PRESSEMITTEILUNG

07. Juni 2011

# IPv6: Datenschutz im Internet der Zukunft sicherstellen

Morgen ist „World IPv6 Day“. An diesem Tag wollen viele große Internetdienste-anbieter ihren Datenverkehr soweit möglich für 24 Stunden über das neue Internet-Protokoll IPv6 abwickeln. Diese neue Technologie löst jedoch nicht nur bestehende Probleme, sondern birgt auch neue Risiken für die Persönlichkeitsrechte von Internetnutzerinnen und Internetnutzern. Das morgige Datum ist daher ein Anlass, sich mit der Technik von IPv6 und den damit einhergehenden Neuerungen kritisch auseinanderzusetzen.

Grund für die Einführung von IPv6 ist, dass unter dem Vorgänger IPv4 „nur“ 4,3 Milliarden IP-Adressen zur Verfügung standen. Diese sind jedoch inzwischen verteilt und es besteht so das Problem der Adressknappheit. IPv6 löst dieses Problem, indem die bisherige Adresslänge von 32 bit auf 128 bit erhöht wird. Aufgrund dieser Länge stehen mehr Kombinationsmöglichkeiten und somit zig Milliarden Mal mehr IP-Adressen zur Verfügung. Doch unterscheiden sich die beiden Protokolle nicht nur durch die unterschiedliche Länge der IP-Adressen. IPv6-Adressen bestehen aus zwei grundlegend unterschiedlichen Teilen. Die erste Hälfte der Adresse (sog. Präfix) wird Internetnutzern vom Access-Provider zugewiesen, die zweite Hälfte (sog. Interface Identifier) wird vom jeweiligen Endgerät (zum Beispiel PC, Smartphone, TV-Receiver) festgelegt. Beide Teile bergen Risiken für den Datenschutz.

IP-Adressen wurden bisher meist dynamisch vergeben. Dies bedeutet, dass Internetnutzern nach jeder Trennung eine neue IP-Adresse zugewiesen wird. Unter IPv6 stehen so viele IP-Adressen zur Verfügung, dass Access-Provider jedem Kunden dauerhaft dasselbe Präfix zuweisen könnten. Dadurch steigt das Risiko, dass Diensteanbietern die Person hinter der IP-Adresse bekannt und sie bei jedem Besuch einer Webseite wiedererkannt wird, auch wenn sie sich nicht namentlich anmeldet. Dies gilt auf Dauer bei jeder Nutzung eines Internetdienstes (zum Beispiel

E-Mail, Voice over IP, Filesharing) und wäre das Ende jedweder Anonymität im Internet – im Ergebnis eine kleine Vorratsdatenspeicherung durch die Hintertür, weil die IP-Adresse dann als Bestandsdatum dauerhaft gespeichert würde.

Das zweite Risiko liegt in dem vom Endgerät erstellten Interface Identifier. Sind die Geräte so eingestellt, dass dauerhaft eine eindeutige Nummer benutzt wird, so ist die Internetnutzung nicht nur einem Anschluss, sondern sogar einem konkreten Endgerät zuzuordnen. Dies lässt sich durch die Nutzung von so genannten Privacy Extensions verhindern. Leider sind Privacy Extensions bei vielen Geräten standardmäßig deaktiviert oder überhaupt nicht verfügbar.

Dazu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: „Der Schutz der Persönlichkeitsrechte von Internetnutzerinnen und Internetnutzern darf nicht ins Belieben der Access-Provider oder Gerätehersteller gestellt werden. Bedauerlicherweise existiert in Deutschland noch keine datenschutzrechtliche Produktverantwortung. Die Einführung von IPv6 zeigt wieder einmal, wie dringend erforderlich eine solche Regelung ist."

Zwar haben mehrere große Access-Provider angekündigt, IP-Adressen auch weiterhin dynamisch zu vergeben. Dabei ist jedoch nicht klar, ob damit eine Vergabe gemeint ist, bei der die Adresse hinreichend häufig gewechselt wird und die so den gleichen Schutz bietet wie bisher unter IPv4. Auch ist eine solche Ankündigung nicht verbindlich. Anreize für eine statische Vergabe könnten zunächst einmal wirtschaftlicher Natur sein, indem man die dynamische Vergabe künftig nur noch gegen Aufpreis anbietet, weil sie dann die Ausnahme darstellt. Ferner könnten Access-Provider unter sicherheitspolitischen Druck geraten, durch statische Vergabe eine kleine Vorratsdatenspeicherung einzuführen und so die strengen Anforderungen des Bundesverfassungsgerichts an die Datensicherheit bei der Vorratsdaten-speicherung von Verkehrsdaten zu umgehen.

„Dauerhaften Schutz kann hier wiederum letztlich nur der Gesetzgeber gewährleisten. Er ist aufgrund seiner Verpflichtung zum Schutz des Grundrechts der informationellen Selbstbestimmung dazu aufgerufen, Access-Provider durch eine entsprechende Regelung im Telekommunikationsgesetz dazu zu verpflichten, kostenneutral eine echte dynamische Vergabe von IP-Adressen auch unter IPv6 anzubieten. Dies gibt den Access-Providern dann auch die notwendige

Rechtssicherheit, insbesondere gegenüber weitergehenden sicherheitspolitischen Forderungen“, so Caspar abschließend.

**Pressekontakt**

**Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit**
**Klosterwall 6, 20095 Hamburg**
**Tel.: 040/42854-4153, Fax: 040/427911-833**
**E-Mail: Presse@datenschutz.hamburg.de**

**Pressekontakt**

**Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit**
**Klosterwall 6, 20095 Hamburg**
**Tel.: 040/42854-4153, Fax: 040/427911-833**
**E-Mail: Presse@datenschutz.hamburg.de**