Deutscher Bundestag **Drucksache 19/10952**

19. Wahlperiode 17.06.2019

Kleine Anfrage

der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Britta Katharina Dassler, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Thomas L. Kemmerich, Pascal Kober, Dr. Lukas Köhler, Carina Konrad, Alexander Graf Lambsdorff, Ulrich Lechte, Michael Georg Link, Till Mansmann, Dr. Jürgen Martens, Roman Müller-Böhm, Dr. Martin Neumann, Bernd Reuther, Christian Sauter, Matthias Seestern-Pauly, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Stephan Thomae, Johannes Vogel (Olpe), Nicole Westig und der Fraktion der FDP

Digitale Souveränität

Die Bundesregierung hat die digitale Souveränität als wichtiges Ziel für ein innovatives und wirtschaftlich starkes Deutschland und Europa benannt. Da Souveränität in diesem Kontext die unabhängige Selbstbestimmung in Bezug auf digitale Systeme und Daten meint, ist der Begriff der „digitalen Souveränität“ sowohl für Staaten als auch für Einzelpersonen anwendbar. Für den Bereich der Staaten steht die digitale Souveränität auf mehreren Säulen, darunter beispielsweise die alleinige Kontrolle über die Speicherung, Weitergabe und Nutzung von Daten oder auch die Fähigkeit, Hardware-Komponenten zu entwickeln, herzustellen und zu kontrollieren. Da eine vollständige digitale Souveränität für Staaten in aller Regel weder realistisch erreichbar noch erstrebenswert ist, muss bei den entscheidenden Aspekten der Souveränität immer eine Abwägung zwischen Kosten und Nutzen stattfinden. So ist beispielsweise die vollständige Neuentwicklung für ein bereits über Dritte verfügbares Tool unter Umständen sehr kostenintensiv, kann aber möglicherweise trotzdem einen großen Mehrwert haben, wenn dadurch beispielsweise betroffene sensible Daten auf europäischen oder deutschen Servern gehalten werden können.

Zur Entwicklung entsprechender Strategien entstanden unter Beteiligung der Bundesregierung im Rahmen des Nationalen IT-Gipfels 2015 in der Fokusgruppe 1 das Papier „Leitplanken Digitaler Souveränität“ (www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1) und im Rahmen des Digital-Gipfels 2018 in der Fokusgruppe „Digitale Souveränität in einer vernetzten Ge-

sellschaft“ das Papier „Digitale Souveränität und Künstliche Intelligenz –Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“ (www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5). Während sich das Papier des Nationalen IT-Gipfels bezüglich der Definition von digitaler Souveränität noch auf die Verhinderung unausweichlicher Abhängigkeiten und die Feststellung beschränkt, dass digitale Souveränität auf verschiedenen Pfeilern ruht, entwickelt das Papier aus dem Jahr 2018 die Definition des Begriffs weiter und ergänzt sie um eine Entscheidungshilfe. Darin wird ein Schichtmodell digitaler Souveränität beschrieben, welches den Fokus auf die Fähigkeit legt, „technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen“ (S. 3 des Papiers).

Die immer wieder festgestellten international unterschiedlichen Datenschutzniveaus (vgl. beispielsweise die Cloud-Speicherung der Bodycam-Daten) und international unterschiedlichen Zugriffsmöglichkeiten durch Sicherheitsbehörden und Geheimdienste (vgl. beispielsweise die Diskussion zu Huawei oder aktuelle Pläne des Bundesministeriums des Innern, für Bau und Heimat zu Hintertüren in verschlüsselten Messengern) zeigen nach Ansicht der Fragesteller die Notwendigkeit auf, sich mit dem Thema der digitalen Souveränität zu befassen.

Wir fragen die Bundesregierung:

1. Inwiefern fühlt sich die Bundesregierung an die von ihr auf dem IT-Gipfel 2015 und dem Digital-Gipfel 2018 mit ausgearbeiteten Papiere zur digitalen Souveränität gebunden?
2. An welchen Stellen sind Projekte zur Förderung des Ziels digitaler Souveränität in der „Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels“ festgehalten?

   Mit welchen konkreten Zielen und Maßnahmen sind die Projekte hinterlegt?
3. Hat sich das Digitalkabinett der Bundesregierung bereits mit Fragestellungen im Bereich der digitalen Souveränität beschäftigt?

   a) Falls ja, mit welchen, und mit welchem jeweiligen konkreten Ergebnis?

      Von welchen Ressorts wurden die Fragestellungen eingebracht?

   b) Falls nein, wann wird sich das Digitalkabinett mit welchen Fragestellungen beschäftigen?

      Welche Wünsche wurden aus den verschiedenen Ressorts schon dahingehend geäußert?
4. Werden staatliche Infrastrukturen mit dem Ziel der Erreichung maximaler digitaler Souveränität aufgebaut?

   a) Falls ja, in welchen Bereichen, und in welchem Umfang?

      Wann sollen diese jeweils fertiggestellt sein?

   b) Falls nein, warum wird auf staatliche Infrastrukturen in den einzelnen Bereichen verzichtet?
5. Wie fördert die Bundesregierung die von ihr in den „Leitplanken Digitaler Souveränität“ erkannten Schlüsselkompetenzen in den Bereichen der Entwicklung offener Standards, der Software-Kompetenzen, der Hardware-Kompetenzen und der IT-Sicherheit?

   Welche konkreten Maßnahmen hat die Bundesregierung ergriffen, um die von ihr erkannten Schlüsselkompetenzen für die öffentliche Hand zu fördern?

6. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Marktsichtbarkeit deutscher Unternehmen der IT-Sicherheitswirtschaft durch öffentliche Auftraggeber als Referenzen zu erhöhen?

   Welche Probleme ergeben sich nach Kenntnis der Bundesregierung insbesondere für die mittelständische IT-Sicherheitswirtschaft, wenn diese sich an der Ausschreibung öffentlicher Aufträge beteiligen will?

7. Wie viele und welche öffentlichen Aufträge hat die Bundesregierung im Bereich der IT-Sicherheit seit 2015 vergeben, die das Ziel verfolgen, ein Signal für IT-Sicherheit „made in Europe“ zu setzen?

   An wen sind die Aufträge vergeben worden?

8. Mit welchen konkreten Zielen und Vorhaben hinterlegt die Bundesregierung die folgenden Forderungen aus den „Leitplanken Digitaler Souveränität“ und welche konkreten Maßnahmen hat sie diesbezüglich bereits ergriffen:

   a) Grundlage für souveränes Handeln ist ein sicherer digitaler Raum;

   b) Europas Wirtschaft, Staat und Bürger müssen in die Lage versetzt werden, vertraulich und geschützt in digitalen Netzen zu kommunizieren;

   c) es darf keine Hintertüren oder sonstigen Kanäle geben, über die Daten unbefugt eingesehen, kopiert oder verändert werden können;

   d) der bewusste Einsatz von Security-Referenzprojekten in Heimatmärkten hat hohe Signalwirkung;

   e) die ENISA (European Network and Information Security Agency) muss als Kooperationsplattform für Cyber-Security gestärkt werden;

   f) die Förderung der Verfügbarkeit offener Standards als innovationsfördernder Gestaltungsrahmen muss insbesondere durch den Einsatz in Wirtschaft und öffentlicher Verwaltung gefördert werden;

   g) die öffentliche Hand sollte mit einem „Cloud First“-Programm eine Vorreiterrolle für die öffentliche Verwaltung einnehmen;

   h) für Start-ups sollten in den ersten vier Jahren ihres Bestehens grundsätzlich wachstumsfördernde Sonderregeln gelten;

   i) für die Wachstumsphase von Unternehmen sowie KMU braucht es zusätzlich Unterstützung, insbesondere im Bereich der internationalen Skalierung und Digitalisierung;

   j) eine Initiative „Start-ups Digitale Wirtschaft“ zur Förderung von IKT-B2B-Start-ups (IKT = Informations- und Kommunikationstechnik; B2B = Business-to-Business) sollte ins Leben gerufen werden?

9. Wie soll nach Ansicht der Bundesregierung das Ziel erreicht werden, dass auch europäische Plattformen globale Standards setzen können und in ihren Bereichen die Marktführerschaft einnehmen?

   Welche Wachstumshürden bestehen für Unternehmen nach Ansicht der Bundesregierung durch die Verantwortlichkeit für Inhalte, die Plattformbetreibern mit der Urheberrechtsrichtlinie (Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt) auferlegt werden?

10. Inwiefern wird bei der IT-Beschaffung durch die Bundesregierung das Prinzip der digitalen Souveränität und die Kriterien des im Papier „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“ erarbeiteten Schichtenmodells berücksichtigt?

11. Mit welchen konkreten Zielen und Vorhaben hinterlegt die Bundesregierung die folgenden Forderungen aus dem Papier „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“, und welche konkreten Maßnahmen hat sie diesbezüglich bereits ergriffen:

    a) Kommunikationsnetze müssen jederzeit verfügbar sein, Menschen, Wirtschaft und Staat eine abhörsichere Kommunikation ermöglichen und Schutz vor Manipulation der transportierten Daten bieten;

    b) die erste Grundvoraussetzung für zuverlässige digitale Infrastrukturen ist vertrauenswürdige Technologie;

    c) Pfeiler für zuverlässige digitale Infrastrukturen ist die Kontrolle über nationale Telekommunikationsnetze, die zwingend in deutscher oder mindestens europäischer Hand sein müssen;

    d) in Krisenfällen muss auch der physische Zugriff auf Rechenzentren gewährleistet sein;

    e) da Digitalisierung im Allgemeinen auf die Speicherung von Daten angewiesen ist, müssen Cloud-Rechenzentren in Europa als kritische Infrastrukturen betrachtet werden;

    f) damit IT-Sicherheit „made in Europe“ bestehen kann, brauchen heimische Anbieter öffentlich geförderte Leuchtturmprojekte;

    g) europäische Initiativen zur Standardisierung von Security by Design und Security by Default müssen vorangetrieben werden;

    h) für Aufbau und Erhalt digitaler Souveränität sind digitale Kompetenzen sowie die Fähigkeit, sichere Künstliche Intelligenz zu entwickeln, erforderlich;

    i) Kontroll- und Innovationsfähigkeit müssen dadurch gesichert werden, dass kritische Daten der Verwaltung nur in Systemen verarbeitet werden, bei denen staatliche Organe die Hoheit darüber haben, wer auf diese Daten zugreifen kann und bei denen Daten jederzeit in andere Systeme übertragbar und durchsetzbar im ursprünglichen System löschbar sind;

    j) bei öffentlichen Beschaffungen sollten Software- und Cloud-Angebote grundsätzlich bevorzugt werden, deren Quellcode geprüft und geändert werden kann; bei kritischen Systemen sollte dies verpflichtend sein?

12. Wie sollen nach Ansicht der Bundesregierung Deutschland und Europa, die aktuell als Standorte für Rechenzentren aufgrund der vergleichsweise hohen Stromkosten eher unbeliebt sind, zu attraktiveren Standorten für Rechenzentren werden?

Berlin, den 5. Juni 2019

Christian Lindner 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