Dennis-Kenji Kipker

Der neue Anforderungskatalog der BNetzA nach § 113f TKG – Datensicherheit der TK-Diensteanbieter für die Vorratsdatenspeicherung

MMR-Aktuell 2016, 378702

Die sicherheitsbehördliche Datenverarbeitung erfährt seit den Anschlägen des 11. September 2001 einen laufenden Ausbau. Grund dafür ist nicht nur die durch den Terrorismus veränderte, qualifizierte Bedrohungslage für die öffentliche Sicherheit, sondern vor allem auch die zunehmende Zahl gespeicherter personenbezogener Daten bei den unterschiedlichsten Institutionen und Personen, verbunden mit einer immer größeren Leistungsfähigkeit von Technologien der automatisierten und vernetzten Datenverarbeitung. Die Speicherung von Vorratsdaten stellt hierfür ein klassisches Beispiel dar, indem Millionen von Verkehrsdaten zu Auswertungszwecken bei den Anbietern von TK-Diensten vorgehalten werden. Mit einer solchen Datenverarbeitung einher gehen jedoch nicht nur potenzielle Vorteile für sicherheitsbehördliche Ermittlungen, sondern es existieren ebenso in Bezug auf die Qualität und Sicherheit der gespeicherten Daten erhebliche technische Risiken, sodass speziell auf die Vorratsdatenspeicherung zugeschnittene Lösungen der IT-Security entwickelt werden müssen.

I. Der Anforderungskatalog nach § 113f TKG

Auf Basis dieser Problemlage für die Datenhaltung im Rahmen der Vorratsdatenspeicherung schreibt § 113f Abs. 1 Satz 1 TKG vor, dass die Erbringer öffentlich zugänglicher TK-Dienste im Rahmen der anlassunabhängigen Speicherung von Verkehrsdaten gem. §§ 113b bis 113e TKG dazu verpflichtet sind, einen besonders hohen Standard der Datensicherheit und Datenqualität zu gewährleisten. Konkretisiert wird diese allgemeine gesetzgeberische Vorgabe durch die Vorschrift des § 113f Abs. 1 Satz 2 TKG, dergemäß die Einhaltung des besonders hohen Standards vermutet wird, soweit alle Anforderungen des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die *BNetzA* im Benehmen mit dem *Bundesamt für Sicherheit in der Informationstechnik (BSI)* und der *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)* erstellt. Indem diesem Katalog eine gesetzliche Vermutungswirkung beigemessen wird, bildet er somit den zentralen Maßstab für die Datenhaltung im Rahmen der Vorratsdatenspeicherung. Inhaltlich geht er über die Anforderungen des ebenfalls von der *BNetzA* herausgegebenen Katalogs von Sicherheitsanforderungen für das Betreiben von TK- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG hinaus. Eine erste Entwurfsfassung des VDS-Anforderungskatalogs nach § 113f TKG in der Version 0.1 mit Stand v. 11.5.2016 gibt bereits jetzt einen Ausblick auf die zu erwartenden Vorgaben für die TK-Diensteanbieter. Die *BNetzA* bietet interessierten Kreisen (Herstellern, Verbänden, Betreibern von TK-Netzen und Diensteerbringern) gem. § 113f Abs. 3 Satz 1 i.V.m. § 109 Abs. 6 Satz 2 TKG die Möglichkeit, bis zum 1.7.2016 eine Stellungnahme abzugeben.

II. Übersicht zu den neuen Vorgaben, Verhältnis zu § 109 TKG und BSI-Grundschutz

Derzeit umfasst der VDS-Anforderungskatalog eine Länge von 27 Seiten und untergliedert sich in insgesamt sechs Kapitel. Zu Beginn werden die für den Sicherheitskatalog wesentlichen technischen Begriffsbestimmungen und Abkürzungen definiert, so die Fachtermini „Abfrageclient", „Ablagesystem", „Datenspeicher", „Schlüsselmanagement", „VDS-System", „Verkehrsdaten" und „Zugriffssystem". Die technischen Begriffsbestimmungen werden nach Fertigstellung des Gesamtdokuments nochmals überarbeitet. In der Präambel im dritten Kapitel wird hervorgehoben, dass die Anforderungen für die Vorratsdatenspeicherung aus § 113f TKG die Verpflichtungen für angemessene technische Schutzmaßnahmen gem. § 109 TKG und den BSI-Grundschutz unberührt lassen. Durch diese Klarstellung des Verhältnisses der verschiedenen Vorgaben zur IT-Sicherheit wird der spezielle Charakter der neuen Anforderungen besonders herausgestellt: So ist ohnehin sicherzustellen, dass die Verkehrsdatenspeicherung in einer physisch sicheren Umgebung erfolgt, indem der Basisschutz realisiert wird – dies ergibt sich auch aus der Anlage zu dem Dokument. Das darüber hinausgehende Sicherheitsniveau für die Vorratsdatenspeicherung ist zusätzlich einzuhalten und zu dokumentieren. Freilich können die verpflichteten Diensteanbieter auch alternative technische Vorkehrungen zur Gewährleistung des besonders hohen Datensicherheitsstandards treffen, diese müssen aber ebenso den Vorgaben des Anforderungskatalogs entsprechen, zudem ist die gesetzliche Vermutungswirkung auf den Katalog beschränkt.

Soweit es die Übermittlung der Vorratsdaten an die auswertenden Behörden betrifft, sind gem. § 113c Abs. 3 Satz 1 TKG die zusätzlichen Vorgaben der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV) sowie der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV) zu beachten.

III. Allgemeine Anforderungen an die Datensicherheit und die Datenqualität

Ausgehend von der zentralen Zwecksetzung des neuen VDS-Anforderungskatalogs, einen besonders hohen Standard der Datensicherheit zu gewährleisten, werden eingangs in Kapitel 4 die zentralen Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der gespeicherten Verkehrsdaten als allgemeine Anforderungen an die Datensicherheit und Datenqualität festgeschrieben. Die Sicherheitsmaßnahmen sollen endgerätebezogen bereits in die jeweiligen informationstechnischen Systeme, Komponenten und Prozesse integriert oder bei deren Anwendung sichergestellt werden und den gesamten Informationsfluss von der Erhebung im Logdatensystem bis hin zur Ermittlung an die berechtigte Stelle über den Abfrage-Client und das VDS-System umfassen. Da die erhobenen personenbezogenen Daten sicherheitsbehördlichen Ermittlungszwecken zugeführt werden sollen, müssen sie nicht nur besonders geschützt sein, sondern im Sinne der ermittlungstechnischen Verlässlichkeit auch qualitativ hochwertig. Z.B. müssen die den Verkehrsdaten zuge-

ordneten Zeitangaben verlässlich sein. Der Anforderungskatalog sieht deshalb vor, dass die Genauigkeit der zu speichernden Zeitstempel durch den Rückgriff auf Zeitserver sicherzustellen ist, die auf der amtlichen Zeit basieren. Daneben werden Maßnahmen vorgeschlagen, um die inhaltliche Richtigkeit der Verkehrsdaten zu überprüfen. Typische Fehlerkategorien in diesem Zusammenhang sind Unregelmäßigkeiten, wie nicht ausgelöste Gespräche oder gleichzeitig geführte Telefonate von unterschiedlichen Orten, die zunächst technisch miterfasst werden. Unter Rückgriff auf bereits bestehende, u.a. automatisierte Fehlererkennungssysteme der Diensteanbieter soll hier eine umfassende Kontrolle stattfinden. Werden dabei fehlerhaft gespeicherte Verkehrsdaten festgestellt, so ist die abrufende Behörde hierüber unverzüglich zu informieren, um spätere Fehler im Ermittlungsverfahren zu vermeiden.

IV. Technische Vorkehrungen und sonstige Maßnahmen für die Umsetzung der Verpflichtungen nach §§ 113b – 113e TKG

Das 5. Kapitel des Anforderungskatalogs nach § 113f TKG bestimmt in Ergänzung des allgemeinen 4. Teils spezielle technische Vorkehrungen und Maßnahmen für die Umsetzung der Verpflichtungen zur Vorratsdatenspeicherung nach den §§ 113b – e TKG. So hat die Speicherung der Verkehrsdaten verschlüsselt und im Inland zu erfolgen, was voraussetzt, dass sich die technischen Speichersysteme physisch in Deutschland befinden. Die Authentizität und Integrität der Daten soll ferner dadurch sichergestellt werden, dass die in ihnen enthaltenen Informationen direkt aus den Abrechnungs-, Log- oder Signalisierungsdaten gewonnen werden. Der Ausschluss der Verkehrsdatenspeicherung für Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen i.S.v. § 113b Abs. 6 i.V.m. § 99 Abs. 2 Satz 1, 3 TKG wird technisch-organisatorisch durch eine Liste geregelt, in welche die privilegierten Institutionen Einmeldungen der auszunehmenden Rufnummern vornehmen. Diese Liste wird für die speicherungsverpflichteten Diensteanbieter auf einem sicheren Kanal zum Download zur Verfügung gestellt.

Dieses Vorgehen entspricht der gegenwärtigen Gesetzeslage und stellt somit keine eigenständige Regelung durch den Anforderungskatalog dar. Zu bedenken ist aber, dass zentrale Datenspeicherungen unter dem Gesichtspunkt der IT-Sicherheit stets vermieden werden sollten, bergen sie doch für den Regelfall das Risiko, nach der Überwindung der Sicherheitsvorkehrungen nur eines informationstechnischen Systems durch einen unbefugten Dritten den Vollzugriff auf den gesamten Datenbestand zu erlangen. Für den Berufsgeheimnisträger-Schutz wurde diese Problematik einer zentralisierten Liste auch schon im Gesetzgebungsverfahren zur neuen Vorratsdatenspeicherung im Jahr 2015 ergebnisoffen diskutiert.

Zur Umsetzung der Anforderung des § 113b Abs. 7 BGB, dass die Speicherung der Verkehrsdaten so zu erfolgen hat, dass Auskunftsersuchen der Sicherheitsbehörden unverzüglich beantwortet werden können, wird im Katalog ebenso die zentrale Speicherung dieser Informationen vorgeschlagen. Vor allem eine solche Speicherung ist unter dem zuvor schon für § 113b Abs. 6 i.V.m. § 99 Abs. 2 Satz 1, 3 TKG dargestellten Aspekt der Datensicherheit problematisch. Relativiert wird dieses Risiko wiederum dadurch, dass alle Komponenten des Vorratsdatenspeicherungssystems die Anforderungen nach BSI-Grundschutz mit dem Schutzbedarf „hoch" erfüllen müssen. Auch sind die Verkehrsdaten physisch von den für die üblichen betrieblichen Aufgaben genutzten Datenspeichern und vom Internet zu trennen. Speziell der letztgenannte Aspekt stellt eine technische Herausforderung dar, da die zu speichernden Verkehrsdaten gerade in solchen Systemen anfallen, die naturgemäß eine Online-Verbindung aufweisen. Da eine physische Trennung des Vorratsdatenspeichers, verbunden mit einer manuellen Eintragung der Verkehrsdaten, im Hinblick auf die Menge des Datenanfalls nicht praktikabel ist, wird die Trennung des VDS-Systems vom Internet durch den Einsatz einer Firewall empfohlen, die Verbindungen von außen in den Vorratsdatenspeicher unterbindet. Soweit von seiten des Diensteanbieters ein interner Zugriff auf die Verkehrsdaten erfolgt, ist das Zugriffssystem ebenfalls durch eine Firewall zu schützen.

Im Hinblick auf die kryptografische Absicherung des VDS-Systems müssen die Empfehlungen aus der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" des *BSI* hinzugezogen werden. Im Kapitel 5.2 wird unter dem Gesichtspunkt der Datensicherheit ein umfassendes Schutzkonzept inklusive einer detaillierten Systemarchitektur präsentiert, das auf der Annahme basiert, dass sich alle Komponenten des Vorratsdatenspeicherungssystems im Wirkbereich eines einzelnen Diensteanbieters befinden. Kritische Bereiche wie das Schlüsselmanagement werden dabei außerhalb des eigentlichen Datenspeichers administriert. Ferner soll durch eine lückenlose Protokollierung wie auch durch ein feingranulares Zugriffs- bzw. Berechtigungsmanagement auf der informationstechnischen wie auf der physischen Ebene verhindert werden, dass unberechtigte Zugriffe auf die gespeicherten Datenbestände stattfinden oder gar unbefugte Kopien erstellt werden können. Der konsequente Einsatz des für die IT-Security etablierten Vier-Augen-Prinzips trägt ebenso zu einem kontrollierten Datenzugriff im laufenden Betrieb bei. Die effektive Löschung der verschlüsselten Verkehrsdaten soll durch eine Vernichtung der für den Zugriff benötigten kryptografischen Schlüssel in Verbindung mit einer einfachen Freigabe zum Überschreiben der Speicherbereiche, auf denen die Verkehrsdaten gespeichert sind, sichergestellt werden. Hierdurch werden die technischen Unzulänglichkeiten herkömmlicher Löschoperationen umgangen. Es handelt sich mithin um eine Art von „organisatorischer Löschung", um der gesetzlichen Anforderung des § 113b Abs. 8 TKG Rechnung zu tragen, die eine „irreversible Löschung" fordert.

Zu jedem Datensicherheits- und Datenschutzkonzept gehört eine Protokollierung sämtlicher erfolgter Zugriffe auf das System, insb. im Hinblick auf das Lesen, Kopieren, Ändern, Löschen und Sperren von personenbezogenen Daten. Vor allem für solche Daten, die zu Zwecken sicherheitsbehördlicher Ermittlungen herangezogen werden sollen, muss ein besonders hoher Maßstab für die Datenauthentizität und Datenintegrität gelten. Diesem Erfordernis trägt im Rahmen der Vorratsdatenspeicherung die Protokollierungspflicht gem. § 113e TKG Rechnung, demgemäß der Zugriffszeitpunkt, die auf die Daten zugreifenden Personen und Zweck und Art des Zugriffs revisions-

sicher zu dokumentieren sind. In technischer Hinsicht wird vom Arbeitsentwurf des Anforderungskatalogs vorgeschlagen, die Protokolldaten in speziellen und gesicherten Einrichtungen zu speichern, da diese keinen Aufschluss über die gelöschten oder verarbeiteten Verkehrsdaten geben dürfen. Antworten an Sicherheitsbehörden oder die Ausgaben bei Anfragen an den Vorratsdatenspeicher dürfen deshalb nicht in den Protokolldaten enthalten sein. Die Löschung der Protokolle findet ebenso nach IT-Grundschutz statt, wobei der Löschvorgang selbst auch zu protokollieren ist.

V. Anhang: Handreichung für das Sicherheitskonzept nach § 113g TKG

Im Anhang befindet sich eine Handreichung für den verpflichteten Diensteanbieter, wie er das im Anforderungskatalog dargestellte Sicherheitskonzept zur Vorratsdatenspeicherung gegenüber der *BNetzA* nachweisen kann; die entsprechende gesetzliche Verpflichtung wird in § 113g TKG festgeschrieben. Deutlich wird auch hier erneut, dass die sichere Datenhaltung und die Gewährleistung von Datenqualität für die Vorratsdatenspeicherung eng mit den bereits nach § 109 TKG bestehenden Verpflichtungen für die Diensteanbieter zusammenhängen. So wird empfohlen, das Sicherheitskonzept nach § 109 Abs. 4 TKG um einen inhaltlich geschlossenen, spezifischen Teil nach § 113g TKG zu erweitern (Sicherheitskonzept technischer Vorkehrungen und sonstiger Maßnahmen für Speicherpflichten und Höchstspeicherfristen für Verkehrsdaten nach § 113g TKG). IT-Security wird somit auch hier, wenig überraschend, als gesamtheitlicher Ansatz verstanden, der auf bereits vorhandenen Maßnahmen aufbaut und Neues hierin integriert.

VI. Fazit und Ausblick

Die technischen und organisatorischen Anforderungen, die mit dem Entwurf des Katalogs nach § 113f TKG zu Zwecken von Datensicherheit und Datenschutz an die von der Vorratsdatenspeicherung betroffenen Betreiber angelegt werden, sind umfassend und entsprechen den Vorgaben des *BVerfG* von 2010 (MMR 2010, 356) sowie denjenigen des *EuGH* von 2014 (MMR 2014, 412, Rdnr. 66 f.). Vieles soll dabei die bisherigen Schutzanforderungen aus § 109 TKG ergänzen und erweitern, nicht Weniges wurde gedanklich aus dem BSI-Grundschutz übertragen, um ein Gesamtkonzept zur IT-Security vorlegen zu können. Dennoch werden für die Umsetzung der neuen Vorgaben erhebliche (finanzielle) Anstrengungen vonseiten der TK-Diensteanbieter zu erwarten sein – allein schon deshalb, weil für sicherheitsbehördliche Datenabrufe einerseits höchste Verfügbarkeit garantiert, andererseits jedoch in jedem Falle vermieden werden muss, dass unberechtigte Dritte sich Zugriff auf das VDS-System verschaffen, um Daten auszulesen oder, schlimmer noch, zu verändern und dadurch die Integrität zu beeinträchtigen. In tatsächlicher Hinsicht ist die Umsetzung der IT-Sicherheitsanforderungen fast ausschließlich von den Betreibern selbst abhängig, sodass regelmäßige und unabhängige Kontrollen unabdingbar sein werden.

Entsprechende Möglichkeiten zur Einzelfallüberprüfung sind durch § 113f Abs. 3 Satz 2 TKG i.V.m. § 109 Abs. 7 TKG für die *BNetzA* vorgesehen. Angesichts der Vielzahl von Unternehmen, die von der Vorratsdatenspeicherung betroffen sind sowie der bei ihnen jeweils anfallenden enormen Datenmengen wird es aber für die Zukunft fraglich sein, ob derlei Maßnahmen ausreichend sind, denn nur die bloße Möglichkeit der Manipulation weniger Vorratsdaten bei einem einzelnen Anbieter ist geeignet, die Tauglichkeit des gesamten Ermittlungsinstruments in Frage zu stellen. Nicht zuletzt steht das Problem im Raum, wie die Datensicherheit innerhalb der Ermittlungsbehörden hinreichend gewährleistet werden kann, denn auch diese können Angriffen von Hackern und Crackern zum Opfer fallen, sodass auch hier die Implementierung geeigneter Maßnahmen notwendig ist. Der Staatstrojaner-Skandal von 2011 hat gezeigt, dass der Umgang staatlicher Behörden mit neuartigen und computerbasierten Ermittlungsinstrumenten teils noch erhebliche Schwächen aufweist, die sich für die neue Vorratsdatenspeicherung keinesfalls wiederholen dürfen.

■ Dieser Beitrag entstand im Rahmen des vom *BMBF* geförderten Forschungsschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen“ als Bestandteil der Hightech-Strategie der *Bundesregierung*. Vgl. auch zur Datenübermittlung *Himmels/Weiglin*, MMR 2015, 710; zu Kritischen Infrastrukturen *Roos*, MMR 2015, 636 und *Mehrbrey/Schreibauer*, MMR 2016, 75.

Dr. Dennis-Kenji Kipker
ist wissenschaftlicher Assistent am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen sowie Vorstandsmitglied der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.