Deutscher Bundestag

17. Wahlperiode

Enquete-Kommission

Internet und digitale Gesellschaft

Projektgruppe Zugang, Struktur und Sicherheit im Netz

Protokoll

des

öffentlichen Expertengesprächs

„IPv6 – Sicherheitsaspekte“

Berlin, den 21. Mai 2012, 15.00 – 17.45 Uhr

Sitzungsort: Berlin, Konrad-Adenauer-Str. 1, Paul-Löbe-Haus

Sitzungssaal: E.400

Vorsitz: Tabea Rößner, MdB (BÜNDNIS 90/DIE GRÜNEN)

Vor Eintritt in die Tagesordnung

Abg. Tabea Rößner (BÜNDNIS 90/DIE GRÜNEN) eröffnet die Sitzung und teilt mit, dass sie stellvertretend für den Vorsitzenden, **SV Harald Lemke**, die Sitzung leiten werde. Sie begrüßt namentlich die sechs eingeladenen Sachverständigen, die Mitglieder der Projektgruppe Zugang, Struktur und Sicherheit im Netz sowie die anwesende Öffentlichkeit.

Die **Vorsitzende** erläutert den formalen Ablauf des Expertengesprächs. Zunächst hätten die anzuhörenden Sachverständigen Gelegenheit zu einem fünfminütigen Statement. Im Anschluss daran könne jede Fraktion bzw. ein von jeder Fraktion benannter Sachverständiger eine Frage an die sachverständigen Anhörpersonen richten. Anschließend finde eine offene Diskussion mittels Rednerliste statt.

Nachdem es gegen das formale Vorgehen keine Einwände seitens der Projektgruppe gibt, leitet die Vorsitzende zum ersten Tagesordnungspunkt über.

TOP 1 Expertengespräch zum Thema „IPv6 – Sicherheitsaspekte“

Die **Vorsitzende** erteilt **Gert Döring** das Wort.

Gert Döring bewertet das Thema IPv6 – Sicherheitsaspekte als sehr interessant. Die vorliegenden schriftlichen Fragen an die Sachverständigen gefielen ihm gut, da ein deutlich weiterer Betrachtungshorizont erkennbar sei. Die Fragen tangierten nicht nur die Einführung von IPv6, sondern setzten sich auch damit auseinander, welche Auswirkungen es habe, IPv6 nicht einzuführen. Dies sei eine Frage der Betriebssicherheit des bestehenden Internets. Er bekräftigt, dass das Netz künftig ohne IPv6 nicht sicher betrieben werden könne.

Die **Vorsitzende** dankt **Gert Döring** für das Statement und übergibt das Wort an **Wolfgang Fritsche**.

Wolfgang Fritsche begrüßt, dass sich die Enquete-Kommission mit dem Thema IPv6 und dem Aspekt der Sicherheit auseinandersetze. Das Thema werde in den

technischen Basen seit sehr vielen Jahren behandelt. Es sei jedoch wichtig, dass es auch Einzug in die politischen Ausschüsse halte. Er regt an, das Thema nicht isoliert als IPv6-Sicherheitsthema zu behandeln und eine „Goldrandlösung“ zu fabrizieren, sondern es ausgewogen mit Blick auf bisherige Errungenschaften mit IPv4 zu betrachten. Man dürfe nicht vergessen, dass auch hinsichtlich der Sicherheit bei IPv4 ein langer Weg zurückgelegt worden sei und teilweise noch heute daran gearbeitet werde, dieses Protokoll sicher zu machen. Viele frühere Fehler werde man bei IPv6 versuchen zu vermeiden.

Die **Vorsitzende** dankt **Wolfgang Fritsche** für seine Ausführungen und übergibt das Wort an **Ulrich Kühn**.

Ulrich Kühn führt aus, dass die Einführung von IPv6 oftmals als harmloser Umbau im Maschinenraum des Internets betrachtet werde, der eher etwas für Mechaniker sei und die Gesellschaft nicht tangiere. Dies sei aus seiner Sicht jedoch eine Fehleinschätzung. Zum einen habe IPv6 das Potenzial, die heutige Vernetzung noch deutlich zu erhöhen. Mobile Computing, das Internet der Dinge, RFID, Smart Meter und Smart Grid seien Entwicklungen, die quasi auf IPv6 warteten.

Anderseits habe man es mit einer Technik zu tun, die wahrscheinlich sehr lange erhalten bleibe. Der hauptsächliche Triebfaktor für den Umstieg von IPv4 auf IPv6 sei die Adressknappheit, die es bei IPv6 sicherlich nicht geben werde. Er halte es für einen wesentlichen Grundsatz einer offenen Gesellschaft, dass der Einzelne in der Ausübung seiner Freiheitsrechte regelhaft unbeobachtet bleiben müsse. Eine Technik, die in die kleinsten Winkel der Lebensgestaltung eindringe, habe jedoch bei nicht datenschutzgerechter Ausrichtung das Potenzial einer umfassenden Beobachtung des individuellen Tuns. Für die Technikentwicklung sei das gesamte Thema IPv6 nicht untypisch, da es aus dem Blickwinkel der Informatik, der Kommunikationstechnik und des Ingenieurwesens betrachtet worden sei. Er wolle nicht bestreiten, dass auch ein gewisses Maß an Datensicherheit und Datenschutz hineingeflossen sei, aber dies sei eher eine Art nachträgliches Add-

On. Insofern könnten für eine datenschutzgerechte Ausgestaltung dieser Technik sicherlich nicht allein die Ingenieure sorgen, die diese Technik entwickelt haben. Aber auch die Datenschutzbeauftragten könnten dies nicht, solange man ihnen nicht die passenden Instrumente an die Hand gebe. Insofern halte er es für wichtig, dass gerade auf der politischen Ebene überlegt werde, welche gesellschaftlichen Normen eine solche Technik begleiten sollten. Es gebe bisher eine Vielzahl an technischen Normen zu IPv6, die festlegten, wie diese Technik funktioniere. Was jedoch fehle, seien begleitende gesellschaftliche Normen und Standards. Das regelhafte Instrument für solche Standards und Normen seien Gesetze und Verordnungen.

Würden IP-Adressen, die relativ fest an ein Gerät und dessen Besitzer gebunden seien, von Nutzungsdaten zu Bestandsdaten, sei dies aus Datenschutzsicht fatal. Man solle sich ein Szenario vorstellen, wo jemandem eine IP-Adresse zugewiesen werde und jeder anhand einer Art IP-Adressbuch nachverfolgen könne, was diese Person im Internet mache. Dies sei eine Situation, die aus Datenschutzsicht versucht werde zu vermeiden. Er vergleiche das Beispiel in der Offline-Welt mit der Möglichkeit, einen Menschen anhand einer zentralen biometrischen Datenbanken mit Hilfe eines Smartphones zu identifizieren. Zwar gebe es diese technische Möglichkeit bereits, aus Sicht des Datenschutzes werde dies glücklicherweise jedoch noch nicht genutzt. Verbote, solche Informationen bereitzustellen oder zu veröffentlichen, seien vor allem bei international agierenden Anbietern oder überhaupt im Internet sehr schwer durchzusetzen. Dies sei eine frustrierende Erfahrung für Datenschützer.

Insofern plädierten Datenschutzbeauftragte dafür, sehr viel früher im Entstehungsprozess von IP-Adressen anzusetzen. IP-Adressen müssten so ausgestaltet werden, dass ungewünschte Identifizierbarkeit und Profilbildungen erschwert würden. Das Stichwort sei Privacy by Design. Aus Datenschutzsicht werde hier vor allem der Endkundenbereich betrachtet. Dieser sei einerseits der wirtschaftlich und technisch schwächste Stakeholder. Andererseits sei er zahlenmäßig der größte und derjenige, der letztlich Träger von

Datenschutzrechten sei.

Technisch gesehen, so erläutert **Ulrich Kühn**, gehe es um zwei wesentliche Bereiche bei den IPv6-Adressen im Endkundenbereich: die dynamische Vergabe des Präfixes und die standardmäßige Aktivierung der Privacy Extensions in allen Endnutzergeräten. In Kombination dieser beiden Maßnahmen könne eine Vermeidung der zuvor geschilderten Szenarien und der damit einhergehenden Datenschutzverletzungen oder -katastrophen erreicht werden. Er plädiere daher für verbindliche und auch kontrollierbare Normen und mache darauf aufmerksam, dass man sich in Anbetracht des Einführungsstandes von IPv6 in einer Situation befinde, wo ein Eingriff noch möglich sei. Dieses Fenster sei jedoch nicht mehr lange geöffnet.

Die **Vorsitzende** dankt **Ulrich Kühn** und bittet **Martin Turba** um sein Eingangsstatement.

Martin Turba erläutert einleitend, dass er im letzten Jahr an einem Projekt zur IPv6-Einführung in Fraunhofer-LANs (LAN für lokale Netzwerke in den Instituten) mitgewirkt habe. Das Projekt habe zwei Hauptziele gehabt: Überlegung eines Adresskonzeptes, welches man für die Einführung in solchen lokalen Netzen verwenden könne, sowie Skizzierung eines konkreten Vorgehens für eine solche Einführung. Vor diesem Hintergrund habe er die ihm gestellten Fragen in seiner schriftlichen Stellungnahme beantwortet und Erfahrungen, die er in diesem Projekt gesammelt habe, einfließen lassen. Aus seiner Sicht sei die Einführung von IPv6 in Deutschland in den Netzen der Internet-Service-Provider (ISP) schon am weitesten fortgeschritten, während sich im Unternehmensumfeld hauptsächlich die großen Unternehmen mit einer IPv6-Einführung auseinandergesetzt hätten.

Die Heimanwendern blieben momentan noch außen vor, was daran liege, dass bisher kaum Angebote für IPv6-fähige DSL- oder Kabelanschlüsse bestünden. Dieser Meilenstein stehe jedoch bevor. Erst danach werde es zu einer

flächendeckenden Einführung und weitreichenden Nutzung von IPv6 im Internet kommen.

Die Frage, wie sich Deutschland im europäischen und internationalen Vergleich positioniere, so **Martin Turba**, sei schwer zu beantworten. Die verfügbaren Zahlen erlaubten zwar eine grobe Abschätzung von unteren oder oberen Nutzungsgrenzen und eigneten sich bedingt, um Entwicklungstendenzen über die Zeit aufzuzeigen. Wirklich verlässliche Kriterien, anhand derer sinnvoll die Nutzung von IPv6 im Internet gemessen werden könne, ließen sich jedoch nicht finden.

Schaue man sich an, wie viele IPv6-Präfixe in der globalen Routing-Tabelle in Deutschland vorhanden seien, liege Deutschland im europäischen Vergleich weit vorne. Schaue man sich an, wie viele autonome Systeme, d. h. große Netzwerke, im Internet IPv6 zusätzlich zu IPv4 verwendeten, sehe die Situation ähnlich aus: Deutschland liege auch hier vorne, wenn auch im unteren Bereich des oberen Feldes. Betrachte man relativ, wie viele autonome Systeme bereits IPv6 einsetzten, dann liege Europa gemeinsam mit Südamerika direkt hinter Asien.

Des Weiteren sei er nach den Problemen bei der Einführung von IPv6 gefragt worden. Aus seiner Sicht betreffe die Einführung von IPv6 sämtliche IT-Bereiche, nicht – wie man meinen könnte – nur den Netzwerkbereich. Dies mache eine Einführung sehr aufwendig, da sehr hohe Abstimmungs- und Schulungsaufwände entstünden. Diese Aufwände seien extrem schwierig zu rechtfertigen. Klassische Argumente wie Return on Investment oder Total Cost of Ownership griffen hier nicht. In erster Linie handle es sich bei der Einführung von IPv6 aus Sicht einer Instituts- oder Unternehmensleitung um einen reinen Kostenfaktor. Darüber hinaus werde eine IPv6-Einführung häufiger auch zum Anlass genommen, gewachsene Unternehmensstrukturen zu revolutionieren. Dies führe häufig dazu, dass die Einführung stagniere oder schleppend vorwärts ginge.
Er betont, dass es trotz der derzeit fehlenden Applikationen absolut notwendig sei IPv6 einzuführen. Neben der Adressknappheit könne die Notwendigkeit IPv6

einzuführen auch auf ein Unternehmen zukommen, das heute noch der Überzeugung sei, es brauche kein IPv6. Als Beispiel seien hier Projektpartner zu nennen, die auf die Nutzung von IPv6 zur Kommunikation angewiesen seien.

Die **Vorsitzende** dankt **Martin Turba** und erteilt **Christoph Weber** das Wort.

Christoph Weber macht einleitend darauf aufmerksam, dass er aus der Schweiz angereist sei und hebt hervor, dass man sich in der Schweiz mit den gleichen Problemen hinsichtlich der Einführung von IPv6 auseinandersetze wie in Deutschland. Er arbeite für einen ISP und bewerte die Probleme einerseits aus technischer Sicht, aber auch aus Sicht eines Endkunden. Aus technischer Sicht befinde sich vieles noch in der Entwicklung. Es gebe immer neue Regeln und immer neue rechtliche oder technische Anforderungen. Diese seien an sich schwer umzusetzen. Darüber hinaus sei die zeitnahe Umsetzung eine Herausforderung. Die Situation sei für alle neu und man versuche mittels Leitplanken, die teilweise auch noch fehlten, IPv6 umzusetzen. Er befürchtet, dass Endkunden mit den technischen Anforderungen überfordert seien. Sollten früher oder später sämtliche Haushaltsgeräte eine IPv6-Adresse erhalten, bekomme der Enduser dies nicht unter Kontrolle. Diese Tatsache ziehe nach sich, dass durch Fachleute wie ISP oder durch Regulierungsmaßnahmen gewisse Sicherheitsvorschriften vorgegeben werden müssten, die auf Wunsch des Kunden umzusetzen seien. Wie dies aussehen werde, werde sich in den nächsten Jahren zeigen.

Die Einführung von IPv6 werde mindestens über die nächsten zehn bis 15 Jahre andauern. Auch wenn Unternehmen gerne mehr machen wollten, so fehlten doch die finanziellen Mittel. Die Einführung von IPv6 verursache enorme Kosten für ISP. Diese Investitionen brächten aktuell keinen Gewinn.

Die **Vorsitzende** dankt **Christoph Weber** und bittet **Björn Zeeb** um sein Eingangsstatement.

Björn Zeeb teilt mit, dass für ihn als Entwickler IPv6 ein Hauptwerkzeug sei, da er es zum Testen benötige. Die Einführung von IPv6 habe man aus seiner Sicht in gewissem Sinne verschlafen und da es am Schluss etwas schneller gehen müsse, werde man vermutlich eher in Sicherheitsprobleme „hineinrennen“. Er stimme **Wolfgang Fritsche** zu, dass man das Thema IPv6 nicht isoliert betrachten, sondern mit IPv4 zusammen korrigieren solle. IPv4 habe ein paar Jahre Vorsprung. Aus den damaligen Fehlern habe man jedoch gelernt und entsprechende Vorkehrungen getroffen.

Aus seiner Sicht finde aktuell noch keine Auseinandersetzung mit den Sicherheitsproblemen statt. Um die Einführung voranzutreiben, seien jedoch zunächst andere Bereiche in den Griff zu bekommen. Den Umgang mit den Endusern bewertet **Björn Zeeb** als das größere Problem. Auf der einen Seite wolle man die Endnutzer technisch nicht mit dem Thema konfrontieren. Auf der anderen Seite gebe es jedoch Probleme mit dem Datenschutz und der Sicherheit. IPv6 sei oftmals ohne das Wissen der Nutzer eingeschaltet. Entsprechend seien diese nicht darauf vorbereitet.

Der Aussage, dass sich Unternehmen bereits intensiver mit der Einführung von IPv6 auseinandergesetzt hätten, wolle er nicht uneingeschränkt zustimmen. Unternehmen müssten sich zwar zwangsweise mit diesem Thema beschäftigen, aber auch dort habe er die Befürchtung, dass dies, wie auch bei den Herstellern, verschlafen worden sei.

Auf die Frage, was der Staat für die Einführung von IPv6 tun könne, erklärt er, dass er sich als Endbenutzer freuen würde, die öffentlichen Angebote des Staates in naher Zukunft über IPv6 erreichen zu können.

Die **Vorsitzende** dankt **Björn Zeeb** für seine Ausführungen und eröffnet die Fragerunde. Sie bittet einen Vertreter der CDU/CSU-Fraktion um eine Frage an die Experten. **SV Prof. Dr. Wolf-Dieter Ring** bittet darum, zunächst den Vertretern der anderen Fraktionen das Wort zu erteilen.

SV Alvar Freude möchte von den sachverständigen Anhörpersonen wissen, ob neben dem enormen Adressraum, der mit IPv6 einhergehe, weitere positive Aspekte mit der Einführung von IPv6 verbunden seien.

Abg. Jimmy Schulz (FDP) erläutert eingehend zu seiner Frage, dass mit der Einführung von IPv6 auch die Befürchtung einhergehe, dass jedem Mensch eine eigene IP-Adresse zugewiesen werde. Bei dynamischer Vergabe der Präfixe und eingeschalteten Privacy Extensions sei eine Rückverfolgbarkeit zwar nicht möglich. Aber auch bei der dynamischen Zuweisung unter IPv4 lasse sich bereits weitgehend die Region, möglicherweise sogar der Straßenzug, zuordnen. Er vermute, dass dies auch bei den dynamisch zugeordneten Präfixen unter IPv6 so bleibe. Nun sei ihm jedoch an einem Mehr an Privatsphäre gelegen. Er wolle daher wissen, ob es technisch und finanziell möglich sei, dies bei der dynamischen Zuordnung der IPv6-Präfixe zu ändern und somit auch Rückschlüsse auf Stadt oder Straße zu verhindern.

SV Prof. Dr. Wolf-Dieter Ring wendet sich an **Ulrich Kühn**. Er begrüße die Aussage, dass die Entwicklung nicht alleine den Technikern überlassen bleiben solle, sondern auch begleitende gesellschaftliche Normen erforderlich seien. Ihn interessiere, wie mögliche Standards aussehen könnten.

SV Constanze Kurz richtet ihre Fragen an **Christoph Weber** und **Gert Döring**. Sie erläutert, dass die Aufgabe der Enquete-Kommission darin bestehe, dem Gesetzgeber Handlungsempfehlungen zu unterbreiten. Sie bittet die beiden Experten daher um Vorschläge von regulatorischen Vorschriften für den Bereich der Endgeräte und für den Bereich der Provider. Darüber hinaus fragt sie nach Angriffsvektoren in Bezug auf IT-Sicherheit – insbesondere ausgelöst durch das neue IPv6-Protokoll –, die in fünf Jahren denkbaren wären.

SV Markus Beckedahl knüpft an die erste Frage von **SV Constanze Kurz** an. Er bittet **Ulrich Kühn** um Vorschläge für Maßnahmen, die der Gesetzgeber treffen

solle, um das Datenschutzniveau auch bei IPv6-Adressen gewährleisten zu können. Des Weiteren interessiere ihn, welche Auswirkungen IPv6 auf die Datenschutzstandards bei mobilen Endgeräten habe. Wie könnten Geräte- und Betriebssystemhersteller einbezogen werden, um Datenschutz zu gewährleisten?

Die **Vorsitzende** bittet die sachverständigen Anhörpersonen um Beantwortung der an sie gerichteten Fragen und stellt ihnen frei, auch auf weitere Fragen einzugehen. Sie erteilt **Gert Döring** das Wort.

Gert Döring beantwortet zunächst die Frage von **SV Alvar Freude**. Seiner Einschätzung nach sei bei der Einführung von IPv6 primär der Zuwachs an Adressen entscheidend. Mit weiteren Aspekte wolle man die Schwachpunkte von IPv4 ausgleichen. Diese seien aber auch unter IPv4 bereits behoben worden. Als Beispiel führt er das Dynamic Host Configuration Protocol (DHCP) an, welches die automatische Konfiguration eines Computers zur Einbindung in ein Netzwerk ermöglicht. Der Adressraum von IPv6 bringe viele Nebeneffekte mit sich. So gestalte sich die Verwaltung von Netzen künftig sehr viel einfacher. Indirekte Kosten durch Adresskollisionen würden vermieden.

Hinsichtlich der Frage nach der regionalen Zuordnung der IP-Adressen erklärt **Gert Döring**, dass bei dynamischen Präfixen oder dynamischen IP-Adressen letztendlich Regionen bei einem Provider und auch der Provider selber tatsächlich eingrenzbar seien. Man könne beispielsweise die Deutsche Telekom als ISP zuordnen und mit weiteren Informationen auch die Region München – im Zweifelsfall sogar München Nord – anhand der IP-Adresse ablesen. Ein Straßenzug sei jedoch wahrscheinlich nicht erkennbar. ISP wollten ihr internes Routing übersichtlich gestalten, daher komme es zu der regionalen Zuordnung. Als Beispiel führt er die Deutsche Telekom an, die in ihrem IPv6-Adressraum schätzungsweise 500 Millionen Endbenutzer-Präfixe verwalten müsse. Erlaube man diesen Präfixen, an beliebiger Stelle in Deutschland „aufzutauchen“, müssten die Router der Telekom intern 500 Millionen Präfixe verteilen können und wissen, welches Präfix aktuell wo verwendet werde. Aggregiere man jedoch

standorttechnisch, sei die Routingtabelle sehr viel übersichtlicher und die Kosten für die nötige Hardware sinke drastisch. Dies gehe jedoch mit dem Problem der regionalen Identifizierbarkeit einher. Möglicherweise könne die Deutsche Telekom eine gewisse Art der Blockrotation einführen, die alle paar Monate erfolge. Eine komplett freie Zuordnung, d.h. die Zuteilung eines beliebigen Blocks aus diesen 500 Millionen Präfixen, halte er für technisch jedoch nicht sinnvoll umsetzbar.

Anschließend geht er auf die zweite Frage von **SV Constanze Kurz** ein. Da man heute noch nicht wisse, was die Angriffe von morgen sein werden, sei es auch sehr schwierig, fünf Jahre in die Zukunft zu schauen. Er erwarte jedoch keine wesentlichen Angriffsszenarien, die am Unterschied IPv4 / IPv6 auszumachen seien. Sogenannte Klick-mich-Angriffe würden immer häufiger, wohingegen direkte Netzwerkangriffe auf Windows-Freigaben, die ohne Passwort aus dem Internet erreichbar seien, nachgelassen hätten. Bei den Klick-mich-Angriffen würden Nutzer über eine E-Mail, die sie anklickten, infiziert. Hierbei sei es jedoch unerheblich, ob IPv4 oder IPv6 verwendet werde. Im großen Stil stattfindende Angriffe auf Netzwerkebene sehe er nicht. Es werde jedoch sicherlich Schwachstellen in bestimmten Betriebssystemen im IPv4- oder IPv6-Stack geben, sodass man mit geeignet geformten Paketen einen Rechner „abschießen“ könne. Dies würden jedoch keine Mainstream-Angriffe sein. Mit Mainstream-Angriffen lasse sich Geld verdienen, sodass es sich üblicherweise um Banking-Trojaner handle. Hinsichtlich der regulatorischen Vorschriften fielen ihm spontan keine Vorschläge ein. Er verweise jedoch auf die Geschichte, die zeige, dass man in Deutschland mit dem Internet gute Erfahrungen gemacht habe, solange niemand regulierend tätig geworden sei.

Wolfgang Fritsche erklärt, dass er sich hinsichtlich der neuen Funktionen von IPv6 seinem Vorredner anschließe. Der Adressraum sei der treibende Aspekt. Viele der neuen Funktionen von IPv6 seien im Laufe der Zeit auch in IPv4 als Workaround eingebaut worden. Es gebe einige zusätzliche funktionale Aspekte im Bereich der Mobilitätsunterstützung bei IPv6, aber das Kernthema sei der

Adressraum. Daher lasse sich der Umstieg auch nicht vermeiden. Die Risiken dieser neuen Funktionen betrachte er jedoch nicht per se als IPv6-spezifisch.

Hinsichtlich der zweiten Frage führt er aus, dass die Standardisierungsorganisationen alles ihnen Mögliche getan hätten. Es seien technische Möglichkeiten definiert worden, wie man mittels Privacy Extensions eine für das Endgerät zufällig generierte ID erzeugen könne. Wie dies anschließend verwendet werde, müsse gesondert betrachtet werden. Die Firma Microsoft habe beispielsweise bei verschiedenen Zugangspunkten zum Netz nicht immer eine neue zufallsgenerierte ID erzeugt. Dies liege jedoch nicht in der Verantwortung der Standardisierungsorganisationen.

Er bezweifle, dass ein Provider wirtschaftlich die Möglichkeit habe, beliebige Präfixe an beliebigen Zugangspunkten zuzuteilen. Der Vorteil einer hierarisch gut strukturierten Adressvergabe, die mit IPv6 eingeherginge, könne dann nicht genutzt werden. Diese diene jedoch der Entlastung des Backbones mit zu vielen Routingeinträgen und sei auch relevant für die Performance.

In Bezug auf das Thema Regulierung plädiert **Wolfang Fritsche** für mehr Sensibilisierung des Endnutzers. Dieser Aspekt sei auch in einem Gespräch des deutschen IPv6 Rates mit dem Bundesbeauftragten für Datenschutz diskutiert worden. Die Endnutzer seien darüber aufzuklären, dass es künftig zwei Möglichkeiten des Surfens im Internet gebe: anonym und identifizierbar. Das identifizierbare Surfen sei nicht immer negativ zu bewerten. Es könne für sehr viele Peer-to-Peer-Anwendungen in Zukunft von erheblichem Vorteil sein, dass man identifizierbar sei und damit bestimmte lokalbasierte Dienste in Anspruch nehmen könne. Er plädiert dafür, Anwender über beide Möglichkeiten aufzuklären. Wolle man regulativ eingreifen, so sei den Herstellern von Endgeräten aufzuerlegen, dass ihre Geräte beide Möglichkeiten unterstützten. Zudem solle die Option ‚anonymisiert' oder ‚identifizierbar' durch den Endnutzer über einen leicht zugänglichen Button auswählbar sein. Er betont, dass auch immer eine Restverantwortung beim Endnutzer verbleibe. Diese habe er auch

heute schon, wenn er seine Kreditkarteninformation im Internet verwende. Auch hier sei er selbst dafür verantwortlich und müsse entscheiden, ob er einer Webseite vertraue oder nicht. Soweit müsse man den Nutzer mitnehmen, indem man ihn über die beiden genannten Möglichkeiten aufkläre.

Ulrich Kühn knüpft an die Ausführungen seines Vorredners an. Der Endnutzer müsse in seinem Bedürfnis, Verantwortung zu übernehmen, ernst genommen werden. Aber es seien auch Lösungen für die Mehrheit der Endnutzer zu finden, die technisch nicht versiert seien. Er unterstreicht, dass auch an den Standardnutzer gedacht werden müsse. Hier gebe es aus seiner Sicht Bedarf für Regelungen, die den Providern vorzugeben seien. Die Provider sollten Zugänge anbieten, die den Nutzern keine datenschutzrechtlichen Bürden auferlegten. Möchte jemand etwas anderes haben, weil er ein Peer-to-Peer-Netz brauche oder seinen eigenen Server betreiben wolle, so solle dies auch möglich sein. Aber wenn man die Mehrzahl der 51 Millionen Internetnutzer in Deutschland betrachte, handle es sich bei diesen Personen nur um einen sehr kleinen Bereich von Anwendern. Die Sichtweise der Datenschutzbeauftragten sei schon immer auf die Mehrzahl der Bevölkerung, die mit dem Internet datenschutzfreundlich umgehen können solle, ausgerichtet gewesen. Es seien bestimmte Rahmenbedingungen zu setzen, die es weiterhin ermöglichten, sich vor Profilbildung und Identifizierung zu schützen. Er betrachtet das Telekommunikationsgesetz als möglichen Ort, an dem man solche Regelungen aufnehmen könne. Eventuell seien auch entsprechende Verordnungs-ermächtigungen hilfreich, um weitere Spezifikationen vorzunehmen.

Bei mobilen Endgeräte habe man es mit einer relativ überschaubaren Anzahl von Herstellern zu tun. Die Erfahrung der Datenschützer sei es, dass Hersteller schnell reagierten, wenn der Markt oder die Gesellschaft Techniken zum anonymen Surfen verlangten und anderenfalls Kunden fernblieben. Dann würden solche Techniken relativ schnell implementiert. Im Falle von Android-Systemen, in denen die Möglichkeit bereits vorhanden sei, die Privacy Extensions einzuschalten, seien diese auch standardmäßig aktiviert. Er bewerte es nicht als

Problem, solche deutlichen Anforderungen an Hersteller heranzutragen, da diese keine Kunden verlieren wollten.

Abschließend wendet er sich der Frage hinsichtlich der mit IPv6-Adressen verbundenen Geoinformationen zu. Er bestätigt, dass auch IPv4-Adressen bereits gewisse Geoinformationen beinhalteten. Diese seien je nach Anbieter unterschiedlich eindeutig. Hier habe man es bisher relativ erfolgreich geschafft, Hersteller oder Unternehmen, die diese Informationen verwerten wollten, davon zu überzeugen, dass Geoinformationen auch mit gekürzten IP-Adressen noch wertvoll seien. Dies werde sich nach seiner Überzeugung bei IPv6 nicht ändern. Auch bei IPv6-Adressen sei eine Kürzung erforderlich, um keinen Personenbezug herstellen zu können. Diese gekürzten Adressen seien aber durchaus noch ausreichend für die meisten Analysen, die man auf Basis der Geoinformationen mit IP-Adressen durchführen wolle.

Martin Turba stimmt den Ausführungen von **Gert Döring** hinsichtlich der Gründe für die Einführung von IPv6 zu. Auch er halte die Adressknappheit für die hauptsächliche Motivation, IPv6 einzuführen. Die meisten Funktionen, die mit der Entwicklung von IPv6 aufgekommen seien, seien zu IPv4 rückportiert geworden. Als Beispiel nennt er die Internet Protocol Security (IPsec), welche heutzutage zur Verschlüsselung von Kommunikation im Internet und zwischen Standorten von Unternehmen verwendet werde.

Die Möglichkeit, anhand einer IPv6-Adresse den Standort eines Benutzers ablesen zu können, sei implizit darauf zurückzuführen, wie Paketweiterleitung im Internet funktioniere. Man könne sich dies baumartig vorstellen, quasi eine Routinghierarchie. Am Ende dieses Baumes hinge eine einzelne IPv4- oder IPv6-Adresse, d.h. das Problem bestehe für beide Protokolle. Es gebe erste Ansätze, wie man diese überladenen Informationen einer IPv4 oder IPv6-Adresse auseinanderziehen könne. Dieses Locator/Identifier Separation Protocol (LISP) sei ein interessanter Ansatz, aber noch sehr wenig verbreitet. Nichtsdestotrotz sei es einfach notwendig, dass in irgendeiner Art von globaler Datenbank notiert sei, wo

eine bestimmte IP-Adresse verwendet werde, damit die Pakete dorthin geleitet würden können.

Als möglicher Angriffsvektor falle ihm nur die „Krücke“ ein, die man mit IPv4 geschaffen habe, um der Adressknappheit zu begegnen: die Funktion der Network Adress Translation (NAT). Er hoffe, dass diese Übersetzung von mehreren Rechnern auf eine öffentliche Adresse mit IPv6 wegfalle. Ohne NAT werde es möglich sein, Pakete direkt an Endrechner zu transportieren, sofern keine Filterung durch andere Sicherheitsmechanismen erfolge. Damit steige der Anspruch an die Endanwender bzw. an die Anbieter von Produkten für Endanwender, über eine sichere Basiskonfiguration zu verfügen, die verhindere, dass Pakete aus dem Internet direkt an Endgeräte weitergeleitet werden.

Christoph Weber bewertet mobile IPv6 als eine weitere große Entwicklung. Der Anwender könne über ein mobiles Endgerät mit seinem Heimnetzwerk verbunden sein und habe die Möglichkeit, ohne Unterbrechung in ein anderes Netz zu wechseln (Roaming). Diesem Vorteil stehe der Nachteil der Rückverfolgbarkeit gegenüber. In IPv6 seien auch Mechanismen für verschlüsselte IP-Verbindungen implementiert, die aber bisher – und wie es momentan aussehe auch in Zukunft – nicht genutzt würden.

Hinsichtlich der Frage zu den Geoinformationen erläutert er, dass die Zuteilung der IP-Adressen geografisch erfolge. Dies sei ein reiner Betriebsaspekt der ISP, um mit möglichst wenig Aufwand die IP-Adressen so zu verteilen, dass man eine übersichtliche Tabelle erhalte und wisse, wohin die Datenpakete zu senden seien. Eine komplett dynamische Zuteilung, d.h. der Kunde bekomme beispielsweise zweimal pro Tag einen neuen Adressbereich zugeteilt, bringe aber auch technische Probleme mit sich. Einerseits sei es für den Provider schwierig zu wissen, welcher User aktuell an welche Adresse angeschlossen sei. Diese Informationen seien aber auch aus rein rechtlichen Gründen notwendig. Andererseits müsse beispielsweise ein TV-Stream kontinuierlich erfolgen. Bekomme der Enduser plötzlich eine neue Adresse, so sei sein TV-Stream für

kurze Zeit unterbrochen. Es gebe zwar neue Protokolle, die dies unterstützten, aber bis diese von den Geräteherstellern implementiert und in den Businessanwendungen der ISP umgesetzt seien, werde noch sehr viel Zeit vergehen. Zudem sei dies sehr zeit- und kostenaufwendig.

Angriffsvektoren sehe er in den nächsten fünf Jahren viele neue, da viele Endbenutzer noch beide Protokolle, IPv4 und IPv6, verwenden werden. Es werde viele Angriffe geben, die über IPv4 erfolgten und bei denen der Rückkanal IPv6 sein werde. Er halte auch Angriffe über die Namensauflösung für denkbar, da der Enduser nicht wisse, welches Protokoll er aktuell verwende. Es werde auch Angriffe gegen das neue Protokoll geben. Dies führe er darauf zurück, dass Millionen Zeilen von Programmiercode neu zu schreiben seien. Dort komme es bestimmt zu Fehlern, so dass die Verletzlichkeit im IPv6-Umfeld größer sein werde als im IPv4-Umfeld.

Bei Mobilgeräten, so betont **Christoph Weber**, müssten dem Anwender möglichst einfache Mechanismen zur Verfügung gestellt werden, um zwischen Privatsphäre und Identifizierbarkeit wählen zu können. Auch er denke hier an einen einfachen und leicht zugänglichen Button. Mehr überfordere den Nutzer. Hersteller implementierten solche Lösungen seiner Meinung nach jedoch erst auf Druck der Kunden oder Behörden.

Björn Zeeb fügt den Antworten auf die Frage von **SV Alvar Freude** noch das Secure Neighbor Discovery Protocol (SEND) hinzu. Auch wenn der Verteilungsprozess auf Grund notwendiger Zertifikate schwierig erscheine, rechne er damit, dass es in der Zukunft genutzt werde.

Zum Thema mobile IPv6 falle ihm ein Papier des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein, in welchem auf Grund zahlreicher noch vorhandener Sicherheitsprobleme momentan von der Verwendung von mobile IPv6 abgeraten werde. Es helfe jedoch nichts, dieses Thema abzutun. Die Probleme gelte es zu beheben, damit mobile IPv6 benutzbar werde. Er schätzt,

dass dies jedoch noch fünf Jahre dauern werde.

Als er angefangen habe das Internet zu nutzen, habe er noch eine feste öffentliche IP-Adresse zugewiesen bekommen. Darüber habe er sich keine Gedanken gemacht. Mit der Einführung von NAT habe man in der Gesellschaft eine Erwartungshaltung geschaffen, dass IP-Adressen nicht mehr rückverfolgbar sein dürfen. Er sei sich nicht sicher, ob dies gut gewesen sei. Als Techniker habe er viele Möglichkeiten, die Identität einer Person herauszufinden, wenn sich jemand im Netz bewege, sei es durch Zusammenfügung von Browserfenster und Desktophintergrund oder den klassischen Cookie. Er bezweifelt, ob die IP-Adresse vor diesem Hintergrund so relevant sei.

Bezugnehmend auf die Frage nach möglichen Angriffsvektoren äußert **Björn Zeeb**, dass man sich in fünf Jahren in einer besseren Situation befinde als heute. Es sei jedoch wichtig, dass mit der Einführung vorangeschritten werde, sodass letzte Probleme gefunden und behoben werden können. Generell ließen sich Probleme jedoch nie vermeiden; Software werde immer Fehler beinhalten, die ausgenutzt würden. Bei IPv6 habe man jedoch den Vorteil, aus den Erfahrungen von IPv4 zu profitieren. Es habe von Anfang an Testframeworks gegeben. Diese seien zwar nicht grandios gewesen, stellten aber einen Anfang dar. Dies sei auch beim World IPv6 Launch Day für die nächsten Monate beim Testen von Endgeräten ein Aspekt. Die Endgeräte müssten spezielle Kriterien erfüllen, damit sie zugelassen würden. Dazu gehöre leider weiterhin NAT und die Stateful Firewall, die weiterhin auf Routern bleibe. Betrachte man die End-to-End-Kommunikation, werde der einzelne Arbeitsplatz mehr und mehr geschützt werden müssen. Der Schutz werde weniger im Netz stattfinden. Dies könne auch Vorteile haben, denn die Netzwerke würden schneller. Ob die Hersteller jedoch bereits soweit seien, wage er zu bezweifeln.

Die **Vorsitzende** leitet nun zur offenen Fragerunde über. Die erste Wortmeldung kommt von **Abg. Gerold Reichenbach (SPD)**.

Abg. Gerold Reichenbach (SPD) bewertet die Aussage, dass man künftige Angriffe gegen IPv6 nicht abschätzen könne, als unbefriedigend. Bisher sei nur über die Anwendung von IPv6 im traditionellen Spektrum diskutiert worden. Er wolle daher seine Fragen in Richtung Sicherheit neuer Bereiche stellen. Ein Großteil der Industrie – von der Automobilindustrie bis hin zu anderen Gerätelieferanten – sei dabei, die Vorteile und Möglichkeiten der Steuerung und auch sonstiger Kommunikation ihrer Endgeräte über das Internet und IPv6-Adressen zu entdecken und auszuschöpfen. Er wolle wissen, welche Konsequenzen die Experten dort in Zukunft für die Einhaltung des Datenschutzes sehen, da man Informationen über den Nutzer nun möglicherweise über die Geräteinformationen erhalte. Des Weiteren interessiere ihn, welche Angriffsszenarien denkbar seien. Als Beispiel nennt er Angriffe auf die Steuerung und den Boardcomputer von Fahrzeugen.

Gert Döring sagt, dass hier Bereiche angesprochen würden, in denen heute noch gar keine Angriffe denkbar seien, weil die entsprechenden Geräte zu „dumm“ seien, um angegriffen zu werden. Sofern ein elektrischer Stromzähler per Internet mit den Stadtwerken verbunden sei und diesen ausgesprochen detaillierte Informationen über das Nutzungsverhalten des Kunden wie den Zeitraum mitteile, in dem etwa eine Waschmaschine laufe, handle es sich um datenschutzrechtliche Informationen. Diese gingen aus seiner Sicht niemanden etwas an.

An dieser Stelle müsse er aber auch betonen, dass es sich hierbei nicht um ein IPv6-Probleme handle. IPv6 könne hier als „Enabler“ verstanden werden, aber gleiches könne man auch zu wesentlich höheren Kosten mit IPv4 tun. Daher sei IPv4 in diesem Zusammenhang nicht interessant. Dass es heutzutage möglich sei, mit geringen Extrakosten in Haushaltsgeräte wie eine Waschmaschine einen Internetanschluss einzubauen, falle nur zeitlich mit IPv6 zusammen. Man könne dies auch mit IPv4 und volldynamischen und vollanonymisierten Adressen erreichen.
Sofern der Stromzähler aber alle 15 Minuten eine Meldung an die Stadtwerke schicke, die notwendigerweise auch die Zählernummer enthalte, nutze die

Anonymität nichts. In dem Sinne handle es sich wieder um die gleiche Angriffsklasse, die er vorhin mit Klick-mich-Angriffen beschrieben habe. Wenn das Gerät über das Netzwerkprotokoll, sei es IPv4 oder IPv6, Informationen übertrage, könne man sich weder mit dem einen noch mit dem anderen Protokoll dagegen schützen.

Wenn man vom Stromnetzanbieter eine detaillierte Rechnung haben wolle, müsse man dem Stromzähler auch erlauben, mit ihm zu kommunizieren. Hier habe er den Wunsch, dass die Stadtwerke durch die Datenschützer stark in die Pflicht genommen würden, diese Daten intern nur anonymisiert zu verarbeiten und nicht weiterzugeben. Dies könne durch die IP-Protokolle nicht geleistet werden.

Christoph Weber erklärt, dass es sich bei IPv4 und IPv6 hinsichtlich der Sicherheit um die gleichen Probleme handle. Wenn jeder Nutzer mehrere Geräte habe, die mit dem Internet verbunden seien, könnten große Firmen, die gewisse Dienstleistungen zur Verfügung stellten, herausfinden, wo sich ein Nutzer gerade befinde und was er mache. Dadurch, dass es immer mehr Geräte gebe, fielen auch mehr Daten an. Dies sehe er als problematisch an. Fasse man diese Daten zusammen, so sei es möglich auch Schlussfolgerungen über einen Nutzer zu ziehen. Die große Frage sei, wie mit den Daten umgegangen werde.

Abg. Gerold Reichenbach (SPD) äußert eine Nachfrage. Er sei mit den bisherigen Antworten noch nicht ganz zufrieden. Natürlich sei es zunächst kein Problem von IPv6, aber ohne Ottomotor gebe es auch keine Verkehrsunfälle. Er weist noch einmal daraufhin, dass vor allem bei der Kommunikation über das Internet zwischen einem Auto und dem Hersteller Sicherheitsprobleme auftreten könnten. Diese Problem entstünde erst durch IPv6. Massentauglich werde es erst, wenn man einen Adressvorrat habe, durch den die dynamische Adressvergabe nicht mehr notwendig sei.

Ulrich Kühn merkt an, dass die geschilderten Probleme bereits am Horizont dämmerten. Im Bereich Smart Meter und Smart Grid zeigten sich bereits

datenschutzrechtliche Probleme. Diese versuchten die Datenschützer bereits mit den Herstellern und den Energielieferanten zu klären, aber hier spielten viele Interessen eine Rolle und Datenschutz sei anscheinend nur ein untergeordneter Aspekt. Man habe zwar bereits kleine Erfolge erzielt, aber abgeschlossen sei das Thema noch nicht. Wenn diese Technik Einzug in alle Lebensbereiche halte, könne die einzige Lösung sein, frühzeitig Datenschutzaspekte bei der Technikentwicklung zu berücksichtigen. Versuche man später solche Aspekte zu integrieren, so sei dies sehr teuer und scheitere. Der Gedanke des Privacy by Design müsse stärker in die Produktentwicklung Einzug halten. Anderenfalls entstünden Lösungen, die, davon gehe er aus, von den Herstellern gar nicht gewollt seien. Ein Energielieferant sei daran interessiert Energie zu liefern und nicht seine Kunden dauerhaft zu überwachen. Durch frühzeitige Integration in den Entwicklungsprozess ließen sich diese Probleme verhindern.

Wolfgang Fritsche erklärt, er habe vor einigen Jahren einen großen deutschen Automobilhersteller hinsichtlich der Frage, wie man einen Internetzugang im Auto sicher gestalten könne, beraten. Beim Zugriff auf den Boardcomputer biete sich sogar ein Vorteil, da sich von jedem Fahrzeug – ob per WLAN, Hotspot an der Tankstelle, per WLAN in der Garage oder mobil per UMTS/LTE – ein gesicherter, in diesem Fall VPN-Zugang mittels IPsec, zum Hersteller aufschalten lasse. Dies sei der Ansatz bei IPv4 gewesen, jedoch mit dem Nachteil, dass es dort von der Skalierbarkeit her sehr schwierig sei. Derselbe Ansatz werde nun mit IPv6 umgesetzt. Daher sehe er dort keinen Unterschied zwischen IPv4 und IPv6.

Das Schwerpunktproblem sei, dass der Nutzer neben den Anwendungen, die der Automobilhersteller biete, einen Internetzugang haben wolle, der sich im selben Boardcomputer befinde. Dort müsse nun erreicht werden, dass die sicherheitskritischen Anwendungen bei einem Virenbefall nicht in Mitleidenschaft gezogen werden. Bei dieser Trennung handele es sich aber nicht um ein IPv6-Thema, sondern finde auf höherer Applikationsebene statt.
Gert Döring fügt den Ausführungen von **Wolfgang Fritsche** ein Beispiel hinzu. Der A380 sei an jedem Platz mit einem Ethernet-Anschluss ausgestattet, an den

ein Passagier seinen Laptop anschließen könne. Auch intern gebe es Ethernet-Netzwerkverbindungen für die diversen Boardsysteme – für die Ruder, für den Steuercomputer usw. Diese Netzwerke seien nicht miteinander verbunden. Es sei eine ausgesprochen wirksame Lösung – unabhängig von IPv4 und IPv6 – Netze voreinander zu schützen.

Er äußert, dass er nicht in einem Auto führe, bei dem die Unterhaltungs- und die Motorelektronik auf dem selben Windows-Rechner liefen. Die Steuersysteme in modernen Autos seien komplex und hätten bestimmte Anforderungen zu erfüllen. Zu denen gehöre, dass das System nicht abstürzen dürfe. Funktioniere der Musikspieler einmal nicht, so sei dies zu verkraften. Das Ausfallen des Motors sei jedoch komplett indiskutabel.

Die Kommunikation über das Netz könne zwingend so gestaltet werden, dass das Auto in der Lage sei zu verifizieren, ob ein Softwareupdate vom Hersteller komme. Es gebe entsprechend kryptografische Verfahren. Sofern jedoch jemand beim Hersteller in die Entwicklungszentrale einbreche und damit scheinbar legitime Updates verschicke, könne man sich dagegen nicht per Internettechnik schützen. Dagegen, dass ein Dritter behaupte, er sei der Hersteller, könne man sich schützen, indem entsprechend erzwungen werde, dass die Updates vom Hersteller kommen müssen. Auch er betont, dass dies beim Produktdesign eingeplant werden müsse.

Abg. Jimmy Schulz (FDP) führt aus, dass früher jedem Internetbenutzer eine feste IP-Adresse zugewiesen worden sei. Dies habe sich durch NAT geändert. Durch NAT habe der Anwender mehr Privatsphäre erhalten. Durch IPv6 brauche man NAT eigentlich nicht mehr. Die Nutzer seien aber daran gewöhnt, dass sie durch NAT auch einen Schutz der Privatsphäre erfahren hätten. Nun könne dieser wieder wegfallen. Ihn interessiere, ob in Zukunft wirklich komplett auf NAT verzichtet werde. Von **Gert Döring** erbittet er eine Einschätzung, ob sich durch den Wegfall von NAT die Attacken von Klick-mich-Angriffen auf direkte Angriffe verlagern würden. Des Weiteren möchte er wissen, wie konkret die

Anhaltspunkte seien, dass in den nächsten sechs Monaten die massenhafte Einführung von IPv6 im DSL-Bereich stattfinde.

Gert Döring geht zunächst auf die zweite Frage ein. Auf dem Heise-IPv6-Kongress habe die Deutsche Telekom aus ihrem Friendly User Test berichtet. Diesen habe man sehr wissenschaftlich gestaltet: Von 200 Usern seien über vier Monate alle Fehlerberichte gesammelt und evaluiert worden. Man sei zu dem Schluss gekommen, dass das Einschalten von IPv6 keine Probleme verursache. Vor diesem Hintergrund gebe es keinen Grund, warum die Einführung nicht beginnen solle. Er habe gehört, es solle im September losgehen und es werde kein Opt-in erfolgen, sondern Region für Region werde sukzessive IPv6 eingeschaltet. Die Speedport-Router, die die Telekom heute ausrolle, seien bereits IPv6-fähig. Dies sei aus seiner Sicht ein Meilenstein, denn wenn jeder Kunde einen neuen Speedport kaufen müsse, erfolge eine Umstellung nicht. Insofern seien die Chancen für eine baldige Umstellung sehr gut, aber es gebe von der Telekom kein offizielles Statement. Auch die Kabelnetzbetreiber, so habe er gelesen, seien an dem Thema dran und führten Tests durch.

Die Frage nach der künftigen Verwendung von NAT sei spannend. Es gebe durchaus Router, die NAT-Funktionen für IPv6 anböten, aber niemand werde gezwungen sein, diese einzuschalten. Einige Firewalls seien bereits NAT-fähig. Mit den Speedport-Routern der Telekom sei die Nutzung von NAT nicht möglich. Er glaube, dass man NAT daher künftig nicht mehr im großen Rahmen sehen werde.

Er berichtet, dass das Thema „Firewalls auf Routern“ intensiv diskutiert werde. Die Provider befürchteten, Tür und Tor für Angriffe in den Endkundennetzen zu öffnen, wenn NAT wegfiele und sie den Endkunden komplett offene Router gäben. Die Endkunden hätten durch NAT quasi eine Sicherheit gehabt. Das Gegenargument sei, so führt er aus, dass die Nutzer auch ihre Laptops überallhin mitnähmen und online gingen. Auch dort hätten sie nicht den Schutz einer solchen Firewall. Das Geräte müsse daher in der Lage sein, sich selbst zu

schützen, anderenfalls nütze dem Anwender die Firewall auf dem CPE (Customer Premises Equipment, hier Router) auch nicht.

Martin Turba schließt sich den Ausführungen seines Vorredners bezüglich der bevorstehenden Einführung von IPv6 an. Auch seine Kenntnisse bezögen sich auf den IPv6-Kongress. Da IPv4-Adressen heute wesentlich knapper seien als noch vor einigen Jahren, habe sich der Druck auf die Provider auch erhöht. Wenn die Deutsche Telekom IPv6 standardmäßig für alle Endkundenanschlüsse sukzessive einschalte, werde der Konkurrenzdruck auf die anderen Provider entsprechend groß werden. Es werde dadurch zu einer flächendeckenden Einführung kommen.

Björn Zeeb berichtet, dass er in seinem Heimnetzwerk NAT mit IPv6 betreibe. Bei der Präfix-Translation ändere er zwar nicht den Präfix, der vom ISP zugewiesen werde, aber den Subnetzteil. Dies sei notwendig gewesen, da einige seiner alten Geräte zwar IPv6-fähig waren, aber nicht mit drei Präfixen umgehen konnten. Zwangsläufig habe er sich daher eine Lösung einfallen lassen müssen.

Er erklärt, dass NAT zwar auf gewisse Art und Weise die internen Geräte verstecke, aber hauptsächlich werde der Nutzer durch die Stateful Firewall der Router gegen Angriffe von außen geschützt. Wolle ein Endgerätehersteller die Zertifizierung für den World IPv6 Launch Day erhalten, so müsse er Router mit Stateful Firewall anbieten. In einem Nachbarland Deutschlands werde bereits IPv6 im großen Stil ausgerollt und die Router seien nicht mit einer solchen Firewall versehen. Bisher seien keine Probleme bekannt geworden. Er weist jedoch darauf hin, dass sich dies ändern könne, sobald die Einführung von IPv6 weiter vorangeschritten sei und IPv6 damit ein interessanteres Angriffsziel werden könne.

Prof. Dr. Christoph Weinhardt fragt nach, welche Kosten bei der Einführung von IPv6 anfielen. Es sei bisher mehrfach auf die hohen Kosten hingewiesen worden. Er wolle daher wissen, wo diese anfielen und durch wen sie getragen würden.

Christoph Weber erklärt, dass er aus Sicht des ISP, bei dem er arbeite, sprechen könne. Dort bestehe das Problem, dass die gesamte Kommunikation von den Rechenzentren bis zu den Clients und den DSL-Kunden momentan nicht IPv6-fähig sei. Zum einen habe man die Umstellung bisher versäumt. Zum anderen seien aber auch die Hersteller noch nicht so weit gewesen. Man werde beispielsweise im Zuge von Migrationen nur noch Geräte einsetzen, die IPv6-fähig seien. Dies habe zur Folge, dass die gesamte Kette an Geräten ausgetauscht werden müsse, wodurch zusätzliche Kosten verursacht würden, die im Moment noch nicht eingeplant seien. Des Weiteren fielen auch umfangreiche Managementkosten an, wie die Adressverteilung, die User-Handhabung usw. Auch die Steuersoftware für die Anwender sei neu zu programmieren oder müsse zumindest angepasst werden. Die Mechanismen, wie die IPv6-Adressen an den Enduser verteilt würden, seien neu zu programmieren. Dies sei ein Mehraufwand, den momentan die Provider tragen müssten. Es handle sich dabei um eine Investition in die Zukunft. Sein Arbeitgeber baue neue Datacenter und stelle die Anforderung an die Hersteller, dass alle Geräte IPv6-fähig sein müssen. Auch für die Evaluation und Überprüfung der Geräte ergebe sich ein Mehraufwand. Darüber hinaus müssten Mitarbeiter geschult werden. Die neuen Anforderungen für IPv6 umzusetzen sei ein sehr großer Aufwand.

Gert Döring widerspricht seinem Vorredner. Der ISP, für den er arbeite, habe bereits vor zehn Jahren begonnen, bei Neuanschaffung von Geräten sowie Neuentwicklung von Software darauf zu achten, dass diese IPv6-fähig seien. Dies habe zwar auch einen gewissen Mehraufwand erzeugt, aber dadurch stehe man jetzt nicht vor dieser Aufgabe. Finanziell habe es sich um einen schleichenden Prozess gehandelt, der sich über Jahre hingezogen habe. Natürlich gebe es noch einzelne Bereiche im Netz, wo IPv6 nicht funktioniere. Was man in der Diskussion um die Kosten aber auch tatsächlich nicht aus den Augen verlieren dürfe, seien die Kosten, die auf Grund einer Nichteinführung von IPv6 anfielen.

Die Aussage, dass die Einführung von IPv6 teuer sei, entspreche nur einer Seite der Diskussion. Habe ein Mobilfunkbetreiber aktuell noch wenige Kunden mit

Smartphone, werde dieser in wenigen Jahren eine Vielzahl haben. Der Provider könne daher nun in IPv6 investieren oder in die Brückentechnologie Carrier-grade NAT. Mit IPv4 könne er die Nachfrage nicht mehr befriedigen. IPv4 weiter zu verfolgen sei ab einem gewissen Punkt teurer als IPv6 einzuführen.

SV Markus Beckedahl erkundigt sich, ob es bereits belastbare Zahlen gebe, wie viele Endverbraucher in einem Jahr mit IPv6 in Berührung kommen werden. Schließlich werde sich nicht jeder Kunde neue Geräte kaufen.

Gert Döring meint, dass alle Nutzer, die sich für IPv6 interessierten, dieses bereits verwendeten. Dies sei jedoch ein verschwindend geringer Prozentsatz. Der Großteil der Bevölkerung komme erst mit der Umstellung durch einen Kabelnetzbetreiber oder DSL-Anbieter mit IPv6 in Berührung. Zu welchem Zeitpunkt wie viele Kunden mit IPv6 in Kontakt kämen, hinge von den Providern ab.

Björn Zeeb erklärt, dass in den USA Provider, die am World IPv6 Launch Day teilnehmen wollten, folgendes Kriterium erfüllen müssten: Mindestens ein Prozent ihrer Festnetz-Kunden müssten IPv6 nutzen. Die Provider rechneten damit, dass sie etwa sieben bis acht Prozent ihrer Kunden mit IPv6 zu versorgen hätten, damit sie dieses Kriterium erfüllten. Dies liege beispielsweise daran, dass den Kunden IPv6-fähige Router fehlten oder alte Betriebssysteme wie Windows XP im Einsatz seien. Für Deutschland bedeute dies, dass man nur ein Zwölftel der Anwender erreiche, wenn man heute deutschlandweit IPv6 einführe. Dennoch würde dies die Einführung vorantreiben. Die Anwender wüssten aktuell nicht, dass sie beim Neukauf eines Routers bereits nach IPv6 schauen müssten. Sobald IPv6 jedoch in aller Munde sei, würden die Anwender darauf achten.

SV Constanze Kurz beurteilt die bisherigen Vorschläge für regulatorische Maßnahmen als nicht befriedigend. Sie bittet die sachverständigen Anhörpersonen, mögliche Maßnahmen getrennt nach Endgerätehersteller und Provider zu diskutieren. Als Beispiel führt sie die Beibehaltung der

Dynamisierung von IP-Adressen an. Es sei gesagt worden, dass dies sehr aufwendig sei. Könne man sich trotzdem regulatorisch vorstellen, die Dynamisierung teilweise verpflichtend vorzuschreiben? Wie groß sei der Aufwand? Weiter führt sie für den Bereich der Endgerätehersteller aus, dass viele Smartphones nicht die Möglichkeit böten, die Privacy Extensions einzuschalten. Sie sehe daher die Restverantwortung beim Nutzer eher eingeschränkt vorhanden. Sie erkundigt sich, ob es ein Ziel sein solle, die Privacy Extensions auf Endgeräten standardmäßig eingeschaltet zu haben. Abschließend macht sie darauf aufmerksam, dass die Maßnahmen, die der deutsche Gesetzgeber ergreifen werde, einen Vorbildcharakter für andere Länder hätten. Als Ergebnis der Anhörung sollten daher einige konstruktive Lösungen aufgezeigt werden.

Wolfgang Fritsche bezieht sich in seiner Antwort auf den Bereich der Endgerätehersteller. Er halte an seiner Aussage fest, dass dem Nutzer eine gewisse Art der Selbstverantwortung obliege. Schließlich bewahre man seine Bankkarte auch nicht mit der PIN zusammen in der Geldbörse auf oder gebe man seine Transaktionsnummern (TAN) nicht öffentlich preis.

Dass die Selbstverantwortung technisch nicht unterstützt werden könne, möchte er an einem Beispiel entkräften: Lade man aus dem Microsoft Market Place eine Anwendung herunter, die eine GPS-Funktionalität benötige, werde der Anwender vom Betriebssystem darüber informiert, dass Positionsinformationen an einen Anbieter übermittelt würden. Der Anwender werde gefragt, ob die Anwendung dennoch auf dem Smartphone installiert werden solle. Er fragt sich, warum dies für IPv6 nicht genauso einfach gehen solle. Auch hier könne der Anwender anhand eines Dialogs entscheiden, ob er identifizierbar oder anonym Surfen wolle. Die technischen Möglichkeiten gebe es.

Er halte die Erfolgswahrscheinlichkeiten für höher, dass sich ein solcher Mechanismus durchsetze, wenn dieser von den Nutzern gefordert werde, als ihn „nur“ regulatorisch vorzugeben. Er plädiere daher eindringlich für die Sensibilisierung der Nutzer.

Gert Döring stellt klar, dass die dynamische Verteilung der Präfixe keinen großen Zusatzaufwand darstelle. Eine komplette Dynamisierung über das gesamte Netz, sodass ein Präfix nicht einem geografischen Bereich zugeordnet werden könne und auch der Provider nicht identifizierbar sei, sei jedoch nicht umsetzbar, solange man IP-basierte Protokolle verwende.

Hier komme er nun zu seiner Wunschliste: Wolle man, dass Anwender komplett anonym surfen können, brauche man etwas wie ein TOR-Netzwerk. Dieses müsse in Deutschland betrieben werden können, ohne damit unter Verdacht einer illegalen Handlung zu stehen. Hier sehe er Regulierungsbedarf. Die Möglichkeit, ein anonymisierendes Netzwerk betreiben zu können, ohne juristische Konsequenzen fürchten zu müssen, wenn ein Nutzer damit Unfug betreibe, halte er für sehr wichtig. Dennoch wisse er, dass dies eine ausgesprochen schwierige Gratwanderung sei.

Es müsse nicht unbedingt TOR sein, aber eine Technik dieser Art, d.h. ein anonymisierendes Multi-hop-Proxy-Routing, wo selbst der Betreiber eines Proxy-Servers nicht sehen könne, wer wohin surfe, sei wünschenswert. Dennoch sei auch dies noch nicht ausreichend, denn auch die Browser sammelten Informationen über einen Nutzer.

Er spricht sich dafür aus, dass die Provider keine einzelnen IPv6-Adressen an Endgeräte oder DSL-Kunden weitergeben. Damit würde ein „NAT-Zwang“ erzeugt werden. Es müsse mindestens ein Präfix vergeben werden, welches wählbar statisch oder dynamisch sein müsse. Der Standardkunde müsse ohne Aufpreis eine dynamische IPv6-Adresse erhalten. Zudem sollten die Mobilfunkanbieter beginnen, IPv6 zu Endgeräten anzubieten.

Ulrich Kühn betont, dass er durchaus für eine Regelung sei, nach der auf allen Endgeräten die Privacy Extensions standardmäßig eingeschaltet sein müssten. Ob dies gelinge und ob man damit möglicherweise internationale Handelsabkommen

oder ähnliches problematisiere, sei gesondert zu betrachten. Eine solche Anforderung sei jedoch im Sinne einer Anforderung an Produkte vorstellbar, die in den deutschen Markt eingeführt werden. Dennoch sehe er in diesem Bereich auch allein durch Marktmechanismen eine Chance auf Durchsetzung einer solchen Maßnahme.

Anders verhalte sich dies bei den dynamischen Präfixen. Hier sehe er überhaupt keine Möglichkeit, dass sich die dynamische Zuteilung von Präfixen durchsetze, wenn man dies dem Zufall oder guten Willen der Provider überlasse.

Christoph Weber widerspricht dem Vorschlag eines anonymisierenden Netzwerkes. Bei TOR sei bekannt, dass es Sicherheitsprobleme mit den TOR-Providern gebe. Er sehe TOR daher nicht als möglichen Ansatz.

Bezugnehmend auf die vollständig zufällige Adressverteilung erläutert er, dass dies technisch nicht möglich sei. Bei 1,5 Millionen Kunden seien Router mit 1,5 Millionen Einträgen notwendig. Dies sprenge den Rahmen. Man müsse ein Mittelmaß zwischen geografischer Verteilung finden und dem, was betrieblich vertretbar sei. Dies könne regulatorisch vorgegeben werden, sodass man beispielsweise festlege, dass 100.000 Einwohner eine Einheit bildeten, innerhalb derer die Adressen zufällig verteilt werden müssten.

Hinsichtlich der Selbstverantwortung der Nutzer wendet er ein, dass der Großteil der Anwender gar nicht wisse, was GPS oder IPv6 sei. Der Endbenutzer wolle einfach ein Gerät, mit dem er ins Internet könne und das seine Daten zuverlässig schütze. Die Anbieter seien hier in der Pflicht, Grundschutzmechanismen zur Verfügung zu stellen. Auch Gerätehersteller müssten verpflichtet werden, dem Anwender eine einfache Möglichkeit einzuräumen, sich zu schützen. Denkbar sei auch, den Schutz als Grundeinstellung vorzugeben.

SV padeluun richtet seine erste Frage an **Ulrich Kühn**. Dieser möge mitteilen, was er konkret vom Gesetzgeber erwarte, damit Privacy by Default und Privacy by

Design umgesetzt werden könnten. **Gert Döring** und **Martin Turba** bittet er, die Frage zu beantworten, ob mit IPv6 nicht noch einmal mehr eine Regelung notwendig sei, dass Hardware in der Kontrolle der Nutzerinnen und Nutzer verbleiben müsse. Schließlich sei das Gerät Eigentum des Anwenders.

Ulrich Kühn sagt, Ansätze seien bereits im Datenschutzrecht enthalten. Hier müsse man sich jedoch noch stärker auf die Produktentwicklung beziehen. Momentan betrachte man eher die Anwendungsebene, d.h. den Bereich, wo mit Daten gearbeitet werde. Das Datenschutzrecht sei jedoch hinsichtlich der Produktebene eher unterentwickelt. Man habe es bisher noch nicht geschafft, die im Bundesdatenschutzgesetz angelegte Auditierung und Zertifizierung von Produkten in eine operationalisierbare Form zu gießen. Die Stiftung Datenschutz schiebe dies noch immer vor sich her. Letztlich sollten auch Produktaudits gemacht werden, in denen die Hersteller nachweisen könnten, dass bestimmte Datenschutzstandards in ihre Produkte eingeflossen seien. Hier sei auch gesetzgeberisch noch viel zu tun, um tatsächlich Standards zu etablieren und auch positiv zu fördern. Es sei durchaus ein interessanter Aspekt, nicht nur im Falle von Fehlentwicklungen zu sanktionieren, sondern im Gegenteil auch positive Entwicklungen rechtzeitig zu fördern. Diese Elemente seien unterentwickelt.

Gert Döring erklärt, dass die Frage nach der Hardwarekontrolle nicht eindeutig zu beantworten sei. Er sei jemand, der seine Hardware kontrollieren wolle. Er wolle dort eigene Firmware installieren und sei daran interessiert zu verstehen, wie das Gerät funktioniere. Dazu wolle er das Gerät auch aufschrauben dürfen. 99 Prozent der Anwender, so glaubt er, seien jedoch ganz zufrieden, wenn sie nicht wissen müssen, wie ihr Gerät funktioniere, sondern es einfach das tue, was sie wollten. Man müsse hier auch das Sicherheitsdebakel bei nicht aktualisierten IT-Produkten anschauen. Ein Windows Betriebssystem, welches keine Updates installiert habe, sei im Prinzip eine Gefahr für die Allgemeinheit. Mit der Zeit werde es andere Rechner mit Viren infizieren und Schaden anrichten. Daher begrüßt er eigentlich, dass 99 Prozent der Geräte automatisiert aktualisiert

werden. Die Frage der Verantwortung und Haftung liege hier jedoch eindeutig beim Anbieter des Gerätes. Funktioniere ein Router beispielsweise nach einem Update nicht mehr, so müsse der Anbieter einen neuen zur Verfügung stellen. Das dies juristisch nicht einfach zu fassen sei, wisse er.

Die Frage ziele auf ein spannendes Themenfeld ab. Auf der einen Seite sei es schön, die Möglichkeit zu haben, selbstständig die volle Kontrolle über seine Geräte auszuüben, ohne das dies der Hersteller verbieten könne. Andererseits seien Geräte, über die der Hersteller die Verantwortung übernehme und sich um die Updates kümmere, eigentlich ein Segen. Es seien also zwei Seiten zu betrachten. Der Gesetzgeber könne hier vielleicht vorgeben, dass dem Anwender auf Wunsch die vollständige Kontrolle über ein Gerät eingeräumt werden müsse, welches er kauft. So müsse es zum Beispiel bei der Xbox möglich sein, eigene Software zu installieren.

Martin Turba stimmt den Ausführungen seines Vorredners zu. Auch er tue sich schwer, auf die Frage eine sinnvolle Antwort zu finden. Unabhängig davon, ob man vom Provider einen Router zur Verfügung gestellt bekomme oder ein Gerät von einem bestimmten Hersteller wie Apple kaufe, notwendig sei das Vertrauen in die Anbieter bzw. Hersteller. Diesen müsse der Anwender vertrauen können, dass sie für ihre Produkte immer aktuelle Updates zur Verfügung stellten. Dies sei aus seiner Sicht die einzige sinnvolle Stelle, an der der Gesetzgeber eingreifen könne. Die Hersteller seien in die Pflicht zu nehmen, dass sie ihrer Update-Verantwortung nachkämen.

Es habe Geräte mit Android-Betriebssystem gegeben, auf denen sehr alte Versionen mit bekannten Sicherheitslücken in Browsern und dem Betriebssystem liefen. Der Benutzer habe keine einfache Möglichkeit gehabt, die Updates eigenständig zu installieren.

Wolle man regulierend eingreifen, sei es sinnvoll dafür zu sorgen, dass ein interessierter Kunde die Möglichkeit bekomme, sich selber um die Wartung

seines Gerätes zu kümmern. Auf der anderen Seite müssten die Hersteller in die Pflicht genommen werden, für die 99 Prozent der Kunden, die dies nicht könnten, Updates bereitzustellen.

SV Alvar Freude erkundigt sich, ob die Provider statische und dynamische Präfixe gleichzeitig vergeben könnten. Er wirft die Frage auf, ob es eine sinnvolle Option sei, sowohl ein statisches als auch ein dynamisches Präfix zu vergeben, sodass der Nutzer in der Software oder dem Gerät zwischen beiden auswählen könne. Des Weiteren interessiere ihn, ob es Prognosen gebe, wie viele Jahrzehnte man auf Grund diverser alter Geräte noch mit IPv4 umgehen werden müsse. Gebe es Möglichkeiten, dies zu beschleunigen?

Christoph Weber bewertet die Idee, beide Präfix-Arten zu vergeben, als sehr interessant. Dennoch sehe er mehrere Probleme. Zum einen frage er sich, wie der Nutzer entscheiden solle, welches Präfix er aktuell brauche oder ob die Wahl von der Software getroffen werden solle. Technisch könne man einem Endgerät mehrere Adressen aus verschiedenen Bereichen zuteilen. IPv6 erlaube, explizit mehrere Adressen zu handhaben, ein Problem sehe er aber bei der Entscheidung durch den Nutzer. Für den Provider ergebe sich ein hoher zusätzlicher Aufwand. Es müssten jedem User oder Gerät zwei Adressbereiche oder zwei oder mehrere Netze zugeteilt werden. Er bezweifle, dass ein Provider dies umsetzen wolle. Zudem komme der administrative Aufwand hinzu. Schließlich müsse der Provider wissen, welcher Kunde zu welcher Zeit welchen Präfix gehabt habe. Die Idee sei aus seiner Sicht daher nicht als Lösung geeignet.

Die Zeitspanne, in der IPv4 noch genutzt werde, sei relativ lang. Die Migration werde aus seiner Einschätzung heraus mindestens zehn bis 15 Jahre dauern.

Gert Döring erklärt, dass er sich mit der von **SV Alvar Freude** gestellten Frage bereits auseinandergesetzt habe. Relativ einfach ließe sich diese Idee noch in den Provisionierungssystemen der Provider realisieren. Hier sei quasi nur ein Haken zu setzen, dass der Kunde nun beide Arten von Präfixen beziehen wolle.

Schwieriger werde es an der Stelle, wo der Kunden-Router beim Provider-Router dynamisch zwei Präfixe anfrage. Der Router beim Kunden müsse sich automatisch konfigurieren, da eine manuelle Einstellung durch den Provider beim Kunden vor Ort zu teuer sei. Die Router, die er auf ISP-Seite einsetze, könnten zwar statische oder dynamische Präfixe ausgeben, aber es sei nicht möglich, zwei Präfixe an denselben Kunden zu geben. Hier müsse er sich an den Gerätehersteller CISCO wenden und dieses Feature einfordern, wozu jedoch eher die Marktmacht der Deutschen Telekom erforderlich sei. Technisch könne man es also heute nicht realisieren, sodass er sich der Meinung seines Vorredners anschließt.

Selbst wenn es netzwerktechnisch möglich sei, habe der Rechner des Kunden nun zwei IP-Adressen und der Browser wisse nicht, ob er die statische oder die dynamische Adresse nehmen solle. Zudem wisse der Browser nicht, welche überhaupt statisch und welche dynamisch sei. Diese Information müsse mitgeschickt werden. Hier fehle im Browser zum Beispiel eine Art Plug-In, welches beide Adressen inklusive der Information, ob statisch oder dynamisch, anzeige.

Bezugnehmend auf die zweite Frage halte **Gert Döring** es für realistisch, den Großteil der Anwender relativ schnell auf IPv6 umgestellt zu haben. Bei den Betriebssystemen wie Windows XP, Windows Vista, Windows 7, Mac OS oder Linux sei IPv6 lediglich einzuschalten. Die wenigen Anwender, die noch ältere Hardware in der „Bastelecke“ benutzten, könne man tatsächlich vernachlässigen. Trotzdem werde die Migration seiner Meinung nach noch zehn Jahre dauern. Schließlich müssten die Server manuell umgestellt werden. Im Laufe der Zeit würden die Serveranbieter feststellen, dass sie eine höhere Qualität mit IPv6 ausliefern könnten. Dann hätten auch sie ein Interesse daran ihre Server IPv6-fähig zu machen. Bis dies jedoch eingetreten sein werde, dauere es sicherlich noch zehn bis 15 Jahre.

Er fährt fort, dass im Internet Hardware und Software so schnelllebig seien, dass IPv4 relativ schnell abgelöst sein werde. In den Firmennetzen hingegen werde IPv4 vermutlich noch in 100 Jahren eingesetzt. Meist gebe es irgendeine unternehmenskritische Spezialanwendung, die auf einem alten Rechner laufe, der nicht IPv6-fähig sei. In diesem Bereich werde IPv4 daher noch sehr lange eingesetzt werden. Dies könne man auch nicht beeinflussen. Die Firmen müssten irgendwann selbst lernen, dass dieses Vorgehen keine zukunftsführende Strategie sei.

Björn Zeeb geht auf die Frage ein, wie lange IPv4 noch eingesetzt werde. Er habe sich einen PC eingerichtet, der kein IPv4 mehr nutzen könne. Schließlich suche er als Entwickler nach Software, die angepasst werden müsse. Im Open Source Umfeld gebe es sehr viel Software, die in der Theorie zwar IPv6-fähig sei, aber ohne IPv4 nicht mehr funktioniere. Er sehe bei den Herstellern momentan kein Interesse, hier aktiv zu werden. Er räumt jedoch ein, dass man seit Windows 7 IPv4 komplett ausschalten könne. Im Anwenderbereich gebe es auch noch Probleme. Als Beispiel zieht er den Browser Firefox heran. Dieser liefe zwar auf seinem IPv6-Arbeitsplatz, aber nur ohne Plug-Ins.

In den Firmennetzen werde IPv4 erst abgelöst werden, wenn die Kosten, ein altes System zu betreiben, zu hoch würden. Er hoffe jedoch, dass IPv6 auch hier relativ schnell Einzug halten werde. Schließlich sei der Management-Aufwand, sowohl IPv4 als auch IPv6 zu betreiben, relativ groß. Heutzutage wolle man nicht mehr IPv4 und IPv6 gleichzeitig auf einem Gerät betreiben (so genannter Dual-Stack-Modus).

Wolfgang Fritsche nimmt sich der Frage, wie lange es IPv4 noch geben werde, an. Es sei hier zwischen Betriebssystem und Anwendung zu unterscheiden. Im Bereich der Betriebssysteme sei man auf einem guten Wege. Letztendlich werde es nur noch den Faktor des Zeitpunkts geben, an dem Kunden ihre Betriebssysteme austauschten. Es gebe sicherlich im öffentlichen Bereich Kunden, die ihre Betriebssysteme in einem längeren Zyklus austauschten. Im privaten

Bereich werde es vielleicht Kunden geben, die dies häufiger täten. Im Bereich des Betriebssystems werde es sicherlich nicht zehn Jahre dauern, hier werde die Mehrheit viel früher IPv6-fähig sein.

Im Anwendungsbereich sehe es jedoch anders aus. Man könne drei Kategorien unterscheiden: Als die Proaktiven fasst er verschiedene Browserhersteller bzw. auch die Firma Acamai, die Content Distribution Services anbiete, zusammen. Diese investierten proaktiv in die neue Technologie, weil sie davon überzeugt seien, dass sie einen Mehrwert bringe.

Dann werde es Hersteller geben, die nur auf Druck umstellten. Als öffentlicher Kunde habe man hier definitiv die Möglichkeit in Ausschreibungen bzw. in Softwarepflegeänderungsverträgen die Unterstützung von IPv6 ab einem bestimmten Zeitpunkt zu fordern.

Schließlich werde es sicherlich Insellösungen für Fachanwendungen geben, wie es **Gert Döring** angesprochen habe. Diese werde es nicht nur im Bereich der Industrie, sondern auch im Bereich des öffentlichen Dienstes geben. Hier werde man sicherlich auch in zehn bis 20 Jahren noch IPv4-Anwendungen vorfinden.

Abg. Gerold Reichenbach (SPD) fragt, ob die Experten glaubten, dass sich im Bereich des Internets ein Schutz vor Angriffen selbstregulatorisch durchsetzen werde oder ob eine Entwicklung wie beim Automobil bis hin zur Automobilzulassung notwendig sei. Lasse sich dies unter Umständen über bestimmte Gremien auch international regeln?

Die zweite Frage, so fährt er fort, befasse sich mit der Portabilität von Daten. Im Rahmen der europäischen Verordnung um den Datenschutz gebe es eine intensive Auseinandersetzung um die Frage der Portabiliät von Daten. Ihn interessiere, ob die Gefahr bestehe, dass Anwender durch eine Entscheidung für einen Gerätehersteller oder für ein integriertes Modell von Software und Hardware an diesen Hersteller gebunden würden. Er denke hier beispielsweise daran, dass

Hersteller bestimmte IP-Adressen in Geräte oder Dienste einprogrammierten. Bestehe die Möglichkeit vorher regulatorisch festzulegen, dass es möglich sein müsse, IP-Adressen mitzunehmen?

Ulrich Kühn fasst zusammen, dass sich die erste Frage mit dem Thema der allgemeinen Betriebssicherheit für diesen Technikbereich auseinandersetze. Dies sei ein wichtiges Ziel, von dem man aber noch weit entfernt sei. Das habe sicherlich damit zu tun, dass es sich in der Regel um Technik handele, die weitaus komplexer sei als beim Automobil. Die Hersteller scheuten solche Zusagen daher und mieden Haftungsfragen.

Dann habe man aber das Ergebnis, dass nach Jahren des normalen Betriebs angeblich verschlüsselte Daten offen zugänglich und dadurch Angriffen ausgesetzt seien. Insofern halte er es für sehr wichtig, hier bessere Standards zu schaffen und diese auch international umzusetzen. Ein wichtiger Faktor, vor dem sich die Hersteller scheuten, sei Transparenz. Der Markt sei hart umkämpft, weswegen oft die „Karte“ der Betriebsgeheimnisse gezogen werde. Selbst für die Aufsichtsbehörden sei es sehr schwierig, einen Einblick in den Quellcode eines Herstellers zu erhalten. Hier sehe er Bedarf, die Hersteller zu stärkerer Offenheit zu verpflichten.

Die Idee der Portabilität von Daten sei sicherlich ein wichtiger Punkt, da auch dadurch der Markt etwas transparenter werde. Er betont, dass auch Datenschutz ein Marktfaktor sein könne, wenn sich Kunden auf Grund von Datenschutzdefiziten von einem Unternehmen abwendeten.

Ob durch feste IP-Adressen solche Portabilitätsbestrebungen oder -regelungen konterkariert würden, sei zu überlegen. In jedem Fall solle auf diesen Punkt geachtet werden. Momentan sehe er kein konkretes Problem, wenn er sich vorstelle, ein Anwender nehme seine Daten beispielsweise von Facebook zu Google mit. Aber er könne sich durchaus vorstellen, dass die Betreiber hier findig seien, um dies doch wieder zu erschweren.

Wolfgang Fritsche erklärt, dass auch der Automobilhersteller, den er beraten habe, diverse Ideen gehabt habe, wie man eine Bankverbindung im Auto herstellen oder eine E-Mail-Funktion anbieten könne, damit ein Kunde möglichst wenig Motivation habe, zu einem anderen Hersteller zu wechseln. Er stellt die Frage in den Raum, was ein Anwender von einer permanent eindeutigen IP-Adresse habe. Bei Bankverbindungen und bei E-Mail sehe er noch einen Sinn, da es um die Inhalte gehe. An anderer Stelle könne er sich dies nicht vorstellen. Außerdem gebe es Regulatoren, die eindeutig sagten, dass eine IP-Adresse kein persönliches Gut sei, sondern von Organisationen wie RIPE vergeben würden. Diese IP-Adressen könnten nicht von einem Hersteller beliebig missbraucht werden, um sie beispielsweise fest in ein Smartphone „einzubrennen".

Bei der zweiten Frage gehe es, so fasst er zusammen, um das Thema geschlossene Systeme und Verantwortung bzw. Haftung der Hersteller auseinandergesetzt. Natürlich habe der Hersteller eine Haftung zu übernehmen. Dennoch übernehme auch ein Fahrzeughersteller keine Haftung mehr, wenn man beliebige Software installiere. Dies sei verständlich. Nichtsdestotrotz könne sich ein Hersteller in gewisser Art und Weise öffnen, um sich zertifizieren zu lassen, dass er Sicherheitsvorschriften umsetze.

In diesem Bereich tue sich auch einiges: Was man in der Flugzeugindustrie für Software Quality Management schon lange gemacht habe, finde nun auch Einzug in den Automobilbereich. Dort gehöre zum Thema Software auch das Thema Netzwerke und IPv6. Hier könnten Praktiken zertifiziert werden, mit denen ein Schutz der Privatsphäre erreicht werden solle.

SV Constanze Kurz wendet sich mit einer Nachfrage an **Wolfgang Fritsche**. Sie bittet ihn zu konkretisieren, ob er Common Criteria Schutzprofile meine.

Wolfgang Fritsche erklärt, dass es sich um Funktionalitätssicherheitsmaßnahmen handle, die im Flugzeugbereich schon lange für Softwareerstellung Anwendung

fänden. Diese qualifizierten, dass eine bestimmte Funktionalität auch wirklich durch die Software erfüllt werde. Welche Funktionalität dies sei, müsse vorher definiert werden. Denkbar wäre zum Beispiel die Gewährleistung dafür, dass für verschiedene Anwendungen sowohl die Anonymität gewahrt werde als auch auf Anwenderwunsch mit einer identifizierbaren Adresse gearbeitet werden könne. Hier seien nicht die Common Criteria gemeint, sondern eine bestimmte Norm.

SV Markus Beckedahl wendet sich an **Ulrich Kühn**. Es gebe ein Urteil des Bundesverfassungsgerichts vom Januar 2012, welches Patrick Breyer erstritten habe (BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. (1 - 192), http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html). Ihn interessiere, welche Auswirkungen die Feststellung, dass dynamische IP-Adressen personenbezogene Daten seien, auf IPv6 habe und ob es regulative Maßnahmen gebe, die der Gesetzgeber treffen müsse.

Ulrich Kühn begrüßt die Frage von **SV Markus Beckedahl**. Man müsse als Datenschützer noch immer argumentieren, dass IP-Adressen personenbezogene Daten seien. Es gebe leider kein Gesetz, in dem dies so klar festgeschrieben sei. Insofern müssten die Datenschützer dies immer relativ aufwendig rechtlich herleiten. Die eine Seite sage, IP-Adressen seien doch gar keine personenbezogenen Daten, weil sie damit frei umgehen wollten. Da die Webserver die IP-Adressen mitschrieben, seien die Informationen vorhanden. Wolle man die Daten nicht speichern, so müsse man aktiv werden. Die Datenschützer forderten die Anbieter auf, diese Logfiles zu bereinigen. Dies sei ein ewiger Kampf. Insofern sei den Datenschützern sehr geholfen, wenn es eine rechtliche Norm gebe, in der zweifelsfrei stehe, dass IP-Adressen personenbezogene Daten seien. Dies sei bisher immer einer juristischen Fachdiskussion anheimgestellt.

Leider griffen auch die Vorschläge der EU-Kommission nicht in die Richtung vor, dass IP-Adressen als personenbezogen Daten anzusehen seien. Dies hätten die Datenschützer dort sehr vermisst.

Zu verschiedenen Fragen komme man gar nicht, etwa wie solle man mit den angefallenen Daten umgehen, wie könne man diese entschärfen, könne man dennoch Geolokalisierung betreiben und dürfe man IP-Adressen vielleicht doch in bestimmen Fällen für die Aufklärung von Sicherheitsvorfällen oder für Strafverfolgung nutzen. Dies liege daran, dass man zunächst über die Frage diskutieren müsse, ob es sich überhaupt um personenbezogene Daten handle. Insofern sei diese Klarstellung ein wichtiger Punkt.

Gert Döring habe sich mit der Frage, ob es sich um personenbezogene Daten handle, im Rahmen der Erstellung seiner schriftlichen Stellungnahme auseinandergesetzt. Letztlich sei der Unterschied zwischen IPv4 und IPv6 bei aktivierten Privacy Extensions vernachlässigbar. Bei der Zuteilung eines statischen Präfixes sei der Anschluss wieder identifizierbar, wie auch bei einer statischen IPv4-Adresse und NAT.

Bei einem dynamischen Präfix mit Privacy Extensions sei der Anschluss nicht als solcher identifizierbar. Bestenfalls sei Provider und Region erkennbar.
Schalte man die Privacy Extensions aus, sei IPv6 hinsichtlich der Nachverfolgbarkeit eines User sehr viel schlimmer als IPv4. In diesem Fall könne ein bestimmtes Gerät wiedererkannt werden und nicht nur ein Anschluss. Des Weiteren sei dieses Gerät auch über Anschlussgrenzen hinweg verfolgbar. Man könne also den gleichen Laptop vom Heimanschluss, in die Firma, zu Freunden und wieder zum Heimanschluss zurückverfolgen. Dies müsse man im Blick behalten. Bei eingeschalteten Privacy Extensions sei IPv6 auf dem gleichen Niveau wie IPv4 – nicht besser, nicht schlechter.

Abg. Jimmy Schulz (FDP) trägt eine Frage vor, die über Twitter gestellt worden sei. Dort wolle man wissen, ob sich die Situation bei staatlichen Überwachungsmaßnahmen durch die Einführung von IPv6 ändere.

Ulrich Kühn erklärt, dass sich diese Frage anders stelle, wenn eine IP-Adresse zum Bestandsdatum werde, weil einem Anschlussteilnehmer diese dauerhaft

zugewiesen werde. Hier seien die rechtlichen Bestimmungen auch andere. Bestandsdaten ließen sich von Bedarfsträgern sehr viel leichter abfragen als Verkehrs- und Nutzungsdaten. Insofern sei dann die Diskussion über die Vorratsdatenspeicherung hinfällig. Er bewerte es als unbefriedigend, wenn lange gesellschaftlich um diese Frage gerungen werde und die Entscheidung durch eine rein technische Entwicklung falle.

Die **Vorsitzende** dankt den Anhörpersonen, den Mitgliedern der Projektgruppe sowie der interessierten Öffentlichkeit für das informative Gespräch. Sie ruft abschließend den Tagesordnungspunkt 2 „Verschiedenes“ auf.

TOP 2 Verschiedenes

Die Vorsitzende weist auf den nächsten Sitzungstermin der Projektgruppe am 11. Juni 2012 von 16 bis 18 Uhr hin. Da es keine weiteren Wortmeldungen gibt, schließt die Vorsitzende die Sitzung um 17.45 Uhr.