

Vorratsdatenspeicherung und der gläserne Bürger

Jan Schmidt, <jbs@guug.de>

Man fühlt sich an George Orwells „1984“ erinnert, wenn man die Pläne der Bundesregierung zur Vorratsdatenspeicherung betrachtet. Bundesjustizministerin Zypries geht mit ihren Plänen weit über die Vorlage der EU-Kommission hinaus, möchte noch mehr Daten noch länger speichern als im Entwurf der EU-Kommission vorgesehen. Doch der Reihe nach.

Die EU plant seit 2004, eine gesetzliche Grundlage zu schaffen um Verbindungs- und Standortdaten aller Arten von Telekommunikation (u. a. DSL, Mail, SMS, VoIP) längerfristig zu speichern. Auf die gespeicherten Daten sollen staatliche Einrichtungen wie beispielsweise Zoll, Polizei, die Finanzkontrolle Schwarzarbeit des Zolls sowie die Nachrichtendienste Zugriff haben.

Die „Richtlinie des Europäischen Parlaments und des Rates über die Vorratsdatenspeicherung von Daten (...)“ soll nunmehr mit Hilfe des „Gesetzes zur Neuregelung der Telekommunikationsüberwachung“ in nationales Recht gegossen werden.

Dies würde konkret bedeuten, dass ab dem 1.1.2008 sämtliche Verbindungsdaten aller Bundesbürger mindestens 6 Monate lang gespeichert werden. Bislang ist die Speicherung nur für Abrechnungszwecke zulässig, bei Nutzern einer DSL-Flatrate entfällt die Speicherung, da sie für die eigentliche Abrechnung nicht benötigt wird. Bundesjustizministerin Zypries sieht sogar bis zu 24 Monate Speicherung vor, obwohl die EU nur 6 Monate fordert.

Gespeichert würden nicht die Inhalte, allerdings ist es anhand des Kommunikationsprofils eines Menschen natürlich möglich, Rückschlüsse auf seine Lebensumstände zu ziehen. Wann surft jemand privat im Internet? Zu wem hat der/die Betreffende Kontakt? Auch die Kontaktaufnahme zu einem Arzt, einem Seelsorger, einem Anwalt würde gespeichert und könnte mindestens 6 Monate lang abgerufen werden. Mit Hilfe der Verbindungsda-

ten ließe sich außerdem ein umfassendes Bewegungsprofil erstellen.

Diese allumfassende Überwachung verstößt gegen diverse Grundrechte, so unter anderem das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis. Auch die Schweigepflicht von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten sowie der Informatenschutz für Journalisten wären letztlich betroffen.

Begründet wird diese Stasi-ähnliche Ausweitung der Überwachungsbefugnisse natürlich wie so oft mit dem Hinweis darauf, dass die Ermittlungsbehörden diese Daten benötigen, um z. B. Terroranschläge oder schwere Straftaten zu verhindern.

Interessanterweise existiert die Vorratsdatenspeicherung in Irland bereits seit 3 Jahren, auf die Kriminalitätsstatistik hat sie sich nicht ausgewirkt. Man spricht von 0,006% mehr aufgeklärten Verbrechen. Kriminelle haben genügend Möglichkeiten, weiterhin verdeckt zu kommunizieren – ob im direkten Kontakt, durch die Nutzung von im Ausland erworbenen Pre-Paid-Handys, über Boten, per Post, durch die Nutzung von Anonymisierungsdiensten oder die Nutzung von ausländischen Mailanbietern.

Umso mehr stimmt es bedenklich, dass hier ein neuer grosser Datenpool geschaffen wird. Die Erfahrung zeigt, dass solche Daten nach einiger Zeit auch für andere Parteien als die ursprünglich angekündigten zugänglich gemacht werden. Man denke hier nur an den Zugriff auf gespeicherte Daten von Bankkonten, anfangs nur für

die Steuerbehörden vorgesehen. Heute haben sowohl die Bundesagentur für Arbeit, das Bundesamt für Ausbildungsförderung und andere Zugriff darauf.

Ähnlich sieht es mit den Daten der Mautbrücken aus. Erfasst werden alle Fahrzeuge, ob Laster oder PKW. Gespeichert und ausgewertet werden derzeit nur die Daten der LKWs – aber das lässt sich natürlich schnell ändern. Die PKW-Maut war schon oft genug im Gespräch.

Würde man alle Daten zusammenfassen die heute bereits irgendwo gespeichert werden (Bankdaten, Bewegungsdaten per PKW, Bewegungsdaten des Handys, Kaufverhalten anhand der diversen Bonuskarten, Kommunikationsprofile aus der Vorratsdatenspeicherung) und sie mit einem eindeutigen Schlüssel indizieren (hier würde sich die „lebenslange Steuernummer“ anbieten, die jeden Bundesbürger eindeutig identifiziert) wäre man in einem Zeitalter angelangt, in dem nur noch Mönche in einem Kloster keine permanente Datenspur hinter sich herziehen würden.

Ein weiterer Schwachpunkt des neuen Gesetzes: Bislang durften die Verbindungsdaten nur auf richterliche Anordnung weitergegeben werden, da sie gem. §88 TKG dem Fernmeldegeheimnis unterliegen:

(1) 1 Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand

an einem Telekommunikationsvorgang beteiligt ist oder war. 2 Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) 1 Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. 2 Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

Ab dem 1.1.2008 würde auch eine Eilanordnung der Staatsanwaltschaft bei Gefahr im Verzug ausreichen – die richterliche Kontrolle bei Eingriffen in die Privatsphäre wäre ausge-

belt. Zudem könnten auch ausländische Behörden auf den Datenpool zugreifen – was mit den Daten im Ausland passiert ist allerdings nicht kontrollierbar.

Glücklicherweise gibt es um das Vorhaben zur Vorratsdatenspeicherung genügend Gegenwind. An vorderster Stelle sei der „Arbeitskreis Vorratsdatenspeicherung“ mit seiner Initiative „Stoppt die Vorratsdatenspeicherung“ genannt. Interessierte können sich hier auch einer Sammelverfassungsbeschwerde gegen die Vorratsdatenspeicherung anschließen. Die Verfassungsbeschwerde wird dem Bundesverfassungsgericht vorgelegt falls das neue Gesetz am 9.11.2007 durch den Bundestag beschlossen wird.

Die German Unix User Group hat sich der gemeinsamen Erklärung des Arbeitskreises Vorratsdatenspei-

cherung angeschlossen.

Die Erfolgsaussichten für eine solche Klage sind gut. Nicht alles, was in Brüssel beschlossen wird muss in nationales Recht umgewandelt werden. Ist die Vorlage der EU bereits nicht ordnungsgemäß zustande gekommen (ein einstimmiger Rahmenbeschluss des Ministerrats fehlte) wird das neue Gesetz hinfällig – und wir könnten weiterhin die Vorteile der Informationstechnologie nutzen ohne uns zum gläsernen Bürger zu machen. *(wost)*



Jan Schmidt ist als Systemingenieur bei der audius GmbH in Weinstadt angestellt und derzeit als Senior System Engineer bei der UPM Kymmene Corporation in Augsburg tätig.

Literatur

1. Telekommunikationsgesetz: http://bundesrecht.juris.de/tkg_2004/index.html
2. AK Vorratsdatenspeicherung: <http://www.vorratsdatenspeicherung.de/>
3. Link zur Sammelklage: <http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de/>
4. Zusammenfassung wichtiger Meldungen: <http://www.heise.de/ct/hintergrund/meldung/66857>