Deutscher Bundestag **Drucksache 18/12253**

18. Wahlperiode 05.05.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/11863 –

Umsetzung der Vorratsdatenspeicherung – Datenschutz, Technik und Sicherheit

Vorbemerkung der Fragesteller

Das Bundesverfassungsgericht erklärte die deutschen Vorschriften zur Vorratsdatenspeicherung mit Urteil vom 2. März 2010 für verfassungswidrig und nichtig. Das Urteil verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin gesammelten Daten. Das Bundesverfassungsgericht begründete seine Entscheidung u. a. damit, dass das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und zudem die Hürden für staatliche Zugriffe auf die Daten zu niedrig seien. Die Regelung zur Vorratsdatenspeicherung verstoße daher gegen Artikel 10 Absatz 1 des Grundgesetzes (GG). Am 8. April 2014 erklärte auch der Europäische Gerichtshof (EuGH) die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig, da sie mit der Charta der Grundrechte der Europäischen Union nicht vereinbar sei.

Mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (VerkDSpG) wurde in Deutschland im Oktober 2015 durch die Große Koalition dennoch ein neues Gesetz zur Vorratsdatenspeicherung verabschiedet, welches am 18. Dezember 2015 in Kraft getreten ist. Durch das VerkDSpG sind Erbringer öffentlich zugänglicher Telefon- und Internetzugangsdienste für Endnutzer verpflichtet, nach den §§ 113a, 113b des Telekommunikationsgesetzes (TKG) zentrale Verkehrsdaten für zehn bzw. vier Wochen zu speichern und entsprechend dem Auskunftsverlangen der Behörden an diese zu übermitteln.

Bis zum 1. Juli 2017 sind die Telekommunikationsunternehmen verpflichtet, die nötigen Voraussetzungen zur Speicherung der Verkehrsdaten umgesetzt zu haben (§ 150 Absatz 13 TKG). Die Bundesnetzagentur wurde u. a. mit der Erstellung eines Anforderungskatalogs nach § 113f TKG für die Umsetzung der Speicherpflicht und der Höchstspeicherpflicht für Verkehrsdaten sowie der Ausarbeitung einer Technischen Richtlinie (TR TKÜV) beauftragt.

Zum Datentransfer heißt es in Kapitel 4.1 des Anforderungskataloges, dass der Datentransport über ungesicherte Netze eine Transportverschlüsselung mit Authentizitäts- und Integritätsschutz (z. B. TLS) aufweisen muss. Insbesondere in

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 3. Mai 2017 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

TLS-Implementierungen wie OpenSSL und GnuTLS, aber auch in IPSec-Implementierungen wurden in den letzten Jahren wiederholt erhebliche Probleme festgestellt, die erfolgreiche Angriffe ermöglichten.

Im Anforderungskatalog ist in Kapitel 5.1.2 der Ausschluss von der Verkehrsdatenspeicherung geregelt. Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen nach § 99 Absatz 2 Satz 1 und 3 TKG können die Aussetzung der Speicherung der telefonischen Verkehrsdaten bei der Bundesnetzagentur beantragen. Weitere Ausnahmen von der Speicherung sind nicht vorgesehen. Am 21. Dezember 2016 urteilte der Europäische Gerichtshof, dass Daten von Berufsgeheimnisträgern nach den nationalen Rechtsvorschriften (hier § 203 StGB, § 53 StPO) ebenfalls von der Speicherung ausgenommen sein müssen (C 203/15 und C 698/15).

Die verpflichteten Telekommunikationsunternehmen können nach Kapitel 4.1 des Kataloges sogenannte Erfüllungsgehilfen beauftragen, um die komplette Verkehrsdatenspeicherinfrastruktur oder Einzelkomponenten auszulagern. Dabei bleibt die Verantwortung bei der Umsetzung und der Anlagensicherheit bei den verpflichteten Unternehmen.

Der eco – Verband der Internetwirtschaft e. V. berichtete in einem Politikbrief, dass aufgrund der variablen IP-Adressen-Vergabe sowohl der Port als auch der exakte Zeitstempel für eine eindeutige Endnutzeridentifikation gespeichert werden müsse (eco Politikbrief, Ausgabe 2. 2015/ 3. Quartal). Dadurch könne jedoch laut eco das Nutzungsverhalten der Endnutzer protokolliert werden. Den FAQ zur Speicherung und Übermittlung von speicherpflichtigen Verkehrsdaten nach den §§ 113a und 113b TKG vom Referat IS 16 der Bundesnetzagentur ist zu entnehmen, dass die Portadressen von der Speicherung ausgenommen sind, da andere Lösungen zur Identifikation gefunden worden sind. Aufgrund der gefundenen Lösung besteht das Problem, dass Endnutzer, sofern sie sich über nicht geschützte Hotspots anmelden, nicht eindeutig identifizierbar sind.

Der zentrale Bestandteil der Verschlüsselung der Verkehrsdaten ist der Schlüsselspeicher, mit dem die Daten entschlüsselt und ausgelesen werden können. Beim Löschvorgang liegt das Hauptaugenmerk auf dem Schlüsselspeicher. Die erhobenen Verkehrsdaten können nicht rückstandsfrei gelöscht (persistente Speicher) werden und daher muss der kryptographische Schlüssel (der Schlüsselspeicher) zusätzlich zu den Verkehrsdaten gelöscht werden (Anforderungskatalog nach § 113f, Kapitel 5.2.5). Das Speichermedium des Schlüsselspeichers muss dabei irreversibel löschbar oder zerstörbar sein. Bei Suchanfragen im Zugriff- oder Abfragesystem werden sensitive Daten (Klardaten und kryptographischer Schlüssel) im RAM des Zugriffsystems zwischengespeichert und dabei auf persistente Speicher ausgelagert (SWAP). Im Anforderungskatalog wird als Lösung die Deaktivierung oder Verschlüsselung des SWAP vorgeschlagen.

1. Wurde in der Bundesnetzagentur ein Stab eingerichtet, der die Verkehrsdateninfrastruktur der Provider kontrolliert und diese organisatorisch, soweit es gesetzlich vorgesehen ist, unterstützt, oder existieren Pläne, einen solchen Stab einzurichten?

   Wenn ja, mit welchem Zeitplan?

Die sich aus den gesetzlichen Vorschriften für die Bundesnetzagentur ergebenden Aufgaben werden von den bereits vorhandenen Organisationseinheiten wahrgenommen. Die Einrichtung eines Stabes war nicht notwendig.

2. Wird bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine neue Stabsstelle zur Überprüfung der Sicherheit beim Transport der Verkehrsdaten eingerichtet?

   Wenn ja, wann wird dies geschehen, und mit wie viel Personal und Sachmitteln soll diese Stabsstelle ausgestattet werden?

   Wenn nein, kann mit dem bestehenden Personal die Überprüfung qualitativ gewährleistet werden?

Die BfDI ist eine unabhängige eigenständige oberste Bundesbehörde. Auf Anfrage teilte sie mit, sie beabsichtige derzeit keine Einrichtung einer neuen Stabstelle. Die erforderliche Personalausstattung werde im Rahmen der Haushaltsberatungen erörtert.

3. Wie stellt die Bundesregierung sicher, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Bundesnetzagentur ihren Kontrollpflichten bei technischen Dienstleistern nachkommen können?

Die BfDI unterliegt keiner Aufsicht durch die Bundesregierung, sie unterliegt aber einer parlamentarischen und gerichtlichen Kontrolle. Als völlig unabhängige Behörde entscheidet allein die BfDI, ob und wie sie technische Dienstleister kontrolliert.

Bei der Bundesnetzagentur werden die entsprechenden Aufgaben durch bereits vorhandene Organisationseinheiten wahrgenommen, die bisher schon für die Überprüfung der nach § 109 des Telekommunikationsgesetzes (TKG) von den Telekommunikationsunternehmen vorzulegenden Sicherheitskonzepte und für deren Umsetzung durch die Unternehmen und gegebenenfalls durch deren technischen Dienstleister als Erfüllungsgehilfen vor Ort zuständig waren. Diese Einheiten werden bei Bedarf personell verstärkt.

4. Sind nach Ansicht der Bundesregierung die verpflichteten Erbringer verpflichtet, einen Datenschutzbeauftragten zu bestellen (bitte aktuelle Rechtsgrundlage und Rechtsgrundlage nach Inkrafttreten der Datenschutzgrundverordnung benennen)?

Gemäß § 4f Absatz 1 des Bundesdatenschutzgesetzes (BDSG) muss ein Datenschutzbeauftragter bestellt werden, wenn (1) personenbezogene Daten automatisiert verarbeitet werden und damit mindestens zehn Personen ständig beschäftigt sind oder (2) personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Zur Anpassung des allgemeinen deutschen Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) hat die Bundesregierung am 1. Februar 2017 den Entwurf eines neuen BDSG (BDSG-neu) beschlossen. In § 38 Absatz 1 BDSG-neu ist (unter Ausnutzung der Öffnungsklausel des Artikels 37 Absatz 4 DSGVO) eine dem § 4f Absatz 1 BDSG entsprechende Regelung vorgesehen.

5. Welche Stelle bzw. Behörde ist dafür zuständig zu kontrollieren, dass die gespeicherten Verkehrsdaten in der Bundesrepublik Deutschland verbleiben?

Die Zuständigkeit für die Kontrolle der Einhaltung der Verpflichtung zur Speicherung der Verkehrsdaten im Inland liegt nach § 115 Absatz 1 Satz 1 i. V. m. § 113b Absatz 1 Satz 1 TKG bei der Bundesnetzagentur.

6. Warum sind in dem Anforderungskatalog nach § 113f TKG, außer einer Art Sperrnummernliste von Telefonverbindungen für Organisationen nach § 99 Absatz 2 Satz 2 bis 7, die von der Speicherung ausgeschlossen sind, nicht auch anderweitige Verbindungen solcher Organisationen, wie z. B. die Internetverbindung, von der Speicherung ausgeschlossen?

§ 113b Absatz 6 TKG nimmt durch den Verweis auf § 99 Absatz 2 TKG Telefonverbindungen der Stellen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, von der Pflicht zur Speicherung von Verkehrsdaten aus. Ausschlaggebend ist hierbei, dass diese Beratungsangebote grundsätzlich anonym genutzt werden können. Diese Zielsetzung würde ohne eine entsprechende Ausnahme von der Speicherpflicht unterlaufen, da § 113b Absatz 2 Satz 1 Nummer 1 TKG für Telefonverbindungen die Speicherung der Rufnummer des anrufenden und des angerufenen Anschlusses vorsieht.

Bei Internetverbindungen verhält es sich dagegen anders: § 113b Absatz 3 TKG sieht die Speicherung der Verkehrsdaten vor, die den Internetzugang des jeweiligen Nutzers betreffen. Aus diesen Daten ergibt sich gerade nicht, mit wem über das Internet kommuniziert wurde, sondern nur, wann, wie lange und unter welcher Internetprotokoll-Adresse ein bestimmter Anschlussinhaber seinen Internetzugang genutzt hat. Im Falle von Online-Beratungsdiensten wird daher nicht erfasst, mit wem diese kommunizieren. Die Anonymität der Nutzer des Beratungsdienstes wird durch die Speicherung der Verkehrsdaten der Beratungsdienste selbst also nicht berührt.

7. Plant die Bundesregierung Nachbesserungen am VerkDSpG nach dem Urteil des EuGH vom 21. Dezember 2016, um auch Berufsgeheimnisträger von der Speicherung der Verkehrsdaten auszuschließen (s. Vorbemerkung der Fragesteller)?

   Wenn ja, wie sehen diese konkret aus?

   Wenn nein, warum nicht?

Die Bundesregierung plant derzeit kein entsprechendes Gesetzgebungsvorhaben (vgl. hierzu die Antwort zu den Fragen 1 bis 4 der Kleinen Anfrage auf Bundestagsdrucksache 18/12229). Denn auch ohne eine Ausnahme von der Speicherpflicht sind die Verkehrsdaten von Berufsgeheimnisträgern nach § 100g Absatz 4 der Strafprozessordnung (StPO) durch ein striktes Erhebungs- und Verwendungsverbot geschützt.

8. Was sind nach Ansicht der Bundesregierung Berufsgeheimnisträger nach der nationalen Rechtsvorschrift, und wären bei Nachbesserungen an dem VerkDSpG alle Berufsgeheimnisträger nach nationaler Rechtsvorschrift von der Speicherung ausgeschlossen?

Das bereits in der Antwort zu Frage 7 bezeichnete, die Daten von Berufsgeheimnisträgern betreffende Erhebungs- und Verwertungsverbot des § 100g Absatz 4 StPO, bezieht sich auf die in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 StPO genannten Personen. Im Übrigen ist nach der Antwort zu Frage 7 derzeit keine Gesetzesänderung geplant.

9. Wie wird die genaue Identifikation der einzelnen Endnutzer bei Mehrfachnutzungen von öffentlichen IP-Adressen bewerkstelligt, wenn keine Portverbindungen gespeichert werden (s. Vorbemerkung der Fragesteller; bitte detailliert erklären)?

In registrierungsfreien Hotspots lässt sich anhand der IP-Adresse in der Regel der Betreiber des registrierungsfreien Hotspots identifizieren.

10. Ist es richtig, dass in registrierungsfreien Hotspots die genaue Identifikation der Endnutzer nicht gewährleistet werden kann, und wenn ja, wie groß schätzt die Bundesregierung die Gefahr ein, dass diese Identifizierungslücke gezielt ausgenutzt wird (s. Vorbemerkung der Fragesteller)?

Anhand der IP-Adresse lässt sich in der Regel der Betreiber des registrierungsfreien Hotspots identifizieren.

11. Existieren weitere Szenarien neben den erwähnten, in denen die Endnutzer nicht identifiziert werden können (bitte detailliert auflisten)?

Bei jedem Szenario, bei dem sich mehrere Personen eine IP-Adresse teilen, werden weitere Informationen benötigt, um den Endnutzer eindeutig zu identifizieren. Durch Zuordnungsmöglichkeit der IP-Adresse zum Anschlussbetreiber (z. B. ein Haushalt) wird der in Frage kommende Personenkreis stark eingeschränkt.

12. Wie schätzt die Bundesregierung das Sicherheitsrisiko ein, das entsteht, wenn die gespeicherten Verkehrsdaten im Zuge der Verarbeitung ausgelesen werden und dabei vom RAM in den SWAP ausgelagert werden (s. Vorbemerkung der Fragesteller)?

Während der Verarbeitung im Zugriffssystem oder im Abfragesystem liegen die Verkehrsdaten notwendigerweise im Klartext im Arbeitsspeicher (RAM) vor. Eine ungesicherte Auslagerung (Swap) von Verkehrsdaten in die Auslagerungsdatei (swap file) des Massenspeichers würde bedeuten, dass Verkehrsdaten unverschlüsselt auf einem persistenten Speichermedium liegen. Um das zu verhindern, untersagt der nach § 113f TKG erstellte Anforderungskatalog eine ungesicherte Auslagerung sensitiver Daten aus dem RAM. Das kann entweder durch eine vollständige Deaktivierung der Auslagerungsdatei realisiert werden (damit findet gar keine Auslagerung mehr statt) oder durch eine Verschlüsselung der Auslagerungsdatei, so dass die Verkehrsdaten dann wieder ausschließlich verschlüsselt im Massenspeicher vorliegen. Zusätzlich sind das Zugriffssystem und das Abfragesystem durch die physischen und organisatorischen Sicherungsmaßnahmen so abgesichert, dass ein unberechtigter Zugriff sowohl auf den Arbeitsspeicher als auch auf die Auslagerungsdatei nicht möglich ist. Vor diesem Hintergrund schätzt die Bundesregierung das in der Frage angesprochene Sicherheitsrisiko als gering ein.

13. Wie hoch schätzt die Bundesregierung das Risiko ein, dass gelöschte Verkehrsdaten aus persistenten Speichern durch Dritte wiederhergestellt werden können, und welcher Aufwand ist nach Einschätzung der Bundesregierung notwendig, um das Verschlüsselungssystem zu entschlüsseln?

Die Verkehrsdaten werden nach den Vorgaben des Anforderungskatalogs nicht aus dem persistenten Speicher gelöscht, sondern verschlüsselt abgelegt und die Schlüssel werden vernichtet. Um Verkehrsdaten aus dem persistenten Speicher

wiederherzustellen, müsste die Verschlüsselung gebrochen werden. Der Anforderungskatalog nach § 113f TKG verlangt zum Schutz der Verkehrsdaten gegen unbefugte Kenntnisnahme und Verwendung den Einsatz eines besonders sicheren Verschlüsselungsverfahrens. Für ein geeignetes Verfahren verweist der Anforderungskatalog auf die Technische Richtlinie TR-02102-1 des BSI, die alle vom BSI empfohlenen kryptographischen Algorithmen inklusive der geforderten Schlüssellängen und anderen zu beachtenden Nebenbedingungen enthält. Wird ein solches Verschlüsselungsverfahren nach Stand der Technik implementiert, ist ein Angriff auf die Verschlüsselung nach heutigem Kenntnisstand nicht praktisch realisierbar.

14. Wie hoch schätzt die Bundesregierung die Gefahr ein, dass die kryptographischen Schlüssel oder entschlüsselte Klardaten aus dem RAM des entsprechenden Zugriffsystems durch Spähsoftware, Cyberangriffe oder anderweitige Methoden ausgelesen werden können?

Die Maßnahmen zur Absicherung des Zentralsystems schützen auf dem im Gesetz geforderten hohen Sicherheitsniveau hinreichend, um Cyberangriffe oder die Installation von Spähsoftware zu vermeiden. Als Beispiele sind die massiven Zutrittsbeschränkungen, die kompromisslose Umsetzung des Vier-Augen-Prinzips sowie die klare Entkopplung des Zentralsystems vom Internet zu nennen.

15. Kann die Bundesregierung Aussagen zum organisatorischen Aufwand und zu den Kosten beim Zerstören von Schlüsselobjekten (RAM) oder Speichermedien (CD) während des Löschvorganges des Schlüsselspeichers treffen, und warum wird nicht generell eine kostengünstigere, aufwandsärmere und sicherere Variante vorgeschrieben?

Der Anforderungskatalog nach § 113f TKG enthält zur Umsetzung der Löschung von Verkehrsdaten nach § 113b Absatz 8 TKG verschiedene Alternativen. Insofern obliegt es den Unternehmen, eine für sich geeignete Umsetzung zu wählen. Dabei ist es wichtig, dass zur Speicherung der Schlüssel ein Medium gewählt wird, das eine sichere Aufbewahrung aber auch eine sichere Löschung der Schlüssel ermöglicht.

Da bei der Verarbeitung von Verkehrsdaten sensitive Daten im Arbeitsspeicher anfallen, muss eine sichere Löschung im Arbeitsspeicher umgesetzt werden. Zusätzlicher Aufwand oder Kosten fallen beim Löschen von Schlüsseln aus dem Arbeitsspeicher nicht an. Im Falle einer Sicherungskopie auf CD ist das physische Zerstören der CD die sicherste Art, alle gespeicherten Daten unwiederbringlich zu löschen. Aufwand und Kosten für das Schreddern einer CD (z. B. pro Tag) sind gering.

16. Existieren Vorschriften, welches Betriebssystem auf den Zugriffsterminals installiert sein muss, und welche Sicherheitsstandards müssen generell durch das Betriebssystem gewährleisten sein?

Die Wahl des Betriebssystems auf den Zugriffsterminals ist freigestellt. Alle Clients, die zur Beauskunftung oder zu Wartungszwecken eingesetzt werden, müssen physisch gegen den Zugriff durch nicht ermächtigte Personen geschützt sein. Die eingesetzten Clients sind nach IT-Grundschutz mit dem Schutzbedarf „hoch“ und nach dem Stand der Technik abgesichert. Die genauen Maßnahmen sind anwendungs- und betriebssystemspezifisch. Sie werden im Sicherheitskonzept dokumentiert. Beim Zugriff auf die Verkehrsdaten ist die Einhaltung des

Vier-Augen-Prinzips zu gewährleisten. Es ist zudem eine umfangreiche Protokoll- und Dokumentationspflicht vorzusehen. Die zur Beauskunftung nötigen Abfragesysteme werden von dem Anforderungskatalog sowie der TKÜV und der TR TKÜV gleichermaßen erfasst.

17. Welche Stelle bzw. Behörde ist für die Kontrolle der Protokollierung des Löschvorganges zuständig, und wie wird sichergestellt, dass Fehler im Löschvorgang schnellstmöglich festgestellt und behoben werden?

Die Bundesnetzagentur ist nach § 115 Absatz 1 Satz 1 i. V. mit § 113e TKG für die Kontrolle der Protokollierung des Löschvorgangs zuständig. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert die ordnungsgemäße Protokollierung des Löschvorgangs im Rahmen der Datenschutzkontrolle nach § 113e Absatz 2 i. V. m. § 115 Absatz 4 TKG. Die Bundesnetzagentur ist gemäß § 115 Absatz 1 Satz 2 und 3 TKG zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- oder Betriebsräume während der üblichen Betriebs- und Geschäftszeiten zu betreten und zu besichtigen und die erforderlichen Auskünfte zu verlangen. Soweit Fehler im Löschvorgang festgestellt werden, kann die Bundesnetzagentur Anordnungen und sonstige Maßnahmen treffen, um die Einhaltung der Verpflichtung zur Löschung der Verkehrsdaten nach § 113b Absatz 8 TKG und zur Löschung der Protokolldaten nach § 113e Absatz 3 TKG sicherzustellen. Die Anordnungen können, wenn erforderlich, im Wege des Verwaltungszwangs nach dem Verwaltungsvollstreckungsgesetz (VwVG) durchgesetzt werden. Gemäß § 137 TKG haben Widerspruch und Klage gegen Entscheidungen der Bundesnetzagentur keine aufschiebende Wirkung.

18. Können am Anforderungskatalog nach § 113f TKG Version 1.0 (www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html) vom 23. November 2016 noch Änderungen, die sich z. B. aus dem EuGH-Urteil vom 21. Dezember 2016 ergeben, vorgenommen werden, und wenn nein, warum nicht?

Grundsätzlich können Änderungen am Anforderungskatalog nach § 113f TKG vorgenommen werden. Dies gilt insbesondere, wenn Anpassungen an technische Neuerungen erforderlich werden. Eine Anpassung des Anforderungskatalogs aufgrund des EuGH-Urteils vom 21. Dezember 2016 ist derzeit nicht vorgesehen. Der Anforderungskatalog nach § 113g TKG konkretisiert den besonders hohen Standard der Datensicherheit und Datenqualität, wie er in den geltenden gesetzlichen Verpflichtungen gemäß §§ 113b bis 113e TKG vorgesehen ist.

19. Hat die Bundesregierung Erkenntnisse über den Umfang der Auslagerung der technischen Umsetzung des VerkDSpG durch verpflichtete Erbringer an einzelne große Dienstleister (sog. Erfüllungsgehilfen)?

Wenn ja, welche Dienstleister sind dies?

Die Bundesregierung hat derzeit keine Erkenntnisse über den Umfang der Auslagerung an einen sog. Erfüllungsgehilfen bei der zum 1. Juli 2017 umzusetzenden Speicherpflicht.

20. Sieht die Bundesregierung bei der Auslagerung der Infrastruktur die Gefahr, dass die Sicherheitsstandards sinken, da erstens die Anweisungskette verlängert wird und da zweitens die verpflichteten Erbringer und nicht die Dienstleister für das Sicherheitskonzept verantwortlich sind, was die Gefahr vergrößert, dass das Konzept nicht gesetzeskonform umgesetzt wird?

    Wenn ja, welche Schlüsse zieht sie daraus?

    Wenn nein, warum nicht?

Die Bundesregierung sieht eine derartige Gefahr grundsätzlich nicht. Sie stellt im Gegenteil fest, dass etwa die Möglichkeit zur Auslagerung der Umsetzung von Überwachungsmaßnahmen der Telekommunikation nach § 5 Absatz 3 TKÜV an einen Erfüllungsgehilfen bei kleineren Unternehmen zu einem höheren Standard bei der Umsetzung geführt hat.

21. Wer muss nach Ansicht der Bundesregierung im Falle eines Datenmissbrauchs, eines erfolgreichen Angriffs oder eines Datendiebstahls durch Dritte die Haftung übernehmen, wenn die Daten an Dienstleister (sog. Erfüllungsgehilfen) ausgelagert wurden?

Grundsätzlich ist der Erbringer öffentlich zugänglicher Telekommunikationsdienste für die Einhaltung der Verpflichtungen der §§ 113b bis 113e TKG verantwortlich. Dies gilt auch dann, wenn er hierfür einen sog. Erfüllungsgehilfen beauftragt. Gegebenenfalls bestehende zivilrechtliche Haftungsansprüche aus dem Innenverhältnis bleiben hiervon unberührt und richten sich insbesondere nach der Vertragsgestaltung im Einzelfall.

22. Wie beurteilt die Bundesregierung das dadurch entstehende Bündelungsrisiko von IT-Angriffen und das Missbrauchspotential der Daten, wenn de facto die Datenbestände fast aller Anbieter bei sehr wenigen Dienstleistern konzentriert sind?

Nach § 113f Absatz 1 TKG muss unabhängig von der Art der Umsetzung bei den Unternehmen selbst oder bei einem Erfüllungsgehilfen ein besonders hoher Standard der Datensicherheit eingehalten werden. Die Dienstleister unterliegen dementsprechend dem selben hohen Schutzniveau. Die Verantwortung für die Umsetzung des Anforderungskatalogs und für die Einreichung des Sicherheitskonzeptes verbleibt bei dem jeweiligen Verpflichteten. Somit kann Fehlentwicklungen rechtzeitig entgegen gewirkt werden. Die Bundesregierung hat zudem keine Anhaltspunkte dafür, dass etwa die großen Unternehmen, die rund 98 Prozent des Marktes abdecken, ihre Speicherpflicht an Erfüllungsgehilfen auslagern.

23. Was versteht die Bundesregierung unter einem „zeitnahen“ Einspielen von Sicherheits-Updates (Patches) auf den für die Durchführung des VerkDSpG verwendeten Systemen (Anforderungskatalog nach § 113f TKG, Kapitel 5.2.3)?

Sicherheitslücken in IT-Produkten sind nicht auszuschließen. Daher müssen die von den Herstellern zur Verfügung gestellten Sicherheits-Updates zeitnah eingespielt werden. Der Begriff „zeitnah“ ist einzelfallabhängig zu betrachten und etwa in Abhängigkeit der potenziellen Auswirkung auf die konkrete eingesetzte Technik der Unternehmen auszulegen. Dabei ist zu beachten, dass das Einspielen eines Updates niemals risikofrei ist und im Extremfall auch zu einem Ausfall des Gesamtsystems oder zu Datenverlust führen kann. Daher sollte jedes Update individuell vor dem Einspielen ausreichend getestet werden.

24. Welche Behörde ist für die konkrete technische Überprüfung des Patch-Standes auf den Systemen zuständig, und in welchem Abstand erfolgt diese Überprüfung?

Die Verpflichtung nach § 113f TKG betrifft zunächst die Unternehmen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzeptes. Die Überprüfung soll mindestens alle zwei Jahre erfolgen, § 109 Absatz 4 Satz 7 und 8 TKG.

25. Wie beurteilt die Bundesregierung das Risiko der Kontaminierung von für VerkDSpG-Zwecke verwendeten Systemen durch möglicherweise in den Sicherheits-Updates enthaltene Hintertüren (Backdoors)?

Die Möglichkeit, dass Sicherheits-Updates selbst schadhafte Funktionen enthalten, ist in der IT grundsätzlich gegeben. Aufgrund der in dem Anforderungskatalog nach § 113f TKG enthaltenen Regelungen und Vorgaben zum hohen Schutz vor dem Zugriff aus dem Internet und der Regelungen zu den zu betreibenden Firewalls einschließlich der Protokollpflichten geht die Bundesregierung von einer weitgehenden Reduzierung der Gefahr aus, die durch eine schadhafte Software in einer Einzelkomponente gegeben sein könnte. Darüber hinaus sollten nur Updates aus vertrauenswürdigen Quellen genutzt werden, die eindeutig (z. B. mit einer Signatur) verifiziert werden können.

26. Wie beurteilt die Bundesregierung die technischen Risiken durch den Einsatz von Transportverschlüsselungskomponenten mit Authentizitäts- und Integritätsschutz?

Zu dieser Art der Transportverschlüsselung verweist der Anforderungskatalog nach § 113f TKG auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in seiner Technischen Richtlinie „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, die regelmäßig an neue Erkenntnisse angepasst wird. Es ist sehr wichtig, eine Implementierung zu verwenden, deren Hersteller zeitnah gefundene Schwachstellen beseitigt und Updates bereitstellt. Wenn die oben genannten Aspekte unter Berücksichtigung der Empfehlungen des BSI beachtet werden, kann ein Maß an Sicherheit erreicht werden, das vor den meisten Angriffen schützen kann. Die Bundesregierung ist daher der Auffassung, dass bei Einhaltung dieser Empfehlungen der nach § 113f TKG geforderte hohe Standard der Datensicherheit eingehalten wird und mögliche Risiken auf ein Mindestmaß reduziert werden.

27. Welche Maßnahmen werden ergriffen, und was sind die konkreten Zeitfenster, um ein Update auf gepatchte Versionen zu erzwingen (s. Vorbemerkung der Fragesteller)?

Die Bundesnetzagentur hat nach § 109 Absatz 4 Satz 7 und 8 TKG regelmäßig Überprüfungen durchzuführen. Sollte sie dabei ein zu bemängelndes Verhalten beim Aufspielen notwendiger Sicherheits-Updates feststellen, kann sie einzelfallabhängig geeignete Maßnahmen nach § 115 und § 149 Absatz 2 TKG ergreifen. Im Übrigen wird auf die Antwort zu Frage 26 verwiesen.

28. Wie beurteilt die Bundesregierung den Interessenkonflikt der betroffenen Unternehmen bei ihren wirtschaftlichen Erwägungen hinsichtlich der Kosten der IT-Sicherheit, wenn bei der Speicherung der Vorratsdaten mit steigenden personellen und finanziellen Anforderungen zur Aufrechterhaltung einer sicheren Speicherung zu rechnen ist?

Die Bundesregierung ist der Überzeugung, dass die Unternehmen hinsichtlich der Kosten der IT-Sicherheit grundsätzlich, d. h. auch ohne die Verpflichtung zur Verkehrsdatenspeicherung, bereits ein Eigeninteresse sowohl an einer sicheren Speicherung ihrer Kundendaten als auch an der Sicherheit ihrer IT haben. Gerade bei den Telekommunikationsunternehmen bildet die IT-Sicherheit die Grundlage für das erfolgreiche Erbringen der Telekommunikationsdienste, für den Markterfolg eines Unternehmens und damit auch für dessen wirtschaftlichen Erfolg. Die Bundesregierung sieht insofern keinen auf Verkehrsdatenspeicherungspflicht gründenden Interessenkonflikt hinsichtlich der IT-Sicherheitskosten.

29. Wie beurteilt die Bundesregierung das Risiko, dass durch den teilweise mehrmonatigen Zyklus zwischen Auffinden eines Sicherheitsproblems in den verwendeten Software-Komponenten und der Verfügbarkeit von Sicherheits-Updates sehr lange Angriffszeitfenster entstehen können?

Die Bundesregierung schätzt das Risiko als relativ gering ein. Im Übrigen verweist sie auf die Antwort zu Frage 25.

30. Welche Maßnahmen werden ergriffen, um die verwendeten Systeme regelmäßig auf Hinweise von möglicherweise erfolgten Angriffen zu prüfen, und welche Konsequenzen ergeben sich aus der Feststellung eines erfolgreichen Angriffs?

Der Anforderungskatalog sieht hierzu unter Punkt 5.2.4 Absatz 3 bestimmte Schutz- und Kontrollmaßnahmen vor. Die Verpflichteten haben in ihren Sicherheitskonzepten die konkrete technische und organisatorische Umsetzung dieser Maßnahmen aufzuzeigen. Etwaige Konsequenzen aus einem Angriff sind einzelfallabhängig und richten sich u. a. nach Art und Schwere des festgestellten Angriffs.

31. Plant die Bundesregierung eine regelmäßige Unterrichtung des Parlaments über relevante IT-Sicherheitsvorkommnisse in Systemen nach dem Anforderungskatalog nach § 113f TKG?

Wenn ja, durch welche Behörde und wie oft?

Nein.

32. Inwieweit könnte die Vorratsdatenspeicherung die Entwicklung und Verbreitung technischer Mittel zur Verschleierung elektronischer Spuren begünstigen und so eine Überwachung selbst in konkreten Verdachtsfällen vereiteln (bitte begründen)?

Die Bundesregierung hat hierfür keine Anhaltspunkte.

33. Wie sieht nach Einschätzung der Bundesregierung „eine hinreichende physische Sicherheit“ der Speichereinrichtung aus, fernab von der Kontrolle des Zugangs (s. Anforderungskatalog nach § 113f TKG, Kapitel 5.2.62)?

Die hinreichende physische Sicherheit ist individuell auf Grundlage einer Risikoanalyse des Verpflichteten zu bewerten. Einschlägig ist Kapitel B2 aus dem BSI-Standard IT-Grundschutz. Eine hinreichende „physische Sicherheit“ kann daher grundsätzlich bei Umsetzung der Maßnahmen, die sich aus den Grundschutzbausteinen Kapitel B2 Infrastruktur ergeben, angenommen werden. Ist ein hoher Standard der Datensicherheit erforderlich, so sind zusätzlich Maßnahmen aus dem HV-Kompendium des BSI umzusetzen.

34. Wie sieht ein „geschlossener Sicherheitsbereich“ aus (s. Anforderungskatalog nach § 113f TKG, Kapitel 5.2.62)?

Aufgrund der hohen Anforderungen der Datensicherheit sollte ein „geschlossener Sicherheitsbereich“ innerhalb des Rechenzentrums in allen raumbildenden Teilen mindestens der Widerstandsklasse RC4 nach EN 1627 entsprechen. Weiterhin sollte mittels der technischen Einrichtungen der Zutrittskontrollanlage sichergestellt sein, dass der Zutritt zu dem geschützten Bereich nur durch das zeitlich unmittelbar zusammenhängende berechtigte Handeln einer weiteren Person neben dem Zutrittsberechtigten möglich ist (Vier-Augen-Prinzip). Eine Videoüberwachung mit automatischer Ereignismeldung an qualifiziertes Personal und alle Maßnahmen zum Sabotageschutz aus dem HV-Kompendium des BSI sollten umgesetzt sein.

35. Ist die physische Absicherung nach Einschätzung der Bundesregierung hinsichtlich des unerlaubten Zugriffes durch ausländische Geheimdienste oder Kriminelle ausreichend gesichert (bitte begründen)?

Die Anforderungen an die physische Absicherung richten sich nach den Vorgaben des Anforderungskatalogs nach § 113f TKG. Die Bundesregierung hält die physische Absicherung bei Umsetzung der Vorgaben durch die verpflichteten Unternehmen für ausreichend, um Zugriffe zu verhindern.

36. Welche Kriterien und Maßstäbe muss das Sicherheitspersonal einer Speichereinrichtung erfüllen?

Nach § 113d Nummer 5 TKG muss der Zugriff auf die Verkehrsdaten in jedem Einzelfall durch mindestens zwei Personen im Vier-Augen-Prinzip erfolgen, die dazu durch den Verpflichteten einzeln besonders ermächtigt worden sind. Zudem ist vorgesehen, dass die Aktivitäten der einzelnen Personen protokolliert werden. Darüber hinaus besteht derzeit keine Regelung.

37. Wie genau ist die unabhängige Stelle gestaltet, die die Eignung der Auftragnehmer (sog. Erfüllungsgehilfen) kontrollieren soll, und wie ist die Unabhängigkeit zu verstehen – ist sie innerhalb der Bundesnetzagentur organisiert oder ist es eine externe Stelle (s. FAQ, Referat IS 17, www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html)?

Eine Auslagerung des Datenspeichersystems an einen Auftragnehmer (sog. Erfüllungsgehilfen) im Inland ist grundsätzlich möglich. Es würde sich in diesem

Fall um eine Auftragsdatenverarbeitung nach § 11 BDSG handeln. Der Auftragnehmer ist daher unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen von dem zur Speicherung der Verkehrsdaten gesetzlich verpflichteten Unternehmen nach § 11 Absatz 2 BDSG sorgfältig auszuwählen. Der Auftraggeber hat dies regelmäßig dann erfüllt, wenn sich der Auftragnehmer einer Überprüfung durch eine qualifizierte unabhängige Stelle unterzogen hat und dabei bescheinigt wurde, dass die von ihm zur Verfügung gestellten Systeme und Verfahrensabläufe den Anforderungen an einen besonders hohen Standard der Datensicherheit und Datenqualität nach Maßgabe des § 113f TKG entsprechen. Die qualifizierte und unabhängige Stelle liegt außerhalb der Bundesnetzagentur.

38. Sind Clients zur Beauskunftung oder zu Wartungszwecken (Management-Konsole) innerhalb der Speichereinrichtung nochmals gesondert physisch gesichert, fernab der Zugangskontrolle oder genügt die physische Absicherung der Gesamtanlage?

Gemäß Anforderungskatalog nach § 113f TKG muss das Abfragesystem nach dem Stand der Technik abgesichert sein. Demnach ist eine physische Absicherung der Clients (PC) notwendig. Üblicherweise sind auch die Räumlichkeiten, in denen die Bearbeitung von Anfragen zu betrieblich gespeicherten Verkehrsdaten erfolgt, bereits zusätzlich physisch abgesichert. Die von den Verpflichteten eingerichteten Maßnahmen müssen in jedem Einzelfall konkret im Sicherheitskonzept beschrieben werden.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333