10750/02/DE/endg.
WP 58

Stellungnahme 2/2002 über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6

Angenommen am 30. Mai 2002

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung und insbesondere auf Artikel 12 und 14 -

hat folgende Stellungnahme angenommen:

Mitteilung der Kommission über IPv6

Am 21. Februar 2002 verabschiedete die Europäische Kommission eine Mitteilung an den Rat und das Europäische Parlament, die sich mit dem Internet der nächsten Generation und den vorrangigen Maßnahmen beim Übergang zum neuen Internetprotokoll IPv6 befasst. Diese Mitteilung steht im Zusammenhang mit der aktuellen Entwicklung bei Netzdiensten und netzwerkfähigen Telekommunikationsendeinrichtungen.

Das neue Internetprotokoll wurde erarbeitet, um die Möglichkeiten zum drahtlosen oder drahtgebundenen Netzzugang über eine Vielfalt von Endgeräten, darunter Mobiltelefone, Personalcomputer oder persönliche digitale Assistenten (PDAs), zu erleichtern und zu vereinheitlichen.

Diese Entwicklungen können nur befürwortet werden; gleichzeitig möchte die Datenschutzgruppe aber betonen, dass die Auswirkungen des neuen Protokolls auf den Schutz personenbezogener Daten sorgfältig und gründlich untersucht werden müssen.

Die Gruppe begrüßt die Position, die die Kommission in ihrer Mitteilung eingenommen hat, wonach eine Auseinandersetzung mit Fragen des Daten- und Persönlichkeitsschutzes bei der Weiterentwicklung des Internet erforderlich ist. Die Gruppe betont allerdings, dass auf die Fragen, die die Entwicklung des neuen Protokolls IPv6 aufwirft, noch keine Antwort gefunden wurde.

Zu besonderer Besorgnis gibt die Möglichkeit Anlass, eine eindeutig zuordbare Kennung in die IP-Adresse zu integrieren, so wie es das neue Protokoll vorsieht. Unter diesem Gesichtspunkt bedauert die Datenschutzgruppe, dass sie von der Annahme der Mitteilung nicht konsultiert wurde, und wünscht, an den künftigen Arbeiten auf europäischer Ebene in bezug auf IPv6 beteiligt zu sein.

Datenschutzaspekte im Zusammenhang mit der Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen

Die Datenschutzgruppe nimmt zur Kenntnis, dass die Internationale Arbeitsgruppe „Datenschutz in der Telekommunikation“ kürzlich ein Arbeitspapier zur Frage der Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen vorgelegt hat, und dankt ihr für die dabei erarbeiteten Ergebnisse.

[1] ABl. L 281 vom 23.11.1995, verfügbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

Die Datenschutzgruppe befürwortet die Schlussfolgerungen des Arbeitspapiers, das am 27. März 2002 in Auckland angenommen wurde[2], und möchte dessen Erkenntnisse untermauern, indem sie insbesondere auf mehrere Grundsätze verweist, die in der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und in der Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[3] ausdrücklich erwähnt sind.

Die Datenschutzgruppe möchte betonen, dass es sich bei IP-Adressen, die den Internetnutzern zugewiesen werden, um personenbezogene Daten[4] handelt, die durch die Richtlinie 95/46/EG und 97/66/EG geschützt sind.

Unter Verweis auf die bisher geleisteten Arbeiten zum Schutz personenbezogener Daten im Internet[5] möchte die Datenschutzgruppe besonders folgende Aspekte hervorheben:

- Bei der eindeutigen Kennung einer Schnittstelle, wie sie z. B. in IPv6 integriert werden könnte, würde es sich um eine Kennung von allgemeiner Bedeutung handeln; ihre Verwendung als solche ist im innerstaatlichen Recht der EU-Mitgliedstaaten geregelt.

- Der Grundsatz der Verhältnismäßigkeit verlangt, dass nach Abwägung der Grundrechte des Betroffenen gegen die Interessen der einzelnen, an der Übertragung von Telekommunikationsdaten beteiligten Akteure (z. B. Unternehmen, Zugangsanbieter) so wenig personenbezogene Daten wie möglich verarbeitet werden.

  Dieser Grundsatz hat Auswirkungen einerseits auf die Konzeption der neuen Kommunikationsprotokolle und –geräte, andererseits auf den Inhalt einzelstaatlicher Strategien im Zusammenhang mit der Verarbeitung von Telekommunikationsdaten: Die Technik an sich ist neutral, um so mehr sollte bei den Anwendungen und der Konzeption neuer Telekommunikationsgeräte a priori auf die Gewährleistung des Privatsphärenschutzes geachtet werden. Darüber hinaus sollte es vermieden werden,

---

[2] Siehe Anhang.

[3] Die Richtlinie 97/66/EG wird derzeit geändert, um sie an die technologische Entwicklung anzupassen. Die neue Richtlinie soll die Nutzer öffentlich zugänglicher elektronischer Kommunikationsdienste schützen, und zwar unabhängig von der eingesetzten Technik.

[4] Laut Erwägungsgrund 26 der Richtlinie 95/46/EG gelten Daten als personenbezogen, sobald der für die Verarbeitung Verantwortliche oder ein Dritter mit vertretbarem Aufwand einen Bezug zur Identität des Betroffenen (in diesem Fall zum Nutzer der IP-Adresse) herstellen kann. Anhand der IP-Adresse können die Informationsdienstanbieter immer einen Bezug zwischen IP-Adresse und Identität des Nutzers herstellen und dies könnte auch anderen gelingen, z. B. indem sie auf die verfügbaren Verzeichnisse zugewiesener IP-Adressen zurückgreifen oder andere technische Möglichkeiten nutzen.

[5]
§ Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet, angenommen von der Datenschutzgruppe am 23. Februar 1999, 5013/99/DE/endg., WP 16;
§ Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware, angenommen am 23. Februar 1999, 5093/98/DE/endg., WP 17;
§ Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs, angenommen am 3. Mai 1999, 5005/99/endg., WP 18;
§ Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke, angenommen am 7. September 1999, 5085/99/DE/endg., WP 25;
§ Stellungnahme 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Geschäftsverkehrs, vorgelegt von der Internet-Taskforce, angenommen am 3. Februar 2000, 5007/00/DE/endg., WP 28;
§ Stellungnahme 2/2000 zur allgemeinen Neugestaltung des Rechtsrahmens für den Telekommunikationssektor, vorgelegt von der Internet-Taskforce, angenommen am 3. Februar 2000, 5009/00/DE/endg., WP 29;
§ Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 - KOM (2000) 385, angenommen am 2. November 2000, 5042/00/DE/endg., WP 36.
§

Maßnahmen zu verallgemeinern, die die systematische Identifizierbarkeit von Telekommunikationsdaten erzwingen/forcieren.

So gesehen sollten Netz– und Zugangsanbieter jedem Nutzer einer Telekommunikationsverbindung anbieten, das Netz oder einen Dienst anonym bzw. unter einem Pseudonym in Anspruch zu nehmen.

Laut Richtlinie 97/66/EG ist jedem Nutzer die Möglichkeit einzuräumen, die Anzeige des rufenden und angerufenen Anschlusses einzuschränken. Bei Internetverbindungen könnte die Anonymität z. B. dadurch erreicht werden, dass die IP-Adressen, die ein Betroffener nutzt, regelmäßig geändert werden[6].

- In Anbetracht der Risiken der Manipulation oder betrügerischen Verwendung einer eindeutigen Kennung erinnert die Datenschutzgruppe daran, dass Schutzmaßnahmen erforderlich sind, wobei insbesondere der Tatsache Rechnung zu tragen ist, dass Telekommunikationsanbieter für die Sicherheit der von ihnen angebotenen Dienste verantwortlich sind. Das Gemeinschaftsrecht verlangt von Zugangsanbietern, ihre Abonnenten über Sicherheits-Restrisiken zu informieren.

- Die Erfordernisse datenschutzgerechter Voreinstellungen von Kommunikationsgeräten und datenschutzgerechter Telekommunikationsdienste wurden auf europäischer Ebene durch besondere Verpflichtungen umgesetzt, die hauptsächlich den Herstellern von Telekommunikationsgeräten sowie den Telekommunikationsbetreibern und Dienstanbietern[7] auferlegt sind.

Fazit

Die Datenschutzgruppe befürwortet nachdrücklich alle Forschungsinitiativen, die der Erarbeitung technischer Lösungen zum Schutz von Telekommunikationsdaten dienen.

Die Datenschutzgruppe ist sich der Tatsache bewusst, dass verschiedene Arbeitsgruppen bereits Initiativen ergriffen haben, um technische Lösungen für einige bekannte Datenschutzrisiken zu erarbeiten; es erscheint ihr notwendig, vorrangig den Dialog mit Vertretern dieser Arbeitsgruppen aufzunehmen, insbesondere mit der Internet Engineering Task Force und der IPv6 Task Force.

Die Datenschutzgruppe behält sich vor, bei der Begutachtung der neu konzipierten Kommunikationsprotokolle, –geräte und –dienste und parallel zu den Gesprächen mit den Akteuren, die an der Konzeption dieser neuen Kommunikationsinstrumente beteiligt sind, weitere Schritte zu ergreifen.

---

[6] Einige Zugangsanbieter haben bereits eine derartige Lösung gewählt; sie ändern etwa jeden zweiten Tag die IP-Adresse ihrer ADSL-Kunden.
Die Entwickler einiger Endgeräte richten sich bereits nach dem Standard RFC 3041 der Internet Engineering Task Force IETF (siehe Veröffentlichung vom Januar 2001 „Privacy Extensions for Stateless Address Autoconfiguration in IPv6“): Das Endgerät verwendet zwei unterschiedliche Adressen; eine Adresse wird auf der Basis der eindeutigen MAC-Adresse generiert und wird für ankommende Verbindungen genutzt (das Endgerät ist immer unter dieser permanenten Adresse erreichbar); die zweite Adresse stammt von einem (Pseudo-)Zufallsgenerator und wird vom Endgerät für abgehende Verbindungen verwendet.
Wenn also das Endgerät (und der sich dahinter verbergende Benutzer) die Verbindung aufbaut, kann es nicht über seine MAC-Adresse identifiziert werden.

[7] Siehe Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ferner Richtlinie 99/5/EG über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität, ABl. L 91 vom 7.4.1999.

Anhang

Arbeitspapier über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6

31. Sitzung der Internationalen Arbeitsgruppe „Datenschutz in der Telekommunikation“ vom 26.–27. März 2002 in Auckland (Neuseeland)

Aufgrund eines vorhersehbaren Engpasses beim derzeit für die meisten Internetverbindungen verwendeten Protokoll (IP Version 4), hat die internationale Internet Engineering Task Force ein neues Konzept erarbeitet. Das neue Protokoll, IPv6, verwendet eine Zeichenkette von 128 Bit anstelle von 32 Bit in der früheren Version, um die einzelnen IP-Adressen im Internet zu bilden.

Die neue Adresse hat dank ihrer erweiterten Kapazität viele Vorteile und ermöglicht neue Funktionen wie z. B. Multicasting (raschere Übermittlung großer Datenbestände an mehrere Empfänger gleichzeitig, z. B. Online-Video), Internettelefonie (Voice over IP) usw.

Allerdings gibt das neue Protokoll auch Anlass zu Bedenken, da es so konzipiert wurde, dass jede IP-Adresse eine eindeutig zuordbare Zahlenreihe enthalten kann, praktisch wie eine auf der ganzen Welt eindeutige Kennung. Mit der Einführung von IPv6 könnte das Risiko steigen, dass Profile der Internet-Aktivitäten der Benutzer erstellt werden[8].

Die folgenden vorläufigen Erwägungen zeigen die Risiken auf und verweisen auf die Datenschutzgrundsätze, denen Rechnung zu tragen ist, wenn bei der Bildung von IP-Adressen eine eindeutige Kennung verwendet wird.

I. Risiken

Die Eigenheiten von IPv6 lassen besondere Datenschutzrisiken erkennen, die von der Konfiguration des neuen Protokolls abhängen.

- *Probleme der Profilerstellung* ergeben sich, wenn eine eindeutige Kennung (die Schnittstellenkennung, z. B. auf der Basis der eindeutigen MAC-Adresse der Ethernet-Karte) in die IP-Adressen aller elektronischen Kommunikationsgeräte des Nutzers integriert wird. In solchen Fällen kann wesentlich leichter ein Bezug zwischen allen Kommunikationsverbindungen des Nutzers hergestellt werden, als es heute mit den Cookies der Fall ist.

- **Es sind auch *Probleme mit der Sicherheit und Vertraulichkeit* festzustellen. Diese Risiken stehen im Zusammenhang mit der Entwicklung von Netzdiensten, die ihrerseits eine Vervielfachung der Gerätetypen mit sich bringen, die über dasselbe Kommunikationsprotokoll an das Netz angebunden werden: Mobiltelefone, Personalcomputer, elektronische Steuerungen für Hausgeräte (Heizung, Beleuchtung, Alarmanlagen usw.).**

[8] Ein umfassendes Aktivitätsprofil könnte selbst dann erstellt werden, wenn dasselbe Endgerät in unterschiedlichen Netzen verwendet wird.

Das neue Protokoll IPv6 ermöglicht feste Verbindungen, wobei die Adresse auch dann bestehen bleibt, wenn das Endgerät sich im Netz bewegt. Sicherheit und Vertraulichkeit stehen hierbei auf dem Spiel, da die Gefahr besteht, dass Daten über den jeweiligen Standort des mobilen Knotens ermittelt werden[9].

II. Für IPv6 geltende Datenschutzgrundsätze

Die Arbeitsgruppe hält es für notwendig, die Aufmerksamkeit aller Akteure, die für die Erarbeitung und Umsetzung des neuen Protokolls zuständig sind, auf die rechtlichen Erfordernisse nationaler und internationaler Prägung im Zusammenhang mit dem Schutz der Privatsphäre und der Sicherheit auf dem Gebiet der Telekommunikation zu lenken.

Es besteht inzwischen weitgehend Einigkeit darüber, dass IP-Adressen - und erst recht eine eindeutig zuordbare Kennziffer innerhalb der Adresse - nach geltendem Recht[10] als personenbezogene Daten anzusehen sind.

Im Einklang mit ihren früheren Arbeiten und den zu diesem Thema bereits verabschiedeten gemeinsamen Standpunkten[11] erinnert die Arbeitsgruppe an folgende Grundsätze, die bei der Implementierung des neuen Internet-Protokolls beachtet werden sollten.

Telekommunikationsinfrastruktur und technische Geräte müssen so konzipiert sein, dass entweder überhaupt keine personenbezogenen Daten oder so wenige wie technisch möglich für den Netz– und Dienstbetrieb verwendet werden. Die eindeutige Kennung einer Schnittstelle, wie sie in IPv6 integriert ist, würde eine Kennung von allgemeiner Bedeutung darstellen.

§ Die derartige Verwendung einer eindeutigen Kennung steht im Widerspruch zum Grundsatz der Datenminimierung und beschwört die Gefahr herauf, dass über die Betroffenen Profile aller ihrer Aktivitäten im Netz erstellt werden.

§ Vor dem Hintergrund der möglichen Profilerstellung muss als oberster Grundsatz bei der Analyse der verschiedenen Aspekte des neuen Protokolls, z. B. seines Facility Management, der Schutz des Grundrechts auf Privatsphäre gelten.

§ Verkehrsdaten, insbesondere Standortdaten, sind besonders sensibel und verdienen daher besonderen Schutz[12].

---

[9] Siehe z. B. A. Escudero Pascual, “Anonymous and untraceable communications: location privacy in mobile iternetworking”, 16. Mai 2001; “Location privacy in Ipv6 – Tracking the binding updates”, 31. August 2001; http://www.it.kth.se/~aep/

[10] Siehe z. B. auf europäischer Ebene die Mitteilung der Kommission über die Organisation und Verwaltung des Internet-Bereichsnamensystems vom April 2000 sowie die von der Datenschutzgruppe angenommenen Papiere, insbesondere „Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz“, WP 37, vom 21. November 2000.

[11] Gemeinsamer Standpunkt zu Online-Profilen im Internet, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000;

§ Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001;

§ 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;
siehe http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm.

[12] Siehe Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001.

Falls Standortdaten bei der Nutzung mobiler Geräte und anderer mittels IP angebundener Objekte erzeugt werden müssen, dann sind die Daten gegen rechtswidriges Abhören und Missbrauch zu schützen. Es sollte ferner vermieden werden, Standortdaten (und durch die Mobilität des Nutzers bedingte Standortveränderungen) unverschlüsselt im Kopf der verwendeten IP-Adresse an den Empfänger der Information zu übermitteln.

Protokolle, Produkte und Dienstleistungen sollten so konzipiert werden, dass zwischen ständigen und temporäre Adressen gewählt werden kann. Die Voreinstellungen sollten ein hohes Datenschutzniveau gewährleisten.

Da sich diese Protokolle, Produkte und Dienstleistungen ständig weiterentwickeln, muss die Arbeitsgruppe die Entwicklungen gewissenhaft weiterverfolgen und bei Bedarf eine gezielte Regulierung verlangen.

Brüssel, den 30. Mai 2002
Für die Gruppe
Der Vorsitzende
Stefano RODOTA