Humanistische Union

Es geht noch mehr ...

Technische Standards zur Vorratsdatenspeicherung ebnen Weg für noch umfangreichere Erfassung, Mitteilungen Nr. 199, Seite 9 - 10

Die Umsetzung der Vorratsdatenspeicherung (VDS) in Deutschland ist beschlossen, doch wie sollen die entstehenden Datenberge durchsucht werden? Schließlich soll für sechs Monate gespeichert werden, wer wann mit wem von wo aus wie lange telefonierte, wer wann im Internet war und wem wann E-Mails geschrieben hat. Ohne einen entsprechenden technischen Standard zum Durchsuchen und Übermitteln der Informationen schafft die VDS nur einen Datenberg, der keinen Nutzen haben kann, also schon im ersten Stadium einer Verhältnismäßigkeitsprüfung scheitern muss. Doch sowohl die Richtlinie selbst als auch das Umsetzungsgesetz schweigen zu Fragen der genauen technischen Durchführung. Nachdem bereits Ende September Entwürfe für einen solchen technischen Standard zur Umsetzung der VDS bekannt wurden, sind Mitte November Teile der endgültigen Spezifikation veröffentlicht worden. Sie stammen vom European Telecommunications Standards Institute (ETSI), einer der drei von der EU anerkannten regionalen Standardisierungsinstitutionen. Von ihm stammt z.B. der Mobilfunkstandard UMTS. Standards für die Überwachung von Telekommunikation werden bei ihm - hinter verschlossenen Türen - vom Lawful Interception Committee erarbeitet. Die interessante Frage hier ist nun, ob die Spezifikation technisch eine Erfassung und Übermittlung von Daten ermöglicht, die rechtlich nicht gedeckt ist - mit anderen Worten: Kann sie mehr als sie darf? Daher soll nun erstens dargestellt werden, nach welchen Kriterien die Datenberge durchsucht werden können und zweitens, welche Daten vorgehalten und bei einem Treffer übermittelt werden sollen. Die Kriterien, nach denen gesucht werden können soll, sind - jeweils mit der zusätzlichen Angabe eine Zeitpunktes oder Zeitfensters - die folgenden:

- Netzwerk- oder Dienstadresse (z.B. Telefonnummer oder IP-Adresse)
- Hardware-Nummer eines Gerätes (Bsp.: Mobiltelefone haben eine weltweit einmalige Seriennummer, die IMEI
- Netzwerkelement (z.B. eine Funkzelle)
- Name und Adresse eines Teilnehmers (inkl. eventuell abweichenden Rechnungsadressen u.Ä.)
- Herkunft oder Ziel einer Verbindung (bestimmt z.B. über Telefonnummer, IMEI, IP-Adresse)
- Positionsinformationen (z.B. Funkzelle)

Bemerkenswert ist dabei, dass für jedes der Kriterien nicht nur nach einem einzelnen Wert, sondern auch nach mehreren Werten oder einem Bereich von Werten gesucht werden kann. Diese Suche mit „Wildcards" erlaubt Abfragen, die zum Beispiel auf unvollständigen Telefonnummern oder verschiedenen Schreibweisen von Namen basieren. Ein Beispiel wäre die Suche nach einem Teilnehmer „Otto M??er" mit der Telefonnummer „12??56". Zu den Abfragekriterien heißt es in den Dokumenten lapidar, dass nicht jede nach den technischen Vorgaben mögliche Suche und Übermittlung auch notwendigerweise in jedem Staat, der die Richtlinie anwendet, legal sein müsse. Dies zu klären, sei Sache der einzelnen Staaten.
Wenn nun eine solche Suche einen oder mehrere Treffer ergibt, sollen nach dem Standard folgende Daten übermittelt werden:

Daten zu Quelle, Ziel und Art der Kommunikation:

- Netzwerk- oder Servicenummer (z.B. IP-Adresse, E-Mail-Adresse)
- Hardwarenummer (z.B. IMEI)
- Namen, Adressen, Benutzerkennungen der registrierten Teilnehmer
- Beginn und Ende eines Kommunikationsvorgangs
- Beginn und Ende der Verbindung mit einem Dienst (z.B. Einwahl in das Internet)
- Daten zur Bestimmung der Art des Kommunikationsvorgangs (Telefongespräch, SMS-Versand, E-Mail-Versand, Chat etc.)

Daten zur Positionsbestimmung bei mobilen Endgeräten:

- Position bei Beginn der Kommunikation (z.B. Ort der aktuellen Funkzelle)
- Ort (z.B. über Postleitzahl) oder IP-Adresse bei Zugang zu einem öffentlichen drahtlosen Netzwerk
- Ort und Zeit der ersten Aktivierung von Prepaid-Diensten, Ort und Zeit der Aufladevorgänge (letzteres optional).
- (optional) Positionsdaten unabhängig von einem Kommunikationsvorgang, z.B. beim Wechsel von Funkzellen oder auf einer periodischen Basis, sowie Daten zum Status des Geräts (im Netz eingeloggt oder nicht)

Wo gehen diese Bestimmungen über die Vorratsdaten-Richtlinie hinaus?

Der wichtigste Punkt ist die mögliche Erfassung von Standortdaten bei Mobilgeräten. Die europäische Richtlinie zur Vorratsdatenspeicherung schreibt vor, dass der Standort eines Mobilgerätes zu Beginn eines Kommunikationsvorganges festgestellt wird. Nach dem ETSI-Standard soll es aber auch möglich sein, die Daten abzufragen, wenn keine Kommunikation im alltäglichen Sinne stattfindet, also beim Wechsel von Funkzellen und bei den regelmäßig durchgeführten „Location Updates", bei denen sich das Telefon kurz beim nächsten Funkmast meldet. Nach der europäischen Richtlinie dürften solche Standortdaten nicht gespeichert werden. Der ETSI-Standard sieht hier eine folgenreiche Erweiterung vor: Während die Bestimmungen der Richtlinie die Erstellung von einigermaßen präzisen Bewegungsprofilen nur bei Vieltelefonierern erlaubt, ermöglicht der technische Standard die Erstellung solcher Profile für alle Besitzer von Mobiltelefonen, selbst wenn sie nicht telefonieren, sondern ihr Gerät nur im eingeschalteten Zustand mit sich herumtragen. Auch die mögliche Erfassung von Ort und Zeit des Aufladens von Prepaid-Diensten ist nicht über die Richtlinie gedeckt. Gleiches gilt für die Erfassung von zusätzlichen Postanschriften der Kunden und deren Änderungen. Die Richtlinie nennt an Internetdiensten, deren Nutzung protokolliert werden soll, abschließend Internettelefonie und E-Mail. Der ETSI-Standard hingegen fordert generell eine Erfassung des genutzten Internetdienstes – also auch von anderen Diensten wie einem Internet Relay Chat (IRC). Die Erfassung umfangreicherer Standortdaten sowie die Erfassung von Adresswechseln sind optional. Allerdings ist zu befürchten, dass Daten, die erhoben werden können, früher oder später auch erhoben und verwendet werden. Was technisch möglich ist, wird auch rechtliche Begehrlichkeiten bei der Exekutive wecken – die Diskussion um den Einsatz von Mautdaten zur Strafverfolgung kann hier als Beispiel dienen. Doch warum gehen die technischen Möglichkeiten überhaupt über die rechtlichen hinaus? Eine erste Antwort darauf liefert die Zusammensetzung des Lawful Interception Committee. Einige seiner Mitglieder haben Verbindungen zu Herstellern von Telekommunikationstechnik, zu Geheimdiensten und zu Strafverfolgungsbehörden. Interessant ist auch die starke Beteiligung von Vertretern, die ihren Tätigkeitsschwerpunkt außerhalb der Europäischen Union haben, etwa des US-Unternehmens VeriSign und der Australischen Kommunikations- und Medienagentur – ein Schelm, wer Böses dabei denkt.
Owe Langfeldt ist Student der Politikwissenschaft und arbeitet als freier Mitarbeiter für das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein in Kiel.

Quellen:
Handover interface for the request and delivery of retained data V0.2.1 - technische Spezifikation der

Übergabeschnittstelle [Entwurf], http://www.quintessenz.at/d/000100003928
Requirements of Law Enforcement Agencies for handling Retained Data V0.4.0 - Pflichtenheft für Telekommunikationsanbieter [Entwurf],
http://www.quintessenz.at/d/000100003929 - Lawful Interception (LI); Retained Data V1.1.1 - Pflichtenheft für Telekommunikationsanbieter [endgültige Version],
http://webapp.etsi.org/action%5CPU/20071113/ts_102656v010101p.pdf

---

https://www.humanistische-union.de/thema/es-geht-noch-mehr/
Abgerufen am: 29.01.2023