Projektgruppe Zugang, Struktur und Sicherheit im Netz

3 Fragen zum Thema „IPv6 - Sicherheitsaspekte“

Fragen an Herrn Ulrich Kühn

- Welche Verbreitung des IPv6-Standards besteht derzeit bzw. wie viele Verbraucher als Endkunden sind von der Erfassung betroffen und wie viele zum Ende dieses Jahres sein? Worauf stützt sich diese Datenlage?

- Die Verbreitung des IPv6-Standards wird von den Datenschutzbeauftragten des Bundes und der Länder kritisch bewertet und es werden Schutzvorkehrungen gefordert. Wie bewerten Sie die grundsätzlichen Einschätzungen aus datenschutzrechtlicher Sicht?

- Welche technischen, organisatorischen und rechtlichen Maßnahmen und Vorkehrungen sind möglich und im Ergebnis am effektivsten, um angesichts des mit IPv6 einhergehenden Endes dynamischer Adressvergabe und des damit einhergehenden Verlustes eines relativen Schutzes der Daten der Bürger einen vergleichbaren, kompensierenden Schutzstandard zu erzielen?

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Enquete-Kommission Internet und digitale Gesellschaft: Projektgruppe Zugang, Struktur und Sicherheit im Netz

3 Fragen zum Thema „IPv6 – Sicherheitsaspekte“

Antworten von **Dipl.-Inf. Ulrich Kühn**, Leiter des Referats für Technikangelegenheiten beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

1. *Welche Verbreitung des IPv6-Standards besteht derzeit bzw. wie viele Verbraucher als Endkunden sind von der Erfassung betroffen und wie viele zum Ende dieses Jahres sein? Worauf stützt sich diese Datenlage?*

Als Experte für Fragen des Datenschutzes und der Datensicherheit verfüge ich über keine eigenen oder unabhängigen Erkenntnisse über die betrieblichen und unternehmerischen Aspekte der IPv6-Umstellung. Meine Antwort stellt daher eine Zusammenfassung der öffentlich verfügbaren Daten dar.

Folgende Quellen wurden dabei berücksichtigt (unter Fokussierung auf die Situation in Deutschland):

- Die Verkehrsstatistiken von DE-CIX (dies ist der deutsche Internet-Austauschknoten und vom Durchsatz her der größte der Welt), http://www.de-cix.net/about/statistics/
- Statistiken des Deutschen IPv6-Rats (https://www.ipv6council.de/ipv6day/ipv6_dashboard.html) und von Google (http://www.google.com/intl/en/ipv6/statistics/) über den Verbreitungsgrad von IPv6

Danach beträgt der IPv6-Verkehr aktuell (Anfang Mai 2012) lediglich ca. 1/1000 des Gesamtverkehrs (ca. 1,6 Milliarden Bits pro Sekunde IPv6 gegenüber ca. 1600 Milliarden Bits pro Se-

www.datenschutz-hamburg.de

E-Mail: mailbox@datenschutz.hamburg.de

Klosterwall 6 - D-20095 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00

kunde IPv4). Würde dieser Verkehr gleichmäßig von den ca. 52 Millionen Internetnutzern in Deutschland stammen, entspräche dies gerade mal der Datenmenge von ein oder zwei E-Mails pro Nutzer und Tag.

Aber natürlich ist IPv6 keineswegs gleichmäßig verbreitet. Im Gegenteil – bislang ist es eher eine Technik für sehr wenige Spezialisten. Google misst aktuell einen Anteil von 0,2% aller deutschen Suchanfragen per IPv6 (bei einem weltweiten Durchschnitt von 0,6%). Laut Deutschem IPv6-Rat haben lediglich drei der deutschen TOP-100-Sites und keines der DAX30-Unternehmen einen IPv6-fähigen Webauftritt.

Ob sich diese Situation bis zum Jahresende wesentlich ändern wird, hängt vorrangig von den großen Zugangsprovidern und deren Marktstrategien ab. Erst wenn diese eine nennenswerte Anzahl von Endkunden (auch) über IPv6 anbinden, wird sich die Gesamtdurchdringung erkennbar erhöhen. Langfristig jedoch werden alle Endkunden und Netzteilnehmer von der Umstellung auf IPv6 betroffen sein.

2. *Die Verbreitung des IPv6-Standards wird von den Datenschutzbeauftragten des Bundes und der Länder kritisch bewertet und es werden Schutzvorkehrungen gefordert. Wie bewerten Sie die grundsätzlichen Einschätzungen aus datenschutzrechtlicher Sicht?*

Zunächst möchte ich feststellen, dass die Einführung von IPv6 von den Datenschutzbeauftragten nicht per se kritisch betrachtet wird. Im Gegenteil werden die damit verbundenen Chancen für die Datensicherheit ebenso gesehen wie vorhandene Risiken.

Das Internetprotokoll IPv4 ist vor über 30 Jahren mit dem Schwerpunkt auf Flexibilität und Übertragungsqualität entstanden. Moderne Fragen der Datensicherheit (etwa Verschlüsselung, Authentifizierung) oder gar des Datenschutzes (etwa Anonymität, Nutzeranalyse) spielten dabei keine Rolle. In einem gewissen Umfang sind diese Aspekte in den Standard IPv6 eingeflossen. Dies wird von Seiten der Datenschutzbeauftragten begrüßt und die Nutzung der entsprechenden Möglichkeiten (zum Beispiel IPsec, Privacy Extensions) eingefordert.

Dabei gilt das Hauptaugenmerk dem sowohl schwächsten als gleichzeitig auch am stärksten betroffenen Teilnehmer in einem IPv6-basierten Internet: dem (privaten) Endnutzer. Dessen Schwäche besteht darin, dass er weitgehend von den technologischen Entscheidungen der Zugangsprovider und Hersteller von Hard- und Software abhängig ist. Hier werben die Datenschutzbeauftragten seit einiger Zeit für Lösungen, die die Prinzipien des *privacy by design* (das heißt frühzeitig in die Technik integrierte Datenschutzmaßahmen) und *privacy by default* (das heißt datenschutzfreundliche Grundeinstellungen) berücksichtigen. Der Nutzer muss kostenneutral und alltagstauglich in der Lage sein, die für sie/ihn aktuell geeigneten Einstellungen zu wählen. Die jüngsten Diskussionen des BfDI mit dem Deutschen IPv6-Rat machen Hoffnung,

dass diese Versuche erste Erfolge zeigen (https://www.ipv6council.de/documents/leitlinien_ipv6_und_datenschutz.html).

Aktuell befindet sich eine umfangreiche Orientierungshilfe zur Einführung von IPv6 in Vorbereitung. Sie wird die Punkte aufgreifen und verfeinern, die bereits in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom September 2011 genannt wurden (http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/82DSK_IPv6.pdf?__blob=publicationFile). Es ist geplant, die Orientierungshilfe im Herbst 2012 zu veröffentlichen.

3. *Welche technischen, organisatorischen und rechtlichen Maßnahmen und Vorkehrungen sind möglich und im Ergebnis am effektivsten, um angesichts des mit IPv6 einhergehenden Endes dynamischer Adressvergabe und des damit einhergehenden Verlustes eines relativen Schutzes der Daten der Bürger einen vergleichbaren, kompensierenden Schutzstandard zu erzielen?*

Ob mit der Einführung von IPv6 das Ende der dynamischen Adressvergabe einhergeht, ist keineswegs gewiss. Zunächst einmal fällt aufgrund der Adressexplosion bei IPv6 lediglich der ökonomische Zwang für diese Form der Adressverteilung weg. Technisch ist sie aber ebenso wie bei IPv4 möglich und dem Grunde nach auch vom Aufwand her vergleichbar.

Andererseits werden häufig die funktionalen Vorteile statischer Adressen genannt. Sie ermöglichen permanente Verbindungen und eine permanente Erreichbarkeit (zum Beispiel für Dienste wie IP-basiertes Fernsehen (IPTV), IP-Telefonie (VoIP) oder den Betrieb eigener Server) und erleichtern den Betrieb von Peer-to-Peer-Netzen ohne zentrale Server. Dort wo ein tatsächlicher Bedarf für solche Anwendungen besteht, wird ein Festhalten an der bisherigen dynamischen Adressvergabe kaum möglich sein.

Würde jedoch generell bei IPv6 auf eine statische Adressvergabe umgestellt, stiege das Risiko, dass Diensteanbietern die Person hinter der IP-Adresse bekannt wird. Sie könnte dann bei jedem Besuch einer Webseite wiedererkannt werden, auch wenn sie sich dort nicht namentlich anmeldet. Dies wäre das Ende jedweder Anonymität im Internet – im Ergebnis eine kleine Vorratsdatenspeicherung durch die Hintertür, weil die IP-Adresse dann als Bestandsdatum dauerhaft gespeichert würde.

Am effektivsten ist es daher aus meiner Sicht, anwendungs- und bedarfsbezogen differenziert vorzugehen. Dort wo keine funktionale Notwendigkeit einer permanenten IP-Adresse besteht, also insbesondere bei der Nutzung von WWW, E-Mail und ähnlichen Diensten, ist weiterhin eine dynamische Adressvergabe wie bei vielen Providern aktuell üblich (das heißt Neuvergabe nach spätestens 24 Stunden) geboten. Bei Diensten wie IPTV oder VoIP, bei denen ein plötzlicher Adresswechsel zu Verfügbarkeitsverlusten führen würde, wäre eine permanente oder nur

mit Zutun des Nutzers wechselnde Adresse auch aus datenschutzrechtlicher Sicht eher akzeptabel. Denn bei diesen Diensten exponiert sich der Nutzer mit seiner IP-Adresse deutlich weniger gegenüber Dritten.

Das bedeutet, dass auch die einzelnen Bestandteile eines konvergenten Telekommunikationsangebots (Triple oder Quad Play) in Hinblick auf die Adressvergaberegeln gesondert betrachtet werden sollten. Aus Sicht des Nutzers ist es zum Schutz seiner Privatsphäre erforderlich, dass die IP-Adresse für das Internet-Surfen regelmäßig automatisch wechselt. Demgegenüber kann diejenige (andere), die dem Zugriff auf das TV-Angebot des Providers dient, seltener, zum Beispiel nur bei Anforderung gewechselt werden.

Ob sich solche Geschäftsmodelle allein durch Marktgeschehen etablieren, ist zweifelhaft. Dauerhaften Schutz kann hier letztlich nur der Gesetzgeber gewährleisten. Er ist aufgrund seiner Verpflichtung zum Schutz des Grundrechts der informationellen Selbstbestimmung dazu aufgerufen, Access-Provider z.B. durch eine entsprechende Regelung im Telekommunikationsgesetz dazu zu verpflichten, kostenneutral eine dynamische Vergabe von IP-Adressen auch unter IPv6 anzubieten. Dies gibt den Access-Providern dann auch die notwendige Rechtssicherheit, insbesondere gegenüber weitergehenden sicherheitspolitischen Forderungen.

Abschließend möchte ich darauf hinweisen, dass zur Vermeidung eines dauerhaft zuordenbaren Identifikators nicht nur die Adressvergabe durch die Provider (also der Präfix) betrachtet werden muss. Ebenso wichtig ist die Berücksichtigung des im Endgerät gebildeten Adressbestandteils (Host Identifier). Nur wenn beide regelmäßig gewechselt werden, ist die permanente Zuordnung der Adresse zu einem Teilnehmer ausgeschlossen. Gerade im Bereich der mobilen Endgeräte besteht hier noch Nachholbedarf durch die Betriebssystemhersteller in Hinblick auf die standardmäßige Aktivierung der sog. Privacy Extensions.