Deutscher Bundestag **Drucksache 18/11863**

18. Wahlperiode 28.03.2017

Kleine Anfrage

der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, Katrin Kunert, Martina Renner, Dr. Petra Sitte, Halina Wawzyniak und der Fraktion DIE LINKE.

Umsetzung der Vorratsdatenspeicherung – Datenschutz, Technik und Sicherheit

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 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.

Wir fragen die Bundesregierung:

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?

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?

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?

4. Sind nach Ansicht der Bundesregierung die verpflichteten Erbringer verpflichtet, einen Datenschutzbeauftragten zu bestellen (bitte aktuelle Rechtsgrundlage und Rechtsgrundlage nach Inkrafttreten der Datenschutzgrundverordnung benennen)?
5. Welche Stelle bzw. Behörde ist dafür zuständig zu kontrollieren, dass die gespeicherten Verkehrsdaten in der Bundesrepublik Deutschland verbleiben?
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?
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?
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?
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)?
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)?
11. Existieren weitere Szenarien neben den erwähnten, in denen die Endnutzer nicht identifiziert werden können (bitte detailliert auflisten)?
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)?
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?
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?
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?
16. Existieren Vorschriften, welches Betriebssystem auf den Zugriffsterminals installiert sein muss, und welche Sicherheitsstandards müssen generell durch das Betriebssystem gewährleisten sein?

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?

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?

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?

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?

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?

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?

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)?

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

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

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

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

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?

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?
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?
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?
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)?
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)?
34. Wie sieht ein „geschlossener Sicherheitsbereich“ aus (s. Anforderungskatalog nach § 113f TKG, Kapitel 5.2.62)?
35. Ist die physische Absicherung nach Einschätzung der Bundesregierung hinsichtlich des unerlaubten Zugriffes durch ausländische Geheimdienste oder Kriminelle ausreichend gesichert (bitte begründen)?
36. Welche Kriterien und Maßstäbe muss das Sicherheitspersonal einer Speichereinrichtung erfüllen?
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)?
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?

Berlin, den 28. März 2017

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

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