Lutz Donnerhacke
lutz@donnerhacke.de

Referat R B 3
Anton-Wilhelm-Amo-Straße 37
10117 Berlin

gesetzentwurf_stpo@bmjv.bund.de

Jena, den 29.01.2026

Stellungnahme zum Referentenentwurf für ein „Gesetz zur Einführung einer Speicherpflicht für IP-Adressen und zur Anpassung weiterer digitaler Ermittlungsbefugnisse“

Werte Damen und Herren,

als Entwickler von Kommunikationslösungen und Dienstleister im Umfeld von Internet-Service-Providern bin ich mit den Realitäten der Internetversorgung für die typischen privaten Haushalte vertraut. Mir ist der Referentenentwurf erst vor wenigen Tagen zugegangen und ich möchte auf ein paar grundsätzliche Punkte in diesem Entwurf hinweisen. Dazu beschränke ich mich auf den Teil, der den Massenmarkt der Internetversorgung für Privatleute betrifft.

In der Begründung des Referentenentwurfes heißt es:

> *Nach dem Entwurf werden Internetzugangsdiensteanbieter erstens verpflichtet, für drei Monate die von ihnen an Endkunden vergebenen IP-Adressen und weitere Daten wie die Portnummer zu speichern, sofern dies für eine eindeutige Zuordnung der IP-Adresse zu einem Anschlussinhaber erforderlich ist. Dadurch können Strafverfolgungs- und Gefahrenabwehrbehörden anhand eines **Zeitstempels**, einer **IP-Adresse** und gegebenenfalls einer **Portnummer** die **Bestandsdaten** beim Internetzugangsdiensteanbieter abfragen, […]*

Der Referentenentwurf sieht dazu insbesondere folgende Änderungen vor:

> *TKG §176 Speicherpflicht und Verwendungsbefugnis von **Verkehrsdaten** zur **Identifizierung von Anschlussinhabern***
> *(1) Anbieter von Internetzugangsdiensten sind verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten für drei Monate zu speichern:*
> 1. *die dem Anschlussinhaber **für eine Internetverbindung zugewiesene, öffentliche Internetprotokoll-Adresse**,*
> 2. *eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt, sowie eine zugewiesene Benutzerkennung,*
> 3. *das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone sowie*
> 4. *die der **Internetprotokoll-Adresse** zugehörigen **Portnummern** und weitere **Verkehrsdaten**, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind.*

*BKAG § 10b Sicherung von **Verkehrsdaten***
*(1) Zur Erfüllung der Aufgabe als Zentralstelle nach § 2 Absatz 1 kann das Bundeskriminalamt zum Zwecke einer etwaigen Erhebung gegenüber demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, anordnen, **Verkehrsdaten** gemäß § 3 Nummer 70 des Telekommunikationsgesetzes von betroffenen Personen unverzüglich zu sichern (**Sicherungsanordnung**), wenn die zuständige Strafverfolgungsbehörde oder die zuständige Polizeibehörde noch nicht erkennbar ist […]*

Lassen Sie mich dazu einige Begrifflichkeiten aus den referenzierten Gesetzen zitieren:

*TKG §3(6): **Bestandsdaten** Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste*

*TKG §3(70): **Verkehrsdaten** Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind*

*BSIG §2(31): **Protokolldaten** Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die a) zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind und b) unabhängig vom Inhalt des Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden*

*TDDDG §2(3) **Nutzungsdaten** die personenbezogenen Daten eines Nutzers von digitalen Diensten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen und abzurechnen; dazu gehören insbesondere a) Merkmale zur Identifikation des Nutzers, b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und c) Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste*

Die offenkundige Intention des Referentenentwurfs ist, aus Protokolldaten, die an einer bestimmten Stelle (z.B. einem bestimmte Daten bereitstellenden Server) erfasst wurden, einen Rückschluss auf den Kommunikationspartner (z.B. den PC eines Benutzers, der die Daten abruft) ziehen zu können. Wie die gesamte Gesetzeslage so atmet auch der Referentenentwurf die Idee der klassischen Telefonie: Es besteht die (irrige) Annahme, es gäbe eine direkte Kommunikationsverbindung zwischen zwei Teilnehmern, die man – dem Kabel folgend – finden kann. Da Internet-Protokolle i.d.R. tatsächlich eine Kommunikation zwischen zwei Endstellen abbilden, besteht die (irrige) Annahme, jede Gegenstelle sei bereits der Endpunkt der Kommunikation und damit einem Benutzer zuordenbar.

Der fundamentale Irrtum besteht im Glauben an das Prinzip der Ende-zu-Ende-Kommunikation. Dieses Prinzip wurde Mitte der 2000er Jahre durch fortschreitenden Mangel an IPv4 Adressen aufgegeben. Stattdessen entwickelte sich das Privatkunden-Internet in drei Richtungen, die oft gleichzeitig angeboten werden:

1. Kunden bekommen öffentliche IPv4-Adressen als Premiumprodukt
2. Kunden bekommen öffentliche IPv6-Adressen
3. Kunden bekommen nicht-öffentliche IPv4-Adressen zugewiesen und erreichen das Internet über Mittelboxen, die die Adressen umschreiben (Carrier Grade Network Address Translation – CGNAT)

Um aus den (entfernt erfassten) Protokolldaten auf die Bestandsdaten der (unbekannten) Gegenstelle schließen zu können, müssen die Verkehrsdaten beim ISP rechtzeitig abgefragt werden. Bisher gibt es keine Notwendigkeit für eine längere Speicherung der Verkehrsdaten beim ISP. Aktuell wird seitens der Datenschützer aber eine Frist von einigen Tagen zwecks Beseitigung von Betriebsstörungen toleriert. Dieses Zeitfenster soll der Referentenentwurf auf drei Monate ausdehnen.

Gestatten Sie mir zunächst eine Abschätzung der dabei anfallenden Datenmengen: Im Fall der Zuteilung von öffentlichen IP-Adressen an den Kunden bleibt diese Zuteilung meist mehrere Stunden stabil. Es genügt also zu erfassen, welcher Kunde wann welche Zuteilung für wie lange bekam. Die Datenmengen liegen dabei pro Kunde bei ca. 50 Byte pro Zuweisung (128bit Adresse, 64bit Zeitstempel, 64bit Kundenkennung plus weitere Metadaten). Bei durchschnittlich vier Änderungen pro Tag sind das 20kByte pro Kunde für drei Monate. Ein

mittlerer ISP mit ca. 100000 Endkundenanschlüssen benötigt dafür also minimal 2 GByte Speicherplatz. In der Praxis wird die Art der Datenspeicherung das Zehnfache (plus Backup) benötigen.

Im Fall von (CG)NAT ist die Situation deutlich schwieriger. Viele Kunden mit nicht-öffentlichen IPv4-Adressen werden durch Mittelboxen auf weniger öffentliche IPv4-Adressen umgesetzt. Dabei werden die Portnummern der (TCP oder UDP)-Verbindungen umgeschrieben. Ein Verhältnis von 250 Kunden pro öffentliche IPv4-Adresse ist für einen mittleren ISP durchaus typisch. Als Faustformel gilt: Je mehr Kunden ein ISP hat, desto mehr Kunden teilen sich eine öffentliche NAT-IP.

Da nur ca. 64000 Port-Nummern (es gibt reservierte Bereiche) pro IPv4-Adresse zur Verfügung stehen, kann ein Kunde bei einer direkten Zuordnung der Portnummer zum Kunden (**Cone-NAT**) nur ca. 250 Ports benutzen. Offenbar hat der Referentenentwurf dieses Modell im Blick, wenn von der Erfassung der Portnummern zusammen mit der öffentlichen IPv4-Adresse gesprochen wird.

Leider ist Cone-NAT in der Praxis völlig unzureichend: Die meisten modernen Webseiten benötigen in schneller Folge mehrere hundert Verbindungen. Dazu kommen hunderte von DNS Anfragen. Eine Webseite wie z.B. Google Maps wird mit 250 freien Ports schlicht nicht vollständig aufgebaut. Bei vielen Social-Media Seiten fehlen dann Bilder oder andere Teile des Inhaltes. Eine Wiederverwendung der Port-Nummern ist insbesondere bei UDP Kommunikation schwierig, da es kein definiertes Ende der Kommunikation gibt. Der Port muss also über längere Zeit auf Verdacht mit diesem Kunden belegt bleiben.

Bei der Verwendung von **Symmetric-NAT** geht auch die Gegenstelle der Kommunikation mit ein. So stehen alle 64000 Ports einer öffentlichen IPv4-NAT-Adresse für jede Server-IP und jeden Server-Port (i.d.R. immer 443) zu Verfügung. Eine Anfrage *welcher Nutzer hatte zum Zeitpunkt x die IP y mit Port z* ist deswegen nicht beantwortbar. Es wird zusätzlich die Information *die eine s-Verbindung mit Server a auf Port b hatte* benötigt.

Man benötigt ca. 100 Byte pro Verbindung (3·32bit IPv4, 3·16bit Port, 16bit Protokoll, 64bit Zeitstempel, 64bit Kundenkennung plus Metadaten). Mit durchschnittlich einem Verbindungsaufbau pro Minute (über den Tag gerechnet, d.h. einige zig-tausend in kurzer Zeit und dann lange Pausen) bei Wenignutzern entstehen so 13 MByte pro Kunde für drei Monate. Ein mittlerer ISP wird also 2 TByte Verkehrsdaten verwalten müssen, die real sich auf 20 TByte Plattenplatz plus Backup ausdehnen.

Hat der ISP auch einige Poweruser (Familien mit Kindern reichen da schon), so kann man mit dem Mehrfachen an Platzbedarf rechnen. 10% der Nutzer machen jeder für sich so viele Verbindungen auf, wie der Rest aller Kunden zusammen, so dass der Platzbedarf um den Faktor 10 auf 200 TByte (plus Backup) anwächst.

Die Rechnung ist allerdings für normale Nutzung ohne besondere Vorkommnisse. Sollte ein(!) Nutzer Teil einer(!) dDOS-Attacke sein (z.B. durch ein(!) gekapertes IoT-Device), so generiert allein ein(!) solcher Vorgang ca. 1000 Verbindungsaufbauten pro Sekunde: Es entstehen hierbei 360 MByte pro Stunde an Verkehrsdaten für den einzelnen(!) Angriff.

Solche Angriffe passieren leider täglich und sind für die Strafverfolgung von hohem Interesse. Derartige explosionsartig anfallende Datenmengen sind also genau die Verkehrsdaten, auf die der Referentenentwurf abzielt. Deswegen ist es nicht möglich, in Anbetracht der Datenmenge eine Ausnahme für Angriffe von der Speicherpflicht zu machen, wenn der Referentenentwurf überhaupt nützlich sein soll.

Zusammenfassend kann man bei einem mittleren ISP also von ca. **500 TByte an Plattenplatz** für die Speicherung von Verkehrsdaten beim Einsatz von CGNAT ausgehen. Backup kommt extra dazu, um im Falle einer Störung nicht die Daten der letzten Monate zu verlieren. Die zusätzlichen Anforderungen an einen mittleren ISP landen also im PByte Bereich, wenn dieser Referentenentwurf so realisiert würde.

Weiter heißt es in der Begründung des Referentenentwurfs:

> *Die Speicherpflicht betrifft zwar alle Nutzer von Internetzugangsdiensten in Deutschland. Allerdings lassen die Daten nichts anderes zu als die Identifizierung des Anschlussinhabers anhand einer IP-Adresse. Es handelt sich gerade nicht um eine Vorratsdatenspeicherung von allen Verkehrs- und Standortdaten. Aus den gespeicherten IP-Adressdaten lassen sich insbesondere keine Surf- oder Bewegungsprofile erstellen. Die Beeinträchtigung insbesondere der unbescholtenen Nutzer ist damit überschaubar.*

Diese Aussagen sind bei NAT nicht haltbar. Da für die korrekte Zuordnung beide Seiten der Kommunikation bekannt sein müssen, handelt es sich bei der geplanten Speicherung von Verkehrsdaten um eine **unzulässige Vorratsdatenspeicherung**, die genaue Rückschlüsse über das Kommunikationsverhalten des Nutzers zulässt. Das betrifft nicht nur die genauen Zeiten der Kommunikation, sondern auch die Kenntnis der Kommunikationspartner, so dass ein genaues Surf- und Bewegungsprofil erstellt werden kann.

Abschließend gibt es also drei Möglichkeiten:

1. Alle Referenzen auf Portnummern werden aus dem Referentenentwurf entfernt. Dies führt dazu, dass nur die Speicherfrist für die Zuordnung öffentlicher IP-Adressen erweitert wird. **CGNAT-Nutzer werden dann nicht erfasst**. Dies entspricht einer graduellen Ausweitung der aktuellen Rechtslage.
2. Der Einsatz von **CGNAT wird verboten**. Da es nicht genügend IPv4 Adressen für alle Kunden gibt, wird die Anzahl der Internetanschlüsse für Haushalte beschränkt.
3. Die **verpflichtende Umsetzung des RFC 6540** für die deutschen ISPs wird eingefordert: Mit dem Wechsel auf IPv6 only besteht kein Bedarf mehr an NAT. Die Umsetzung des RFC muss deswegen gesetzlich verpflichtend sein, damit die ISPs sich nicht in einem ruinösen Wettbewerb für legacy IPv4-Nutzer gegenseitig kaputt machen. Während der Übergangszeit bleibt es bei Möglichkeit 1 für Bestandsverträge. Neuverträge sind ab einem Stichtag generell nur noch IPv6 only.

Danke für Ihr Interesse.

Lutz Donnerhacke