Handlungsempfehlungen zur Einführung von IPv6

1 Einleitung

Die Initiative zur Einführung von IPv6 wurde im Nachgang zum Nationalen IT-Gipfel 2010 ins Leben gerufen – als Reaktion auf die notwendige Förderung der Einführung des Internetprotokolls Version 6 (IPv6) in Deutschland. Nachdem die Initiative im Jahr 2011 im IT-Gipfelprozess noch als Sonderthemengruppe geführt wurde, hat sie aufgrund der Relevanz des Themas sowie der großen Resonanz bei den Mitgliedsunternehmen seit 2012 als reguläre Projektgruppe ihren festen Platz in der AG2 des Nationalen IT-Gipfels.

Ziel der Projektgruppe ist es, die im Rahmen der Einführung von IPv6 auftretenden technologischen, marktwirtschaftlichen und gesellschaftlichen Fragestellungen zu erarbeiten sowie Handlungsempfehlungen für Entscheidungsträger aus Politik und Wirtschaft zu formulieren. Hierbei versteht sich die Projektgruppe als unabhängiges, marktübergreifendes Gremium von Marktbeteiligten und Experten zum Thema IPv6. Sie wird getragen von führenden Unternehmen der Telekommunikations- und IT-Wirtschaft, aber auch von Vertretern der Wissenschaft sowie dem Bundesministerium für Wirtschaft und Technologie. Zum IT-Gipfel 2011 hat die Arbeitsgruppe ein Strategiepapier verfasst, welches die Notwendigkeit der Einführung von IPv6 sowie den diesbezüglichen Status in Deutschland aufzeigt. Dieses beschreibt auch grundlegende Eigenschaften des Protokolls und diskutiert allgemeine Fragestellungen zu IPv6.[1] Dieses Jahr hat sich die Projektgruppe mit zwei Fokusthemen beschäftigt:

1. Geschäftsmodelle mit IPv6,
2. Privatsphäre und Sicherheit mit IPv6.

Von den Mitgliedern der Projektgruppe wurde unter Hinzuziehung ausgewählter Gastexperten die Relevanz der Themenkomplexe für die Einführung von IPv6 diskutiert. Außerdem wurden Handlungsempfehlungen an Marktteilnehmer und öffentliche Institutionen formuliert.

Die Ergebnisse der Projektgruppe sind im vorliegenden Dokument zusammengefasst. Kapitel 3 und 4 reflektieren die Diskussion der Projektgruppe zu den beiden Fokusthemen und beinhalten jeweils eine Liste an Diskussionsergebnissen. Ziel der Auflistung ist es, für ein besseres Verständnis über die Auswirkungen – Chancen und Risiken – der Einführung von IPv6 zu sorgen und mögliche Maßnahmen zu Förderung vorzuschlagen. In Kapitel 5 werden konkrete Handlungsempfehlungen an Politik und Wirtschaft gerichtet, die aus Sicht der Projektgruppe eine zeitnahe und reibungslose Einführung von IPv6 ermöglichen.

2 Hauptaussagen

Die Einführung von IPv6 schreitet weiter voran und eine flächendeckende Verbreitung ist absehbar. Allerdings ist die Einführung kein Selbstläufer: Sie kann mit mehr oder weniger Chancen bzw. Risiken, mit mehr oder weniger Kosten für die deutsche Volkswirtschaft und auch mit mehr oder weniger Unsicherheit für alle Internetnutzer gestaltet werden. Aus diesem Grund sieht die Projektgruppe zur Einführung von IPv6 aktuellen Handlungsbedarf, um die Weichen für einen reibungslosen Übergang von IPv4 zu IPv6 in Deutschland zu stellen und den IKT-Standort Deutschland weiter zu stärken.

Generell sieht die Projektgruppe in Deutschland die Notwendigkeit, dass

- neue IT-Kommunikationsnetzwerke, wie beispielsweise Intelligente Netze, von Beginn an auf Basis von IPv6 geplant werden;
- IPv6-Fähigkeit in Einkaufsrichtlinien für IKT-Produkte von Unternehmen sowie öffentlichen Institutionen fest aufgenommen wird;
- in der Ausbildung vertiefte IPv6-Kenntnisse vermittelt werden.

1 Strategiepapier zur Förderung der Einführung von IPv6 – http://www.it-gipfel.de/IT-Gipfel/Navigation/archiv,did=459940.html (letzter Zugriff 12.09.2012)

Als Handlungsempfehlungen an die Bundesregierung sieht die Projektgruppe

- das Aufsetzen einer Initiative zur Erarbeitung von Referenzarchitekturen für sichere IPv6-basierte Netzwerke mit besonderem Augenmerk auf die Zielgruppe der kleinen und mittelständischen Unternehmen;

- das Prüfen, ob Programmbausteine zu IPv6 in bestehende IKT-Förderinitiativen aufgenommen werden können und im Rahmen der Forschungs- und Entwicklungspolitik Handlungsbedarf zu IPv6 über das bereits vorhandene Maß hinaus besteht.

Bei Unternehmen der Privatwirtschaft sieht die Projektgruppe den Bedarf, dass

- sich Unternehmen verstärkt mit dem Thema beschäftigen, um die Umstellung ihrer IT-Netzwerke auf IPv6 besser vorzubereiten und voranzutreiben und um die neuen Möglichkeiten mit IPv6 auch als strategische Option zu betrachten;

- Gerätehersteller ihre Endgeräte standardmäßig IPv6-fähig und in einer Konfiguration ausliefern, die den Schutz der Privatsphäre und die IT-Sicherheit beim Endnutzer sicherstellt.

In Kapitel 5 werden diese Handlungsempfehlungen detailliert beschrieben.

3 IPv6 ermöglicht neue Geschäftsmodelle

Unternehmen investieren in Technologie, wenn die Aussicht besteht, auf Basis dieser Technologie tragfähige Geschäftsmodelle entwickeln zu können. Die Projektgruppe hat sich daher intensiv mit der Frage auseinandergesetzt, welche Geschäftsmodelle auf Basis IPv6 möglich und welche Rahmenbedingungen für ihre Umsetzung notwendig sind.

3.1 Zusammenhang zwischen Geschäftsmodellen und der Einführung von IPv6

Neben den technologischen Vor- und Nachteilen entscheiden bei der Einführung von neuen Standards oftmals auch marktrelevante Fragestellungen über die flächendeckende Akzeptanz und Einführung eines Standards. Prominente Beispiele hierfür liefert die Einführung von Standards für Speichermedien für Bild und Ton (zum Beispiel VHS, CD, DVD, BlueRay). Oftmals spielte neben technologischen Eigenschaften die Unterstützung der Hardwarehersteller sowie der Medienkonzerne eine entscheidende Rolle bei der Durchsetzung und Einführung eines gewissen Standards. Nur wenn ein Unternehmen ein tragfähiges Geschäftsmodell auf Basis eines Standards erwartet, werden Investitionen getätigt und die Einführung durch Marketingmaßnahmen unterstützt.

Im Falle von IPv6 ist die Situation etwas anders gelagert: IPv6 ist bereits im Einsatz und wird flächendeckend kommen – hierzu gibt es keine Alternative; daher stellt sich jetzt die Frage, bis wann IPv6 flächendeckend im Einsatz ist und wie die Übergangsphase gestaltet wird.

Die Schwierigkeit bei der Einführung von IPv6 ist, dass zyklische Abhängigkeiten zwischen Nachfrage und Angebot bestehen:

- Provider verspüren zu wenig Nachfrage, um flächendeckend auf IPv6 umzustellen; Dienstanbieter bleiben bei IPv4, da sich durch die nicht durchgängige End-to-End-Unterstützung von IPv6 nicht alle Vorteile von IPv6 voll nutzen lassen.

- Endanwender haben keine direkte Nachfrage nach IPv6, da IPv6 für sie im Normalfall keine Veränderung bewirkt.

Der erste Punkt führt dazu, dass einzelne Provider mit der Einführung von IPv6 zögern, da nur eine vollständige Abdeckung aller Provider und Dienstanbieter IPv4 ablösen und den Betrieb zweier IP-Protokolle gleichzeitig beenden kann. Der zweite Punkt führt zu einer weiteren Schwierigkeit: Ohne klar darstellbaren Kundennutzen kann die Umstellung auf IPv6 nur

schwer über die Preise an Endkunden weitergegeben werden. In diesem Umfeld ist es für Marktteilnehmer schwierig, tragfähige Geschäftsmodelle auf Basis der Einführung von IPv6 zu erarbeiten und hier eine Vorreiterrolle zu übernehmen.

Die Projektgruppe sieht aber durchaus Potenziale für tragfähige Geschäftsmodelle im Bereich IPv6. Diese werden im folgenden Abschnitt im Rahmen der Diskussionsergebnisse der Projektgruppe dargestellt.

3.2 Diskussionsergebnisse

Im folgenden Abschnitt wird eine Liste an Diskussionsergebnissen zum Thema Geschäftsmodelle mit IPv6 zusammengestellt.

- Potenzielle Geschäftsmodelle mit IPv6:
  - Beratung für die IPv6-Umstellung; es ist temporär eine hohe Nachfrage zu erwarten, bis IPv6 flächendeckend eingeführt ist. Der Bedarf ist definitiv da und als Volkswirtschaft kann Deutschland jetzt durch entsprechende Maßnahmen bestimmen, ob der Bedarf von deutschen Fachkräften bedient oder im Ausland nachgefragt wird;
  - Anwendungen, bei denen Netzwerkteilnehmer direkt miteinander kommunizieren (zum Beispiel Peer-to-Peer-Anwendungen, VoIP (QoS));
  - Generierung von Umsatzerlösen durch Vergabe statischer IP-Adressen (entsprechend dem heutigen Geschäftsmodell statische IPv4-Adresse);
  - Kosteneinsparungen durch Vereinfachung im Netzdesign (zum Beispiel durch Autokonfiguration von Endgeräten, kein NAT, Ende-zu-Ende-Verschlüsselung);
  - Kosteneinsparungen bei Zusammenlegungen von Netzwerken, zum Beispiel bei Zusammenschlüssen von Unternehmen oder Geschäftsbereichen, da verschiedene logische Netzwerke mit IPv6 einfach verbunden werden können (ohne überlappende Adressbereiche und mit der Möglichkeit bidirektionaler Kommunikation).
  - IPv6 als Integrationsprotokoll für verschiedene Gerätenetzwerke mit (unter anderem) proprietären Bussen (zum Beispiel Haus- und Heimvernetzung).
- Herausforderungen für Geschäftsmodelle mit IPv6:
  - IPv6 hat als Transportprotokoll für den Endanwender nur wenig sichtbaren Nutzen; ein Großteil der Nutzer sollte vom Wechsel der Version des IP-Protokolls idealerweise nichts mitbekommen.
  - Es ist schwierig, die Einführung von IPv6 als Basistechnologie mit einem Business Case zu rechnen.
- Die Bundesregierung und Behörden, aber auch private Unternehmen, sollten bei der Beschaffung von neuen IT-Infrastrukturen zwingend auf die Unterstützung der Empfehlung RIPE-554 achten, um Integratoren und Herstellern die Notwendigkeit der vollständigen IPv6-Unterstützung darzustellen.
- Weitere Beobachtungen:
  - Aktuell gehen die großen Investitionen im Internet eher in die Richtung, den Zuwachs auf Basis bestehender Technologien zu ermöglichen, weniger durch technologische Innovationen.
  - Die Suche nach Geschäftsmodellen mit IPv6 ist vielversprechender, wenn IPv6 als „Enabler-Technologie“ für gänzlich neue Geschäftsfelder genutzt wird, da dann sowieso in neue Infrastruktur investiert werden muss.
  - Motivation zur Beachtung von IPv6-Fähigkeiten bei Netzwerkinfrastrukturinvestitionen könnte die Möglichkeit bewirken, potenzielle Folgekosten zu vermeiden.
  - Schutz der Privatsphäre sowie Sicherheit sind Bedingungen für viele Geschäftsmodelle.

4 IPv6 befördert Privatsphäre und Sicherheit im Internet

Der Schutz der Privatsphäre sowie Sicherheitsaspekte stehen im Kontext der Einführung von IPv6 oftmals im Fokus der medialen Berichterstattung. Nach Ansicht der Projektgruppe hat die Einführung von IPv6 bei korrekter Umstellung allerdings keine negativen Auswirkungen auf Privatsphäre und Sicherheit – im Gegenteil: an bestimmten Stellen bieten neue Protokollfunktionen von IPv6 auch zusätzliche Möglichkeiten für den Schutz der Privatsphäre und die Sicherheit. So

sieht auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, in der notwendigen Einführung von IPv6 eine Chance, die Potenziale von IPv6 auch hinsichtlich des Schutzes der Privatsphäre auszugestalten.[2]

Allerdings sieht die Projektgruppe die Gefahr, dass eine inhaltlich verzerrte Diskussion über Privatsphäre und Sicherheit die Einführung von IPv6 erschweren kann und greift das Thema aktiv auf. Im folgenden Kapitel werden kurz die Begriffe Privatsphäre und Sicherheit erklärt und der Zusammenhang mit der Einführung von IPv6 erläutert. Darauf aufbauend werden dann Handlungsempfehlungen formuliert, die einen sicheren Betrieb sowie den Schutz der Privatsphäre bei der Einführung von IPv6 gewährleisten.

4.1 Abgrenzung von Privatsphäre und Sicherheit

Unter *Privatsphäre* bzw. dem Schutz der Privatsphäre versteht man die Sicherstellung des Grundrechts auf informationelle Selbstbestimmung im Sinne des Bundesdatenschutzgesetzes. Vereinfacht ausgedrückt geht es darum, dass die persönlichen Daten eines Nutzers nicht automatisch und ohne Einwilligung Dritten zugänglich sind; dies beinhaltet auch Daten über das Nutzerverhalten, wie zum Beispiel Ortsinformationen oder den Verlauf von besuchten Webseiten.

Unter dem Begriff *Sicherheit* werden Maßnahmen zusammengefasst, die sicherstellen, dass sowohl Daten vor unberechtigtem Zugriff geschützt als auch die Funktionsweise von IT-Systemen gegen Fremdeinwirkung abgesichert werden.

Sicherheitsmaßnahmen dienen daher auch dem Schutz der Privatsphäre.

4.2 Zusammenhang zwischen IPv6 und Privatsphäre und Sicherheit

Im Folgenden wird der Zusammenhang zwischen der Einführung von IPv6 und der Privatsphäre der Nutzer sowie der Sicherheit von IT-Systemen aus Sicht der Projektgruppe kurz dargestellt.

Zusammenhang zwischen der Einführung von IPv6 und dem Schutz der Privatsphäre

Durch die Einführung von IPv6 stehen um einige Größenordnungen mehr IP-Adressen zur Verfügung als bei der Vorgängerversion IPv4. Dies ermöglicht es prinzipiell, jedem Gerät, das an der Kommunikation im Internet teilnimmt, eine feste Adresse zuzuweisen. Bewegt man sich mit einer festen Adresse im Internet, heißt das nicht zwangsläufig, dass die Identität des Nutzers preisgegeben ist, denn die Verbindung zwischen IP-Adresse und Nutzerdaten kennt zu Beginn nur der Provider. Allerdings besteht mit einer dauerhaft festen IP-Adresse die Möglichkeit, von Diensten im Internet als ein und derselbe Nutzer wiedererkannt zu werden (auch ohne Kenntnis des Namens; anonyme Nutzerprofile). Durch Eingabe von persönlichen Daten bei Internet-Diensten können diese dann unter Umständen mit der IP-Adresse in Verbindung gebracht werden. Diese feste Zuweisung von IP-Adressen ist bei IPv4 genauso möglich, aber aus Gründen der Adressknappheit nicht praktikabel – Adressen werden hier von Providern meist nur temporär zugewiesen und bei Bedarf zwischen privaten und öffentlichen Adressen übersetzt (Network Address Translation).

Allerdings bedeutet die theoretisch eindeutige Adressierbarkeit aller Geräte mit IPv6 nicht, dass diese auch in der Praxis durchgeführt wird, bzw. nicht mit einfachen Mitteln verhindert werden kann. Vereinfacht gesprochen, besteht eine IPv6 Adresse aus einer Netzwerkadresse, die vom Provider vergeben wird, und einem gerätespezifischen Teil. Beide Adressteile können mit bestehenden Technologien (zum Beispiel dynamische Adresspräfixe, Privacy Extensions) geändert

2 Diskussion mit Peter Schaar (Bundesbeauftragten für den Datenschutz und die Informationsfreiheit) im deutschen IPv6 Rat – http://www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html (letzter Zugriff 12.09.2012)

werden, sodass eine dauerhaft feste IP-Adresse mit einfachen Mitteln umgangen werden kann.

Ergänzend ist an dieser Stelle zu erwähnen, dass eine dauerhaft feste IP-Adresse für gewisse Dienste notwendig und gewünscht ist, wie zum Beispiel die direkte Erreichbarkeit eines Geräts aus dem Internet oder auch die Wiedererkennung anhand der IP-Adresse; das ist bei IPv6 nicht anders als bei IPv4. Des Weiteren ist anzumerken, dass es noch zahlreiche von der IP-Adresse unabhängige Merkmale gibt, an denen ein Benutzer im Internet identifiziert werden kann (zum Beispiel Cookie, Browser-Speicher, Benutzung von Plug-Ins und Programmversionen, die extern abgefragt werden können etc.) – diese sind unabhängig von der Version des IP-Protokolls.

Zusammenhang zwischen der Einführung von IPv6 und der Sicherheit von IT-Systemen

Der Zusammenhang zwischen der Einführung von IPv6 und Sicherheit wird zweistufig betrachtet: einerseits im Zielzustand, in dem nur noch IPv6 im Einsatz ist, andererseits in der Übergangsphase von IPv4 zu IPv6.

Generell ist in einer IPv6-Umgebung ein mindestens gleichwertiger Sicherheitsstandard für Endgeräte im Internet möglich, wenn dies gewünscht wird. Oftmals wird von Kritikern angeführt, dass durch den Wegfall von Network Address Translation (NAT) ein Schutz vor eingehenden Verbindungen verloren geht. Dieser Schutz kann allerdings vollkommen gleichwertig durch Firewall-Funktionalitäten unter IPv6 bereitgestellt werden und stellt somit keinen Verlust von Sicherheit im Zielzustand dar. Da sich durch IPv6 und den Wegfall von NAT die Netzwerkarchitektur vereinfacht, und eine durchgängige Ende-zu-Ende-Kommunikation möglich wird, sieht die Projektgruppe das Potential, mit IPv6 die notwendigen Kosten für den Betrieb von IT-Systemen mit identischem Sicherheitsniveau zu senken.

In der Übergangsphase zwischen IPv4 und IPv6 ergeben sich zwei Herausforderungen hinsichtlich der Sicherheit von IT-Systemen. Einerseits wird mit IPv6 eine neue Technologie eingeführt – der sichere Einsatz erfordert Wissen und praktische Erfahrung im Einsatz von IPv6. Anderseits müssen in der Übergangsphase zwei Protokolle gleichzeitig unterstützt werden – dies führt zu einem komplexeren und damit potenziell aufwendiger zu wartenden System. Zusammenfassend kommt die Projektgruppe daher zu der Einschätzung, dass mit IPv6 ein mindestens identisches Sicherheitsniveau wie mit IPv4 erreicht wird, allerdings in der Übergangsphase durch zunehmende Komplexität bzw. fehlende Erfahrungswerte Sicherheitsbedenken entstehen. Im folgenden Kapitel findet sich eine Reihe an Punkten, die nach Meinung der Projektgruppe der Unsicherheit in der Übergangsphase entgegenwirken können.

4.3 Diskussionsergebnisse

Im folgenden Abschnitt wird eine Liste an Diskussionsergebnissen zum Thema Schutz der Privatsphäre und Sicherheit mit IPv6 zusammengestellt.

- → Erarbeitung von Best Practices/Referenzarchitekturen für sichere IPv6-Netzwerke:
  - Organisationen sollten schnell Einsatzerfahrung sammeln, um erprobte Best Practices formulieren zu können.
  - Die Best Practices sollten durch eine starke Organisation ausgegeben werden (zum Beispiel BMWi bzw. Verbund mehrerer Organisationen) – es muss für Anwender klar ersichtlich sein, dass er sich auf die Quelle verlassen kann.
  - Der Fokus sollte auf verschiedene Anwendergruppen gelegt werden; verschiedene Guidelines für verschiede Nutzergruppen (zum Beispiel (Provider-)Netzwerkbetreiber, WLAN-Hotspots, Endanwender, Content-Netzwerkbetreiber).
  - Zielgruppenorientiertes Marketing der Best Practices sollte erfolgen.
  - Es sollte dazu aufgefordert werden, Sicherheit (Security) und Privatsphäre (Privacy) gleich bei der Planung mitzubedenken („Security and Privacy by Design“).
  - Es sollte sichergestellt werden, dass Mindeststandards hinsichtlich Security und Privacy von allen Anbietern eingehalten werden, die nicht durch

unsichere und dadurch für den Anbieter günstigere Lösungen am Markt verdrängt werden, da der zusätzliche Nutzen von Privatsphäre und Sicherheit auf Konsumentenseite potenziell schwer zu argumentieren ist. Dies kann durch Selbstverpflichtung der Provider oder regulatorische Maßnahmen geschehen. Ein erster Schritt in diese Richtung wäre die Prüfung der Entschließung der Datenschutzbeauftragten zur „Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)“ zum Beispiel als freiwillige Selbstverpflichtung, als Best Practice, als regulatorische Vorgabe.
  - Ein Vergleich mit bestehenden IPv4 Architekturen sollte stattfinden (zum Beispiel Aufzeigen der entsprechenden IPv6-Architektur mit identischem Sicherheitsniveau zu einer bestehenden IPv4-Architektur).
  - Mögliche Szenarien für Best Practices sind: Konfiguration von Firewalls, Tunneling-Szenarien.
  - Es sollte der Hinweis gegeben werden, dass Best Practices nur Vorschläge sein können, die für den spezifischen Einsatzzweck auf jeden Fall geprüft und gegegenenfalls angepasst werden müssen.

→ Gezielte Kommunikation hinsichtlich Privatsphäre und Sicherheit beim Einsatz von IPv6 zur Sensibilisierung und Aufklärung von Anwendern:
  - Darstellung der Unterschiede von IPv6 zu IPv4: Was ändert sich hinsichtlich Privatsphäre und Sicherheit?
  - Keine generelle Verschlechterung bei IPv6 gegenüber IPv4.
  - Potenzielle Chance, sich bewusst für statische oder dynamische Adressierung zu entscheiden.
  - Betreiber soll nicht einfach ein Adressierungsmodell vorschreiben, sondern den Nutzer in die Entscheidung einbinden.
  - Darstellung des Einflusses von IP/Transportprotokoll auf Privatsphäre und Sicherheit im Gesamtsystem.
  - Einfache, zielgruppenorientierte Kommunikation, zum Beispiel durch Ampeldarstellung.
  - Matrix aus Stakeholder (zum Beispiel Endanwender, KMU) und Aspekten (wie Tunneling, Firewall etc.) jeweils für Privatsphäre und Sicherheit.
  - Kommunikation von Privatsphäre und Sicherheit im Gesamtkontext, also nicht losgelöst von positiven Aspekten und Chancen der Technologie (zum Beispiel reicht für manche Anwendungen im Bereich Intelligente Netze gegebenenfalls kein Privatanschluss).
  - Sensibilisierung der Kunden für die Themen Privatsphäre und Sicherheit: Man muss sich mit den Themen beschäftigen, wenn man sicher kommunizieren und seine Privatsphäre schützen will (“Jeder hat seine Aufgabe”)?
  - Einrichten einer öffentlich zugänglichen Seite, sodass Internet-Nutzer feststellen können, ob der eigene Rechner IPv6-fähig ist, mit weiterführenden Informationen rund um Privatsphäre und Sicherheit mit IPv6 (ähnlich www.dns-ok.de[3]).
  - Folgende beispielhafte Gegenüberstellung (siehe Tabelle) könnte den Kunden verständlich machen, welche Sicherheitsmerkmale von IPv4 sich bei IPv6 wiederfinden (damit könnte zum Beispiel das BSi den IPv6-Leitfaden entsprechend ergänzen).
  - Heben von Synergien zwischen den verschiedenen Initiativen zu IPv6.
  - Es existieren viele verschiedene Publikationen zum Thema IPv6 von verschiedenen Gremien.
  - Für den Anwender ist schwer nachvollziehbar, was die geeignete Referenz ist.
  - Eine koordinierende Rolle könnte hier das BMWi einnehmen (zum Beispiel auch durch Ausrichtung einer weiteren Konferenz zu dem Thema).

Tabelle 2.3-1: Sicherheitsmerkmale von IPv4 und IPv6

Sicherheitsmerkmal	IPv4	IPv6
Sicherheit vor direkten Angriffen aus dem Internet auf das Heimnetzwerk	Port-Filterung und NAT	Port-Filterung
Nicht-Verfolgbarkeit der IP-Adresse bei Web-Diensten	NAT und dynamische IPv4-Adressen	Privacy Extension und dynamische IPv6-Adressen

3 https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2012/Hilfe-gegen-Schadsoftware_DNS-Changer_10012012.html (letzter Zugriff 12.09.2012)

- Sicherstellung, dass Endkundengeräte standardmäßig in einer sicheren Konfiguration ausgeliefert werden:
  - Dadurch sind Anwendungsfälle für grob geschätzt 99 % der Nutzer abgedeckt.
  - Expertennutzer können noch Anpassungen machen.
  - Die Hersteller von Endgeräten und Betriebssystemen sollten die „Privacy Extensions“ im Ursprungszustand einschalten. Auch damit ist die Verfolgbarkeit des Interface Identifiers über die Zeit von Internetdiensten nicht mehr möglich. Das BSI sollte eine Empfehlungsliste mit entsprechenden Betriebssystemen und Endgeräten herausgeben und die Netzbetreiber sollten Einfluss auf Endgerätehersteller ausüben, um diese Einstellungen vorrangig zu behandeln.
  - Im Auslieferungszustand von Endgeräten für Endverbraucher (DSL-Router, Mobilfunkgeräte) sollten die Voreinstellungen für eingehende Verbindungen auf blockieren gesetzt und lediglich mit dem Eingreifen des Nutzers zu öffnen sein. Damit kann der gleiche Schutz wie mit NAT in IPv4 erreicht werden. Für Endgeräte, die für andere Kundensegmente gedacht sind, könnte von dieser Vorgehensweise abgewichen werden. Um dies zu erreichen, sind die Endgerätehersteller und Netzbetreiber aufgefordert, entsprechend zu handeln.

- Einsatz für ein stabiles regulatorisches Umfeld und Mitwirkung bei Standardisierungsgremien:
  - Mitdiskussion in den entsprechenden Gremien (IETF, IEEE, W3C),
  - Umsetzung bzw. Mitgestaltung von EU-Gesetzgebung.

- Aufnahme von Security und Privacy bei IPv6 in die Lehrpläne (Studium, Ausbildung):
  - Zum Beispiel heute kein IPv6 in der Berufsschule;
  - Motivation über Fachkräftemangel: notwendig für zukünftige Anwendungen und Netzwerkadministration.

5 Handlungsempfehlungen

Um die flächendeckende Einführung von IPv6 weiter voranzutreiben, möchte die Projektgruppe Entscheidungsträgern in Politik und Wirtschaft in diesem Abschnitt Handlungsempfehlungen geben. Die Handlungsempfehlungen leiten sich aus den Diskussionen der Projektgruppe zu den Fokusthemen Geschäftsmodelle mit IPv6 (Kapitel 3.2) sowie Privatsphäre und Sicherheit (Kapitel 4.3) ab.

5.1 Generelle Handlungsempfehlungen an Politik und Wirtschaft

- Neue IT-Kommunikationsnetzwerke, wie beispielweise Intelligente Netze in den Bereichen Energie, Verkehr oder Gesundheit, müssen von Beginn an auf Basis von IPv6 geplant werden. Dies betrifft sowohl die Endgeräte als auch die Netzwerkkomponenten und die Netzwerkstruktur.

- Sowohl öffentliche Einrichtungen als auch Unternehmen der freien Wirtschaft müssen IPv6-Fähigkeit in ihre Einkaufsrichtlinien für IKT-Produkte fest aufnehmen. Hierbei ist es empfehlenswert, sich an bestehenden sowie aktuell erarbeiteten Richtlinien zu orientieren, zum Beispiel dem Dokument „Requirements for IPv6 in ICT Equipment“ der RIPE NCC[4] und den Ergebnissen des Forschungsprojekts des Fraunhofer Instituts „IPv6-Profile für die öffentliche Verwaltung“[5], welches durch das Bundesministerium des Inneren beauftragt ist.

- Sowohl in der schulischen und universitären als auch der betrieblichen Ausbildung sollten vertiefte IPv6-Kenntnisse vermittelt werden. Hierfür ist in den Lehrplänen die Vermittlung von erweiterten IPv6-Kenntnissen sicherzustellen.

4 http://www.ripe.net/ripe/docs/current-ripe-documents/ripe-554 (letzter Zugriff 12.09.2012)
5 http://www.fokus.fraunhofer.de/de/ngni/projects/current_projects/ipv6/index.html (letzter Zugriff 12.09.2012) – die Ergebnisse des Forschungsprojekts waren zum Zeitpunkt der Redaktion dieses Textes noch nicht veröffentlicht

5.2 Spezielle Handlungsempfehlungen an die Politik

- Die Bundesregierung, beispielsweise vertreten durch das Bundesministerium für Wirtschaft und Technologie, sollte ein Programm zur Zusammenstellung von Referenzarchitekturen für sichere IPv6-basierte Netzwerke ins Leben rufen. Startpunkt sollte eine Bestandsaufnahme von vorliegenden Arbeiten sein, um dann gezielt fehlende Referenzen zu erarbeiten. Ziel sollte eine Sammlung von Referenzarchitekturen für verschiedene Anwendergruppen sein, in denen der jeweils gängigen IPv4-basierten Architektur für ein Anwendungsszenario die entsprechende IPv6-basierte Architektur gegenübergestellt wird. Zielgruppe sollten insbesondere kleine und mittelständische Unternehmen sein, die anhand von erprobten Referenzarchitekturen die Umstellung ihrer Netzwerke sicher planen können. Eine Mandatierung durch eine Regierungsorganisation ist wichtig für Vertrauen seitens der Anwender und hilfreich für die Verbreitung des Inhalts durch Branchenverbände oder Handelskammern.

- Die Bundesregierung sollte bestehende IKT-Förderinitiativen nutzen, um auf die IPv6-Thematik aufmerksam zu machen und die Einführung zu fördern. Konkret könnten beispielsweise in den Initiativen „Netzwerk elektronischer Geschäftsverkehr“ oder „SimoBIT – Sichere mobile Informationstechnik in Mittelstand und Verwaltung“ Themenbausteine zu IPv6 aufgesetzt werden. Auch im Rahmen der Forschungs- und Entwicklungspolitik sollte geprüft werden, ob Handlungsbedarf zu IPv6 über das bereits vorhandene Maß hinaus besteht.

5.3 Spezielle Handlungsempfehlungen an die Wirtschaft

- Die deutschen Unternehmen aller Branchen sollten sich verstärkt mit IPv6 befassen. Je nach Geschäftsfeld eines Unternehmens sollten IPv6-Aktivitäten auch einen strategischen Aspekt über den reinen IT-Betrieb hinaus verfolgen:
  - Für den Betrieb der eigenen IT-Infrastruktur sollten Unternehmen zeitnah Erfahrungen sammeln, beispielsweise in eigenen Testlabors. So kann vermieden werden, dass bei einer durch den Markt getriebenen schnellen Einführung von IPv6 unvorhergesehene Probleme entstehen, wie etwa unnötige Zusatzkosten für externe Spezialisten oder nicht eingeplante Investitionen in Infrastruktur.
  - Insbesondere weltweit tätige Unternehmen sollten die Anbindung ausländischer Standorte sowie mobiler Geräte, die im Ausland eingesetzt werden, auf IPv6-Fähigkeit prüfen, da die Umstellung auf IPv6 insbesondere in asiatischen Staaten weitaus schneller vorangeht als in Europa oder den USA.
  - IPv6 ist die Basistechnologie für neue IT-basierte Geschäftsmodelle in den Bereichen „Internet der Dinge“, „Industrie 4.0“ und Intelligente Netze. Daher ist es von strategischer Bedeutung für Unternehmen, ein Verständnis der Möglichkeiten von IPv6 und der notwendigen Schritte zu entwickeln, um IPv6-basierte Lösungen anbieten zu können.
  - Hersteller von Geräten für Endanwender sollten die Geräte in einer Konfiguration ausliefern, die den Schutz der Privatsphäre der Nutzer sowie die Sicherheit der Kommunikation sicherstellt. Konkret beinhaltet dies das initiale Einschalten von „Privacy Extensions“ und das Blocken von eingehenden Verbindungen.

Anhang

Übersicht der Mitwirkenden der Projektgruppe „Einführung IPv6“

Prof. Dr. Christoph Meinel (Leiter)	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
Wolfgang Dorst	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)
Dr. Michael Hasemann	T-Systems International GmbH
Ingolf Karls	Intel Mobile Communications GmbH
Thomas Knebel	Bundesministerium für Wirtschaft und Technologie (BMWi)
Georg Merdian	Kabel Deutschland Vertrieb und Service GmbH & Co. KG
Uwe Mühlender	Deutsche Telekom AG
Jens Mühlner	T-Systems International GmbH
Steffen Müller	Kabel Deutschland Vertrieb und Service GmbH & Co. KG
Dr. Harald Sack	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
Dr. Ulrich Sandl	Bundesministerium für Wirtschaft und Technologie (BMWi)
Tacio Santos	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
Thorsten Schoog	Alcatel-Lucent Deutschland AG
Uwe Welter	Cisco Systems GmbH
Eric Weltersbach	Telefónica Germany GmbH & Co. OHG
Geriet Wendler	Xantaro Deutschland GmbH
Johannes Wust	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH

Gastexperten

Wilhelm Boeddinghaus	Strato AG
Constanze Bürger	Bundesministerium des Innern (BMI)
Dr. Markus Dunte	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Wolfgang Fritsche	Industrieanlagen-Betriebsgesellschaft mbH

Redaktion

Projektgruppe „Einführung IPv6“ der AG2 „Digitale Infrastrukturen für innovative Anwendungen“