Pressemitteilung – Experten-Statement

Vorratsdatenspeicherung: Wenn nichts mehr hilft, hilft Technik?

Telekommunikationsanbieter müssen ab Juli 2017 die Verkehrsdaten aller Verbindungen zehn Wochen lang speichern. Können raffinierte Technologien helfen, die Grundrechte der Nutzer doch noch zu bewahren?

Ein Experten-Statement von Dr. Hubert Jäger

(München, 03.04.2017) Im Februar hat das Bundesverfassungsgericht (BVerfG) angekündigt, welche Verfassungsbeschwerden es dieses Jahr zu behandeln gedenkt. [1] Die Vorratsdatenspeicherung ist nicht unter den Kandidaten. Somit müssen Telekommunikationsanbieter ab Juli alle Verkehrsdaten speichern, zehn Wochen lang aufbewahren und gegebenenfalls den Behörden zur Verfügung stellen. Unter Verkehrsdaten sind jene Daten zu verstehen, die bei der Vermittlung von Telekommunikation anfallen, also zum Beispiel die Rufnummer der beteiligten Anschlüsse sowie Zeit und Ort eines Gesprächs. Es geht hierbei nicht um die Inhalte, sondern um die Frage, ob und wann überhaupt Telekommunikation stattgefunden hat. Für die Bürger bedeutet dies konkret, dass aufgezeichnet wird, wie lange sie mit wem, wann und wo kommunizieren – Informationen, die ermöglichen, das Leben, die Beziehungen und Aufenthaltsorte einer Person sehr genau nachzuvollziehen.

Unter Verkehrsdaten sind jene Daten zu verstehen, die bei der Vermittlung von Telekommunikation anfallen, also zum Beispiel die Rufnummer der beteiligten Anschlüsse sowie Zeit und Ort eines Gesprächs. Es geht hierbei nicht um die Inhalte, sondern um die Frage, ob und wann überhaupt Telekommunikation stattgefunden hat. Für die Bürger bedeutet dies konkret, dass aufgezeichnet wird, wie lange sie mit wem, wann und wo kommunizieren – Informationen, die ermöglichen, das Leben, die Beziehungen und Aufenthaltsorte einer Person sehr genau nachzuvollziehen.

Aus diesem Grund sehen das BVerfG und der Europäische Gerichtshof (EuGH) in ihren Urteilen eine Speicherung der Verkehrsdaten für zwar „nicht grundsätzlich unvereinbar“ mit den §§ 1,10 GG bzw. den Art. 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union an. Jedoch verlangen sie, dass „die Verhältnismäßigkeit des Eingriffs durch hinreichende technische und organisatorische Einschränkungen der Zugriffsmöglichkeiten“ gewährleistet ist. Welche technischen und organisatorischen Anforderungen gegenwärtig erfüllt sein müssen, um diese Verhältnismäßigkeit zu erreichen, hat die Bundesnetzagentur (BNetzA) bereits klar formuliert. Jetzt liegt es also an den genutzten Technologien.

Auslesen der Daten aller – und das ohne Anlass?

Bei der Vorratsdatenspeicherung werden diese Daten in ihrer Gesamtheit – vorsorglich und ohne Anfangsverdacht -„eingefroren“. Sie sollen zur Aufklärung schwerer Straftaten zur Verfügung stehen, sobald ein Verdacht beziehungsweise ein juristisch berechtigtes Interesse vorliegt. Diese Art der Vorratsdatenspeicherung betrifft somit nicht nur Personen, gegen die strafrechtlich ermittelt wird, sondern auch unbescholtene Bürger. Daher darf sie weder zu

einer Schwachstelle für eventuelle Angriffe Krimineller noch zu einer Bedrohung für die freiheitlich demokratische Grundordnung werden.

Wie sieht Vorratsdatenspeicherung technisch aus?

Bei der bisher üblichen Speicherung werden Daten auf einem Medium persistent - d.h. dauerhaft und nicht nur flüchtig - abgelegt und können anschließend, wann immer gewünscht, gelesen werden. Und zwar von jenen Personen die Zugriff zu diesem Medium haben.

Eine Sicherheitsbarriere gegen unbefugtes Lesen bietet die verschlüsselte Speicherung der Daten. Das Lesen der verschlüsselten Daten ist daher nur noch den Personen möglich, die neben der Leseberechtigung außerdem Zugriff zu den Leseschlüsseln haben. Jedoch kann jeder, der Zugriff auf die Leseschlüssel hat, die verschlüsselten Daten auch ohne konkreten Anlass lesen. Diese Tatsache ist ein zentraler Punkt für die Experten-Kritik an der Vorratsdatenspeicherung.

Wie lässt sich dabei anlassloses Lesen verhindern?

Dafür sind zusätzliche Maßnahmen erforderlich: Meist setzt man organisatorische Regelungen wie zum Beispiel das Vier-Augen-Prinzip ein. Das Problem mit den organisatorischen Maßnahmen: Sie hängen von der Disziplin der Bearbeiter ab und lassen sich relativ einfach umgehen. Damit ist die Wirksamkeit begrenzt. Daher halten Experten organisatorische Maßnahmen für wenig geeignet, die vom EuGH geforderte „Verhältnismäßigkeit“ sicherzustellen.

Gibt es andere effektive Technologien?

Die Vorbehalte gegenüber der Vorratsdatenspeicherung lassen sich reduzieren, wenn man den technischen Vorgang in „Einfrieren“ (freezing) und „Auftauen“ (unfreezing) zerlegt.

Beim Freezing werden die Verkehrsdaten verschlüsselt gespeichert, jedoch verfügt niemand - auch nicht mehrere Personen gemeinsam - über die Leseschlüssel. Daher wäre das Einfrieren von Daten anlasslos und grundrechtskonform möglich. Würde man zum Beispiel, die Leseschlüssel in technisch versiegelten Anlagen aufbewahren, könnte niemand auf die Schlüssel zugreifen. Sollte es doch jemand versuchen, würden sie gelöscht, bevor ein Auslesen überhaupt erfolgen kann.

Das Unfreezing könnte über einen technisch fest implementierten Zugriffsfilter, ein „policy gate“ erfolgen. Allerdings werden Daten in dem Fall „aufgetaut“, dass das Auskunftsersuchen den zuvor gesetzlich festgelegten Filterkriterien entspricht. Dieser Zugriffsfilter gibt nur diejenigen Leseschlüssel frei, mit denen genau die anlassbezogen gesuchten Daten entschlüsselt werden können. Das Auslesen geschieht vollautomatisch und ohne dass Betreiber oder Administratoren auf die Daten zugreifen können. Auskunftsersuchen, die den fest implementierten Filterkriterien nicht genügen, können nicht beantwortet werden.

Anders als bei der technisch-organisatorischen Umsetzung wären die Maßnahmen, die einen ausschließlich anlassbezogenen Zugriff erlauben, rein technischer Art. Diese ließen sich nur durch die aktive Mitwirkung vieler Personen, mithin durch Änderungen der Soft- und Hardware und deren Installation, außer Kraft setzen.

Welches Restrisiko bleibt noch bei diesen Technologien?

Setzt man voraus, dass das Sicherheitsniveau beim Einfrieren und Auftauen so hoch ist, wie von der Bundesnetzagentur gefordert, kann man das Risiko eines anlasslosen Lesens der Verkehrsdaten praktisch ausschließen.

Bei dieser technischen Aufteilung bestimmt also die Qualität des Zugriffsschutzes, inwieweit die Grundrechte gewahrt bleiben. Auf der einen Seite steht das anlasslose, jedoch grundrechtskonforme Einfrieren, auf der anderen Seite erfolgt das Auslesen ausschließlich anlassbezogen.

Für Datenschutz- und IT-Sicherheits-Experten ist die Qualität des Zugriffschutzes bei der bisherigen Speicherung nicht akzeptabel: Die Wahrscheinlichkeit, dass jemand auf die Daten ohne Anlass zugreift, ist so hoch, dass innerhalb von zehn Jahren mit an Sicherheit grenzender Wahrscheinlichkeit mit mindestens einem solchen Vorfall zu rechnen ist. Die Vorschriften aus dem Telekommunikationsgesetz hinsichtlich des Vier-Augen-Prinzips helfen, das Risiko etwas zu senken.

Doch erst zusätzliche technische Maßnahmen, wie sie teilweise von den großen Netzbetreibern implementiert werden, und die über den von der BNetzA formulierten Anforderungskatalog hinausgehen, oder eine rein technische Umsetzung wie zum Beispiel die Sealed Freeze Technologie führen zu einer erheblichen Verbesserung. Bei diesen Technologien erwartet man einen anlasslosen Zugriff erst innerhalb von 10.000 Jahren.

Zeit genug also, um die Entscheidung des BVerfG gelassen abzuwarten.

Dr. Hubert Jäger, Geschäftsführer der Uniscon GmbH, entwickelt technische Lösungen, die den Schutz der Grundrechte mit Anforderungen der Cyber - Sicherheit vereinbaren.

Hintergrund:

[1] http://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2017/vorausschau_2017_node.html
[2] https://malte-spitz.de/wp-content/uploads/2014/04/C_0293_2012-DE-ARR.pdf
[3] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/Anforderungskatalog.pdf?__blob=publicationFile&v=1
[4] http://www.cloudcomputing-insider.de/sealed-freeze-baendigt-vorratsdatenspeicherung-a-431669/