Positionspapier

„Freiheit statt VDS"

Gegen die Vorratsdatenspeicherung.

Herausgeber: CSUnet
Franz Josef Strauß-Haus, Nymphenburger Straße 64, 80335 München
Tel.: 0 89/12 43-372
csunet@csu-bayern.de
twitter.com/csu_net
facebook.com/csunet
www.csunet.de

Präambel

Das Internet mit all seinen Kommunikations- und Handlungsmöglichkeiten bietet Chancen für alle Menschen unserer modernen Welt.
Für uns ist das Internet immer auch mit dem Begriff der Freiheit verbunden, die einhergeht mit dem Schutz dieser Freiheit und dem Vertrauen in den mündigen Bürger. Die Rechte der freien Meinungsäußerung zu schützen und ein möglichst hohes Maß an Datenschutz zu gewährleisten, halten wir für zentrale Aufgaben der Politik und des Staates.
Auf diesem Selbstverständnis basiert dieses Positionspapier, mit dem wir uns gegen die Vorratsdatenspeicherung aussprechen.

Ausgangslage hierfür ist die EU Richtlinie 2006/24/EG, welche die Vorratsdatenspeicherung beinhaltet und ein Spannungsfeld zwischen Innen-/Sicherheitspolitik und Netzpolitik darstellt.

Außerdem hat das Bundesverfassungsgericht mit dem Urteil vom 2. März 2010 (BVerfG, 1 BvR 256/08[1]) entschieden, dass die bisherige Umsetzung mit dem Grundgesetz nicht vereinbar ist. Ebenfalls zu beachten ist ein Urteilsspruch des Verwaltungsgerichts Wiesbaden aus dem Jahre 2009, wonach die ursprüngliche Vorratsdatenspeicherung gegen die Europäische Menschenrechtskonvention verstoße.

Der CSUnet hat als netzpolitischer Arbeitskreis der CSU das folgende Konzept zum Themenbereich der Vorratsdatenspeicherung erarbeitet.

Keine Speicherung von Standort und E-Mail Daten

Die Speicherung von Standortdaten lehnen wir generell ab. Durch Smartphones mit ihrer dauerhaften Internetverbindung und einer Vielzahl von Flatrateangeboten entstehen bei normaler Nutzung nahezu lückenlose Bewegungsprofile.
Die massenhafte Auswertung von Handydaten in Dresden im Februar 2011 sollte ein Mahnmal dafür sein, dass die Speicherung und Nutzung von Standortdaten mehr zu falschen Verdächtigungen als zu konkreten Spuren führt. Damals sammelte die Polizei im Zuge einer gewaltsamen Demonstration Handydaten von einer Million Menschen, darunter in der deutlichen Mehrzahl auch von friedlichen Demonstranten und Anwohnern.
Ähnlich verhält es sich bei der Speicherung von E-Mail Daten. Übertragen auf die alltägliche Briefpost würde Folgendes gespeichert werden:

[1] http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

- Beim Verschicken: Wer (Name + Adresse) wann einen Brief an wen (Name + Adresse) verschickt und in welchen Briefkasten er Ihn eingeworfen hat.
- Beim Empfangen: Wer (Name + Adresse) wann einen Brief von wem (Name + Adresse) von welchem Briefträger zugestellt bekommen hat und wann er seinen Briefkasten geleert hat.

Dies ist (auch ohne Kenntnisse des Inhalts des Mailverkehrs) ein Überwachungsausmaß, das die Grenze zur Verhältnismäßigkeit in nicht hinnehmbarer Weise übersteigt.

Ein weiteres Problem sind Spammails. Jede Spammail (auch wenn sie niemals für den Empfänger relevant ist oder er sie nie zu Gesicht bekommt) muss mitprotokolliert werden. Da rund 99% des weltweiten E-Mailverkehrs aus Spam besteht, wird hier eine erhebliche Menge an Daten angesammelt, die nicht den geringsten Nutzen darstellen.

Telefondaten nur aus Abrechnungsbestandsdaten

Die EU-Richtlinie setzt auf die Speicherung der Telefondaten; also Informationen darüber, wer, wann und mit wem telefonischen Kontakt hat. Auch in Zeiten von Flatrate-Angeboten sind Einzelverbindungsnachweise immer noch Standard. Da diese in der Regel mindestens zwei bis drei Monate verfügbar sind (bei Onlinerechnungen sogar länger), sieht der CSUnet hier keinen zusätzlichen Speicherbedarf durch das Gesetz.

Richterentscheid und Quellen-TKÜ

Besteht gegen Personen ein konkreter Verdacht, eine schwere Straftat begangen zu haben oder zu planen, soll eine Speicherung von Daten durch einen Richterentscheid möglich sein. Hierbei sind insbesondere die Zugangswege, die TK-Anbieter (wie beispielsweise Skype) den Strafverfolgungsbehörden zur Verfügung stellen können, zu nutzen, bevor die gesetzlichen Möglichkeiten der Quellen-TKÜ genutzt werden.
Da die Richter hierbei über einen starken Grundrechtseingriff entscheiden, müssen die Maßnahmen von Richtern angeordnet werden, die den nötigen technischen Sachverstand besitzen und die technisch teilweise sehr spezifischen Details einer eingesetzten Software oder ermittlungstechnischer Instrumente verstehen und deshalb einschätzen können. Wir wollen, dass die betreffenden Richter diese Erfahrung durch tägliche Praxis und regelmäßiger Befassung mit der Thematik und der dazugehörigen Technik vorweisen können.
Zu prüfen wäre dabei, ob entsprechende Kompetenzcluster auf Länderebene gebildet werden sollten.

Speicherung von IP-Daten

Bei der Verfolgung von Straftaten im Internet ist die IP-Adresse oftmals die einzige Spur. Aus diesem Grund ist eine Zuordnung von IP-Adressen zu konkreten Anschlüssen wichtig. Eine Speicherung eröffnet aber auch großes Missbrauchspotential (z.B. durch die Abmahnindustrie). Eine zivilrechtliche Nutzung dieser Daten wäre im Falle einer gesetzlichen Speicherpflicht deswegen in jedem Falle auszuschließen.

Generell ergeben sich beim Komplex der Vorratsdatenspeicherung **zwei grundlegende Fragestellungen:**

Welche Daten sind überhaupt brauchbar?

Politiker und Behördenspitzen diskutieren ausführlich über Mittel zur Strafverfolgung. Letztendlich wissen jedoch die Beamten, die diese Mittel schließlich einsetzen (müssen), am besten, welche Daten wirklich brauchbar wären. Aus diesem Grund muss vor einem erneuten Gesetzgebungsverfahren eine gründliche und umfangreiche Evaluierung des realen Bedarfs auf Dienstebene des BKA und der LKAs stattfinden. Dabei ist sicherzustellen, dass die Beamten anonym bleiben können, damit ihnen keine direkten oder indirekten Nachteile entstehen, wenn sie eine andere Meinung als ihre Vorgesetzten vertreten.

Neben der Evaluierung durch die betreffenden Ermittlungsbeamten sind unabhängige Gutachten über die Sinnhaftigkeit der zu speichernden Daten einzuholen.

Ist die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht tragbar?

In der Vergangenheit wurden große Internetkonzerne wie Facebook und Google immer wieder für ihre Datensammelwut kritisiert. Mit der Vorratsdatenspeicherung würde man eine ähnliche Sammelwut per Gesetz fordern, die oftmals ebenso bedenklich ist, wie die der betreffenden Unternehmen.
Wenn Daten - in welchem Umfang auch immer - gespeichert werden sollten, dann muss zweifellos sichergestellt werden, dass diese in keiner Weise missbraucht werden können - weder von Staat noch der Wirtschaft. Dies technisch einwandfrei garantieren zu können, halten wir für nicht darstellbar.

Grundsätzlich bleibt festzuhalten,

- dass bis zum Ende der Evaluierung der Vorratsdatenspeicherung im Frühjahr 2012 durch die EU, kein neues Gesetzgebungsverfahren angestrengt werden soll. Ein Vertragsverletzungsverfahren kann und muss im Hinblick auf die

verfassungsrechtliche Brisanz und die hohen Vorgaben des Verfassungsgerichts billigend in Kauf genommen werden.

- Außerdem muss sich die Gesellschaft klar darüber werden, ob sie einen so umfangreichen Eingriff in ihre Grundrechte hinnehmen will, um einige wenige Verbrechen mehr aufklären zu können. Anschläge wie in Norwegen oder durch Naziterrorgruppen in Deutschland lassen sich nachweislich auch durch die Vorratsdatenspeicherung nicht verhindern.

- Der CSUnet ist der Meinung, dass die Speicherung von Daten einen so tiefen Eingriff in die Privatsphäre bedeutet, dass wir in den Diskussionsprozess um eine neue Gesetzgebung ausreichende Möglichkeiten bieten müssen, die Bevölkerung an diesem Prozess teilhaben zu lassen. Dieser Prozess muss von einem hohen Maße an Transparenz, Offenheit und Information geprägt sein.

- Eine Vorratsdatenspeicherung gemäß der derzeitigen EU-Richtlinie lehnen wir ab. Eine Überprüfung der Anschlusskennung über die beim Provider gespeicherte IP-Adresse bei Verdacht auf schwere und schwerste Straftaten und nach fundiertem richterlichem Beschluss halten wir für ein geeignetes Instrument der Verbrechensbekämpfung.

- Die Speicherdauer betreffend ist einer Entscheidung eine ausführliche und den wirklichen Bedarf erhebende Evaluierung durch Ermittlungsbeamte und unabhängige Institutionen voranzustellen. Unser Ziel ist es, grundsätzlich Daten nicht länger zu speichern als unbedingt notwendig.