Pressemitteilung

Verkehrsdaten für Verbrecherjagd nutzen – aber nicht an den Grundrechten vorbei!

München, 19. August 2015. In der heutigen Informations- und Kommunikationsgesellschaft ist der Wunsch nach einer effektiven Strafverfolgung für viele Menschen nachvollziehbar. Dem gegenüber steht jedoch das vom Grundgesetz garantierte Fernmeldegeheimnis (1). Das Bundesverfassungsgericht hat in seinem Urteil vom März 2010 (2) klargestellt, dass dessen Missachtung eine Verletzung der Grundrechte darstellt und somit die freiheitlich-demokratische Grundordnung gefährdet. Doch das Gericht hat die Vorratsdatenspeicherung auch „nicht für grundsätzlich unvereinbar“ mit dem Grundgesetz genannt, sofern „hinsichtlich der Datensicherheit ein hoher Standard normenklar und verbindlich vorgegeben wird“. Ein neuer Gesetzentwurf (3) wird daher nach der Sommerpause im September dem Bundestag zur Abstimmung vorgelegt. Kritiker betonen allerdings, dass auch dieser Gesetzesentwurf nicht den rechtlichen Vorgaben der Richter entsprechen wird. (4)

Einer der Ansätze des Regierungsentwurfs (3), den Vorgaben des BVG gerecht zu werden, ist, den Schutz von Informationssystemen und darin gespeicherten Daten stark zu erhöhen. TK-Anbieter sollen zum Beispiel verpflichtet werden, Datensicherheit gemäß dem Stand der Technik zu gewährleisten. Zur Eingrenzung des „Standes der Technik“ soll die Bundesnetzagentur einen Anforderungskatalog erstellen, der fortlaufend aktuell gehalten wird. Dabei unterstützt das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragen für Datenschutz und Informationsfreiheit (BFDI)die Bundesnetzagentur. Der Fokus liegt dabei auf Anforderungen, die den rechtlichen Vorgaben zum Schutz des einzelnen Bürgers entsprechen.

In herkömmlichen Systemen werden heute die Daten verschlüsselt gespeichert. Wenn eine Behörde um Auskunft ersucht, können dann aber einzelne Mitarbeiter des Telekommunikations-Providers (TK-) die Daten entschlüsselt einsehen. Sie müssen diese ja exportieren und an die anfragende Behörde weitergeben. Sie können sie theoretisch jedoch auch illegal verwenden. Außerdem sind bei den herkömmlichen Systemen keine technischen Grenzen gesetzt, die die Einhaltung gesetzlicher

Regelungen erzwingen. Das bedeutet: Selbst wenn alle technischen Komponenten zur Sicherung der Daten auf den neusten Stand gebracht und vorbeugende organisatorische Maßnahmen getroffen werden, so bleibt als Sicherheitsrisiko in diesen Systemen stets der Faktor „Mensch“. Die Aufrüstung der Systeme und den erhöhten Personalbedarf, den die organisatorischen Maßnahmen, wie zum Beispiel das 4-Augen-Prinzip erfordern, müsste jeder einzelne TK-Provider tragen.

Anders sieht es bei der neuartigen Sealed-Freeze-Technologie aus, die durch rein technische Maßnahmen den Zugriff auf versiegelte Daten reglementiert und damit den Unsicherheitsfaktor Mensch ausschließt. Diese Versiegelungstechnik vermeidet das manuelle Schlüssel-Management im Bereich der Speicherung. Sie schützt damit die für die Auskunft benötigten Schlüssel gegen jeglichen Zugriff des TK-Anbieters. Einfacher gesagt: Mitarbeiter des Providers können nach verschlüsselter Speicherung der Verkehrsdaten nicht mehr auf diese zugreifen. Einzig staatliche Behörden können die bei einer Erhebung angefragten Daten im Klartext einsehen. Die Einsicht der Behörden wird anhand klarer, im Vorfeld definierter Regelungen (Policies) allerdings nur dann möglich, wenn alle rechtlichen Voraussetzungen vorliegen.

Wenn beispielsweise eine Auskunft zu einem bestimmten Gespräch in einem bestimmten Zeitraum in einer bestimmten Funkzelle verlangt wird, so kann die Anfrage eindeutig eingegrenzt werden: „Fand in diesem Zeitraum in dieser Funkzelle eine Kommunikation mit dieser Telefonnummer statt?“

Diese technischen Regeln bieten deutliche Konkretisierungsmöglichkeiten gegenüber Verfahren, bei denen Menschen Rohdaten durchsuchen müssen. So lässt sich, „Beifang“ von Daten vermeiden, also dass die Daten von Bürger mitgelesen werden können, die sich zum fraglichen Zeitpunkt zufällig auch in dieser Funkzelle aufgehalten haben. Ausschließlich die zur Einsicht berechtigte staatliche Behörde verfügt über Zugangsdaten und einen zweiten Authentifizierungsfaktor. Über eine sichere elektronische Verbindung erfolgt dann die Übertragung der berechtigt angefragten Verkehrsdaten an eben diese Behörde.

Durch ein Sealed-Freeze-Verfahren lassen sich die Daten der Bürger bestmöglich

schützen. Die Technologie verhindert den Datenzugriff von Unbefugten und Unbeteiligten. Technische Regeln konkretisieren die Abfragemöglichkeiten. Der TK-Dienstleister wird zudem enorm entlastet. Aufwändige organisatorische Sicherheitsmaßnahmen beim Provider fallen weg. Sogar eine Auslagerung der Sicherheitstechnik an einen zentralen Dienstleister wäre möglich. Dieser Dienstleister könnte aus einer Hand die Schlüssel der Verkehrsdaten vieler Provider verwalten und würde damit hohe Kosteneinsparungen sowohl für die TK-Provider als auch für die Behörden realisieren, was letztendlich dem Steuerzahler zu Gute kommt.

(1) https://de.wikipedia.org/wiki/Fernmeldegeheimnis
(2) http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
(3) http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoechstspeicherfrist.pdf?__blob=publicationFile
(4) http://www.heise.de/newsticker/meldung/Datenschutzbeauftragter-erklaert-Vorratsdatenspeicherung-fuer-nicht-machbar-2748433.html

Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de

Über Uniscon GmbH

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service IDGARD für Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt
Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
presse@uniscon.de
www.uniscon.de

PR-Agentur
Xpand21, Doris Loster

Pressemitteilung

Alter Teichweg 9M
22081 Hamburg
040 / 22 61 49 43
0170 / 215 31 72
uniscon@xpand21.com
www.pr-agentur-xpand21.de