Ständige Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Arbeitskreis Technische und organisatorische Datenschutzfragen

Orientierungshilfe

Datenschutz bei IPv6

Hinweise für Hersteller und Provider im Privatkundengeschäft

Version 1.01

Stand: 26. Oktober 2012

Inhalt

1 Zusammenfassung

Da der verfügbare Adressvorrat der Version 4 des Internet-Protokolls (IPv4) weitgehend aufgeteilt ist, werden viele Betreiber und Anwender von Netzwerktechnik künftig das Internet-Protokoll Version 6 (IPv6) einsetzen. Der mit IPv6 zur Verfügung stehende Adressraum reicht nach derzeitigem Kenntnisstand aus, um jedem heutigen oder künftigen elektronischen Gerät mehrere eigene Adressen zuzuweisen. Bei statischer Adressvergabe wäre jedes dieser Geräte an seiner Adresse wiedererkennbar.

Die Umstellung von IPv4 auf IPv6 wirkt sich somit auch auf Datenschutz und Datensicherheit aus und bietet zahlreiche Gestaltungsmöglichkeiten. Die Datenschutzbeauftragten des Bundes und der Länder begleiten diesen Prozess aktiv und sind bereit, Anwender und Betreiber zu beraten. Die vorliegende Orientierungshilfe wendet sich dabei an Provider mit Endkundenbeziehung sowie Hersteller von Geräten für Privatkunden, da diese von der Adressknappheit zuerst betroffen sein werden.

Die Datenschutzbeauftragten des Bundes und der Länder geben in dieser Orientierungshilfe Hinweise und Empfehlungen zum datenschutzgerechten Einsatz von IPv6, die nachfolgend zusammengefasst werden:

(1) In IPv6 wird eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation ermöglicht, ohne dass zusätzliche Verschlüsselungssoftware eingesetzt werden muss. Voraussetzung ist, dass die verwendete IPsec-Implementation starke Verschlüsselungsalgorithmen beherrscht. Wo dies nicht zutrifft, müssen die Hersteller nachbessern (Abschnitt 4.1).

(2) Um das Tracking von Nutzern zu vermeiden, sollen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Sollte sich ein Provider für die Vergabe eines (einzelnen) statischen Präfixes an einen Endkunden entscheiden, dann muss dieser Präfix auf Wunsch des Kunden gewechselt werden können. Hierzu muss dem Kunden eine einfache Bedienmöglichkeit am Router oder Endgerät zur Verfügung gestellt werden. Verlangt ein Kunde ausdrücklich einen statischen Präfix, so kann auf die Wechselmöglichkeit verzichtet werden. Eine Kombination beider Modelle ist möglich (Abschnitt 4.2).

(3) Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln (Abschnitt 4.2).

(4) Broadcast und Multicast können zur Entwicklung von Protokollen zur unbeobachtbaren Kommunikation genutzt werden (Abschnitt 4.3).

(5) An Routern sollten aus Sicherheitsgründen Broadcast- und Multicast-Pakete im erforderlichen Umfang gefiltert werden (Abschnitt 4.3).

(6) Wenn möglich, sollte DHCPv6 mit Nachrichten-Authentisierung benutzt werden (Abschnitt 4.3).

(7) Multicast-Übertragungen lassen sich zurzeit nur schwer mit IPsec sichern. Abhilfe versprechen bisher nur Protokolle, die noch nicht Stand der Technik sind (Abschnitt 4.3).

(8) Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen (Abschnitt 4.4).

(9) Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten einbauen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können (z. B. alle 10 Minuten) bzw.

einen Wechsel zu bestimmten Ereignissen anstoßen lassen können (z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners, Abschnitt 4.4).

(10) Interface Identifier und Präfix sollten synchron gewechselt werden (Abschnitte 4.2, 4.4).

(11) Wünschenswert wäre darüber hinaus, dass Anwendungsprogramme gezielt eine von mehreren lokalen IPv6-Adressen nutzen und unterschiedliche Adressen mit unterschiedlichen Wechselfrequenzen ausstatten können. Außerdem sollten Betriebssysteme mehrere nicht zusammenhängende Präfixe verwalten können (Abschnitt 4.4).

(12) Sind in einem Endgerät Cryptographically Generated Addresses (CGA) implementiert, so können sie unter sonst gleichen Bedingungen als Ersatz für Privacy Extensions genutzt werden (Abschnitt 4.5).

(13) Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6 fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden (Abschnitt 4.6).

(14) Hersteller, deren Firewalls (Firmware und Systemsoftware) bisher nicht IPv6-fähig sind, sollten entsprechende Updates anbieten (Abschnitt 4.6).

(15) Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte verbessern, soweit erforderlich, beispielsweise durch korrekten Umgang mit Header Extensions und und getunnelten Paketen (Abschnitt 4.6).

(16) Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. IPv6 ermöglicht den verstärkten Einsatz von Peer-to-Peer-Ansätzen, da die Erreichbarkeit von IPv6-fähigen Geräten nicht mehr durch Techniken wie NAT beschränkt werden muss. Softwarehersteller sollten das ihnen innewohnende Datenschutzpotenzial nutzen und sich aktiv an der Entwicklung beteiligen. Hersteller von Netzwerktechnik wie Routern sollten ihre Produkte so gestalten, dass sie mit Peer-to-Peer-Anwendungen kompatibel sind, und bei Produkten, die für Privatkunden gedacht sind, an die Integration geeigneter Peer-to-Peer-Anwendungen denken (Abschnitt 4.7).

(17) Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Solche Dienste funktionieren auch bei statisch zugewiesenen IP-Adressen. Es sind bereits einige breit einsetzbare Systeme verfügbar, jedoch noch nicht für IPv6. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung dieser Dienste darf durch Netzbetreiber nicht blockiert werden (Abschnitt 4.8).

(18) IPv6-Adressen müssen ebenso wie IPv4-Adressen als personenbezogene Daten angesehen werden (Abschnitt 3.5). Da bei IPv6-Installationen Mechanismen zur Adressumsetzung wie Network Address Translation (NAT) oder Proxy eine geringere Rolle spielen werden, ist der Informationsgehalt der Adressen höher als bei IPv4. Individuelle Adressen von Clients werden häufiger in Protokolldaten von Internet-Diensten auftauchen. Hinsichtlich der rechtlichen Bedingungen gibt es keine wesentlichen Unterschiede zu IPv4. Sofern diese keine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus zulassen, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten (Abschnitt 4.9).

(19) Sofern die IPv6-Adresse eines Geräts genutzt werden soll, um dessen (ungefähren) Standort zu ermitteln, gelten hierfür ebenfalls vergleichbare Anforderungen wie bei IPv4. Eine solche Standortermittlung ist für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig (Abschnitte 3.5, 4.9).

(20) Zur wirkungsvollen Anonymisierung von IPv6-Adressen sollten nach derzeitigem Kenntnisstand die unteren 88 bis 96 Bit jeder Adresse gelöscht werden (Abschnitt 3.5).

(21) Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte möglichst vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle wie Teredo. Falls Dual-Stack-Betrieb unbedingt erforderlich ist, muss eine sorgfältige Konfiguration und regelmäßige Aktualisierung der betroffenen Systeme sichergestellt sein. Nicht zuletzt sind die Softwarehersteller von IPv4-only Client-/Server-Produkten in der Pflicht, entsprechende Updates zu liefern, um in Zukunft die Einbindung in ein IPv6-Netzwerk ohne Übergangstechniken zu ermöglichen.

2 Einführung

Viele Betreiber und Anwender von Netzwerktechnik sind dabei oder planen, das Internet-Protokoll Version 6 (IPv6) einzuführen. Grund hierfür ist vorrangig, dass alle von der Vorgängerversion IPv4 nutzbaren Adressen seit 2011 vergeben sind; lediglich regionale Adressverwalter sowie Provider verfügen noch über Bestände, die jedoch ebenfalls knapp werden. Kein Anwender oder Betreiber wird sich dieser Entwicklung entziehen können.

Mit der Einführung von IPv6 wird die Knappheit an Adressen durch einen Überfluss abgelöst, denn es sind nun $2^{128} \approx 3{,}4 \cdot 10^{38}$ Adressen verfügbar. Auch wenn einige davon besonderen Zwecken dienen oder für künftige Anwendungen reserviert sind, so reicht dieser Adressraum nach derzeitigem Kenntnisstand aus, um jedem heutigen oder künftigen elektronischen Gerät mehrere eigene Adressen zuzuweisen. Bei statischer Adressvergabe wäre jedes dieser Geräte an seiner Adresse wiedererkennbar. Damit können leicht Nutzungsprofile zu einem Gerät gebildet und zusammengeführt werden. Um eine Adresse nicht nur einem Gerät, sondern auch einer Person zuordnen zu können, muss häufig nicht einmal der Zugangsanbieter mitwirken. Insbesondere Betreibern von Internetdiensten, die eine Identifikation erfordern, wie Online-Shops oder Soziale Netzwerke, stehen dazu bereits genügend Informationen zur Verfügung.

Die Umstellung von IPv4 auf IPv6 wirkt sich somit auch auf Datenschutz und Datensicherheit aus und bietet zahlreiche Gestaltungsmöglichkeiten. Die Datenschutzbeauftragten des Bundes und der Länder begleiten diesen Prozess aktiv und sind bereit, Anwender und Betreiber zu beraten. Erste Hinweise gaben die Datenschutzbeauftragten in der Entschließung „Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!“[1] und in dem Positionspapier „Datenschutz bei der Einführung des Internet-Prokolls Version 6 (IPv6)“[2]. Das nun vorliegende Papier erläutert und vertieft diese Ansätze.

Die Adressknappheit des noch verwendeten IPv4 wird sich zuerst bei denjenigen Betreibern bemerkbar machen, die Endkunden direkt versorgen. Aufgrund des Wachstums in diesem Marktsegment ist eine Umstellung auf IPv6 hier unvermeidbar, da insbesondere neueren mobilen Endgeräten und Routern mit ständig erreichbaren Diensten wie Internet-Telefonie global eindeutige Adressen zugewiesen werden müssen. Institutionellen Anwendern wie Unternehmen und Behörden stehen mehr Möglichkeiten zur Verfügung, ihre vorhandenen Netzwerke schrittweise umzurüsten. Sie können ihre nach außen angebotenen Services und Gateways vorrangig IPv6-fähig machen und die vielfältigen intern genutzten Geräte später nachziehen. Deshalb wendet sich die vorliegende Orientierungshilfe an Provider mit Endkundenbeziehung sowie Hersteller von Geräten für Privatkunden.

Die vorliegende Orientierungshilfe wurde von einer Arbeitsgruppe des Arbeitskreises Technische und organisatorische Datenschutzfragen der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet. An dieser Arbeitsgruppe waren beteiligt: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (Federführung). Die Autoren danken herzlich folgenden Personen für ihre Mitwirkung und ihre wertvollen Hinweise: Herrn Markus de Brün (Bundesamt für Sicherheit in der Informationstechnik), Frau Christine Arndt, Herrn Dominik Herrmann und Herrn Prof. Dr. Hannes Federrath (Universität Hamburg, Fachbereich Informatik, Arbeitsbereich Sicherheit in Verteilten Systemen) sowie Herrn Dr. Christoph Wegener (wecon.it-consulting).

---

1 http://www.datenschutz-mv.de/datenschutz/themen/beschlue/82_DSK/IPv6.pdf
2 http://www.datenschutz.rlp.de/downloads/oh/Positionspapier_IPv6.pdf

3 Grundlagen

3.1 Aufbau und Notation von IPv6-Adressen

IPv6-Adressen sind 128 Bit lang und bestehen aus einem Präfix und einem Interface Identifier mit je 64 Bit Länge. Folgende Regeln gelten für die Notation von IPv6-Adressen[3]:

Präfix (Bits 127 ... 64)				Interface Identifier (Bits 63 ... 0)			
2001	0db8	0804	a082	0000	0000	0001	0225

Regeln der Notation von IPv6-Adressen:

Langform:	Hexadezimalzahl in Blöcken von 4 Stellen durch Doppelpunkte getrennt
Verkürzungsregeln:	1. In jedem Viererblock können führende Nullen weggelassen werden. 2. Genau ein Mal dürfen aufeinanderfolgende Blöcke aus Nullen weggelassen werden; es bleiben zwei Doppelpunkte als Auslassungszeichen stehen.
Beispiel:	
Langform:	2001:0db8:0804:a082:0000:0000:0001:0225
Kurzform:	2001:db8:804:a082::1:225

Der 64 Bit lange Präfix ist weiter untergliedert, beispielsweise in einen Subnet Identifier (untere 16 Bit) und einen Global Routing Prefix (obere 48 Bit).

3.2 Schutzobjekte

Im Allgemeinen definiert man ein Schutzobjekt als Anwendung, IT-System, Netz, Raum oder Gebäude, aber auch die in einem Datenübertragungssystem transportierten Daten zählen maßgeblich zu dieser Kategorie. Bei IPv6 handelt es sich um ein paketorientiertes, verbindungsloses, transparentes Transportprotokoll. Daher kommen als Schutzobjekte zunächst die übertragenen Daten in Betracht. Außerdem sind alle diejenigen Systeme und Systembestandteile zu berücksichtigen, die das Protokoll implementieren oder durch dessen möglicherweise fehlerhafte Implementationen beeinträchtigt werden können. Unter Transparenz versteht man im Sinne der Kommunikation in Netzwerken, dass ein bestimmter Teil eines Systems zwar vorhanden und in Betrieb, aber ansonsten „unsichtbar“ ist. Er wird in der Regel vom Benutzer nicht wahrgenommen. Da IPv6 viele Eigenschaften seines Vorgängers IPv4 teilt, sind auch die zu betrachtenden Schutzobjekte weitgehend identisch.

Verkehrsdaten

Zu den Verkehrsdaten, auch Verbindungsdaten genannt, zählen Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, wie z.B. Beginn und Ende der jeweiligen Verbindung (Datum und Uhrzeit) und die übermittelten Datenmengen. Diese Daten fallen in IPv6-Netzen bei allen an einer Kommunikation beteiligten Geräten an, beispielsweise bei Endgeräten, Servern, Routern und Firewalls.

Bestandsdaten

Bestandsdaten umfassen die Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Diese dürfen nur erhoben und verwendet werden, soweit dieses zur Erreichung des Zweckes erforderlich ist. In IPv6-Netzen fallen solche Daten vorrangig bei Providern an.

Standortdaten

IPv6-Adressen haben häufig einen geographischen Bezug. Wie schon bei IPv4 werden die Adressen üblicherweise Providern oder anderen großen Organisationen zugewiesen und

[3] RFC 3513

von diesen meist nach geographischen Gesichtspunkten verteilt, um die Wegwahl der Pakete im Netz (das Routing) sinnvoll zu gestalten. Mit IPv6 können die Provider diese Strategie konsequent umsetzen, da ihnen große zusammenhängende Kontingente von IPv6-Adressen zur Verfügung stehen werden. Dadurch wird der Ortsbezug genauer und einfacher ermittelbar sein als bei IPv4. Bei stationären Geräten bzw. Anschlüssen (z.B. DSL) wird der geografische Bezug eher dauerhaft sein, bei mobilen Geräten eher dynamisch.

Inhaltsdaten

Die zu übertragenen Inhalte sind als zentrales Schutzobjekt anzusehen. Werden nicht besondere Sicherheitsmaßnahmen ergriffen, können Anbieter von Telekommunikationsdiensten, möglicherweise aber auch andere Personen oder Stellen diese Daten unbefugt zur Kenntnis nehmen.

Betriebssystemumgebung

Die Betriebssystemumgebungen der Endgeräte und der zur Infrastruktur der beteiligten Dienstleister gehörenden Systeme können durch Fehler oder Manipulationen des IPv6-Protokoll-Stapels beeinträchtigt werden. Solche Probleme sind in IPv6-Umgebungen mittelfristig wahrscheinlicher als bei IPv4, da die Implementationen von IPv6 noch nicht so ausgereift sind wie die von IPv4 und es bisher noch wenig Erfahrung im Umgang mit IPv6 gibt. Die Sicherheit der Betriebssystemumgebung ist wichtig für die Sicherheit der Übertragung und der weiteren Verarbeitung von Kundendaten.

Infrastrukturkomponenten (Proxy, Firewall etc.)

An der Übertragung sind viele Infrastrukturkomponenten beteiligt, wie Proxys und Firewalls. Störungen oder Manipulationen dieser Einrichtungen gefährden die Sicherheit der übertragenen Daten. Deshalb gelten für diese Geräte ähnliche Erwägungen wie für Betriebssystemumgebungen.

3.3 Schutzziele

Alle Datenschutzgesetze fordern, personenbezogene Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen (Datensicherheit). Hinreichende Datensicherheit ist eine Voraussetzung für effektiven Datenschutz. Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, dass personenbezogene Daten nicht in die Hände von Unbefugten gelangen. Die Datensicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. In der Praxis orientiert sich die Datensicherheit heute unter anderem an der ISO/IEC Standard-Reihe 2700x aber auch zunehmend an ISO/IEC 15408 bzw. gemeinsamen Kriterien zur Evaluierung von IT-Sicherheit (bzw. Common Criteria). Dort werden zunächst Schutzziele definiert, die durch geeignete Maßnahmen erreicht werden sollen.

Die klassischen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit beziehen sich nach den genannten Standards auch auf nicht personenbezogene Daten und reichen daher über den Anwendungsbereich dieser Orientierungshilfe hinaus. Diese Verallgemeinerung ist möglich und bietet praktische Vorteile, da die bewährten Methoden der Datensicherheit so für den Datenschutz nutzbar werden. Dennoch lehnen sich die folgenden Definitionen an die Datenschutzgesetze von Bund und Ländern an und beschränken sich auf den Schutz personenbezogener Daten. Zusätzlich zu diesen klassischen Schutzzielen werden im Folgenden weitere datenschutzspezifische Schutzziele eingeführt. Diese sind nicht widerspruchsfrei, sondern müssen mitunter je nach

Anwendungsfall gewichtet werden. Beispiele hierzu sind in den folgenden Abschnitten zu finden.[4]

Verfügbarkeit

Verfügbarkeit ist allgemein definiert als die Gewährleistung, dass personenbezogene Verfahren und Daten zeitgerecht zur Verfügung stehen und diese ordnungsgemäß angewendet werden können. Die Verfügbarkeit der Übertragung über IPv6-Netzwerke entspricht damit der von den jeweiligen Betreibern angegebenen Ausfallsicherheit.

Vertraulichkeit

Vertraulichkeit ist allgemein definiert als die Gewährleistung, dass nur Befugte auf personenbezogene Verfahren und Daten zugreifen können. Im Falle von IPv6 muss ein Bezug sowohl auf den Inhalt der Daten als auch auf die näheren Umstände der Kommunikation (Verbindungsdaten) hergestellt werden. Nur Befugte dürfen personenbezogene Daten und deren Kommunikationsverlauf zur Kenntnis nehmen, sei es zu Abrechnungszwecken oder zur Behebung von Störungen und Fehlern.

Vertraulichkeit und Verfügbarkeit stehen teilweise in Widerspruch zueinander. Für einen Unbefugten müssen personenbezogene Daten dauerhaft nicht verfügbar sein.

Integrität

Integrität ist allgemein die Gewährleistung, dass personenbezogene Daten in IT-Verfahren unverändert bleiben. Im Falle des Einsatzes von IPv6 bedeutet dies, dass die Inhaltsdaten und Verbindungsdaten unverändert erhalten bleiben bzw. jede Veränderung erkennbar wird. Es geht hierbei um Instanz- und Datenauthentisierung. Um die Identität des Absenders (bzw. des absendende Gerätes) anhand der Quell-IP-Adresse bei einer IP-Kommunikation feststellen zu können, muss das Protokoll das Schutzziel sichere Sende-Instanz garantieren können. Kann ein Angreifer die Quell-IP-Adresse fälschen und somit eine falsche Identität vortäuschen, ist eine sichere Kommunikation nicht mehr möglich. IPv4 war bereits für das sogenannte IP-Spoofing anfällig, bei IPv6 sind unter bestimmten Umständen ebenfalls solche Angriffe denkbar. Dadurch kann ein Angreifer sich auch Zugang zu einem Netzwerk verschaffen, wodurch er dann Daten lesen, verändern, umleiten oder Daten löschen kann.

Zurechenbarkeit

Zurechenbarkeit ist die Zusicherung, dass den Aktionen in einem System jeweils eine verantwortliche Person oder ein auslösendes Systemelement zugeordnet werden kann. In der Netzwerk- und Kommunikationstechnik wird in diesem Zusammenhang oft auch von dem Schutzziel der Nichtabstreitbarkeit gesprochen.

Revisionssicherheit, Transparenz

Unter Revisionssicherheit und Transparenz wird allgemein die Zusicherung verstanden, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. Hierzu sind bei IPv6 entsprechende Protokolle vorhanden. Unter bestimmten Umständen kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise übertragen hat. Auch die Frage des Auflösens, wer wann welche IP-Adresse verwendet hat, ist hierunter zu verstehen.

Anonymität, Unbeobachtbarkeit

Die Schutzziele Anonymität und Unbeobachtbarkeit stehen in direktem Zusammenhang mit dem Datenschutz. Anonymität bedeutet, dass die Kommunikation ohne Aufdeckung der

---

[4] Die Systematik der klassischen und der datenschutzzpezifischen Schutzziele wird genauer beschrieben in Pfitzmann/Rost: Datenschutz-Schutzziele - revisited. In: Datenschutz und Datensicherheit 6/2009, S. 353 ff.

Identität der Kommunizierenden, durchgeführt werden kann. Dies ist neben der Vertraulichkeit ein zentrales Anliegen des Datenschutzes und bei IPv6 genauso wie bei IPv4 ohne zusätzliche Verfahren oder Maßnahmen nicht zu gewährleisten. Unbeobachtbarkeit bedeutet, dass über die Anonymität hinaus sogar die Tatsache der Kommunikation vor allen Unbeteiligten verborgen wird.

Damit stehen sowohl Anonymität als auch Unbeobachtbarkeit in Widerspruch zur Zurechenbarkeit. Aus Datenschutzsicht ist dieser Widerspruch im Sinne des Betroffenen zu lösen. So kann es sinnvoll sein, dass ein Nutzer eines Portals seine Identität und den Ort verheimlicht, an dem er sich gerade befindet. Trotzdem könnte er zur Bezahlung eines kostenpflichtigen Dienstes ein Pseudonym nutzen, das bei fehlgeschlagener Zahlung zur Offenlegung seiner Identität führt.

Unverkettbarkeit

Auch die Unverkettbarkeit ist ein typisches Schutzziel des Datenschutzes. Unverkettbarkeit heißt, dass Kommunikationspartner und Dritte Handlungen eines Nutzers nicht mit früheren Handlungen desselben Nutzers in Zusammenhang bringen können. Bei der Nutzung von IPv6 besteht grundsätzlich die Möglichkeit, solche Zuordnungen anhand der IP-Adresse vorzunehmen.

Unverkettbarkeit kann damit ebenso wie Anonymität und Unbeobachtbarkeit dem Schutzziel der Zurechenbarkeit widersprechen.

3.4 Bedrohungen

Im Internetprotokoll Version 6 gibt es spezifische Risiken und Bedrohungen für die oben genannten IT-Sicherheits- und Datenschutz-Grundwerte.

Personenbezogene Zuordnung der IP-Adresse und Profilbildung

Wegen der Knappheit der IP-Adressen in der Internet-Protokoll-Version 4 und um Netzwerke mit mehreren Rechnern an das Internet anbinden zu können, wurde neben der dynamischen Adressvergabe auch Network Address Translation (NAT)[5] eingeführt. Hierbei können mehrere Rechner mit dem Internet über nur eine einzige im Internet sichtbare Adresse verbunden werden, wobei NAT diese öffentliche IP-Adresse auf die nicht-öffentlichen Adressen der Rechner in dem angeschlossenen Netzwerk umsetzt. Der einzelne Rechner ist bei IPv4 durch diese Maßnahmen z.B. bei Verbindungen zu Webservern nicht dauerhaft und damit direkt für den anderen Kommunikationspartner durch die verwendete IP-Adresse eineindeutig identifizierbar. Bei IPv6 sind NAT sowie die dynamische IP-Adressvergabe durch die Provider wegen des 2^{128} IP-Adressen umfassenden Adressraumes obsolet geworden (siehe auch Abschnitt 4.2). Bei Verwendung von festen Adress-Präfixen oder festen Interface Identifiern sind IPv6-Adressen z.B. bei der Verwendung von mobilen Endgeräten sehr oft direkt einzelnen Personen zuzuordnen. Bei mobilen IPv6-Teilnehmern hat dies aber auch zur Folge, dass Geodaten[6] die Bildung eines Bewegungsprofils ermöglichen. Die Zuordnungen von IP-Adresse und Geodaten können in diesem Fall zu einem Bewegungsbild des Betroffenen genutzt werden. Dies gilt es zu verhindern. Auch Zuordnungen einer IP-Adresse zu einem Dienst und damit die Erstellung eines Nutzungsprofils wären möglich.

Mittels protokollierten Verbindungsdaten von IPv6-Teilnehmern ist es zudem möglich, personenbezogenes Verhalten zu Nutzungsprofilen zusammenzufassen.

Dies hat die Bedrohung der Schutzziele der Anonymität, Unbeobachtbarkeit und Unverkettbarkeit zur Folge.

---

[5] siehe http://de.wikipedia.org/wiki/Network_Address_Translation

[6] Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet (Art. 3 Nr. 2 Richtlinie 2007/2/EG - „INSPIRE-Richtlinie“).

Risiko Gruppenkommunikation und IPsec

Eine Schwachstelle bei der Verwendung von Multicast-Adressen zur Gruppenkommunikation im Zusammenhang mit IPsec (siehe Abschnitt 4.3) kann dazu führen, dass Kommunikationspartner falsche Identitäten vorgeben können.

Kommt bei IPsec z.B. „Pre Shared Keying“ zum Einsatz, so kann dies durch das Bekanntwerden des Schlüssels den Verlust der Vertraulichkeit bezüglich aller beteiligten Kommunikationspartner zur Folge haben. Es droht neben dem Verlust der Vertraulichkeit auch ein Verlust der Instanzauthentisierung und damit von Integrität oder Zurechenbarkeit.

3.5 Rechtsgrundlagen[7]

Die Umstellung auf den Standard IPv6 wird nicht nur die beschriebenen technischen Änderungen zur Folge haben. Aus diesen technischen Änderungen ergeben sich unmittelbar rechtliche Folgen.

Personenbezug von IP-Adressen

Ob IP-Adressen personenbeziehbare Daten sind, ist in Rechtsprechung und juristischer Literatur immer noch umstritten. Aus Sicht der Aufsichtsbehörden für den Datenschutz besteht jedoch kein Zweifel an der Datenschutzrelevanz dieser Daten[8]. Es ist zu erwarten, dass diese Streitfrage künftig an Bedeutung verlieren wird.[9]

IP-Adressen werden den Nutzern von ihrem jeweiligen Access-Provider zugeteilt. Dieser speichert, welchem seiner Kunden er zu welchem Zeitpunkt welche IP-Adresse zugeteilt hat. Während der Speicherdauer kann der Access-Provider den Personenbezug herstellen, weshalb es sich für ihn unzweifelhaft um personenbezogene Daten handelt.[10] Bei Flatrate-Tarifen ist eine Speicherung derzeit nur noch für maximal sieben Tage zulässig.[11]

Für andere Personen als den Access-Provider ist zwischen dynamischen und statischen IP-Adressen zu unterscheiden. Bei statischen IP-Adressen wird dem Nutzer bei jeder Anmeldung zur Internetnutzung beim Access-Provider die gleiche IP-Adresse zugeteilt. Wenn ein Nutzer mit statischer IP-Adresse sich zu irgendeinem Zeitpunkt identifiziert, zum Beispiel bei der webbasierten Nutzung eines E-Mail-Kontos mit personalisierter Adresse (Vorname.Nachname@Provider.de), weiß der Anbieter, wer sich hinter der statischen IP-Adresse verbirgt. Er kann dann den Nutzer bei jedem weiteren Besuch auf dieser oder anderer Webseiten des Anbieters nicht nur als denselben wiedererkennen, er weiß auch, wer sich hinter der IP-Adresse verbirgt. Dies gilt für jedes Angebot im Internet, bei dem eine Identifizierungspflicht besteht. Deswegen ist nach allgemeiner Ansicht bei statischen IP-Adressen immer von einer Personenbeziehbarkeit des Datums auszugehen.[12]

Bei dynamischen IP-Adressen wird dem Nutzer bei jeder Anmeldung zum Internet eine neue Adresse aus dem Adresspool des Access-Providers zugeteilt. Ob die IP-Adresse auch für

---

7 Gekürzte und leicht geänderte Fassung von: Freund/Schnabel, MMR 2011, 495 ff., abrufbar unter http://www.datenschutz-hamburg.de/uploads/media/IPv6_Aufsatz_in_MMR-08-2011.pdf

8 siehe etwa den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund über „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile

9 So hat auch der Europäische Gerichtshof jüngst IP-Adressen als personenbezogene Daten angesehen (Urteil C-70/10 vom 24. November 2011, Rn 51).

10 Schnabel, K&R 2009, 358 ff., Fn. 22; Härting, CR 2008, 743, 745; Voigt, MMR 2009, 377, 379; Roßnagel/Banzhaf/Grimm, Datenschutz im Electronic Commerce, 2003, 154 m.w.N.

11 OLG Frankfurt, MMR 2010, 645 ff.

12 Schnabel, in: Koenig/Braun/Bartosch/Romes, EC Competition and Telecommunications Law, 2009, 533; Weichert, in: Däubler/Klebe/Wedde/ders., BDSG, 3. Aufl. 2010, § 3, Rn. 14; differenzierend: Voigt, MMR 2009, 377, 380.

Telemedienanbieter, die keinen Zugriff auf die Zuordnungsdatei des Access-Providers haben, als personenbezogenes Datum zu bestimmen ist, hängt von einer Reihe von Faktoren ab und kann sich durch verschiedene, auch außerhalb ihres eigenen Dienstes liegende Begleitumstände ändern. Zur Vermeidung datenschutzrechtlicher Probleme ist daher eine Behandlung als personenbezogene Daten geboten.

Webtracking-Dienste

Beim Webtracking wird individuelles Surfverhalten statistisch ausgewertet. Dazu werden die Aktivitäten von Internetnutzern, welche zum Beispiel über Cookies wiedererkannt werden, in Profilen gespeichert, die zumeist auch die jeweilige IP-Adresse enthalten. Um diese datenschutzgerecht zu anonymisieren, fordern die Datenschutzaufsichtsbehörden bei IPv4-Adressen – analog zur Rufnummernkürzung im Telekommunikationsbereich – die Kürzung um die letzten 8 Bit[13], empfohlen werden 16 Bit[14]. Fraglich ist, wie diese Anforderung sinnvoll auf IPv6-Adressen übertragen werden kann. Ein sinnvoller Kompromiss liegt in der vollständigen Löschung des Interface Identifiers und einer Kürzung des verbleibenden 64-Bit-Präfixes. Dabei ist dann im Wege einer Abschätzung davon auszugehen, dass das 64-Bit-Präfix aus einem (mindestens) 48 Bit langen Global Routing Präfix und einem entsprechend (höchstens) 16 Bit langen Subnet Identifier besteht.[15] Dann kann auch der bei Normalanwendern ohnehin nicht genutzte Subnet Identifier verworfen werden, die verbleibenden 48 Bit des Global Routing Präfix stehen im Wesentlichen einer IPv4-Adresse gleich. Eine Kürzung um mindestens 8 Bit erscheint hier erforderlich, um nicht hinter den status quo der Anonymisierung bei IPv4-Adressen zurückzufallen. Besser wäre eine Kürzung um 16 Bit.[16]

Vorratsdatenspeicherung

Am 2.3.2010 hat das Bundesverfassungsgericht (BVerfG) über die Vorratsspeicherung von Telekommunikations-Daten entschieden und die deutsche Umsetzung der Vorgaben der Richtlinie 2006/24/EG als verfassungswidrig verworfen.[17] Inhalt der Richtlinie und der deutschen Umsetzung war unter anderem die Speicherung der Zuordnung der dynamischen IP-Adressen durch den Access-Provider für sechs Monate auf Vorrat. Statische IP-Adressen sind als Bestandsdaten nach § 3 Nr. 3 Telekommunikationsgesetz (TKG) einzuordnen.[18] Für sie gilt die datenschutzrechtliche Löschpflicht nach § 96 I Satz 3 TKG nicht, da diese sich auf Verkehrsdaten bezieht. Für Bestandsdaten gilt § 95 III TKG, wonach Bestandsdaten erst mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen sind. Auskünfte über Bestandsdaten sind für Ermittlungsbehörden nach § 113 TKG ohne richterliche Anordnung möglich[19]. Bei einer ausschließlich statischen Vergabe von IP-Adressen wäre eine Vorratsdatenspeicherung von IP-Adressen bei momentaner Gesetzeslage auch ohne Gesetzesänderung Realität.

Rechtliche Verpflichtung zur dynamischen Vergabe von IP-Adressen?

Die Vergabe von IP-Adressen durch Access-Provider an Kunden unterliegt dem TKG.[20] Das Gesetz enthält aber keine ausdrücklichen Vorgaben zur Frage, ob Kunden aus

---

13 Kühn, DuD 2009, 747 f.

14 So das Unabhängige Landeszentrum für den Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/ip-adressen/.

15 Großorganisationen werden ausnahmsweise Präfixe erhalten, die kürzer als 48 Bit sind. Für diese Fälle kann wegen der dann sehr großen Zahl der dahinter stehenden Rechner die hier beschriebene Vorgehensweise unverändert angewandt werden.

16 Ausführlich Freund/Schnabel, MMR 2011, 495, 497 f.

17 NJW 2010, 833 ff.; siehe dazu Hornung/Schnabel, DVBl. 2010, 824, 827 f.

18 Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, § 95 TKG, Fn. 3; Graf, in: Beck-OK, 2011, § 100a StPO, Rn. 14.

19 Siehe dazu aber BVerfG, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 119 ff.

20 Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, § 91 TKG, Rn. 5 m.w.N.

Datenschutzgründen statische oder dynamische Adressen zuzuteilen sind. Deshalb wird in der Literatur eine Gesetzesänderung gefordert, um Access-Provider zur dynamischen Vergabe von IP-Adressen zu verpflichten.[21] Andere Stimmen gehen davon aus, dass bereits aufgrund der bestehenden Gesetzeslage von einer Pflicht zur dynamischen Adressvergabe auszugehen ist.[22]

---

21 So Freund/Schnabel, MMR 2011, 495, 499.
22 Nietsch, CR 2011, 763, 767 f.

4 Maßnahmeempfehlungen

4.1 IPsec

Das kryptographische Protokoll IPsec (Internet Protocol Security) wurde von der Internet Engineering Task Force (IETF) für IPv4 und IPv6 entwickelt und für IPv6 zum verbindlichen Protokollbestandteil erklärt. Die Einordnung in die 7 Schichten des ISO-Referenzmodells gestaltet sich wie folgt: IPsec ist in Schicht 3 angesiedelt, Secure Sockets Layer (SSL) wird Schicht 4 zugeordnet. Weil das Internet-Protokoll der Version 4 zunächst keine vergleichbaren Sicherheitsmechanismen hatte, wurde IPsec auch für IPv4 nachträglich spezifiziert. Die Funktionen von IPsec sind standardisiert.[23] IPsec kann zur Gewährleistung von Integrität und Vertraulichkeit entweder als Ende-zu-Ende-Protokoll direkt zwei Kommunikationspartner oder etwa zwei Subnetze miteinander verbinden. Es sind auch Konfigurationen möglich, bei denen ein Host mit einem Subnetz verbunden wird. Weiter ist zwischen einer Instanz- und einer Daten-Authentisierung zu unterscheiden (transport vs. tunnel mode). Im Transportmodus wird ein IPsec-Header zwischen dem IP-Header und den Nutzdaten eingefügt und der normale IP-Header bleibt für das weitere Routing unverändert. Im Tunnelmodus hingegen werden die ursprünglichen Pakete verschlüsselt und in neuen Paketen gekapselt. Die Instanzenauthentisierung kann neben einer Pre-Shared-Key-Authentisierung mit nur einem gemeinsam bekannten Geheimnis auch mittels einer zertifikatsbasierten Authentisierung mit X.509 Zertifikaten erfolgen. Bei der Methode mit Zertifikaten kann das Vertrauensverhältnis mittels CAs (Certification Authorities) durch den Aufbau einer Public Key Infrastruktur (PKI) hergestellt werden. Certification Authorities können neben der vertrauenswürdigen Ausstellung von Zertifikaten auch ungültig gewordene sperren.

Die beiden Sicherheitsexperten Bruce Schneier und Niels Ferguson kritisieren neben der Art der Entstehung von IPsec vor allem die hohe Komplexität und damit Fehleranfälligkeit.[24] Allerdings kommen die beiden Sicherheitsexperten auch zu dem Schluss, dass IPsec das ursprüngliche IP nach derzeitigem Stand der Technik „am besten“ absichert. Die gleiche Quelle nennt auch ein mögliches Sicherheitsproblem von IPsec wegen des möglichen Einbaus von Backdoors[25] und Seitenkanalattacken[26] in die Implementierung von IPsec in dem Betriebssystem OpenBSD und einigen seiner Derivate entsprechend einer Behauptung von Gregory Perry. Die Entwickler von OpenBSD konnten nach einem ersten Code-Review jedoch anscheinend keine Anzeichen finden, die diese Behauptungen stützen würden.

Ein weiteres Problem ergibt sich bei der Gruppenkommunikation mittels Multicast-Adressen (siehe Abschnitt 4.3). Sollen Multicast-Pakete verschlüsselt oder authentisiert werden, so müssen alle Absender und Listener den gleichen Schlüssel haben. Hierdurch kann nun aber jeder Absender oder Listener erfolgreich „authentisierte“ Pakete versenden, deren Source-Adresse nicht seine eigene ist. Dies hat den Verlust der Instanzenauthentisierung zur Folge.

Da kryptographische Algorithmen zusätzliche Rechenkapazitäten benötigen, liegt es nahe, dass der Einsatz von IPsec die Verwundbarkeit für Denial of Service Angriffe erhöht. Problematisch ist außerdem, dass Hersteller von IPsec-Implementationen auf starke Verschlüsselungsalgorithmen komplett verzichten dürfen und stattdessen nur den leeren Null-Algorithmus[27] einbauen müssen.[28] Positiv zu sehen ist, dass durch den Wegfall von NAT (Network Address Translation) die Protokolle und Implementierungen von IPsec für IPv6 einfacher sind als in Version 4.

---

[23] RFC 2401, 4301 und weitere dort referenzierte Standards
[24] http://de.wikipedia.org/wiki/IPsec
[25] http://de.wikipedia.org/wiki/Backdoor
[26] http://de.wikipedia.org/wiki/Seitenkanalattacke
[27] http://de.wikipedia.org/wiki/NULL-Algorithmus
[28] RFC 4835, Abschnitt 3.1.1

In IPv6 wird durch die Verwendung von geeigneten IPsec-Implementationen eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation ermöglicht, ohne dass zusätzliche Verschlüsselungssoftware eingesetzt werden muss. Voraussetzung ist, dass die verwendete IPsec-Implementation starke Verschlüsselungsalgorithmen beherrscht. Wo dies nicht zutrifft, müssen die Hersteller nachbessern.

4.2 Vergabe von Adress-Präfixen

Der Provider vergibt bei IPv6 nur noch den ersten Teil der Adresse, das sog. Präfix. Den zweiten Teil der Adresse (Interface Identifier) erstellt jedes Endgerät entweder selbst oder erhält ihn von einem DHCPv6-Server[29]. Präfix und Interface Identifier bilden zusammen die vollständige IPv6-Adresse (siehe Abschnitt 3.1).

Im Vergleich zu IPv4 vergrößert IPv6 den Adressraum um den Faktor 2^{96}. Mit dieser Erweiterung des Adressraumes ändert sich auch die grundlegende Strategie der Adressverteilung. Es ist zukünftig möglich, jedes an das Internet angeschlossene Gerät mit einer eigenen dauerhaften Adresse zu versehen. Zudem müssen sich die einzelnen Endgeräte auch nicht mehr hinter Infrastrukturkomponenten wie Routern, NAT-Gateways oder Proxys „verstecken“. Damit kann die Anonymität der Internetnutzung schlechter als bei IPv4 gewährleistet werden.

Im folgenden werden verschiedene Ansätze zur Präfixvergabe durch den Provider vorgestellt. Außerdem werden Empfehlungen gegeben, wie diese Methoden datenschutzgerecht ausgestaltet werden können. Die Vergabe des Interface Identifiers wird in den Abschnitten 4.4 und 4.5 betrachtet.

Statische Präfixvergabe

Sollte sich ein Provider für die Vergabe eines (einzelnen) statischen Präfixes an einen Endkunden entscheiden, dann sollte dieser Präfix auf Wunsch des Kunden gewechselt werden können. Hierzu sollte dem Kunden eine einfache Bedienmöglichkeit am Router oder Endgerät zur Verfügung gestellt werden. Es reicht nicht aus, dass ein Kundenanschluss nur dann mit einem neuen Präfix versorgt, wenn der Anschluss eine bestimmte Zeitdauer vom System getrennt war. Nach derzeitigem Kenntnisstand müsste der Kunde sein System mehrere Stunden oder Tage außer Betrieb nehmen. Außerdem sichert kein Provider eine Frist zu, nach der der Adresswechsel sicher eintritt.

Verlangt ein Kunde ausdrücklich einen statischen Präfix, so kann auf die Wechselmöglichkeit verzichtet werden. Dies könnte zum Beispiel der Fall sein, wenn der Kunde selbst (auf seinen eigenen Endgeräten) einen Dienst (z.B. ein Internetangebot) zur Verfügung stellen möchte, welcher unter einer festen Adresse verfügbar sein soll.

Gleichzeitige Vergabe statischer und dynamischer Präfixe pro Anschluss

Auch die Vergabe mehrerer statischer und dynamischer Präfixe pro Anschluss ist eine denkbare Variante.

In diesem Fall könnte je eine Adresse für einen unterschiedlichen Dienst verwendet werden. Ein konkretes Anwendungsbeispiel hierfür ist das klassische „Triple-Play“ welches zum Beispiel von vielen Kabelnetzbetreibern angeboten wird. Demnach würde jeder Dienst (Telefon, Internet, Fernsehen) mit einem eigenen Präfix versehen werden, welcher vom Router im Haushalt des Endkunden verwaltet wird. Durch diese Vorgehensweise kann eine datenschutzfreundliche Ausgestaltung der Präfixvergabe gewährleistet werden, indem man unterschiedliche Strategien für die verschiedenen Präfixe verwendet. Zum Beispiel könnte man das Präfix für den Internetzugang häufiger wechseln oder die Präfix-Wechsel-Frequenz durch den Kunden bestimmen lassen, wohingegen die Präfixe für Telefon und Fernsehen

[29] Der DHCPv6-Server kann, wie schon bei IPv4, Zusatzfunktion eines Routers sein.

nicht zwangsläufig gewechselt werden müssen, da diese Dienste bei einer Adressänderung zumindest kurzzeitig unterbrochen würden.

Auch für den Internetzugang ist die parallele Vergabe mehrerer Präfixe denkbar. So kann ein Internetanschluss gleichzeitig mit einem statischen und einem oder mehreren dynamischen Präfixen ausgestattet werden.[30]

Dynamische Präfixvergabe

Bei IPv4 ist die dynamische Adressvergabe seit langem üblich. Sie ist auch bei IPv6 anwendbar und führt dazu, dass der jeweilige Provider für jeden von ihm vergebenen Präfix ermitteln kann, welchem seiner Kunden er zugeteilt war. Andere Netzteilnehmer können Präfixe mit Identitäten nur aufgrund von Zusatzinformationen wie Login-Daten auf einer Website verknüpfen. Eine so gefundene Zuordnung bleibt gültig, bis das Präfix gewechselt wird.

Diese Variante ist nicht immer die technisch eleganteste Lösung, denn sie eignet sich nicht für jeden Anwendungsfall. Webseiten-Hosting ist nur ein Beispiel für Anwendungen, bei denen ein dynamisches Präfix eher hinderlich ist, da die Dienste nicht direkt und nicht immer unter der selben Adresse erreichbar sind. Sicherlich ist diese Vergabemethode für Endanwender im Privatkundenbereich in den allermeisten Fällen sehr gut geeignet, da sie ein hohes Maß an Dynamik im Präfix aufweist und dort in der Regel keine Anforderungen an dauerhaft feste Adressen bestehen. Die dynamische Vergabe stellt zudem für die Access-Provider eine äußerst flexible Lösung dar, da sie vergleichsweise kurzfristige Änderungen an der Verteilung der Adressen erlaubt.

Risiken und Schutzmaßnahmen

Tracking

Da bei IPv6 häufig auf NAT verzichtet werden wird, werden die Adressen der Endgeräte in der Regel nicht mehr von Routern verschleiert. Dieser Effekt ist aber bereits bei IPv4 im Privatkundenbereich vernachlässigbar, da hier nur wenige Nutzer mit wenigen Geräten jeweils einen Anschluss nutzen. Möglichkeiten zum Tracking von Benutzern bietet IPv6 eher durch statische Adresspräfixe oder Interface Identifier. Ist dem Kommunikationspartner die Identität des Benutzers bekannt, so ist das Tracking des Nutzers anhand dieser Identität möglich.

Wenn die Struktur eines Netzwerkes ermittelt werden kann, sind damit auch Einbußen in der IT-Sicherheit verbunden, weil beispielsweise bestimmte, in ein internes Netz integrierte Komponenten, gezielt angegriffen werden könnten. Außerdem ist ein Informationsgewinn über die Art und Zahl der verwendeten Endgeräte (siehe Abschnitt 4.4) möglich.

Ein relevantes Tracking-Risiko lässt sich prinzipiell nur dann senken, wenn sowohl Präfix als auch Interface Identifier (siehe Abschnitt 4.4) dynamisch vergeben und in regelmäßigen Abständen gewechselt werden oder wenn der Kunde Anonymisierungsdienste (siehe Abschnitt 4.8) verwendet. Die dynamische Adressvergabe ist nur dann voll wirksam, wenn Präfix und Interface Identifier gleichzeitig gewechselt werden, da Diensteanbieter ansonsten Nutzerdaten anhand des jeweils unveränderten Teils miteinander verketten können.

Geolocation

IP-Adressen können immer einem Besitzer zugeordnet werden. Es handelt sich bei den Besitzern häufig um Internetprovider, Universitäten und ähnliche Einrichtungen, die meist nicht nur eine einzelne IP-Adresse, sondern einen ganzen Adressraum verwalten. Der Besitzer einer Adresse kann frei entscheiden, welchem Netzknoten welche Adresse zugeteilt wird. Obwohl die Zuteilung prinzipiell schnell geändert werden kann, wird von dieser

---

[30] Donnerhacke, L.: IPv6 und der Datenschutz. Heise Netze, 10. November 2011, http://www.heise.de/netze/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html

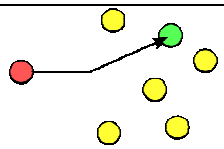
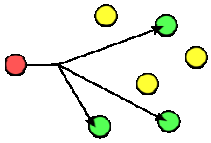
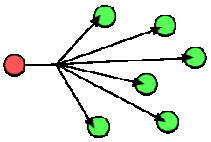
Möglichkeit nur selten Gebrauch gemacht werden, nicht zuletzt, da der Verwaltungsaufwand nicht unerheblich ist. Sollte die Geoposition einer IP-Adresse (als Standort des Geräts, dem die Adresse zugeteilt wurde) bekannt sein, kann man davon ausgehen, dass diese auch Wochen später noch unverändert ist. Da die regionalen Einwahlknoten von Internetprovidern häufig einen festen IP-Adresspool besitzen, funktioniert das Verfahren auch bei dynamischer Adress-Vergabe.

Lösen lässt sich dieses Problem durch die Dynamisierung der Präfixvergabe von IPv6. Zusätzlich sind die Besitzer der Adressen angehalten, die Adressen von Knoten und sonstigen Infrastrukturkomponenten zufällig aus dem ganzen vorhandenen Pool auszuwählen sowie einen Wechselturnus zu etablieren. Ansonsten helfen nur Anonymisierungsdienste (siehe Abschnitt 4.8).

4.3 Multicast

Das Thema Multicast spielt bei IPv6 vor allem im lokalen Netzwerk eine wichtigere Rolle als bei IPv4 und verdient daher auch bei der Betrachtung von Datenschutz und Datensicherheit eine größere Aufmerksamkeit.

Verschiedene Formen der Nachrichtenübertragung können wie folgt veranschaulicht werden:

Übertragungsform	Charakteristik	Veranschaulichung[31]
Unicast	Der Sender schickt die Nachricht an genau einen Empfänger. Dies ist die „normale“ Form der IP-Kommunikation.	
Multicast	Der Sender schickt die Nachricht an eine Gruppe von angemeldeten Empfängern.	
Broadcast	Der Sender schickt die Nachricht an alle Empfänger (nur im LAN möglich).	

Das Verhältnis von Broadcast zu Multicast hat sich von IPv4 zu IPv6 gewandelt. Während Broadcast-Adressen bei IPv4 eine entscheidende Rolle spielen (z.B. für Dienste wie DHCP), wurden sie bei IPv6 komplett abgeschafft; Broadcast ist unter IPv6 nicht möglich[32]. Die entsprechenden Aufgaben werden bei IPv6 über Multicast abgewickelt, welches wiederum unter IPv4 eine geringere Bedeutung hat.

Aus Sicht des Senders unterscheidet sich Multi- bzw. Broadcast von Unicast lediglich in der Adressierung. Ein höherer Aufwand (z.B. mehr Bandbreite) entsteht nicht. Allerdings müssen in Verteilern (Switche, Router) Pakete ggf. vervielfältigt werden.

Anwendungsbereiche von Multicast liegen neben Verwaltungsaufgaben im lokalen Netz bei Diensten wie Videokonferenzen oder IPTV (Internet Protocol Television). Hierfür werden

---

[31] Quelle: http://de.wikipedia.org/wiki/Multicast

[32] Dies gilt nur auf IP-Ebene. Ein darunterliegendes Übertragungsprotokoll wie Ethernet kann einen Broadcast-Modus bereitstellen, der dann allerdings von IPv6 nicht genutzt wird.

gesonderte, multicast-fähige Teilnetze des Internets (bei IPv6 z.B. M6Bone[33]) oder geschlossene Netze genutzt.

Multicast bei IPv6

Multicast-Adressen beginnen bei IPv6 sämtlich mit „FF“. An diese Kennzeichnung schließen sich Flags und eine Scope-Kennzeichnung an:

FF (8 Bits)	Flags (4 Bits)	Scope (4Bits)	Group Identifier (112 Bits)

Die Flags legen u.a. fest, ob es sich um eine fest definierte[34] oder eine temporäre Multicast-Adresse handelt. Die Scope-Angabe bestimmt die Reichweite der Adresse; definiert sind:

Wert	Scope	umfasst
1	Interface local	ein einzelnes Interface eines Rechners (nur Loopback)
2	Link local	lokales Subnetz ohne Routing
4	Admin local	Bereich, der in den Routern speziell administriert werden muss
5	Site local[35]	ein oder mehrere Subnetze einer Organisation, die über interne Router verbunden sind
8	Organization local	ein oder mehrere Subnetze einer Organisation, die auch über externe Router verbunden sind
E	Global	alles

Neben scope-spezifischen reservierten Multicast-Adressen wie der Link-Local-All-dhcp-agents-Adresse (FF02::1:2) existieren scope-variable Adressen, die für verschiedene Scopes definiert sind. NTP-Server (Network Time Protocol) können z.B. mit FF02::101 im lokalen Subnetz, mit FF05::101 in der Site und mit FF0E::101 global (d.h. im gesamten Internet) adressiert werden.

Risiken und Schutzmaßnahmen

Unbeobachtbarkeit

Broadcast kann u.a. zur Erreichung des Ziels der unbeobachtbaren Kommunikation genutzt werden, da aus der Analyse der entsprechenden Pakete kein bestimmter Empfänger erkennbar ist. In eingeschränkter Weise gilt dies auch für Multicast, bei dem je nach Scope ein ganzes Subnetz oder eine Organisation adressiert werden kann. Dabei ist allerdings zu beachten, dass die Unbeobachtbarkeit hier nur ein Nebeneffekt ist, nicht das eigentliche Ziel von Multi- bzw. Broadcast. Sie kann daher durch andere Pakete (z.B. Nachrichten vom Empfänger zurück an den Sender) konterkariert werden.

Netzwerkscans

In IPv6-Netzen ist der Adressraum, den ein Angreifer von außen bei einem Adress- bzw. Portscan durchsuchen müsste, erheblich größer als bei IPv4. Da IPv6-Router jedoch keine Adressübersetzung mit NAT durchführen müssen, sind Geräte in lokalen Netzen von außen in der Regel besser erreichbar. Ob Netzwerkscans durch diese Effekte erleichtert oder erschwert werden, hängt vom konkreten Angriffsszenario ab.

---

[33] http://www.m6bone.net/

[34] Siehe http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml

[35] Nach RFC 3879 ist dieser Scope veraltet. Weil dies nicht in allen Implementationen von IPv6 in Routern, Servern und Endgeräten berücksichtigt sein dürfte, werden in den folgenden Abschnitten auch Manipulationsmöglichkeiten auf Basis dieses Scopes beschrieben.

Allerdings stehen einem Angreifer mit bestimmten fest definierten Multicast-Adressen attraktive Ziele zur Verfügung, die ein Ausforschen bzw. Angreifen des Netzes erheblich erleichtern. Die Site-Local All-Routers-Adresse (FF05::2) oder All-DHCP-Servers-Adresse (FF05::1:3) erreichen sämtliche Router bzw. DHCP-Server einer Site. Diese kann ein mehrere Subnetze überspannendes Netzwerk einer Organisation umfassen[36].

Die entsprechenden Adressen müssen daher in den Zugangsroutern zu einem IPv6-Netzwerk herausgefiltert werden. Entsprechende Filtermöglichkeiten sollte jeder Router zur Verfügung stellen können.

DHCP

Zwar steht unter IPv6 mit der Stateless Address Autoconfiguration ein Protokoll für den Bezug einer IP-Adresse zur Verfügung, das den Einsatz von DHCP entbehrlich machen kann. Allerdings kann auch bei IPv6 DHCP sinnvoll sein, insbesondere zur Verteilung von Adresspräfixen und weiteren Konfigurationsdaten. Version 6 des Dynamic Host Configuration Protocol (DHCPv6) ist zudem in den meisten IPv6-Implementierungen verfügbar. DHCPv6 verwendet verschiedene Multicast-Adressen und ist durch das Einschleusen falscher Server angreifbar (unter Verwendung der Adresse FF05::1:3).

Gegen solche Angriffe bietet DHCPv6 eine optionale Nachrichten-Authentisierung auf Basis von IPsec. Diese ist nicht in allen Implementierungen enthalten, sollte aber dort genutzt werden, wo es möglich ist.

IPsec

IPsec (siehe Abschnitt 4.1) ist integraler Bestandteil von IPv6 zur Gewährleistung der sicheren Kommunikation. Hierbei sind bestimmte Verfahrensweisen für den Schlüsselaustausch (Internet Key Exchange, IKE) vorgesehen, bei denen der Empfänger den Authentisierungs- und Verschlüsselungsalgorithmus festlegt. Dies dreht sich bei Multicast jedoch um und muss vom Sender erledigt werden[37]. Die gewöhnlichen Verfahren zum Schlüsselaustausch müssen daher durch andere Protokolle ersetzt werden (z.B. Logical Key Hierarchy oder Oneway-Function Tree).

Diese Protokolle sind aktuell nicht Stand der Technik. Die Nutzung von IPsec bei Multicast-Verbindungen ist daher zurzeit nur bei einer manuellen Verteilung statischer Schlüssel möglich. Dies ist jedoch mit hohem zusätzlichen Aufwand verbunden.

4.4 Vergabe von Interface Identifiern; Privacy Extensions

Die automatische Einrichtung der IPv6 Adresse per SLAAC[38] nutzt bei einigen Betriebssystemen die eindeutige Hardwareadresse (MAC-Adresse) des Netzwerkadapters zur Generierung des Interface Identifiers der IPv6 Adresse. Dieser konstante Adressbestandteil identifiziert dadurch eindeutig das Endgerät und somit häufig den Nutzer. Dies ist völlig unabhängig von einer etwaigen dynamischen Vergabe des Präfixes (siehe Abschnitt 4.2) durch den ISP[39] möglich. Besonders bei mobilen Endgeräten ist dies als kritisch einzustufen, da hier in der Regel die Nutzung durch eine einzige Person erfolgt. Die Zuordnung der IP-Adresse eines Endgerätes zu seinem Nutzer kann nun nicht mehr nur durch den ISP erfolgen, sondern durch alle Diensteanbieter, gegenüber denen sich ein Nutzer einmal identifiziert hat. Dies gilt völlig unabhängig von anderweitigen Trackingmethoden (Cookies, Webbugs, Browserprofile etc. siehe Abschnitt 3.4). Speziell bei Diensten, bei denen mit echten Anmeldedaten gearbeitet wird, beispielsweise bei sozialen Netzwerken oder Online-Shops, ist der Nutzer auf diese Art und Weise sehr einfach durch den Dienstanbieter persönlich zu identifizieren und zu verfolgen.

---

[36] Site-Local-Adressen dürfen geroutet werden, jedoch nicht von Border-Routern
[37] RFC 2627: Key Management for Multicast: Issues and Architectures
[38] Stateless Address Autoconfiguration (zustandslose Adressenautokonfiguration)
[39] Internet Service Provider

Hier können die Privacy Extensions Abhilfe schaffen, die nachträglich spezifiziert wurden.[40] Sind die Privacy Extensions aktiviert, so wird vom Endgerät ein wechselnder und über Zufallszahlen generierter Interface Identifier verwendet und somit auch eine wechselnde IPv6-Adresse erzeugt. Gegen die oben genannten Trackingmethoden auf Anwendungsebene wird hierdurch prinzipbedingt kein Schutz geboten.

Die Hersteller von Betriebssystemen haben die Privacy Extensions in allen verbreiteten Desktopbetriebssystemen implementiert. Bei den Betriebssystemen für mobile Endgeräte sieht es gemischt aus (siehe Tabelle[41], Stand April 2011).

Betriebssystem	Privacy Extensions	ab Werk aktiv	de-/aktivierbar	Anmerkung
Windows XP	+	+	+/+	
Windows Vista	+	+	+/+	
Windows 7	+	+	+/+	
Windows Server 2003	+	-	+/+	
Windows Server 2008 R2	+	-	+/+	
OpenSuse Linux	+	-	+/+	
Ubuntu Linux	+	-	+/+	
Debian Linux	+	-	+/+	
Fedora Linux	+	-	+/+	
Mac OS X	+	-	+/+	
iOS 4.1	+	-	-/-	Privacy Extensions via Jailbreak
iOS 4.2	+	-	-/-	Privacy Extensions via Jailbreak
iOS 4.3	+	+	-/-	
Android ab 2.1	+	-	-/-	Privacy Extensions über Rooting

Bei den Betriebssystemen für Mobilgeräte sind die Privacy Extensions zwar größtenteils verfügbar; die bei manchen Systemen erforderliche Aktivierung durch den Nutzer gestaltet sich allerdings oft aufwändig. Das ggf. vorher durchzuführende Rooting, bzw. der Jailbreak des Endgerätes, ist außerdem unter Umständen mit dem Verlust der Garantie behaftet. Dies ist nicht nur wenig benutzerfreundlich, sondern auch mit anderen Risiken verbunden und wird somit nur von den wenigsten Nutzern durchgeführt werden. Nachholbedarf besteht auch bei eingebetteten Betriebssystemen, beispielsweise für Streaming Clients.

---

[40] RFC 4941

[41] http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html

Die Hersteller sollten in ihren Betriebssystemen Privacy Extensions nicht nur implementieren, sondern auch ab Werk aktivieren (privacy by default). Hier müssen die Hersteller ebenfalls noch nachbessern. Dies gilt nicht für Server.

Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten einbauen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können (z. B. alle 10 Minuten) bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können (z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners).

Auf der anderen Seite müssen die Nutzer über die möglichen Risiken der Identifizierbarkeit durch IPv6-Adressen und die Möglichkeiten der Privacy Extensions sowie deren Aktivierung informiert werden. Solange ein aktives Eingreifen zur Aktivierung der Privacy Extensions erforderlich ist, muss explizit darauf hingewiesen werden. Außerdem sind verständliche Anleitungen für diese Systeme bereitzustellen.

Die von den Datenschutzbeauftragten empfohlene dynamische Vergabe von IPv6-Präfixen analog zu IPv4[42], ist auch bei Nutzung der Privacy Extensions erforderlich. Nur durch das Zusammenspiel beider Bestandteile – also die Vergabe eines dynamischen Präfix durch den ISP, sowie Generierung eines zufälligen Interface Identifiers durch den Client – wird eine Anonymität auf dem bisherigen IPv4-Niveau ermöglicht. Wichtig ist in diesem Zusammenhang, dass Präfix und des Interface Identifier gleichzeitig gewechselt werden sollten (siehe Abschnitt 4.2).

Je nach Anwendungszweck (siehe Abschnitt 4.2) kann ein Verzicht auf die Privacy Extensions sinnvoll oder gar notwendig sein. Dies muss im Einzelfall erwogen werden. In den Fällen, in denen eine statische IP benötigt wird, beispielsweise zur Bereitstellung eigener Dienste (Webserver, Fileserver, VoIP, etc.), ist die bei IPv6 mögliche mehrfache Vergabe von IP-Adressen für das gleiche Endgerät, also z.B. einer festen und einer dynamischen IP-Adresse[43] ein möglicher Lösungsansatz. Die Nutzer sollten hierbei über eine bedienerfreundliche Oberfläche die Möglichkeit haben, ihre statische Adresse zu wechseln. Hierdurch kann jeder Nutzer wählen, ob und wie er die Vorteile von IPv6 nutzen möchte, ohne Datenschutzdefizite in Kauf nehmen zu müssen (siehe Abschnitt 4.2).

Wünschenswert wäre darüber hinaus, dass Anwendungsprogramme gezielt eine von mehreren lokalen IPv6-Adressen nutzen und unterschiedliche Adressen mit unterschiedlichen Wechselfrequenzen ausstatten können. Dies würde es ermöglichen, z. B. für Instant Messenger bzw. langlebige Downloads (oder Video-Streams) eine Adresse mit selten wechselndem Interface Identifier zu nutzen, während für Websurfen (das von kurzlebigen Verbindungen geprägt ist), eine hohe Wechselfrequenz verwendet werden könnte. Weiterhin könnten dadurch Daten unterschiedlicher Anwendungen den Rechner des Nutzers unter unterschiedlichen Adressen verlassen, was die Unverkettbarkeit weiter begünstigen würde. Wichtig wäre auch hier, dass Präfix und Interface Identifier jeweils gleichzeitig wechseln. Außerdem sollten Betriebssysteme mehrere nicht zusammenhängende Präfixe verwalten können. Auf diese Weise könnten Hersteller von Betriebssystemen und Anwendungssoftware ein höheres Datenschutzniveau als mit IPv4 erreichen.

---

[42] Siehe Positionspapier „Datenschutz bei der Einführung des Internet-Protokolls Version 6“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (http://www.datenschutz.rlp.de/downloads/oh/Positionspapier_IPv6.pdf)

[43] Siehe http://www.heise.de/netze/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html

4.5 Cryptographically Generated Addresses

Cryptographically Generated Addresses (CGA) sind ein weiterer standardisierter[44] Mechanismus zur Generierung der letzten 64 Bit einer IPv6-Adresse, des Interface Identifier (vgl. auch Privacy Extension und SLAAC, Abschnitt 4.4).

CGA sind ursprünglich entstanden, um die Adressverwaltung in lokalen Netzen sicherer zu machen. Per Neighbor Discovery Protocol (NDP)[45] können dort IPv6-fähige Geräte Daten wie den aktuellen Netzwerk-Präfix oder die Adressen von Routern im LAN ermitteln. Außerdem kann man damit ermitteln, ob eine IP-Adresse im LAN bereits vergeben ist. Da NDP mit der Maßgabe entwickelt wurde, dass alle Geräte innerhalb eines lokalen Netzes vertrauenswürdig sind, enthält es keine Sicherheitsmechanismen. Deshalb können mit NDP echte und falsche Nachrichten nicht voneinander unterschieden werden. Auf diese Weise lassen sich leicht Router-Adressen fälschen oder Denial-of-Service-Angriffe durchführen.[46]

Um diesem Missstand zu begegnen, wurde das Protokoll um Secure Neighbor Discovery (SEND)[47] ergänzt. Mit dieser Erweiterung lassen sich Nachrichten daraufhin prüfen, ob sie von dem richtigen Gerät stammen. Neben einem zentralen Modell auf Basis einer Public-Key-Infrastuktur ist hierfür auch ein dezentraler Ansatz vorgesehen, nämlich CGA.

CGA setzen voraus, dass das Endgerät über das Schlüsselpaar eines asymmetrischen kryptographischen Verfahrens verfügt. Aus dem öffentlichen Schlüssel dieses Paars und Zufallszahlen wird der Interface Identifier der IPv6-Adresse des Endgerätes berechnet. Empfänger signierter Nachrichten können dann prüfen, ob der Interface Identifier des Absenders zu dessen öffentlichem Schlüssel passt. Auf diese Weise wird das Fälschen der Absenderadresse (Spoofing) im LAN erkennbar.

Weil CGA mit kryptographischen Hashfunktionen aus jeweils frisch erzeugten Zufallszahlen und öffentlichen Schlüsseln erzeugt werden, sind sie praktisch ebenso schwer vorherzusagen, wie die mit den Privacy Extensions gebildeten Interface Identifier. Um mit CGA dieselbe Schutzwirkung wie mit den Privacy Extensions zu erreichen, müssen CGA in dem für Privacy Extension vorgesehenen Rhythmus neu erzeugt werden. Außerdem sind dazu Zufallszahlen mit hoher Qualität zu verwenden.[48] Mit den Privacy Extensions lässt sich ein Interface Identifier allerdings mit deutlich geringerem Aufwand an Rechenzeit wechseln. Der Vorteil von CGA liegt eher darin, dass sie andere Angriffsmöglichkeiten auf den Host verhindern, nämlich das Stehlen und Fälschen von Adressen. Dieses Ziel erreichen sie im Wesentlichen[49]. Wie die Privacy Extensions betreffen auch CGA nur den Interface Identifier. Möglichem Tracking eines Nutzers anhand des Netzwerk-Präfixes muss mit anderen Mitteln begegnet werden (vgl. Abschnitte 4.2, 4.8).

CGA eignen sich folglich zum Erschweren des Trackings von Internetnutzern in ähnlicher Weise wie die Privacy Extensions. Betriebssystemherstellern ist zu empfehlen, CGA zu unterstützen. Entweder CGA oder die Privacy Extensions sollten standardmäßig aktiv sein. Erste Implementationen sind verfügbar.

4.6 IPv6-fähige Firewalls, NAT

Die bei IPv4 eingesetzte Network Address Translation (NAT)[50] ist ein Verfahren, das u.a. in Routern eingesetzt wird, die ein lokales Netzwerk mit dem Internet verbinden. Dabei ersetzt

---

44 Das Verfahren ist definiert im Standard RFC 3972, der durch RFC 4581 und RFC 4982 erweitert wird.

45 RFC 2461, 2462

46 Genauere Informationen über mögliche Angriffe sind in RFC 3756 zu finden.

47 RFC 3971

48 RFC 3972, Abschnitt 7.3

49 Zu möglichen Angriffen nebst Schätzungen des jeweiligen Aufwandes vgl. Joppe & Onur 2008: http://secowinetcourse.epfl.ch/previous/08/Bos.Joppe_Ozen.Onur/Final_Report.pdf

50 https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m05/m05070.html, RFC 1631

der Router in allen ausgehenden Datenpaketen die private IP-Adresse des netzinternen Endgeräts mit seiner eigenen öffentlichen Adresse. Hierzu wird die Zuordnung der internen IP-Adresse/Port zur externen Adresse/Port in einer Tabelle gespeichert. Die Antwortpakete können so dem korrekten netzinternen Gerät weitergereicht werden. Durch diese Technik werden nicht nur die Auswirkungen der Adressknappheit von IPv4 vermindert, sie sorgt auch für etwas mehr Sicherheit dadurch, dass die Struktur des zu schützenden Netzwerkes verdeckt wird und so netzinterne Endgeräte nicht direkt von außen angesprochen werden können. Schließlich ist sie auch datenschutztechnisch von Bedeutung, da sie die intern genutzten IP-Adressen nach außen hin nicht offenbart. Aufgrund der hohen Anzahl von Adressen ist diese Verfahrensweise bei IPv6 nicht mehr notwendig und im Standard auch nur in Ausnahmefällen vorgesehen[51].

NAT ist jedoch ohnehin nicht als ausreichende Sicherheitsvorkehrung gegen unerwünschte Verbindungen anzusehen. IPv6-Netze und -Rechner benötigen dazu wenigstens eine Firewall. Dies kann in Form eines Paketfilters[52] als Teil einer Firewall auf TCP/IP-Ebene geschehen. Dieser filtert den ein- und ausgehenden Netzwerkverkehr nach bestimmten Regeln und entscheidet anhand der Header-Daten der IP- und Transportschicht (z. B. Absender- oder Ziel-Adresse, Ziel-Portnummer), ob ein Paket weitergeleitet, zurückgewiesen oder verworfen wird. Der eigentliche Inhalt des Paketes bleibt dabei normalerweise unberücksichtigt. Auch ausgehende Datenpakete mit ungültiger Absende- oder Zieladresse werden so idealerweise herausgefiltert. Die in den aktuellen Betriebssystemen integrierten Firewalls/Paketfilter können bereits den Netzwerkverkehr für IPv6 filtern[53].

Bezüglich der im IPv6 vorgesehenen Extension Header ist die Verarbeitung durch einen Paketfilter als schwieriger zu erachten. Extension Header unterliegen keiner Größenbeschränkung (außer der Paketgröße) wie deren IPv4-Äquivalent Header-Options und haben dadurch keine fest definierte Länge. Weiterhin ist vorgesehen, dass diese nur in einer bestimmten Reihenfolge eintreffen. Dies wird in der Praxis allerdings oft missachtet. Durch diese Faktoren ist die Verarbeitung in Paketfiltern schwieriger, da die Extension Header geparst werden müssen, was wiederum die Komplexität erhöht.

Eine Gefahrenquelle ist die grundsätzliche Möglichkeit der Fehlkonfiguration eines Paketfilters, die andere liegt in der prinzipbedingten Nicht-Berücksichtigung des Inhalts eines Paketes. Werden beispielsweise IPv6 Pakete über einen 6to4 Mechanismus getunnelt (z.B. per Teredo oder AYIYA Protokoll), also die Nutzdaten in IPv4-Pakete verpackt, so können diese vom IPv6 Paketfilter nicht als IPv6 Pakete interpretiert werden und so unter Umständen entsprechende Filterregeln ungehindert passieren[54]. Einige Hersteller bieten diesbezüglich bereits Abhilfe in Form einer „Tunneled packet inspection“ an.

Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6 fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im SoHo-Router[55] sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden. Mit solchen Features kann der Nutzer beim Gerätekauf und der späteren Nutzung auch den Aspekt der Sicherheit leichter berücksichtigen, der durch die NAT bei IPv4 quasi integriert war.

Bestehende Hard- und Software kann prinzipiell per (Firmware-) Update IPv6-fähig gemacht werden, wenn für den neuen IPv6 Stack genügend Speicherplatz vorhanden ist. Hier sind die Hersteller gefordert, für ihre Geräte entsprechende Updates bereitzustellen. Geräte mit höherem Durchsatz verarbeiten IP-Pakete mit direkter Hardware-Unterstützung. Sind sie

---

51 RFC 4864

52 https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02074.html

53 https://wikispaces.psu.edu/display/ipv6/IPv6+security und http://ipv6int.net/software/index.html

54 http://www.heise.de/security/Teredo-Sicherheitsproblem-IPv6-Kapselung--/artikel/82060

55 Small office, home office

nicht auf IPv6 ausgelegt, können sie nur ausgetauscht werden. Solche Geräte sind allerdings bei privaten Anwendern kaum verbreitet.

Administratoren sollten ihre Hardware entsprechend updaten und konfigurieren[56].

Paketfilter sind als Teil einer Firewall im IPv4-Umfeld Normalität und als ausgereift zu betrachten. Verbreitete Produkte sind bereits seit langem IPv6 kompatibel.[57]

Zusätzliche Maßnahmen zur Erhöhung der Sicherheit wie z.B. die Möglichkeit der Analyse von getunnelten Paketen sowie der korrekte Umgang mit Extension Headern sind seitens der Hersteller voranzutreiben. Insgesamt ist davon auszugehen, dass der aktuelle Reifegrad von IPv6 Firewalls sich unterhalb des Niveaus der aktuellen IPv4 Firewalls und Paketfiltern befindet.

4.7 Peer-to-Peer Services

Peer-to-Peer-Computing bezeichnet verteilte Anwendungen, in denen eine gemeinsame Aufgabe unter gleichberechtigten Teilnehmern aufgeteilt wird. Kein Teilnehmer hat höhere Rechte oder andere Funktionen als ein anderer[58]. In einem Peer-to-Peer-Netz gibt es keine zentrale Instanz und damit keinen zentralen Punkt, an dem die Aktivitäten des Netzwerks überwacht oder gesteuert werden könnten.

Peer-to-Peer-Anwendungen setzen voraus, dass die beteiligten Rechner direkte Verbindungen zueinander aufbauen können. Diese Möglichkeit ist mit IPv6 grundsätzlich gegeben, insbesondere wegen des großen verfügbaren Adressraums. Techniken wie NAT, die zu einer Einschränkung der direkten Adressierbarkeit führen, sind bei IPv6 obsolet (siehe Abschnitt 4.6). Damit erlangt ein wichtiges Gestaltungsprinzip des Internets wieder größere Geltung, das Ende-zu-Ende-Prinzip[59]. Es geht davon aus, dass beliebige Rechner im Netzwerk Verbindungen zueinander aufbauen können und verlangt, dass Funktionen, die vollständig und korrekt an den Endpunkten implementiert werden können, auch dort realisiert werden sollen und nicht auf Zwischenstationen. Das Ende-zu-Ende-Prinzip gilt als Eckpfeiler der Robustheit des Internets und seiner Anpassbarkeit an neue Anforderungen. NAT verstößt gegen dieses Prinzip, weil es IP-Pakete manipuliert, insbesondere Adressen übersetzt, und so als Nebenwirkung in ganzen Netzsegmenten keine kommenden Verbindungen zulässt. Peer-to-Peer-Anwendungen wie Internet-Telefonie (Voice over IP, VoIP) verlangen in solchen Umgebungen nach komplexen Sonderlösungen wie STUN[60].

Bekannte Peer-to-Peer-Anwendungen gibt es im Bereich des File-Sharing. So kann mit BitTorrent[61] die Netzlast für die Verteilung verschiedenster Inhalte auf eine große Gruppe von Nutzern verteilt werden. Wer eine bestimmte Datei oder einen Teil von ihr herunter geladen hat, ermöglicht es anderen Nutzern, diese Daten von seinem eigenen Rechner herunter zu laden. Dadurch stellt er die Kapazität seines Rückkanals anderen Teilnehmern zur Verfügung und entlastet so den Rechner, auf dem die Verteilung der Datei begonnen hat.

Im Bereich der Sozialen Netzwerke gibt es erste praktische Erfahrungen mit Peer-to-Peer-Protokollen. So soll Friendica[62] künftig die üblichen Funktionen eines Sozialen Netzwerks bieten, jedoch auf Basis einer Software, die auf einem nutzereigenen Gerät läuft. Auf diese

---

56 http://www.heise.de/netze/artikel/IPv6-Zugang-fuers-LAN-nachruesten-1260260.html

57 Eine Übersicht über IPv6-fähige Firewalls findet sich beispielsweise auf der Website http://getipv6.info.

58 http://en.wikipedia.org/wiki/Peer-to-peer

59 Saltzer, J.H.; Reed, D.P.; Clark, D.D. (April 1981). "End-To-End Arguments in System Design". Proceedings of the 2nd International Conference on Distributed Computing Systems (IEEE Computer Society): 509-512.

60 RFC 5389

61 http://www.bittorrent.com

62 http://friendica.com, siehe auch Bager, J.: Private Treffpunkte - Diaspora und andere Facebook-Alternativen. In c't 5/2012, S. 136 ff.

Weise erhalten die Nutzer bessere Kontrolle über die Daten, die sie anderen Personen zugänglich machen oder veröffentlichen wollen. Die Nutzerdaten sollen bei Friendica nicht zentral gespeichert werden. Auch die Rechteverwaltung ist dezentral implementiert. Das Einrichten eines eigenen Servers erfordert derzeit noch einen gewissen Aufwand. Zu erwarten ist jedoch, dass dieser Aufwand im Laufe der weiteren Entwicklung sinken wird. Wer Friendica benutzt, hat nicht nur Kontaktmöglichkeiten zu anderen Nutzerinnen und Nutzern dieses Netzwerks, da auch Schnittstellen zu anderen Sozialen Netzwerken implementiert sind.

Auch die Internet-Telefonie (VoIP) mit den bekannten Protokollen SIP und RTP oder ihren mit TLS gesicherten Varianten SIPS und SRTP ist im Grunde eine Peer-to-Peer-Anwendung, da die Sprachdaten über eine direkte Verbindung mit dem Protokoll RTP zwischen den Gesprächspartnern ausgetauscht werden. Zum Aufbau von Verbindungen werden häufig zentrale SIP-Server eingesetzt. Dies ist jedoch nicht notwendig. Wenn die Telefone oder Computer der Teilnehmer an einer Telefonverbindung oder -konferenz direkt adressierbar sind, können sie die Verbindungssteuerung selbst übernehmen. Nur die Gateways (Übergabepunkte) zum herkömmlichen Telefonsystem lassen sich so nicht beliebig dezentralisieren.

In diesem Zusammenhang spielt es grundsätzlich keine Rolle, ob statisch oder dynamisch vergebene Adressen benutzt werden, solange es irgendeine Möglichkeit zum Auffinden von Rechnern gibt. Teilweise sind hierzu Mechanismen in den Peer-to-Peer-Protokollen selbst vorgesehen. So kennt in Kademlia-basierten Netzwerken[63] jeder Netzwerkknoten eine bestimmte Anzahl Nachbarknoten. Zum Auffinden einer Datei im Netz wird nach einem bestimmten Verfahren nach Knoten gesucht, deren Adresse dem Hashwert der gewünschten Datei immer näher kommt. Die Suche endet, wenn die Datei gefunden ist oder, wenn klar ist, dass sie nicht existiert. Die erwähnte Software BitTorrent beherrscht dieses Verfahren neuerdings ebenfalls.

Stehen solche Mechanismen nicht zur Verfügung, kann auch das Domain Name System (DNS) benutzt werden, welches leicht merkbare Rechnernamen wie bob.example.org in IP-Adressen wie 192.0.2.100 (IPv4) oder 2001:db8:804:a082::1:225 (IPv6) umwandelt. Im Zusammenhang mit Internettelefonie ist interessant, dass sich mit dem DNS sich auch Telefonnummern verwalten lassen. Hierzu dient dass Verfahren ENUM[64]. Telefonnummern können damit in einem bestimmten Zweig des DNS auf feste oder wechselnde IP-Adressen abgebildet werden. Die fiktive Telefonnummer 0123-4567890, internationale Schreibweise +49-123-4567890 würde beispielsweise dem Domain-Namen 0.9.8.7.6.5.4.3.2.1.9.4.e164.arpa zugeordnet werden. Auch bei DNS handelt es sich um ein verteiltes System, welches allerdings hierarchisch strukturiert ist. Die DNS-Einträge werden dazu in der Regel nach regionalen Gesichtspunkten und nach Providern gruppiert verwaltet. Normalerweise kann man beliebige DNS-Server nutzen und ist nicht auf die Vorgabe des Providers angewiesen. DNS gewährt keine Anonymität gegenüber dem Betreiber des DNS-Servers. Außerdem ist der Inhalt des DNS prinzipiell im gesamten Internet zugreifbar, wird aber nur durch explizite Abfrage eines Nutzers oder Servers an andere DNS-Server und Nutzer weiter geleitet. Das ENUM-Verfahren hat aus Datenschutzsicht den Nachteil, dass die ENUM-Einträge wie alle anderen Domain-Einträge behandelt werden, für die unter anderem personenbezogene Daten des Domain-Inhabers in den zentralen WHOIS-Datenbanken der Registry hinterlegt werden müssen.[65] Könnte hier ein Provider oder ein Pseudonym eingetragen werden, wäre das Verfahren datenschutzfreundlicher.

Bei der Nutzung von Peer-to-Peer-Anwendungen kommt der Sicherheit von Endpunkten eine erhöhte Bedeutung zu, insbesondere, wenn keine dedizierten Sicherheitsgateways

---

63 http://sarwiki.informatik.hu-berlin.de/Kademlia

64 RFC 6116: E.164 Number Mapping; siehe außerdem http://www.denic.de/enum.html

65 Zum Vorgehen der DENIC e.V. siehe beispielsweise: http://www.denic.de/fileadmin/public/services/ENUM/DENIC-ENUM-Domainrichtlinien.pdf

(Firewalls) benutzt werden. Dieses Problem ist jedoch nicht neu; es tritt bei jeder Art von Ende-zu-Ende-Verschlüsselung auf und ist deshalb in analoger Weise durch Sicherheitsmaßnahmen an den Endpunkten zu lösen. Dazu gehören beispielsweise das konsequente Deinstallieren oder Abschalten nicht benötigter Dienste, der Einsatz von Filtertechniken wie Paket-Filter auf Betriebssystemebene und von Antivirensoftware. In mittleren und großen Umgebungen ist eine zentrale Verwaltung solcher Sicherheitsmaßnahmen angezeigt.

Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. IPv6 ermöglicht den verstärkten Einsatz von Peer-to-Peer-Ansätzen, da die Erreichbarkeit von IPv6-fähigen Geräten nicht mehr durch Techniken wie NAT beschränkt werden muss. Teilweise sind Peer-to-Peer-Anwendungen bereits als marktüblich anzusehen, teilweise befinden sie sich aber auch noch in einer Konzept- oder frühen Entwicklungsphase. Softwarehersteller sollten das ihnen innewohnende Datenschutzpotenzial nutzen und sich aktiv an der Entwicklung beteiligen. Hersteller von Netzwerktechnik wie Routern sollten ihre Produkte so gestalten, dass sie mit Peer-to-Peer-Anwendungen kompatibel sind, und bei Produkten, die für Privatkunden gedacht sind, an die Integration geeigneter Peer-to-Peer-Anwendungen denken.

4.8 Anonymisierungsdienste

Alle Pakete, die mit dem Internet-Protokoll übertragen werden, enthalten die unverschlüsselte IP-Adresse von Sender und Empfänger des Pakets. Technisch können alle an der Übertragung Beteiligten diese Verkehrsdaten aufzeichnen und auswerten. Damit ist es prinzipiell an verschiedenen Stellen im Netz möglich, zu überwachen, wer mit wem kommuniziert, bzw. wer welche Dienste nutzt (Verkehrsflussanalyse). Wird der Interface Identifier der IP-Adresse aus der weltweit eindeutige MAC-Adresse der Netzwerkschnittstelle abgeleitet (SLAAC, siehe Abschnitt 4.4), so sind mitunter sogar Aussagen zu Typ und Charge des verwendeten Endgerätes möglich. Dadurch ist das Schutzziel Unbeobachtbarkeit beeinträchtigt (siehe Abschnitt 3.3). Dies gilt unabhängig davon, ob die übertragenen Inhalte verschlüsselt sind.

Anonymisierungsdienste dienen dazu, Kommunikationsbeziehungen zu verbergen. Im Zusammenhang mit IPv6 müssen sie dazu insbesondere die von einem Endgerät verwendete IP-Adresse verschleiern.

Im einfachsten Fall kann ein Proxy (engl. für Stellvertreter) diese Funktion übernehmen. Web-Proxys beispielsweise nehmen alle HTTP-Anfragen eines Browsers, Hosts oder Subnetzes entgegen, gleichgültig, an wen sie gerichtet sind, und leiten sie unter der eigenen Adresse an das gewünschte Ziel weiter. Die Antworten der Web-Server werden dann ebenfalls an den Proxy gerichtet, der sie an die anfragende Instanz weiter gibt. Proxys dienen häufig zur Beschleunigung von Webzugriffen, indem sie Antworten von Webservern zwischenspeichern. Wird derselbe Inhalt erneut angefragt, kann der Proxy die schon bekannte Antwort ausliefern, ohne dass eine neue Verbindung zum Server hergestellt werden muss. Diese Idee funktioniert auch mit anderen Protokollen. Indem Proxys selbst als Absender und Empfänger auftreten, verbergen sie die IP-Adressen der ursprünglichen Kommunikationspartner. Die Schwäche dieses einfachen Konzepts besteht darin, dass der Proxy-Betreiber seine Nutzer auf einfache Weise überwachen kann, weil am Proxy alle benötigten Daten im Klartext vorliegen.

Wesentlich besseren Schutz bieten Anonymisierungsdienste auf der Basis kryptographischer Verfahren und Protokolle. Die Grundidee hierzu bilden die Mix-Netze des Kryptologen David Chaum.[66] Ein Mix ist ein Rechner, der eingehende Nachrichten umcodieren,

---

[66] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. CACM, Feb. 1981, Vol. 24, No. 2, p. 84

zwischenspeichern, in einer neuen Reihenfolge an andere Mixe oder Empfänger senden und doppelte Nachrichten erkennen und löschen kann. Der Absender verschlüsselt seine Nachricht und sendet sie an den ersten Mix. Dieser schlüsselt die Nachricht um und sendet sie weiter. Die endgültige Empfängeradresse erfährt erst der letzte Mix. Es sollen mindestens zwei Mixe benutzt werden. So haben nur alle Mixe eines Versandweges zusammen genügend Information, um die dort übertragene Nachricht zurück zu verfolgen.

Dieses Konzept lässt sich auf unterschiedliche Weise auf IP-Netze übertragen. Der absendende Host muss den zu übertragenden Datenstrom in gleich große Pakete teilen und mehrfach ineinander geschachtelt verschlüsseln. Außerdem sind passende Hosts notwendig, die als Mixe fungieren.

Es gibt Implementationen, in denen die Hostsoftware als lokal installierter Proxy gestaltet ist. Dies gilt beispielsweise für die Open-Source-Programme JonDonym[67] und Tor[68]. Beiden ist gemeinsam, dass sie eine relativ starke Anonymisierung bieten, wobei geringe Abstriche an dem von Chaum entwickelten Modell hingenommen werden müssen. Wenn beispielsweise bei JonDonym sowohl der IP-Verkehr am Host des Kunden als auch am Zielhost überwacht werden kann, können Verbindungen dem Nutzer zugeordnet werden, indem die übertragenen Datenmengen verglichen werden.[69] Bei Tor wird unter anderem die Mix-Kaskade zufällig zusammengestellt, was die Anonymität des Nutzers schwächt.[70] Für beide genannten Programme sind zum Redaktionsschluss noch keine stabilen Versionen verfügbar, die mit IPv6 zusammenarbeiten. So gibt es von Tor seit Dezember 2011 eine IPv6-fähige Alpha-Version.[71] Alle genannten Probleme sind jedoch prinzipiell technisch lösbar.

Auch mit dem Sicherheitsprotokoll IPsec (siehe Abschnitt 4.1) lassen sich Anonymisierungsdienste aufbauen. Diese sind für IPv6-Netze besonders interessant, da IPsec dort wesentlich weiter verbreitet ist, als in IPv4-Netzen (ebd.). Wissenschaftliche Untersuchungen aus den letzten Jahren legen nahe, dass Dienste dieser Art hohen Anforderungen an die Qualität der Anonymisierung erfüllen können und besonders effizient sind.[72] Aus diesem Umfeld sind auch erste experimentelle Open-Source-Implementierungen bekannt, beispielsweise TFC[73]. Diese haben jedoch bisher keine nennenswerte Verbreitung gefunden. Die Forschungen auf diesem Gebiet dauern an.

Mixbasierte Anonymisierungsdienste sind folglich dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Solche Dienste funktionieren auch bei statisch zugewiesenen IP-Adressen. Es sind bereits einige breit einsetzbare Systeme verfügbar, jedoch noch nicht für IPv6. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung dieser Dienste darf durch Netzbetreiber nicht blockiert werden.

---

67 http://www.jondonym.de

68 https://www.torproject.org

69 Siehe: Beschreibung auf der Seite des Vorläuferprojekts von JonDo http://anon.inf.tu-dresden.de/desc/desc_anon.html

70 Oliver Berthold, Andreas Pfitzmann, Ronny Standtke: The disadvantages of free MIX routes and how to overcome them. In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, July 2000

71 http://www.heise.de/netze/meldung/Anonymisierungsnetz-experimentiert-mit-IPv6-1397167.html

72 (a) Ronggong Song, Larry Korba: Anonymous Internet Communication based on IPsec. Proceedings of the IFIP World Computer Congress, Montreal, August 25-30, 2002
(b) C. Kiraly, G. Bianchi, R. Lo Cigno: Solving Performance Issues in Anonymization Overlays with a L3 approach. University of Trento, Information Engineering an Computer Science Dept., Tech. Report DISI-08-041, Ver. 1.1, September 17, 2008.

73 http://minerva.netgroup.uniroma2.it/discreet/wiki/TfcProject

4.9 Anforderungen an die Protokollierung

Bei dem Umstieg eines Dienstes oder eines Netzes von IPv4 auf IPv6 ändern sich die rechtlichen Bestimmungen nicht, auf deren Grundlage der Dienst erbracht bzw. das Netz betrieben wird. Dies gilt auch in Hinblick auf die Fragen der Protokollierung personenbezogener Daten. Allerdings sind die Rahmenbedingungen und die Bedeutung von IP-Adressen anders.

Unter Protokollierung (Logging) wird hier ein Prozess verstanden, der automatisiert bestimmte Ereignisse in Dateien (Logfiles) festhält. Die Gründe hierfür können vielfältig sein und reichen von der Fehlerverfolgung über die Erfüllung datenschutzrechtlicher Verpflichtungen[74] bis zur Abrechnung von Leistungen.

Aus datenschutzrechtlicher Sicht relevant sind solche Protokolle, die personenbezogen oder personenbeziehbar sind. Beispiele hierfür wären Protokolle, die Anmelde- oder Nutzernamen enthalten (direkter Personenbezug bei Verwendung des Echtnamens) bzw. solche, die IP-Adressen enthalten (Personenbeziehbarkeit, siehe Abschnitt 3.5).

Protokollierung bei IPv6

Eine Protokollierung von IPv6-Adressen kann in sämtlichen Bestandteilen einer IP-Verbindung erfolgen: in Clients, Routern, Proxys oder Servern. Hier besteht kein Unterschied zu IPv4. Allerdings trägt eine IPv6-Adresse in der Regel mehr Information in sich als eine IPv4-Adresse (siehe Abschnitt 3.4). Typischerweise treten die einzelnen Clients mit ihren individuellen Adressen auch nach außen hin in Erscheinung und sind entsprechend auch in Protokolleinträgen erkennbar.

Risiken und Schutzmaßnahmen

Privacy Extensions, dynamische Präfixe, Anonymisierungsdienste

Die Bildung des Interface Identifiers mittels einer wechselnden Zufallszahl (Privacy Extensions, siehe Abschnitt 4.4) vermeidet sowohl eine durch einen statischen Interface Identifier dauerhaft einem einzelnen Client zuordenbare IPv6-Adresse als auch die Offenlegung der MAC-Adresse des Clients. Zur Verschleierung des Präfixes können spezielle Anonymisierungsdienste (siehe Abschnitt 4.8) genutzt werden. Wenn die protokollierende Instanz außerhalb des Nutzernetzes liegt und nicht mit dem Provider des Nutzers kollaboriert, hilft auch die Nutzung dynamisch vergebener Präfixe (siehe Abschnitt 4.2).

Dies ist aus Sicht der Privatsphäre sinnvoll, kann jedoch die Auswertung von Protokolldaten erschweren. Sofern etwa eine Protokollierung zum Zwecke der Fehlersuche oder zur Gewährleistung datenschutzrechtlicher Vorgaben erfolgt, ist die IPv6-Adresse dann nicht geeignet, (nachträglich) ein bestimmtes Gerät zu identifizieren. (Zu den konkreten Einsatzempfehlungen der genannten Techniken siehe Abschnitte 4.2, 4.4 und 4.8.)

Anonymisierung von Adressen bei der Protokollierung

Da IPv6-Adressen personenbezogen sind, stellt sich aus Sicht eines Diensteanbieters oder anderen Netzteilnehmers die Frage, unter welchen Bedingungen und in welchem Umfang solche Adressen protokolliert werden dürfen.

Hinsichtlich der rechtlichen Bedingungen gibt es keine wesentlichen Unterschiede zu IPv4. Sofern diese keine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus zulassen, dürfen IPv6-Adressen allenfalls nach einer Anonymisierung gespeichert und verarbeitet werden. Die Anforderungen an eine solche Anonymisierung sind in Abschnitt 3.5 benannt und richten sich an die Provider und die Diensteanbieter.

---

[74] Siehe hierzu die Orientierungshilfe „Protokollierung“ (http://www.datenschutz-mv.de/datenschutz/publikationen/informat/protokol/oh-proto.pdf)

Geolokalisierung

Sofern die IPv6-Adresse eines Geräts genutzt werden soll, um dessen (ungefähren) Standort zu ermitteln, gelten hierfür ebenfalls vergleichbare Anforderungen wie bei IPv4. Eine solche Standortermittlung ist nur nach Anonymisierung der Adresse zulässig, da es sich um eine Verarbeitung für einen zusätzlichen Zweck handelt, die im Geltungsbereich des TMG nicht zulässig ist.

Welche Auswirkungen die Anonymisierung einer IPv6-Adresse auf die Standortbestimmung hat, lässt sich zum jetzigen Zeitpunkt nur schwer absehen. Dies wird vor allem davon abhängen, wie die einzelnen Provider IPv6-Präfixe vergeben. Enthalten die Präfixe viel geografische Information, etwa weil sie stadtteil- oder straßenorientiert vergeben werden, kann eine Anonymisierung zu einem Verlust der maximalen Genauigkeit führen. Eine Verschlechterung gegenüber IPv4 ist jedoch nicht zu befürchten.

Diese Anforderungen richten sich ebenfalls an Provider und Diensteanbieter.

4.10 Parallelbetrieb von IPv4 und IPv6 (Dual-Stack-Betrieb)

Dual Stack (auch Dual IP Layer)[75] und Tunneling (s.u.) sind Verfahren, um IPv4 und IPv6 parallel zu betreiben und so eine stufenweise Migration zu ermöglichen. Hierzu werden beide Protocol Stacks bei IPv6-fähigen Hosts und Routern vollständig implementiert und der IPv6-Verkehr über eine herkömmliche IPv4-Netzwerkinfrastruktur getunnelt. Die IPv6-Pakete werden in IPv4-Header verpackt und über eine Punkt-zu-Punkt-Verbindung transportiert, an deren Ende sie entsprechend wieder ausgepackt und vom IPv4-Header befreit zugestellt werden.

Im Falle des vom IETF vorgeschlagenen „Dual Stack Lite“[76] stattet ein ISP den Endkunden mit einem speziellen Home-Gateway aus. Die IPv4-Adressen der Endgeräte laufen nun über einen IPv6-Tunnel zum NAT des ISP, von wo aus sie anschließend über dessen IPv6-Backbone transportiert werden. Dies hat für die ISP den Vorteil, dass sie dem Endkunden im Gegensatz zum klassischen Dual Stack Betrieb nicht mehr die knappen IPv4-Adressen zuordnen müssen, sondern nur noch eine IPv6-Adresse.

Der Aufwand, der für eine parallele Netzwerk- und Adressverwaltung sowohl für IPv4 als auch für IPv6 von Nöten ist, verdeutlicht, dass ein Dual-Stack-Betrieb nur im unbedingt notwendigen Umfang stattfinden sollte. Weiterhin ist laut BSI-Leitfaden[77] unter dem Aspekt der Sicherheit Dual Stack sogar kritisch zu sehen, denn in einem Dual-Stack-Netzwerk addieren sich die jeweiligen protokollbezogenen Sicherheitslücken in Netzwerkkomponenten, Betriebssystemen und Anwendungen. Gleichzeitig wächst – wegen der erheblich höheren Komplexität – die Fehleranfälligkeit bei der sicheren Konfiguration aller beteiligten Komponenten.

Die wichtigsten Netzwerkhardwarehersteller unterstützen bereits IPv6 und haben in der Regel Dual Stack implementiert. Die korrekte und vollständige Implementierung der beiden IP Stacks und des standardisierten Dual-Stack-Mechanismus ist die Voraussetzung für einen reibungslosen und risikoarmen Übergang von IPv4 zu IPv6 und ist zu prüfen.

Die meisten Open-Source-Server unterstützen den Dual-Stack-Betrieb bereits. Hierzu zählen unter anderem Apache Webserver, Postfix SMTP Server, Dovecot IMAP/POP3 Server. Clientseitig reihen sich hier beispielsweise der Webbrowser Mozilla Firefox und der Mail-Client Mozilla Thunderbird als positives Beispiel ein. Aber auch Microsofts Windows Server ab 2007, Exchange ab 2007 und Windows ab Vista, sowie alle Unix-Plattformen und Mac OS X seit V10.2 unterstützen IPv6 und den Dual-Stack-Betrieb.

---

[75] RFC 4213
[76] RFC 6333
[77] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf.pdf?__blob=publicationFile

Neben den Herstellern müssen auch die Administratoren dafür sorgen, dass die Clients, Server und die Netzwerkhardware entsprechend konfiguriert und aktualisiert wird. So sollte beispielsweise darauf geachtet werden, dass Tunnelprotokolle nur im Bedarfsfall aktiviert werden, damit auf diesem Weg keine Paketfilter umgangen werden (siehe Abschnitt 3.4). Der Nutzer im Homeoffice sollte ggf. ebenfalls das seitens des Betriebssystems oft automatisch aktivierte Teredo-Tunnel-Protokoll deaktivieren[78]. Nicht zuletzt sind die Softwarehersteller von IPv4-only Client-/Server-Produkten in der Pflicht, entsprechende Updates zu liefern, um in Zukunft die Einbindung in ein IPv6-Netzwerk ohne Übergangstechniken zu ermöglichen.

[78] http://www.heise.de/netze/artikel/Teredo-blockieren-223868.html

5 Abkürzungsverzeichnis und Glossar[79]

BSI	Bundesamt für Sicherheit in der Informationstechnik (http://www.bsi.de): deutsche Bundesbehörde mit vielfältigen Aufgaben im Bereich der Informationssicherheit.
Cookie	„Keks“: Textdatei, die auf dem Rechner eines Benutzers abgelegt wird. Kann zur Wiedererkennung von Benutzern in verschiedenen Zusammenhängen benutzt werden, etwa um angemeldeten Benutzern einer Website die für sie bestimmten Daten zu präsentieren, oder aber, um Gewohnheiten und Vorlieben eines Nutzers für Werbezwecke zu ermitteln. Vgl. Webbug.
DHCP	Dynamic Host Configuration Protocol: Netzwerkprotokoll, mit dem IP-Adressen und andere Netzwerk-Konfigurationsdaten übermittelt und verwaltet werden können. Definiert in RFC 2131 für IPv4 und RFC 3315 für IPv6.
DSL	Digital Subscriber Line. Anschlusstechnik für Breitbandanschlüsse in festen Telekommunikationsnetzen.
IETF	Internet Engineering Task Force (http://www.ietf.org): mit der Weiterentwicklung der technischen Grundlagen des Internets befasste Organisation.
IP	Internet Protocol: verbreitetes Netzwerkprotokoll zur Kopplung von Rechnern und Rechnernetzen, Grundlage des als „Internet“ bezeichneten weltweiten Netzverbundes. Zurzeit werden die Versionen 4 und 6 dieses Protokolls verwendet.
IPsec	Internet Protocol Security: Protokoll zur Sicherstellung von Vertraulichkeit, Integrität und Zurechenbarkeit mit kryptographischen Mitteln, spezifiziert für IPv4 und IPv6.
ISO	International Organization for Standardization: Internationale Organisation für Normung mit Sitz in Genf.
ISP	Internet Service Provider: Anbieter eines Internet-Zugangs.
Jailbreak	„(Gefängnis-)Ausbruch“: Umgehen technischer Sicherheitsmaßnahmen, insbesondere in einem Smartphone oder Tablet-PC mit dem Betriebssystem iOS.
MAC-Adresse	Media-Access-Control-Adresse: Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient. Nutzer können diese Adresse häufig nicht ändern.
NAT	Network Address Translation: Übersetzungsverfahren für Netzwerkadressen in einem Router. Ermöglicht beispielsweise den Anschluss eines Netzwerks mit mehreren Rechnern mit einer vom Internet-Provider zugeteilten IP-Adresse.
Pre-shared key	„vorab ausgetauschter Schlüssel“: Verfahren zur Verwaltung von kryptografischen Schlüsseln, bei dem die Teilnehmer einen gemeinsamen Schlüssel nutzen, der zuvor allen Teilnehmern auf sichere Weise übermittelt werden muss.
PKI	Public Key Infrastructure: System, das kryptografische Schlüssel bzw. Zertifikate ausstellen, verteilen, prüfen und zurückziehen kann.

[79] teilweise unter Verwendung von Material von Wikipedia (http://de.wikipedia.org)

RFC	Request for Comment: technisches Dokument zum Internet, abrufbar bei der IETF unter http://tools.ietf.org/rfc/rfcN.txt, wobei N die ein- bis vierstellige Nummer des Dokuments ist. Einige RFCs sind Internet-Standards.
Rooting	abgeleitet von root (Administrator in Unix-artigen Betriebssystemen) Umgehen technischer Sicherheitsmaßnahmen, insbesondere in einem Smartphone oder Tablet-PC mit dem Betriebssystem Android.
SLAAC	Stateless Address Autoconfiguration , zustandslose Adressenautokonfiguration: Protokoll, mit der ein Rechner seine IPv6-Adresse und weitere zur Kommunikation erforderlichen Parameter automatisch ermitteln kann.
SSL	Secure Sockets Layer: Verschlüsselungstechnik für TCP-Verbindungen.
TCP	Transport Control Protocol: verbindungsorientiertes Netzwerkprotokoll auf der Basis von IP.
UDP	User Datagram Protocol: verbindungsloses Netzwerkprotokoll auf der Basis von IP.
VoIP	Voice over IP: Sprachübertragung über das Internet mit verschiedenen Protokollen auf der Basis von TCP und UDP.
Webbug	„Web-Wanze“, auch Zählpixel genannt, kleine Grafik-Datei auf einer Website oder in einer E-Mail. Der Abruf dieser Datei erzeugt auf dem Webserver Protokolldaten, die zur Analyse des Benutzerverhaltens genutzt werden können. Vgl. Cookie.