internet erreicht werden können. Über verschiedene Adressbereiche und durch die Nutzung von verschiedenen Adresstypen lassen sich bei IPv6 die Kommunikationsanforderungen für einzelne Teilnetze abbilden.

Im Workshop wurde die Wiederherstellung der Ende-zu-Ende-Kommunikation als eine sehr wichtige Eigenschaft von IPv6 dargestellt, die eine vielfältige Kommunikation zwischen neuen Endgeräten und Diensten sowie neue Geschäftsmodelle erlaubt. Die dabei auftretenden Fragen des Datenschutzes und der Sicherheit lassen sich lösen, insbesondere da diese Themen bei der Entwicklung von IPv6 berücksichtigt wurden.

3. Technik

3.1 Die Rolle des Internetprotokolls Version 6 für die weltweiten IKT-Netze

Das Internetprotokoll ist von zentraler Bedeutung für die Struktur und Funktionsfähigkeit von Kommunikationsnetzen. Es wird in verschiedenen physikalischen Netzstrukturen genutzt. Auf ihm bauen wiederum weitere Protokolle auf, die eine Vielzahl von Diensten unterstützen. Die IP-Kommunikation kommt sowohl in drahtgebundenen und drahtlosen Netzen als auch in Backbone-Netzen mit hohen und in Sensornetzen mit niedrigen Bandbreiten zum Einsatz. Das Internetprotokoll unterstützt alle Arten von Diensten – von klassischer Rechner-zu-Rechner-Datenübertragung bis hin zur Multimedia-Kommunikation zwischen Smartphones. Damit hat es sich im Laufe der Jahre zu einer übergreifenden Konvergenzschicht der Kommunikation entwickelt. Seine Hauptfunktion ist die Schaffung einer Schnittstelle zwischen einer großen Zahl von Geräten und Diensten, die auf diese Weise miteinander kommunizieren können. Das neue Internetprotokoll IPv6 setzt diese Entwicklung fort, baut die Leistungsfähigkeit des alten Protokolls aus und unterstützt die Entwicklung neuer Dienste und Anwendungen.

Die Weiterentwicklungen beim Internetprotokoll Version 6 werden insbesondere deutlich

- im stark vergrößerten Adressraum und in der Nutzung von eindeutigen, direkt erreichbaren Adressen,
- im effizienteren Aufbau des Protokolls zur vereinfachten Verarbeitung,
- in der Erweiterung von Funktionen zur Autokonfiguration von Netzen und Endgeräten,
- in der Unterstützung von Sicherheitsprotokollen und Dienstqualität.

3.1.1 Die Vergrößerung des Adressraumes

Die stark wachsende Zahl von Internetnutzern weltweit hat dazu geführt, dass der mit IPv4 mögliche Adressraum heute fast ausgeschöpft ist und keine freien Adressen mehr für weitere Nutzer und Dienste zur Verfügung stehen. Geräte und Nutzer müssen heute oft auf eine eindeutige, einmalige Adresse verzichten. Stattdessen werden in einem hohen Maß IPv4-Adressen geteilt. Um dies zu ermöglichen, wird auf Hilfsmechanismen des „alten“ Protokolls zurückgegriffen, die allerdings die Kommunikation erschweren und damit das Wachstum des Internets und seiner Dienste bremsen. So lassen sich beispielsweise Endsysteme in Heimnetzen nicht direkt ansprechen. Ein Zugriff von außerhalb ist nur über Zusatzdienste im Internet und durch zusätzliche Konfigurationen am DSL-Router möglich.

Eine der wichtigsten Fortentwicklungen des neuen Internetprotokolls besteht darin, dass die mit ihm geschaffenen Adressräume fast unerschöpflich sind. Ein Beispiel: Verfügt ein Privatkunde über IPv4 über DSL, so muss eine öffentliche Adresse von verschiedenen Endgeräten eines Haushalts (PCs, Spielekonsolen, Fernseher oder Smartphones über WLAN) gemeinsam genutzt werden. Bei IPv6 kann dieser Privatkunde dagegen über einen Adressbereich verfügen, und es steht ihm in einem einzigen Netz das Vielfache an Adressen im Vergleich zu IPv4 zur Verfügung. So ermöglicht IPv6, alle bestehenden und künftigen Kommunikationsbeziehungen zwischen Endgeräten, Nutzern, Diensten oder Gegenständen abzudecken.

Der große Adressraum von IPv6 erlaubt zudem eine strukturierte Adressplanung bzw. Adressvergabe im Internet, so dass das Wachstum der Routing-Tabellen in Grenzen gehalten werden kann. Die Routing-Tabellen sind ein Teil der Kernrouter des Internets und stellen die weltweite Erreichbarkeit von Teilnetzen des Internets sicher.

3.1.2 Die Wiederherstellung des Ende-zu-Ende-Paradigmas

Eine weitere und tief greifende Fortentwicklung des Internetprotokolls besteht in der Wiederherstellung des sogenannten „Ende-zu-Ende Paradigmas“. Darunter versteht man ein Design-Prinzip, bei dem die anwendungsspezifischen Funktionen nur in den Endsystemen angesiedelt sind und nicht in den Netzknoten auf dem Übertragungsweg. Idealerweise erhält man durch die Anwendung dieses Prinzips ein einfaches, zustandsloses „Universalnetz“, wobei die Steuerung der Kommunikation weitgehend in die Endsysteme verlagert ist. Zwar basierte das Internet ursprünglich

auf diesem Grundprinzip, allerdings konnte es aufgrund der Adressknappheit bei IPv4 nicht überall aufrechterhalten werden.

Da ein solches Netz vergleichsweise wenig Funktionalität erbringen muss, wird eine Kopplung von Netzen und Geräten oder die Nutzung von Diensten mit minimalen gemeinsamen Eigenschaften möglich. Daher spricht man beim Internet auch von einer Konvergenzschicht der Kommunikation. Zudem kann ein Netz nach diesem Prinzip sehr stark wachsen, ohne durch eine Überlast an Steuerungs-Aufgaben beeinträchtigt zu werden oder gar zu kollabieren.

Mithilfe des Ende-zu-Ende-Paradigmas lassen sich neue Funktionen und Dienste einfacher einführen, da das Netz keine anwendungsspezifischen Unterstützungsfunktionen bieten muss. So können Änderungen in einer Auswahl von Endsystemen genutzt werden, ohne dass die komplette Netzinfrastruktur in seiner Funktionalität erweitert werden muss. Das erhöht die Flexibilität und Schnelligkeit, mit denen Unternehmen auf Markttrends reagieren können. Somit können neue Funktionen auch auf spontane Nachfrage bei Nutzern treffen.

Die Einführung von IPv6 bietet die Möglichkeit zur Wiederherstellung des Ende-zu-Ende-Paradigmas und zur Nutzung der Erweiterungsmöglichkeiten, die das Protokoll selbst zur Verfügung stellt (z. B. Extension Header). Innovationen und Wertschöpfung finden mit IPv6 in den Diensten und Endgeräten statt, die sich im Wettbewerb über Designmerkmale differenzieren und weniger über eine nur langsam veränderbare Infrastruktur.

IPv6 erlaubt die direkte Kommunikation von Endsystemen, ohne zentrale Infrastrukturen zu benötigen, und eröffnet so die Chance für eine Weiterentwicklung von Geräten und Anwendungen. Gleichzeitig sinkt die Eintrittsschwelle für Unternehmen in den Markt. Der Hintergrund: Selbst einfache Anwendungen brauchen bei IPv6 für die Kommunikation keine Unterstützung mehr durch Infrastruktur-Server im Internet, stattdessen werden Daten direkt ausgetauscht. So wird die Entwicklung von innovativen Internet-Produkten und -Diensten auch für IKT-fremde Bereiche interessant. Zudem kann die direkte Sichtbarkeit der Kommunikationsteilnehmer ohne Network Address Translation (NAT) die Sicherheit und das Vertrauen in neue Dienste stärken.

3.1.3 Reduzierung von Komplexität der Netze und Infrastrukturen

Durch den Einsatz von IPv6 ergeben sich Vorteile bei der Konfiguration und dem Betrieb von Netzen. Aufgrund des ausreichend großen und gut strukturierbaren Adressraums lassen sich einfache und transparente Netzarchitekturen realisieren. Unter IPv6 stellt das Netz Mechanismen zur Autokonfiguration von Endgeräten und den Netzkomponenten selbst bereit. Dies ermöglicht den Aufbau von großen und flexiblen Infrastrukturen, beispielsweise im Bereich der Sensornetze. Auch die Zusammenlegung von Netzen, etwa nach Firmen-Fusionen oder anderen organisatorischen Maßnahmen, wird mit IPv6 vereinfacht. Eine solche ist bisher unter IPv4 aufwendig und fehleranfällig. Die übliche Verwendung gleicher, privater IPv4-Adressen in verschiedenen Netzen führt dazu, dass diese Netze umnummeriert oder per Adressumsetzung gekoppelt werden müssen.

3.1.4 Autokonfiguration von Endgeräten und Netzkomponenten

Bei der Entwicklung von IPv6 wurden von vornherein viele Funktionen berücksichtigt, die für den Betrieb von großen Infrastrukturen benötigt werden. Dazu gehören Funktionen zur automatischen Konfiguration von Endgeräten und Netzkomponenten, die helfen, den Administrationsaufwand zu verringern. In einigen Anwendungsbereichen, beispielsweise bei Sensornetzen, sind solche Funktionen notwendig, wenn kein menschlicher Eingriff vorgesehen ist. Mittels automatischer Konfiguration verringert sich die Gefahr der Fehlkonfiguration, was sich positiv auf die Leistungsfähigkeit und Sicherheit der Netze auswirkt. Die im Protokolldesign von vornherein enthaltenen Funktionen zur Autokonfiguration helfen, die Netzkonfiguration zu vereinfachen, und tragen damit zur Verringerung der Komplexität der Netze bei.

3.1.5 Weiterentwicklung offener Standards

IPv6 basiert auf offenen Standards, festgelegt in sogenannten RFC (Request for Comments), die für Interessierte frei verfügbar sind. Der Standardisierungsprozess findet unter dem Dach der Internet Society bzw. deren Gremium IETF (Internet Engineering Task Force) in Arbeitsgruppen statt. Typischerweise werden im Standardisierungsprozess experimentelle Implementierungen von neuen Funktionen oder Protokollen von Experten aus Firmen und Forschungseinrichtungen öffentlich vorgestellt, diskutiert und mit ähnlichen Ansätzen abgestimmt.

Durch dieses Vorgehen finden einerseits Ideen aus der Wissenschaft schnell den Weg in die Standardisierung, andererseits können oft schon die ersten Entwürfe eines Standards für eigene Produktideen oder Weiterentwicklungen von Geräten und Diensten genutzt werden. Damit werden nach überwiegender Expertensicht proprietäre Kommunikationsprotokolle und -mechanismen aus dem IPv4-Umfeld an Bedeutung verlieren.

3.2 Herausforderung Interoperabilität beim Übergang von IPv4 zu IPv6

Während der Aufbau neuer Kommunikationsnetze unmittelbar mit dem neuen Internetprotokoll IPv6 erfolgen kann, sollte bei bestehenden IPv4-Netzen die Migration auf IPv6 dem Umstand Rechnung tragen, dass für eine Übergangszeit viele Geräte und Anwendungen IPv4 weiter nutzen. Der Hintergrund: Bei der Entwicklung von IPv6 wurde zwar auf Erfahrungen mit IPv4 zurückgegriffen, jedoch keine direkte Interoperabilität zwischen IPv4 und IPv6 vorgesehen. In der Theorie fällt diese Designentscheidung im Vergleich zu den sich bietenden Möglichkeiten nicht allzu sehr ins Gewicht, da eine abgegrenzte Protokollschicht gegen eine andere ausgetauscht wird. In der Praxis ist diese klare Trennung der Protokollschichten nicht immer gegeben, beispielsweise werden auf höheren Protokollschichten Annahmen über Eigenschaften und Bedingungen niedrigerer Protokollschichten getroffen, die dann im Fall von IPv6 nicht mehr zutreffen. Die direkte Kommunikation zwischen einem IPv4- und einem IPv6-Gerät ist nicht möglich, da beide Protokolle nicht interoperabel sind. Diese Inkompatibilität führt zur Notwendigkeit einer planvollen, technischen Migration. Dabei sollen das neue, leistungsfähigere IPv6-Protokoll eingeführt und gleichzeitig bestehende Netze und Dienste zumindest für einen Übergangszeitraum weiter genutzt werden können.

Dazu sind mit der Entwicklung von IPv6 eine Reihe von Migrationstechnologien oder Transitionsmechanismen geschaffen worden. Jeder Ansatz hat allerdings spezielle Vor- und Nachteile, daher kommt es bei der Anwendung von Übergangstechniken (wie Dual-Stack, Protokollumsetzung u. a.) auf den Einzelfall an. Eine generelle Lösung für die Migration zu IPv6, die alle Anwendungsfälle umfasst, kann es nicht geben. Dabei ist zu beachten, dass Fehler bei der Migration und eine fehlende Interoperabilität von Netzen dazu führen können, dass Dienste oder Netzbereiche nicht mehr erreichbar sind. Um ein solches Szenario von vornherein auszuschließen, sollten vorhandene IKT-Infrastrukturen, wie sie in Deutschland weit verbreitet sind, planvoll und schrittweise von IPv4 zu IPv6 migriert werden. Fragen der Interoperabilität zu IPv4 sollten berücksichtigt, jedoch Investitionen in Entwicklungen auf Basis des alten Protokolls vermieden werden.

Grundsätzlich werden bei der IPv6-Migration die Bereiche Endgeräte und Dienste sowie Netze und Infrastrukturen unterschieden. Im Bereich Endgeräte und Dienste ist die Migration zu IPv6 von zentraler Bedeutung für die Nutzung und Akzeptanz von IPv6. Anwender erwarten einen funktionierenden, unkomplizierten Internetzugang zur Nutzung von Diensten. Das verwendete Netzwerkprotokoll spielt für sie hier keine Rolle. Während der Migrationsphase werden sowohl IPv4- als auch IPv6-basierte Dienste nachgefragt werden. Der naheliegende Weg, dies zu realisieren, liegt in der Nutzung des Dual-Stack-Verfahrens. In dieser Betriebsart ist das Gerät in der Lage, beide Protokollversionen zu verwenden. Der World IPv6 Day im Juni 2011, aber auch die Tests einzelner Anbieter, haben gezeigt, dass die verbreiteten Betriebssysteme den Dual-Stack-Betrieb unterstützen und dieses Verfahren weitgehend ohne Probleme möglich ist.

Die passende Migrationsstrategie für das Dienstangebot hängt von der Nutzungsart ab:

- Neue, in sich geschlossene Dienste können direkt für den IPv6-only-Einsatz konzipiert werden (und ein Übergang zu IPv4 wäre die Ausnahme).
- Populäre Dienste müssen sowohl über IPv4 als auch IPv6 angeboten werden.
- Spezielle Dienste und Fachanwendungen werden sich nicht wirtschaftlich migrieren lassen. Hier wird man bis zum Ende der Lebensdauer auf individuelle Migrationsverfahren wie Protokollumsetzung oder Emulation/Virtualisierung ausweichen müssen.

Die IPv6-Nutzung im Bereich Endgeräte und Dienste hängt stark vom Einsatzbereich ab. Neue Dienste, wie IP-Telefonie in Firmennetzen, wird man von vornherein ausschließlich auf IPv6 aufsetzen. Wird für den Einsatzbereich ein ausreichender Netzzugang zu IPv6 angeboten, so spart man sich bei klar abgegrenzten, neuen Diensten den komplexen Parallelbetrieb von IPv4 und IPv6. Weit verbreitete Dienste müssen sowohl über IPv6 und IPv4 angeboten werden, damit eine möglichst große Anzahl von Nutzern auf diese zugreifen können. Auch hier bietet sich der Dual-Stack-Betrieb an, wobei z. B. bei Diensteanbietern die Produktions- und Redaktionsumgebung durchaus in verschiedenen Stufen des Migrationsplans migriert werden können.

Auch ohne IPv6 in einer Infrastruktur vollständig umgesetzt zu haben, können Geräte und Dienste erreicht werden. Dies lässt sich über eine vorgeschaltete Protokollumsetzung von IPv6 auf die bestehende IPv4-Server-Infrastruktur erreichen. Dieser Weg wird in vielen Unternehmen gewählt, da er in einem frühen Migrationsstadium mit wenig Aufwand einen Zugang über IPv6 anbietet. Es können somit erste Erfahrungen mit IPv6 gesammelt und die Entwicklung der Nachfrage von Kunden über die Zeit beobachtet werden.

Dieser Ansatz birgt jedoch auch Gefahren. Es besteht die Möglichkeit, dass ein IPv6-basiertes Netzdesign zu spät in Angriff genommen wird. Bei einem sprunghaften Anstieg der IPv6-Nachfrage reicht die Kapazität dieses Hilfsmechanismus für die Migration nicht mehr aus.

Darüber hinaus wird der Dual-Stack-Betrieb das Adressproblem nicht lösen können, da keine IPv4-Adressen gespart werden, diese werden ggf. weiter benutzt.

Welche dieser Techniken davon genutzt werden, hängt stark von der Aufstellung des Zugangsanbieters ab, z. B. wie viele IPv4-Adressen ihm zur Verfügung stehen und wie diese von den Kunden genutzt werden, welcher Zeitraum/Aufwand für die Migrationsphase erwartet wird.

Auch bei der Migration von Netzen kommen je nach Nutzung und Netzarchitektur verschiedene Migrationsverfahren in Frage, wie sie schon bei den Endgeräten und Diensten angesprochen sind. Mithilfe der Migrationsplanung wird vor allem die Abfolge der Migrationsschritte festgelegt. In der Praxis wird es eine Teilmigration von einzelnen Netzbereichen geben. Das hat Konsequenzen für das notwendige Wissen zum Netzbetrieb und für die Sicherheit, da sich die Techniker in beiden Welten auskennen müssen.

3.3 Einfluss von IPv6 auf die IKT-Sicherheit

Das IPv6-Design verändert nachhaltig die Netz-Architekturen. Dies hat Auswirkungen auf die Sicherheitskonzepte, die heute noch nicht abschließend einzuschätzen sind. Sicherheit ist ein dynamischer Prozess, bei dem sich Best Practices für IKT-Sicherheit im Laufe der Zeit entwickeln. Ursprünglich waren das Internet und die Protokolle für eine hohe Ausfallsicherheit gegenüber externen Störungen bei der Datenübertragung ausgelegt. Andere Angriffsszenarien hat man zu diesem Zeitpunkt für ein Wissenschaftsnetz nicht betrachtet. Mit der Kommerzialisierung des Internets sind Sicherheitsfunktionen auf anderen Protokollschichten ergänzt worden, wie die TLS/SSL-Verschlüsselungen für Webbrowser. Die Entwickler von IPv6 haben von vornherein Sicherheitsaspekte beim Entwurf des neuen Internetprotokolls berücksichtigt.

Positive Auswirkungen auf die Sicherheit beim Einsatz von IPv6:

- einfacher, transparenter Netzaufbau zur Vermeidung von komplexen Filter- und Zugriffsregeln und Fehlkonfigurationen,

- möglicher Verzicht auf externe Hilfsmechanismen/ Dienste, die zur Mangelverwaltung bei IPv4 notwendig sind, dabei aber mit einem Verlust von Kontrolle einhergehen.

IPv6 muss sich erst im breiten Einsatz bewähren. So bieten beispielsweise die Funktionen zur Autokonfiguration potenzielle Einfallstore für neuartige Angriffe.

Vor allem das Ende-zu-Ende-Paradigma hat einen großen Einfluss auf die Sicherheit. Es erlaubt beispielsweise den Aufbau von Ende-zu-Ende-verschlüsselter Kommunikation und die Authentisierung eines Absenders auf der Netzwerkebene. Allerdings sind dadurch die Endgeräte potenziell direkt aus dem Internet erreichbar und damit angreifbar. Folglich verstärkt sich ein Trend, der auch in anderen Einsatzszenarien erkennbar ist: Der Schutz der Kommunikation verlagert sich vom Netz zum Endsystem.

Diese Verlagerung ist nicht neu und nicht nur im Einsatz von IPv6 begründet, sondern schon durch den notwendigen Schutz auf Anwendungsebene (Malware-Scanner) und den Einsatz von mobilen Geräten in wechselnden Netzumgebungen eingeleitet worden. Sich in Bezug auf Sicherheit ausschließlich auf die Schutzmaßnahmen am Endgerät zu verlassen, ist kritisch zu sehen, da aktuelle Entwicklungen darauf hindeuten, dass viele Endsysteme nicht über die nötigen Schutzmaßnahmen verfügen. Daher wird an vielen Stellen weiterhin eine mehrstufige Sicherheitsarchitektur erforderlich sein, um Angriffen zu begegnen.

Allerdings zeigen aktuelle Entwicklungen auch, dass immer mehr mobile Geräte über wechselnde Zugangsnetze mit dem Internet verbunden sind und dabei über eigene Schutzmechanismen verfügen müssen bzw. eine gesicherte Verbindung (VPN) zu einer sicheren Infrastruktur benötigen. Für Sensornetze und Entwicklungen des Internet der Dinge besteht die Herausforderung darin, einen sicheren Betrieb auch über einen längeren Zeitraum zu gewährleisten, wobei der administrative Zugriff beispielsweise für Sicherheitsupdates aufwendig sein kann.

Sicherheitskomponenten im Netz sind also weiterhin erforderlich, beispielsweise Paketfilter und Application-Layer-Gateways. In vielen Netzen ist keine direkte Verbindung aus dem Internet zu einem Endgerät möglich. In größeren Institutionen wird dieser Bruch beispielsweise zwischen den Arbeitsplätzen und externen Diensten in der Regel bewusst durch ein Application-Layer-Gateway am Internetübergang herbeigeführt. Eine direkte Verbindung zwischen Endgeräten (Ende-zu-Ende) umginge diesen gewollten Schutz und die Sicherheit würde um eine wesentliche Ebene reduziert. Der große Adressraum, der ein planvolles Vorgehen bei der Strukturierung von (Firmen-)Netzen nach Sicherheitszonen besser als bei IPv4 unterstützt, trägt wesentlich zum transparenten Netzaufbau bei, was sich in einfacheren Zugriffs- und Filterregeln niederschlagen wird.

Aufgrund der neuen IPv6-Nutzungsmöglichkeiten werden in Haushalten vermehrt Geräte und Sensoren mit dem Internet verbunden sein. Fehlkonfigurationen und unsichere Kommunikationsbeziehungen müssen dabei vermieden werden. Dazu muss die sichere Konfiguration der normale Betriebszustand sein, auf den sich der Benutzer beim typischen Einsatz verlassen kann (security by default).

Die Übergangsphase ist in Bezug auf die Sicherheit kritisch, da

- potenziell mit IPv4 und IPv6 zwei Netze parallel betrieben werden, die jeweils spezielle Eigenschaften besitzen,
- Erfahrungen mit IPv6 erst aufgebaut werden müssen,
- neue IPv6-spezifische Angriffsmethoden entwickelt werden,
- IPv6-Komponenten insgesamt unreifere Produkte darstellen, die noch ungewohnt viele Schwachstellen enthalten können.

Derzeit können viele Firmen, gerade aus dem erweiterten Umfeld der neuen Geräte im Internet, nur mit großem Aufwand abschätzen, welchen Reifegrad die erhältlichen IPv6-Protokollstacks und Netzkomponenten haben. Hier könnten Projekte durchgeführt werden, um diese Fragen zu untersuchen (vgl. Schwachstellenampel des BSI), oder Informationen über Sicherheitsaspekte beim Einsatz von IPv6 bereitgestellt werden (vgl. ISi-LANA-Reihe des BSI).

4. Wirtschaft

Die Umstellung auf das neue Internetprotokoll IPv6 ist weltweit in vollem Gange. Allerdings ist sie nicht in allen Regionen der Welt gleichermaßen vorangeschritten. Im asiatisch-pazifischen Raum ist der Druck zur Einführung von IPv6 wesentlich höher, da der Pool der freien IPv4-Adressen bei der asiatischen Vergabestelle APNIC seit April 2011 vollständig ausgeschöpft ist. Europa muss aufpassen, mit den wirtschaftlichen Entwicklungen in Asien Schritt zu halten.

4.1 Situation in Deutschland

Die Situation in Deutschland wird durch vielfältige Einflussfaktoren und unterschiedliche Interessenlagen der mit dem Internet und seinen Anwendungen befassten Akteure geprägt. Diese lassen sich in zwei Hauptgruppen zusammenfassen:

- IKT-Infrastruktur- und Zugangsanbieter,
- Endgerätehersteller und Diensteanbieter für Internetanwendungen.

Zwar haben die großen TK-Infrastrukturanbieter und Zugangsanbieter begonnen, ihre internen Strukturen für die Datenübertragung, die sogenannten Backbones, auf das neue Internetprotokoll umzustellen. Bei Herstellern von Endgeräten hingegen ist das Bild heterogen. Viele IT-Produkte wie PCs und mobile Geräte unterstützen vermehrt IPv6, während internet-fähige Systeme aus anderen Branchen heute oft noch nicht für das neue Internetprotokoll ausgelegt sind. Viele Anbieter von Diensten und Endgeräten sind anscheinend noch nicht so weit – obwohl gerade diese Gruppe von der neuen Entwicklung profitieren könnte. Dabei sind die Interessen von Endgeräteherstellern und Diensteanbietern für Internetanwendungen ähnlich. Beide betreiben auf einer fremden Netzinfrastruktur Geschäfte („Over the Top“) und ihre Geschäftsmodelle setzen eine leistungsfähige Infrastruktur voraus:

- Endgerätehersteller und Diensteanbieter profitieren mit neuen, IPv6-basierten Anwendungen (Wertschöpfung), ohne in die Netzinfrastruktur zu investieren.
- Sie haben potenziell ein hohes Return-on-Investment (RoI) für IPv6-basierte Dienste, da dem Erlös keine Investitionen in den Aufbau IPv6-fähiger Netze gegenüberstehen.

Endgerätehersteller müssen für die Umstellung auf IPv6 in der Produktion von Geräten den Protokoll-Stack ersetzen oder ergänzen. Diensteanbieter müssen die in den Standard-Betriebssystemen vorhandene Unterstützung von IPv6 freischalten sowie ihre internen Netze entsprechend konfigurieren.

Unternehmen können den für sie geeigneten Migrationspfad unter Kosten-Nutzen-Abwägung auswählen. So bietet es sich an, die IPv6-Umrüstung auf geplante Innovationszyklen des Unternehmens abzustimmen. Allerdings gibt es in den Branchen und Produktgruppen unterschiedliche Entwicklungszyklen, weshalb die Migration sich über einen längeren Zeitraum erstreckt und in der Praxis – wie im Technik-Kapitel erläutert – Systeme sowohl mit IPv4 als auch mit IPv6 funktionieren sollten (Dual-Stack). Die Herausforderung für Unternehmen ist, einen geeigneten Zeitpunkt für den Einstieg in IPv6 und den Ausstieg aus IPv4 zu wählen. Dabei sollte man die Dynamik der Entwicklung nicht unterschätzen: Je mehr das neue Internetprotokoll und die Dienste nachgefragt werden, desto stärker erhöht sich der Druck auf die Unternehmen.

Die Netze müssen auf einen längeren Parallelbetrieb beider Internetprotokoll-Versionen ausgelegt sein. Doch die Netze gehören den TK-Infrastruktur- und Zugangsanbietern. Während diese auf ihrem lokalen Markt in IPv6-fähige Netze investieren müssen, profitieren Hersteller und Diensteanbieter aus der gesamten Welt von den geschaffenen Möglichkeiten. Für die Infrastrukturanbieter ist die Migration auf IPv6 komplex und kostspielig, den Aufwänden stehen in der Regel keine unmittelbaren Ertragsaussichten gegenüber. Auf mittlere Sicht lassen sich durch eine vereinfachte Netzarchitektur (vergleiche Technik-Kapitel) Einsparungen erreichen. Allerdings steht dem ein erhöhter Aufwand während der Übergangsphase mit einem Parallelbetrieb beider Protokolle gegenüber:

- Für TK-Infrastruktur- und Zugangsanbieter ist die Umstellung auf IPv6 mit hohen Investitionen verbunden.
- Sie haben voraussichtlich ein niedriges Return-on-Investment (RoI) für den Aufbau IPv6-fähiger

Infrastrukturen, da momentan nur geringe Perspektiven für Erlöse den hohen Investitionen gegenüberstehen.

→ Neue TK-Infrastruktur- und Zugangsanbieter haben unter Umständen einen Wettbewerbsvorteil gegenüber etablierten Betreibern, da der Aufbau neuer IPv6-Netze effizienter als die Migration bestehender IPv4-Netze ist.

Diese Konstellation könnte den Konflikt zwischen den großen TK-Infrastrukturanbietern (Carrier) und den Diensteanbietern im Internet weiter verschärfen. Denn die Carrier überlegen derzeit, gegen Gebühren, Daten von Anbietern priorisiert im Internet zu transportieren und so an deren Einnahmen zu partizipieren. Außerdem bieten sie zunehmend selbst „Mehrwertdienste" an, also Dienstleistungen und Inhalte über ihre Netzinfrastruktur, und werden so zu Konkurrenten der Anbieter im Internet.

4.2 Chancen und Herausforderungen des Umstiegs

„Gewinner" des Umstiegs auf IPv6 werden letztendlich diejenigen sein, die auf der vorhandenen Struktur kostengünstig Dienste anbieten können. Die Umstellung der Infrastruktur ist nur eine der Herausforderungen bei IPv6. Die andere Herausforderung liegt darin, Geschäftsmodelle basierend auf den neuen technischen Möglichkeiten zu entwickeln. Denn die bloße Übernahme bestehender Dienste und Geschäftsmodelle reizt die Fähigkeiten des neuen Internetprotokolls nicht genügend aus. IPv6 ist ein Katalysator für den Trend hin zur Vernetzung von Geräten, dem „Internet der Dinge". Objekte bis hin zu Alltagsgegenständen werden durch Programmierbarkeit, Speichervermögen, Sensoren und Kommunikationsfähigkeiten intelligent und können über das Internet eigenständig Informationen austauschen, Aktionen auslösen und sich wechselseitig steuern. Ein Beispiel für diese Entwicklung sind intelligente Stromzähler („Smart Meter"). Die direkte Adressierung von Geräten (siehe Ende-zu-Ende-Paradigma) ermöglicht neue Produkte und Geschäftsmodelle. Es ergeben sich Chancen für Existenzgründer und neue Unternehmen. Neu orientieren müssen sich bei einem Umstieg auf IPv6 jene Anbieter, die für ihre Dienste die in IPv4 vorhandenen Restriktionen auf bestimmten Gebieten durch technische Speziallösungen umgehen. Diese Unternehmen verlieren ihre technische Basis, andere können mit IPv6 vergleichbare Dienste in Zukunft einfacher anbieten. Die Einzelinteressen der Anbieter hinsichtlich IPv6 sind daher heterogen.

4.3 Neue Potenziale für das „Internet der Dinge"

Experten erwarten, dass durch die Verbreitung des neuen Internetprotokolls vor allem die Entwicklung des „Internet der Dinge" einen enormen Schub erhält. Dies ermöglicht einen Anschluss von Endgeräten an das Internet, wie z. B. im Bereich des „Smart Home". Zur Gruppe der Endgerätehersteller gehören deshalb zunehmend auch Unternehmen aus traditionellen Branchen wie die Hersteller „weißer Ware" – der Anschluss ihrer Geräte ans Internet erlaubt Innovationen der Gerätesteuerung und neue Dienstleistungen. So können von IPv6 auch Hersteller traditioneller Produkte profitieren, deren Produkte jetzt zunehmend mit der Informations- und Telekommunikationstechnik verschmelzen. Dabei gilt es, das Problembewusstsein zu schärfen und die Zukunftsfähigkeit gerade dieser Unternehmen in einem globalen Wettbewerb zu stärken.

Weder ist klar, welche Chancen in welchen Geschäftsmodellen stecken, noch ist die Dynamik der Entwicklung einzuschätzen. In Asien und den USA entstehen bereits neue Geschäftsmodelle, werden Start-ups gegründet – begünstigt durch die Entwicklung hin zu offenen Standards. Dank dieser Standards können Unternehmen einfache Anwendungen und Dienstleistungen für fremde Systeme anbieten. Der Druck auf die Hersteller, Schnittstellen offenzulegen, wird durch die technischen Möglichkeiten von IPv6 weiter zunehmen. Nutzer möchten wissen, welche Daten ihre Geräte übermitteln, und erwarten, dass etwa ihr Smartphone unabhängig vom Hersteller mit allen anderen Geräten sicher zusammenarbeiten kann. Im Gegenzug sinken die Markteintrittshürden für Existenzgründer: Die direkte Adressierung bei IPv6, leistungsfähige Netze und offene Standards erleichtern die Entwicklung neuer Geschäftsmodelle und innovativer Angebote.

4.4 Datenschutzaspekte

Bei IPv4 ist es üblich, dass DSL-Zugangsanbieter privaten Internet-Nutzern eine zeitlich begrenzt gültige IP-Adresse (dynamische IP-Adressen) zuweisen, da die Zahl der verfügbaren Adressen begrenzt ist. Alle angeschlossenen Geräte des Nutzers teilen sich die eine öffentliche Adresse des Anschlusses. Bei IPv6 kann jedes Endsystem, auch in privaten Haushalten, eine öffentlich erreichbare, statische Adresse erhalten. Statische IP-Adressen

- erleichtern technisch die Nutzung von Diensten im Internet (etwa IP-Telefonie),
- ermöglichen, dass jeder Dienste im Internet anbieten kann,
- stärken die Entwicklung neuer Dienste bzw. neuer Geschäftsmodelle.

Allerdings erleichtern statische Adressen die Zuordnung zu Nutzerprofilen. Dynamische Adressen stärken zwar die Privatsphäre, erschweren aber die Lokalisierung bei Notrufen. Dienste müssen hier auf externe Infrastrukturen zurückgreifen. Diese externen Hilfsmechanismen erhöhen den Aufwand und können neue Sicherheits- und Datenschutzprobleme mit sich bringen.

Der Umgang mit der IP-Adresse ist aus Sicht des Datenschutzes sensibel. Die in IPv6 vorgesehenen Maßnahmen zum Schutz der Privatsphäre (Privacy Extensions) sollten standardmäßig bei personengebundenen, insbesondere mobilen Endgeräten aktiviert sein. Allerdings ist die IP-Adresse nur ein Ansatz zur Nutzerverfolgung, andere Mechanismen wie Cookies sind aus Datenschutzsicht relevanter und hängen nicht von der IP-Adresse ab.

Aus Datenschutzsicht ist es bei IPv6 weiterhin hilfreich, dass der Zugangsanbieter ein dynamisches Adress-Präfix zuweist. Große deutsche Anbieter haben Pläne vorgestellt, dass Nutzer eine quasi-statische Adresse erhalten und diese „auf Knopfdruck“ wechseln können. Die Zugangsanbieter sehen in einem solchen Angebot die Chance, die Akzeptanz für IPv6 bei Endkunden zu erhöhen und sowohl den technischen Erfordernissen als auch den Belangen des Datenschutzes Rechnung zu tragen. Ein automatischer Wechsel der IP-Adresse ist jedoch nicht sinnvoll, denn für bestimmte Dienste (wie IP-Telefonie, insbesondere Notrufe) ist eine Unterbrechung durch eine dynamische Adresszuweisung nachteilig. Der Kunde kann bei dieser geschilderten Lösung selber entscheiden, welche Prioritäten er für Erreichbarkeit und Datenschutz an seinem Internetzugang setzt. Die Anforderungen an den Datenschutz gilt es daher, je nach Anwendung zu differenzieren: Anbieter und Datenschutzbeauftragte sollten gemeinsam Datenschutzprofile für unterschiedliche Szenarien entwickeln.

4.5 Herausforderungen für den Wirtschaftsstandort Deutschland

Bislang wurde das Thema „IPv6“ in Europa, insbesondere in Deutschland, vor allem unter Aspekten des Datenschutzes diskutiert. Der BMWi-IPv6-Workshop hat jedoch deutlich gezeigt: Datenschutz ist kein Hemmnis für den Umstieg auf IPv6. Experten sehen vielmehr die Gefahr, dass Deutschland zwar in neue Infrastrukturen investiert, aber andere im globalen Wettbewerb die Anwendungen entwickeln und auf den neuen Infrastrukturen betreiben. Deutsche Unternehmen laufen Gefahr, nicht von den Chancen von IPv6 zu profitieren. Es gilt, Maßnahmen zu ergreifen und das Bewusstsein der Beteiligten (insbesondere von kleinen und mittleren Unternehmen (KMUs) in traditionellen Branchen) zu schärfen, damit der Wirtschaftsstandort Deutschland mit IPv6 gestärkt wird und keine Nachteile im globalen Wettbewerb erfährt.

5. Handlungsfelder

Aus den dargestellten Aspekten der Umstellung auf das neue Internetprotokoll IPv6 sehen die Teilnehmer des BMWi-IPv6-Workshops eine Reihe von Handlungsfeldern für Wirtschaft und Verwaltung, um die Chancen von IPv6 für den Wirtschaftsstandort Deutschland zu nutzen.

5.1 Hilfestellung bei der IPv6-Migration

→ **Sensibilisierung und zielgruppenspezifische Information:**
Unternehmen müssen sich hinsichtlich ihrer IT und ihrer Produkte auf IPv6 vorbereiten, damit sie wettbewerbsfähig bleiben. Bei Unternehmen der IKT-Branche kann man dies als bekannt voraussetzen. Politik und Wirtschaftsverbände sollten Unternehmen aus traditionellen Branchen, deren Produkte zunehmend mit der Informations- und Telekommunikationstechnik verschmelzen, auf die Notwendigkeit der Umstellung aufmerksam machen. Es gilt, auch bei KMUs das Bewusstsein zu schärfen. Die Unternehmen benötigen Informationen zu Chancen und Risiken von IPv6 sowie Entscheidungskriterien für die Wahl eines geeigneten Migrationspfads. Aufgrund der langen Planungszeiträume müssen die Nutzer früh einen für sich abgestimmten Migrationsplan erstellen können, um Kosten und Risiken des Umstiegs zu minimieren.

→ **Aufbau und Austausch von Wissen über IPv6:**
Unternehmen benötigen für ihre Migrationsplanung Informationen in verschiedenen Detaillierungstiefen, um die Firmennetze mit geringem Aufwand und wenig Risiken auf IPv6 umzustellen. Die IT-Fachleute müssen in der Lage sein, eine für ihre Organisation geeignete Migration festlegen zu können. Sie benötigen Wissen über die Vor- und Nachteile der Varianten und den Erfahrungsaustausch mit Kollegen sowie Best Practices für IPv6-Netzarchitekturen. Wissenschaft und Wirtschaft sollten mit Unterstützung der Politik folgende Punkte aufgreifen:

- Unterstützung beim Informationsaustausch (etwa Workshops),
- Zusammenstellung von Best Practices,
- stärkere Berücksichtigung von IPv6 in der IT-Ausbildung.

5.2 Migration in Unternehmen

→ **Migration der Kommunikationskanäle:**
Die rasche Migration der Kommunikationskanäle wie Web oder E-Mail zum Dual-Stack-Betrieb ermöglicht, dass Dienste sowohl über IPv4 als auch IPv6 genutzt werden können. Unternehmen sind dann über beide Protokollvarianten erreichbar und auf den Übergang ihrer (weltweiten) Kommunikationspartner zu IPv6 vorbereitet. Allgemein kann ein schnell zunehmendes IPv6-Angebot die Migrationsphase im Sinne alle Nutzer verkürzen.

→ **Planvolle Migration:**
Vorhandene IKT-Infrastrukturen sollten planvoll und schrittweise von IPv4 zu IPv6 migriert werden. Fragen der Interoperabilität zu IPv4 sollten berücksichtigt, jedoch Investitionen in Entwicklungen auf Basis des alten Protokolls vermieden werden.

→ **Abgestimmte Migration:**
Das Vorgehen bei der Einführung von IPv6 ist abhängig vom Einsatzgebiet: Neue Produkte und Netze sollten gleich IPv6 unterstützen oder sogar ausschließlich nutzen. Unternehmen sollten bestehende Produkte und Netze für den Dual-Stack-Betrieb erweitern oder auf andere Migrationsverfahren zurückgreifen, wenn dies unter wirtschaftlichen oder organisatorischen Gesichtspunkten geboten ist.

→ **Nutzung neuer Eigenschaften von IPv6:**
Anbieter von Endgeräten und Diensten sollten früh beginnen, die neuen Eigenschaften von IPv6 zu berücksichtigen, um die Vorteile zu nutzen und Erfahrungen für sichere Konfiguration zu sammeln. Nur so sind ihre Produkte auf globalen Märkten konkurrenzfähig.

5.3 IPv6 und die Sicherheit

→ **Handlungs- und Konfigurationsempfehlungen:**
Die zügige Einführung und Nutzung von IPv6 erfordert Handlungs- und Konfigurationsempfehlungen in Bezug auf die Netzsicherheit. Dies gilt umso mehr, da neue Angriffe erst mit der weiteren Verbreitung von IPv6 entdeckt werden. Hier sind Wissenschaft, Politik und Wirtschaft in Deutsch-

land gleichermaßen aufgefordert, ihre Anstrengungen zu verstärken. Die öffentliche Hand kann Handlungs- und Konfigurationsempfehlungen für IPv6 herausgeben, beispielsweise im Rahmen der anerkannten ISi-Reihe des Bundesamts für Sicherheit in der Informationstechnik (BSI). Hersteller von IKT-Komponenten sollten Hilfestellungen für die sichere Konfiguration ihrer Produkte veröffentlichen. Ein Beispiel hierfür ist der Deutsche IPv6-Rat, der entsprechendes Informationsmaterial seinen Mitgliedern zur Verfügung stellt.

- **Privacy and Security by Default:**
  Anbieter und Hersteller sollten mit der Grundkonfiguration von Netzwerkkomponenten und Endgeräten einen sicheren Betrieb unter Berücksichtigung von Datenschutz-Aspekten in typischen Anwendungsfällen ermöglichen.

- **Untersuchung von IPv6-Stacks:**
  Insbesondere für Hersteller netzwerkgestützter Produkte aus IKT-ferneren Branchen kann sich die Einführung eines IPv6-Stacks wegen möglicher Sicherheitslücken als schwer kalkulierbares Risiko erweisen. Hier sind Wissenschaft und Politik aufgefordert, Unternehmen bei der Auswahl von Betriebssystemen und Protokollstacks mit Schwachstellenanalysen der Implementierungen zu unterstützen. So informiert das BSI über die BSI-Schwachstellenampel bereits regelmäßig Nutzer über den Sicherheitsstand in bekannten Software-Produkten. Solche Angebote sollten auf IPv6 erweitert werden.

- **Zertifizierung vertrauenswürdiger Diensteanbieter:**
  Die fortschreitende Vernetzung von Alltagsgeräten und die direkte Erreichbarkeit dieser Geräte aus dem Internet erfordert besondere Sicherheits- und Datenschutzüberlegungen des Anwenders. Um die Entwicklung neuer Dienste und Geschäftsmodelle zu ermöglichen und die Akzeptanz bei den Anwendern zu erhöhen, sollten Politik und Wirtschaft für den Zugriff durch vertrauenswürdige Diensteanbieter Standards schaffen.

- **Vermeidung unsicherer Übergangstechniken:**
  Unternehmen sollten für übliche Konfigurationen anerkannte Migrationstechniken verwenden bzw. fachlich fundierte Entscheidungen bei speziellen Lösungen einsetzen. Denn Fehler bei der Migration können sowohl die Leistungsfähigkeit als auch die Sicherheit von Diensten und Netzen einschränken.

- Anbieter und Datenschutzbeauftragte sollten gemeinsam Datenschutzprofile für unterschiedliche Szenarien entwickeln.

5.4 Rolle der öffentlichen Hand

- **Integration von IPv6 in Forschungsprogrammen:**
  Bisher ist IPv6 ein eigenständiger Schwerpunkt in nationalen und insbesondere in europäischen Forschungsprojekten. Im nächsten Schritt sollte der Einsatz von IPv6 als Basistechnologie in IKT-Forschungs- und Leuchtturmprojekten vorgesehen werden, etwa im Bereich Internet der Dinge oder Smart Grid. Bei entsprechenden Forschungsprogrammen und Projektaufträgen sollte die öffentliche Hand die IPv6-Fähigkeit der Lösungen in Ausschreibungen als ein Bewertungskriterium definieren.

- **IPv6 bei der öffentlichen Beschaffung und Einkauf:**
  Die öffentliche Verwaltung geht bei der Migration voran und nutzt die IPv6-Einführung zur Konsolidierung von gewachsenen IKT-Infrastrukturen. Sie erhöht auf diese Weise nicht nur das IPv6-Angebot, sondern steigert auch über die Beschaffung IPv6-fähiger IKT-Komponenten die Nachfrage nach derartigen Produkten in Deutschland, was allen Anwendergruppen zugutekommen sollte.

- **Einführung IPv6 in der öffentlichen Verwaltung:**
  Die Bundesregierung sieht in IPv6 einen wesentlichen Beitrag zur Einführung neuer Internet-Technologien in modernen, sicheren Kommunikationsinfrastrukturen. Bereits 2009 hat die Bundesregierung für Bund, Länder und Kommunen einen IPv6-Adressraum beantragt und erhalten. Das Bundesministerium des Innern (BMI) und eine übergreifende IPv6-Arbeitsgruppe auf Verwaltungsebene haben gemeinsam Konzepte zur Struktur und Organisation des Adressraums sowie technische Empfehlungen zur Einführung von IPv6 in einem Referenzhandbuch zusammengefasst. Die Grundlagen für die Einführung von IPv6 in der öffentlichen Verwaltung werden geschaffen. Das

Verbindungsnetz zwischen Bund, Ländern und Kommunen ist heute bereits IPv6-fähig (Dual-Stack). Im Projekt „Netze des Bundes“ werden die zwei zentralen ressortübergreifenden Regierungsnetze (IVBB und IVBV/BVN) in einer leistungsfähigen sicheren gemeinsamen Netzinfrastruktur neu aufgestellt und IPv6-fähig gemacht.

→ **Entwicklung eines IPv6-Profils und Migrationsleitfadens:**
Das BMI erstellt in einem Forschungsprojekt ein IPv6-Profil und einen Migrationsleitfaden und führt beispielhafte Migrationen durch. Das Profil enthält Empfehlungen, die die Mindestanforderungen an einzuhaltende Standards im Bereich IPv6 für unterschiedliche Produktgruppen festlegen. Damit möchte man der Situation entgegenwirken, dass Empfehlungen und Standards in verfügbaren Produkten heute noch teilweise proprietär, unvollständig oder mangels spezifischer Vorgaben und Orientierungshilfen herstellerabhängig umgesetzt werden. Ferner sind die Auswirkungen von IPv6 auf die in Bund und Ländern definierten IT-Standardarchitekturen bisher nur unzureichend betrachtet worden. Für den Migrationsleitfaden werden Empfehlungen erarbeitet, um die mit der IPv6-Einführung verbundenen Chancen zu nutzen und Risiken für die öffentliche Verwaltung zu minimieren. Der Migrationsleitfaden beschreibt die Umstellung auf IPv4/IPv6-Dual-Stack-Betrieb und enthält aus den Migrationsexperimenten abgeleitete Leitlinien und Best Practices. Die Ergebnisse werden 2012 veröffentlicht.

6. Literatur & Quellen

- Strategiepapier zur Förderung der Einführung von IPv6, AG 2 Sonderthemengruppe „Einführung von IPv6“, Nationaler IT-Gipfel, Broschüre der Arbeitsgruppe 2, Dezember 2011, www.it-gipfel.de/IT-Gipfel/Navigation/dokumente.html

- Wilhelm Boeddinghaus, Christoph Meinel, Harald Sack: Einführung von IPv6 in Unternehmensnetzen, Technische Berichte Nr. 52, Hasso-Plattner-Institut für Softwaresystemtechnik an der Universität Potsdam, Universitätsverlag Potsdam 2011, ISSN (online) 2191-1665, November 2011,

- www.ipv6council.de/fileadmin/documents/HPI_52_ipv6_leitfaden.pdf

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden für eine sichere IPv6-Netzwerkarchitektur (ISi-L-IPv6), BSI-Leitlinie zur Internet-Sicherheit (ISi-L), Version 1.0, März 2012, www.isi-reihe.de

- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit und Deutscher IPv6-Rat: Leitlinien IPv6 und Datenschutz, März 2012, www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html

- RFC 6434: IPv6 Node Requirements, Dezember 2011,

- www.rfc-editor.org/rfc/rfc6434.txt

- RFC 6540: IPv6 Support Required for All IP-Capable Nodes, April 2012,

- www.rfc-editor.org/rfc/rfc6540.txt

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Schwachstellenampel https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Gefaerdungslage/Schwachstellenampel/cs_schwachstellenampel_node.html

- World IPv6 Day www.worldipv6day.org

- World IPv6 Launch www.worldipv6launch.org

www.bmwi.de