Vorratsdatenspeicherung: Warum der Stand der Technik eine Rolle spielt

München, 29. Juni 2017 – Das Tauziehen um die Vorratsdatenspeicherung hört nicht auf: Ab 1. Juli sind die Telekommunikationsanbieter in Deutschland verpflichtet, die Verbindungsdaten ihrer Kunden für zehn Wochen zu speichern. Vorige Woche jedoch erwirkte ein kleiner Münchner Anbieter in einem Verfahren des einstweiligen Rechtsschutzes beim Oberverwaltungsgericht Nordrhein Westfalen, dass er vorläufig von dieser Verpflichtung befreit ist. Für die Bundesnetzagentur (BNetzA), die mit der Durchsetzung der Speicherung der Telekommunikationsdaten beauftragt ist, gilt die Verpflichtung aber immer noch. Allerdings sieht sie bis zum Abschluss des Hauptverfahrens *„von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab.“*

Andere, größere Anbieter hingegen legten sich in den letzten Monaten eine ausgeklügelte Infrastruktur zu, damit sie den Vorgaben der BNetzA zur Speicherung der Verkehrsdaten entsprechen können. Denn es gibt strenge technisch-organisatorische Auflagen dafür; sie soll dem Gesetz nach möglichst wenig in die Grundrechte eingreifen.

Auch innerhalb der EU sind die Länder uneins. Die einen fordern stärkere Überwachung, manche speichern die Verbindungsdaten sogar bis zu einem Jahr. Österreich weitete die Überwachung Anfang des Jahres aus – mit der Begründung, eine Vorreiterrolle bei der Terrorbekämpfung einnehmen zu wollen. Die Niederlande hingegen kippte die Vorratsdatenspeicherung bereits 2015. Das Gericht in Den Haag hat sie für verfassungswidrig erklärt. In Deutschland sind ebenfalls mehrere Verfassungsklagen anhängig.

Was liegt dem Tauziehen zugrunde?

Kern der unklaren Lage ist die Tatsache, dass der Europäische Gerichtshof voriges Jahr die Vorratsdatenspeicherung – so wie sie in zwei Mitgliedsstaaten durchgeführt wurde - als nicht mit der Charta der Grundrechte der EU vereinbar erklärte. Die Richter forderten, dass die Regelung über die Vorratsdatenspeicherung klare und präzise Regeln „über die Tragweite und Anwendung der fraglichen Maßnahme vorsehen und einen wirksamen Schutz der personenbezogenen Daten vor Missbrauch, unberechtigten Zugang und unberechtigter Nutzung sicherstellen“ muss. Aus diesem Grund legt das TKG so starken Wert auf „den Stand der Technik“.

Was ist damit genau gemeint? Und was gilt eigentlich als „Stand der Technik“? Diese Fragen stellten wir Dr. Hubert Jäger, CTO der Uniscon und IT-Sicherheitsexperte, der datenschutzkonforme Cloud-Technologien erforscht und entwickelt.

Dr. Hubert Jäger zum Stand der Technik

Das Telekommunikationsgesetz (TKG) besagt, dass jeder Dienstanbieter die erforderlichen technischen Vorkehrungen und Maßnahmen zu treffen hat – erstens zum Schutz des Fernmeldegeheimnisses und zweitens gegen die Verletzung des Schutzes von personenbezogenen Daten. Dabei ist der Stand der Technik zu berücksichtigen. Mehr noch, die BNetzA hat bei Änderung des Standes der Technik unverzüglich den Anforderungskatalog anzupassen. Das meint, dass die betroffenen Unternehmen jene Technologien am Markt für die Speicherung der Verkehrsdaten einsetzen müssen, die am besten schützen. Damit kommt ein dynamisches Element in das Gesetz, das der ständigen Weiterentwicklung von Technologien Rechnung trägt.

Im Fall der Vorratsdatenspeicherung ist der zentrale Punkt die anlasslose, nicht zweckgebundene Speicherung der Daten. Darunter versteht man, dass vorab - auf Vorrat eben – die Verkehrsdaten gespeichert und gegebenenfalls erst im Nachhinein ausgelesen werden. Einmal gespeichert hieß technisch lange auch, dass auf alle Daten im Pool zugegriffen werden konnte, auch auf die Daten von unbescholtenen Bürgern.

Moderne Technologien gehen da jetzt einen Schritt weiter. Zum Beispiel die technisch weit entwickelten Lösungen bei den drei großen Netzanbietern Deutschlands, oder die Technologie Sealed Freeze der Uniscon GmbH. Sie realisieren ein verschlüsseltes „Einfrieren" der Verkehrsdaten. Die Anlagen schützen so, dass niemand Zugriff auf die Leseschlüssel erhalten kann, auch nicht mehrere Personen gemeinsam. Soll es jetzt einen Lesezugriff geben, kann dieser nur anlassbezogen erfolgen und beinhaltet allein die Verkehrsdaten, die genau diesen Anlass betreffen. Alle anderen Verkehrsdaten im Datenpool, also diejenigen Daten, die unbescholtene Bürger betreffen, bleiben unzugänglich. Da die auf diese Weise „eingefrorenen" Daten nie anlasslos gelesen werden können, gilt eine so technisch umgesetzte Speicherung von Verkehrsdaten als rein anlassbezogen.

Zu einer vergleichbaren Einsicht gelangten die Fachleute bereits bei der Löschung von Daten: Früher bestanden IT-Experten darauf, dass ein Datum nur als gelöscht gelten darf, wenn die Daten auf dem physikalischen Medium gelöscht waren. Heute ist allgemein anerkannt, dass Daten als gelöscht gelten, wenn die Schlüssel, die zu einer starken Verschlüsselung der Daten genutzt wurden, zuverlässig gelöscht sind. Mit dem technisch erzwungenen Anlassbezug verhält es sich analog: Sind die anlasslos eingefrorenen Daten gut genug geschützt, dann bewirkt eine rein anlassbezogene Auftaumöglichkeit, dass der gesamte Vorgang rein anlassbezogen ist.

Und diese, nicht nur für die Vorratsdatenspeicherung, sondern auch für Big Data wichtigen Technologien setzen den heutigen Stand der Technik. Die Gerichte müssen sich also auch mit diesen Entwicklungen auseinandersetzen, um eine sachgerechte Entscheidung treffen zu können.

Wenn Sie Fragen haben, wenden Sie sich bitte an presse@uniscon.de.

Über Uniscon GmbH

Die Uniscon GmbH ist Technologieführer im Bereich Cloud Security. Als Experte für versiegelte Cloud-Technologien bieten sie auf Basis der international patentierten Sealed Cloud Technologie technische Lösungen und eigene Cloud Services an. Die Sealed Cloud repräsentiert einen technischen Durchbruch bei

der Realisierung hochsicherer Rechenzentren: Sie schützt Daten auf so hohem Niveau, dass selbst der Anbieter mit ausschließlich technischen Maßnahmen vom Zugriff auf die Daten bei der Speicherung UND während der Verarbeitung ausgeschlossen ist. Weitere Informationen zu Partnern und Produkt: www.uniscon.de und www.idgard.de

Pressekontakt

Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.de
Telefon: 089 / 41 615 988 103