International Working Group
on Data Protection
in Telecommunications

675.24.17

Arbeitspapier zur Nutzung eindeutiger Identifikatoren in Telekommunikationsendgeräten:

Das Beispiel IPv6

31. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 26./27. März 2002 in Auckland (Neuseeland)

- Übersetzung –

Aufgrund einer vorhersehbaren Verknappung in dem gegenwärtig für die meisten Internetverbindungen genutzten Protokoll (IP Version 4) ist durch die Internationale Internet Engineering Task Force (IETF) eine Veränderung des Protokolldesigns ausgearbeitet worden. Dieses neue Protokoll IPv6 nutzt eine Ziffernfolge von 128 Bit anstatt der 32 Bit in der vorherigen Version zur Darstellung individueller IP-Adressen im Internet.

Diese neue Adressierung beinhaltet aufgrund ihrer vergrößerten Kapazität viele Vorteile und ermöglicht neue Dienste wie Multicasting (schnelle Übertragung von großen Datenmengen zu einer Vielzahl von Empfängern, z. B. Video on-line), voice over IP usw.

Allerdings erweckt das neue Protokoll auch Bedenken, da es so beschaffen ist, dass jede IP-Adresse teilweise aus einer eindeutigen Nummernfolge wie einem globalen, eindeutigen Identifikator zusammengesetzt werden kann. Die Einführung von IPv6 könnte zu erhöhten Risiken der Profilbildung von Nutzeraktivitäten im Internet führen[1].

Die folgenden vorläufigen Überlegungen identifizieren die Risiken und verweisen auf die Datenschutzgrundsätze, die in Betracht gezogen werden müssen, wenn eindeutige Identifikatoren bei der Bildung von IP-Adressen genutzt werden.

I. Identifizierte Risiken

Die Charakteristiken von IPv6 bedingen spezifische Risiken für die Privatsphäre, die von der Art der Konfiguration des neuen Protokolls abhängig sind.

- Probleme der Profilbildung stehen zur Debatte, wenn ein eindeutiger Identifikator (die Kennung der Schnittstelle, die z. B. auf der eindeutigen MAC-Adresse einer Internet-Karte basieren kann) in die IP-Adresse jeder elektronischen Kommunikationseinrichtung eines Nutzers

[1] Die zusammenhängende Profilbildung über Aktivitäten eines Nutzers könnte sogar möglich sein, wenn dieselben Endeinrichtungen in verschiedenen Netzen genutzt werden.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Pallasstr 25/26
D-10781 Berlin
Phone +49 / 30 / 7560 7809
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

integriert wird. In diesem Fall kann die gesamte Kommunikation viel einfacher, als dies unter Nutzung von Cookies heute der Fall ist, zusammengeführt werden.

- Es können Probleme der Sicherheit und der Vertraulichkeit festgestellt werden. Diese Risiken hängen mit der Entwicklung neuer Netzwerkdienste zusammen, die die Vervielfachung der Endgeräte beinhalten, die mit dem Netzwerk über dasselbe Kommunikationsprotokoll verbunden sind: Mobiltelefone, Personalcomputer, elektronische Agenten zur Kontrolle von Haushaltsgeräten (Heizung, Licht, Alarmanlagen usw.).

Das neue IPv6-Protokoll ermöglicht dauerhafte Verbindungen, bei denen sogar in den Fällen, in denen ein Endgerät innerhalb des Netzwerkes versetzt wird, dieselbe Adresse beibehalten wird. Hier spielen Aspekte der Sicherheit und der Vertraulichkeit eine Rolle, da ein Risiko der Identifikation von Aufenthaltsinformationen dieser mobilen Knoten existiert[2].

II. Auf IPv6 anwendbare Datenschutzprinzipien

Die Arbeitsgruppe hält es für erforderlich, die Aufmerksamkeit aller Beteiligten, die für die Ausarbeitung und Implementierung des neuen Protokolls verantwortlich sind, auf die nationalen und internationalen gesetzlichen Anforderungen zum Datenschutz und zur Sicherheit der Telekommunikation zu lenken.

Es ist heute weithin anerkannt, dass eine IP-Adresse – und *a fortiori* eine eindeutige Identifikationsnummer, die in die Adresse integriert ist – als personenbezogenes Datum im Sinne der gesetzlichen Bestimmungen angesehen werden kann[3].

Im Einklang mit ihrer bisherigen Arbeit und den gemeinsamen Standpunkten, die zu dieser Problematik bereits verabschiedet worden sind[4], erinnert die Arbeitsgruppe an die folgenden Prinzipien, die bei der Implementierung des neuen Internet-Protokolls in Betracht gezogen werden sollten.

Telekommunikationsinfrastruktur und technische Geräte müssen so konstruiert sein, dass entweder überhaupt keine personenbezogenen Daten oder so wenig personenbezogene Daten wie technisch möglich genutzt werden, um Netze und Dienste zu betreiben. Ein eindeutiger Identifikator einer Schnittstelle, wie er in IPv6 integriert ist, würde einen Identifikator zur generellen Anwendung darstellen.

---

[2] vgl. A. Escudero Pascual „Anonymous and untraceable communications: location privacy in mobile internetworking", 16. Mai 2001; "Location privacy in IPv6 – Tracking the binding updates", 31. August 2001; http://www.it.kth.se/~aep/ .

[3] vgl. z. B. auf der europäischen Ebene die Mitteilung der Kommission «Organisation und Verwaltung des Internet – Internationale und europäische Grundsatzfragen 1998 – 2000» KOM (2000) 202 endg. vom April 2000, und die von der Datenschutz-Arbeitsgruppe nach Art. 29 verabschiedeten Dokumente, besonders „Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz", WP 37, 21. November 2000, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf ;

[4] Gemeinsamer Standpunkt zu Online-Profilen im Internet, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000; http://www.datenschutz-berlin.de/attachments/187/pr.de.pdf
Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001; http://www.datenschutz-berlin.de/attachments//213/locat_de.pdf ;
Zehn Gebote zum Schutz der Privatheit im Internet – Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000; http://www.datenschutz-berlin.de/attachments/215/tc_de.pdf .

- Im Gegensatz zum Prinzip der Datenminimierung würde eine derartige Nutzung eines eindeutigen Identifikators ein Risiko zur Bildung von Profilen Einzelner über all ihre Aktivitäten im Zusammenhang mit einem Netzwerk bilden.

- Der Schutz des Grundrechts auf Datenschutz gegen solche Risiken der Profilbildung muss bei der Analyse der verschiedenen Aspekte des neuen Protokolls, wie seiner Handhabbarkeit*,* als oberster Grundsatz gelten.

- Verbindungsdaten, und insbesondere Aufenthaltsinformationen, verdienen aufgrund ihres sensiblen Charakters einen besonderen Schutz[5].

Wenn Aufenthaltsinformationen bei der Nutzung mobiler Endgeräte und anderer Objekte, die über IP verbunden sind, erzeugt werden müssen, müssen diese Informationen gegen unrechtmäßiges Abhören und Missbrauch geschützt werden. Es sollte auch verhindert werden, dass Aufenthaltsinformationen (und die Veränderung dieser Aufenthaltsinformationen aufgrund der Bewegung des mobilen Benutzers) unverschlüsselt zum Empfänger dieser Informationen über den „Header" der genutzten IP-Adresse übertragen werden.

Protokolle, Produkte und Dienste sollten so beschaffen sein, dass sie Wahlmöglichkeiten für permanente oder veränderbare Adressen bieten. Die Grundeinstellungen sollten für ein hohes Maß an Datenschutz sorgen.

Da diese Protokolle, Produkte und Dienste sich ständig weiterentwickeln, wird die Arbeitsgruppe diese Entwicklungen genau beobachten und, soweit dies notwendig ist, zu einer spezifischen Regulierung aufrufen.

[5] vgl. Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001; ; http://www.datenschutz-berlin.de/attachments//213/locat_de.pdf