Deutscher Bundestag **Drucksache 21/5844**

21. Wahlperiode 07.05.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Sascha Lensing, Dr. Gottfried Curio, Dr. Christian Wirth, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/5573 –

Sicherheitsrisiken staatlicher Überwachungssysteme und Cloud-basierter IT-Lösungen

Vorbemerkung der Fragesteller

Nach übereinstimmenden Medienberichten sollen ausländische Nachrichtendienste im Iran über einen längeren Zeitraum sicherheitsrelevante technische Systeme kompromittiert und hierdurch Bewegungsprofile hochrangiger Zielpersonen erstellt haben. In den Berichten ist insbesondere von gehackten Verkehrs- und Überwachungskameras (www.fr.de/politik/israel-hacked-iranian-traffic-cameras-to-spy-on-khamenei-zr-94195423.html) sowie von der Ausnutzung mobiler Endgeräte im Umfeld von Sicherheitskräften die Rede (www.juedische-allgemeine.de/israel/recherche-israel-hackte-telefone-iranischer-bodyguards/).

Für die Fragesteller stellt sich vor diesem Hintergrund die Frage, in welchem Umfang öffentliche Videoüberwachungs- und sonstige sicherheitsrelevante IT-Systeme gegenüber langfristigen, verdeckten Kompromittierungen durch externe Angreifer geschützt sind. Dies betrifft vor allem Systeme im öffentlichen Raum (z. B. Video- und Verkehrsüberwachung, Bahnhöfe, Flughäfen), aber auch angrenzende Kommunikations- und Steuerungssysteme und gilt insbesondere auch mit Blick auf die anhaltende angespannte IT-Sicherheitslage, zunehmende Vernetzung öffentlicher Systeme, komplexe Lieferketten und Nutzung externer IT-Dienstleister.

Hinzu kommt, dass in der öffentlichen Verwaltung in Deutschland in erheblichem Umfang externe, häufig Cloud-basierte IT- und Kommunikationsdienste eingesetzt werden. Hierzu zählen beispielsweise Videokonferenz- und Kollaborationslösungen von Anbietern mit Sitz in Drittstaaten, die sowohl auf Ebene des Bundes als auch in den Ländern und Kommunen verbreitet genutzt werden. Allein im Jahr 2024 wurden nach einem Medienbericht Ausgaben in Höhe von rund 481,4 Mio. Euro für Lizenzen eines großen ausländischen Softwareanbieters in der Bundesverwaltung veranschlagt (www.heise.de/hintergrund/Microsoft-Abhaengigkeit-Bund-zahlt-in-einem-Jahr-fast-500-Millionen-Euro-11170931.html), was in den Augen der Fragesteller die weitreichende Verbreitung entsprechender Cloud-basierter Lösungen unterstreicht.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 7. Mai 2026 übermittelt.

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

1. Hat sich die Bundesregierung eine eigene Auffassung gebildet zu der Sicherheitslage öffentlicher Überwachungssysteme (insbesondere Videoüberwachung, Verkehrssteuerung und vergleichbare Systeme) in Deutschland im Hinblick auf mögliche langfristige Kompromittierungen durch externe Angreifer, und wenn ja, welche ist dies?

Im Rahmen der Betreuung von durch die Bundespolizei in eigener Zuständigkeit betriebene öffentliche Videoüberwachungssysteme wurde keine von der allgemeinen Sicherheitslage abweichende Auffassung gebildet. Es werden die Vorgaben und Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) entsprechend berücksichtigt und umgesetzt.

2. Welche Rolle spielen nach Kenntnis der Bundesregierung externe Dienstleister (einschließlich Cloud-Anbieter) bei dem Betrieb, der Speicherung und der Auswertung von Daten aus öffentlichen Überwachungs- und Sensorsystemen?

Für die durch die Bundespolizei in eigener Zuständigkeit betriebenen öffentlichen Videoüberwachungssysteme übernehmen teilweise externe Dienstleister Betriebs- und Speicherungsaufgaben.

3. Inwieweit sieht die Bundesregierung beim Einsatz Cloud-basierter Kommunikations- und Kollaborationsdienste aus Drittstaaten (z. B. Videokonferenzlösungen) in der öffentlichen Verwaltung ggf. Risiken für die digitale Souveränität sowie für den Schutz sensibler behördlicher Kommunikation, insbesondere im Hinblick auf mögliche Zugriffe ausländischer Behörden?

Die Bundesregierung sieht grundsätzlich Risiken durch unberechtigte Zugriffe beim Einsatz cloudbasierter Kommunikations- und Kollaborationsdiensten aus Drittstaaten.

Die Verantwortung für die Sicherheit beim Einsatz der genannten Dienste sowie für die Aspekte von digitaler Souveränität liegt bei den einsetzenden Behörden selbst und ist vom Anwendungsfall sowie den verarbeiteten bzw. transportierten Daten abhängig. Aus dem Blickwinkel der digitalen Souveränität kann ein Risiko bestehen, wenn aus der Nutzung ein sogenannter Vendor Lock-in-Effekt, die kritische Abhängigkeit zu einem einzelnen Anbieter, resultiert.

Das BSI stellt verschiedene Hilfsmittel zur Verfügung, um derartigen Risiken zu begegnen. So macht es etwa mit dem „Mindeststandard zu Nutzung externer Cloud-Dienste“ allgemeingültige Vorgaben, die eine nutzende Stelle beachten muss. Die nutzende Stelle kann aber auch zusätzliche Anforderungen stellen, auch zu Souveränitätsaspekten.

Mit den Criteria enabling Cloud Computing Autonomy (C3A) hat das BSI zudem einen Handlungsrahmen vorgelegt, der die Souveränitätseigenschaften von Cloud-Diensten transparent macht (siehe: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf?__blob=publicationFile).

Während die Sicherheitseigenschaften von Cloud-Diensten im Cloud Computing Compliance Criteria Catalogue (C5) des BSI adressiert werden, ermöglicht der Kriterienkatalog C3A eine Bewertung, ob ein Cloud-Angebot im jeweiligen Risikokontext selbstbestimmt genutzt werden kann.

4. Welche Erkenntnisse liegen der Bundesregierung ggf. über Schwachstellen oder bereits erfolgte Angriffe auf die in den vorherigen Fragen genannten Systeme in Deutschland vor?

Wie alle Produkte mit IT-Komponenten können Videoüberwachungs-, Verkehrssteuerungs- und vergleichbare Systeme Schwachstellen enthalten und angegriffen werden. Neben klassischen Schwachstellen in den Produkten selbst, können diese auch unsicher betrieben werden, etwa wenn Dienste und Funktionen unsicher exponiert werden. Neben technischen Schwachstellen ist zusätzlich der Faktor Mensch zu berücksichtigen. Dies umfasst sowohl das Abweichen von Vorgaben zur Handhabung eingesetzter Technik als auch den Zugang via Social Engineering.

Für die durch die Bundespolizei in eigener Zuständigkeit betriebenen öffentlichen Videoüberwachungssysteme liegen keine Erkenntnisse im Sinne der Anfrage vor.

5. In welchem Umfang werden öffentliche Überwachungs- und sicherheitsrelevante Systeme in Bund, Land und Kommunen nach Kenntnis der Bundesregierung zentral oder dezentral betrieben, und welche sicherheitstechnischen Unterschiede ergeben sich daraus nach Auffassung der Bundesregierung?

Zu der Frage, in welchem Umfang Systeme im Sinne der Fragestellung in Bund, Ländern und Kommunen zentral oder dezentral betrieben werden, liegen der Bundesregierung keine Informationen vor.

Die durch die Bundespolizei in eigener Zuständigkeit betriebenen öffentlichen Videoüberwachungssysteme werden teilweise zentral und teilweise dezentral betrieben. Die sicherheitstechnische Betrachtung erfolgt nach den einheitlichen Vorgaben des BSI. Die Einhaltung des IT-Grundschutzes ist für die Polizeien verpflichtend.

6. Welche Abstimmungen erfolgen ggf. zwischen Bund, Ländern und Kommunen zur Sicherstellung einheitlicher Sicherheitsstandards bei öffentlichen Überwachungs- und IT-Systemen?

Abstimmungen zwischen Bund, Ländern und Kommunen zur Sicherstellung einheitlicher Sicherheitsstandards erfolgen in den zuständigen Gremien (z. B. IT-Planungsrat), in denen auch das BSI vertreten ist.

Die Bundespolizei betreibt ihre Systeme in eigener Zuständigkeit.

7. Inwiefern sieht die Bundesregierung ggf. Risiken durch mögliche Zugriffe ausländischer Behörden auf in Deutschland genutzte IT- und Cloud-Infrastrukturen, insbesondere vor dem Hintergrund extraterritorial wirkender Rechtsvorschriften wie beispielsweise dem US-amerikanischen CLOUD Act?

Die Bundesregierung verfolgt mit der Strategie der digitalen Souveränität einen Ansatz, der Zugriffe ausländischer Behörden auf in Deutschland genutzte IT- und Cloud-Infrastrukturen, insbesondere vor dem Hintergrund extraterritorial wirkender Rechtsvorschriften, soweit wie möglich ausschließt. Mit den Criteria enabling Cloud Computing Autonomy (C3A) hat das BSI einen richtungsweisenden Handlungsrahmen vorgelegt, der die Souveränitätseigenschaften von Cloud-Diensten transparent macht (siehe: www.bsi.bund.de/SharedDocs/Down

loads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf?__blob=publicationFile).

Die C3A bieten beispielsweise Auswahloptionen bezüglich der Lokalisierung (z. B. Standort der Rechenzentren, Herkunft des Betriebspersonals). Je nach Kritikalität des Anwendungsfalls und Ergebnis der eigenen Risikoanalyse können Cloud-Nutzende entscheiden, ob sie eine Lokalisierung in Deutschland oder in der EU fordern.

8. In welchen Bereichen der Bundesverwaltung bestehen ggf. Abhängigkeiten von ausländischen Software- oder Cloud-Anbietern, und wie kritisch bewertet die Bundesregierung diese im Hinblick auf die Funktionsfähigkeit staatlicher IT-Systeme?

Die Bundesregierung geht davon aus, dass mit Frage 8 auf Überwachungssysteme im Sinne von Frage 1 Bezug genommen wird. Hierzu kann Folgendes mitgeteilt werden:

Für die durch die Bundespolizei in eigener Zuständigkeit betriebenen öffentlichen Videoüberwachungssysteme sind keine kritischen Abhängigkeiten bekannt.

9. Wie bewertet die Bundesregierung vor dem Hintergrund, dass im Zuge der durch die NSA-Affäre (NSA = National Security Agency) bekannt gewordenen Überwachungsprogramme auch maßgeblich Technologien und Komponenten von Anbietern eingesetzt wurden, die personelle Verbindungen zur israelischen Nachrichtendiensteinheit „Unit 8200“ aufweisen (vgl. u. a. Mondoweiss, 15. Juni 2013; Wired, 3. April 2012 sowie The Guardian, 11. September 2013 zum NSA-ISNU-Memorandum of Understanding [ISNU = Israeli SIGINT National Unit]: www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document, S. 1), das Risiko, dass bei der Nutzung der durch deutsche Sicherheitsbehörden eingesetzten Pegasus-Spyware, deren Entwicklerunternehmen ebenfalls ausgeprägte personelle Verflechtungen mit der „Unit 8200“ aufweist (www.972mag.com/nso-surveillance-companies-israel-army/), eine unbemerkte Datenabschöpfung, nachrichtendienstliche Nutzung oder gezielte Einflussnahme auf politische Entscheidungsträger, Journalisten oder andere relevante Personengruppen durch ausländische Stellen erfolgt oder erfolgen kann, auch vor dem Hintergrund zahlreicher international dokumentierter Einsatzfälle von Pegasus-Spyware gegen politische Entscheidungsträger, Journalisten und Aktivisten, darunter der saudi-arabische Journalist und Regimekritiker Jamal Khashoggi, der Menschenrechtsaktivist Ahmed Mansoor, der indische Oppositionspolitiker Rahul Gandhi sowie der Auswahl von Zielpersonen auf höchster politischer Ebene wie Emmanuel Macron (vgl. Pegasus Project, Forbidden Stories/Amnesty International 2021 sowie Citizen-Lab-Berichte: https://securitylab.amnesty.org/case-study-the-pegasus-project/), und wie rechtfertigt die Bundesregierung vor diesem Hintergrund, dass deutsche Sicherheitsbehörden Pegasus-Spyware einsetzen?

Die Bundesregierung geht aufgrund der im Fragetext enthaltenen Bezugsartikel bzw. -ausarbeitungen davon aus, dass sich der Fragegegenstand auf Aspekte des Einsatzes von Überwachungssoftware durch deutsche Sicherheitsbehörden bezieht. Nach sorgfältiger Prüfung unter Abwägung der im Staatswohl begründeten Geheimhaltungsinteressen der Bundesregierung mit dem parlamentarischen Informationsanspruch ist die Bundesregierung zu der Einschätzung gelangt, dass eine Beantwortung dieser Frage nicht erfolgen kann. Aus den im Rahmen einer Beantwortung der Frage erteilten Auskünften ließe sich ableiten,

ob oder ob nicht spezifische Überwachungssoftware durch Sicherheitsbehörden des Bundes eingesetzt werden kann. Einem öffentlichen Bekanntwerden dieser Informationen stehen überwiegende Belange des Staatswohls entgegen.

Mit den aus diesen Auskünften ableitbaren Informationen über gegebenenfalls zur Verfügung oder nicht zur Verfügung stehende kriminaltaktische bzw. nachrichtendienstliche Vorgehensweisen und damit zu konkreten Maßnahmen oder Ermittlungs-/Analysefähigkeiten würde die Bundesregierung polizeiliche bzw. nachrichtendienstliche Vorgehensweisen zur Gefahrenabwehr oder zur Verhinderung und Aufklärung von Straftaten offenlegen oder Rückschlüsse darauf ermöglichen und damit die Arbeitsfähigkeit und Aufgabenerfüllung der Sicherheitsbehörden bzw. Nachrichtendienste gefährden, weil Täter oder potentielle Zielpersonen ihr Verhalten anpassen und künftige Maßnahmen dadurch erschweren oder gar vereiteln könnten. Eine Preisgabe solcher sensiblen Informationen würde sich auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich wie auch auf die Durchsetzung des Strafverfolgungsanspruchs und die nachrichtendienstliche Informationsbeschaffung außerordentlich nachteilig auswirken.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung bzw. Ermittlungsunterstützung für die Aufgabenerfüllung der Sicherheitsbehörden bzw. Nachrichtendienste des Bundes nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Die angefragten Inhalte beschreiben die technischen Fähigkeiten der betroffenen Sicherheitsbehörden bzw. Nachrichtendienste des Bundes in einem durch den Bezug auf bestimmte Produkte derartigen Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Informationen wäre der Einsatzerfolg der betroffenen Ermittlungs- bzw. Aufklärungsinstrumente stark gefährdet, da Abwehrstrategien dagegen entwickelt werden könnten. Dies würde einen erheblichen Nachteil für die wirksame Aufgabenerfüllung der betroffenen Sicherheitsbehörden bzw. Nachrichtendienste des Bundes bedeuten, und es wäre kein Ersatz durch andere Instrumente möglich.

Daraus folgt, dass die erbetenen Informationen derartig schutzbedürftige evidente Geheimhaltungsinteressen berühren, dass auch das geringfügige Risiko eines Bekanntwerdens, wie es auch bei einer Übermittlung dieser Informationen an die Geheimschutzstelle des Deutschen Bundestags nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In der Abwägung des parlamentarischen Informationsrechts der Abgeordneten einerseits und der im Staatswohl begründeten Geheimhaltungsinteressen der Bundesregierung andererseits muss das parlamentarische Informationsrecht daher ausnahmsweise zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung o. g. Sachverhalts hinsichtlich einer Nutzungs- oder Nichtnutzungsmöglichkeit der in Bezug genommenen Software zu werten.

10. Welche konkreten technischen und organisatorischen Maßnahmen werden beim Einsatz ausländischer IT-Systeme, Cloud-Dienste, Kommunikationsinfrastrukturen sowie Überwachungstechnologien getroffen, um Zugriffe ausländischer staatlicher Stellen auf Daten oder Systeme der Bundesverwaltung auszuschließen, und wie rechtfertigt die Bundesregierung vor dem Hintergrund der in Frage 1 dargestellten Erkenntnisse den fortgesetzten Rückgriff auf Anbieter und Technologien aus genau denjenigen Staaten?

Die Bundesregierung ergreift umfassende Maßnahmen, um Zugriffe ausländischer staatlicher Stellen auf Daten oder Systeme der Bundesverwaltung auszuschließen. Die konkreten technischen und organisatorischen Maßnahmen bei der Nutzung der genannten Systeme finden sich in den Vorgaben des BSI, insbesondere in den einschlägigen IT-Grundschutz-Bausteinen. Zudem unterstützen die in der Antwort zu Frage 3 genannten BSI-Standards.

Das Programm P20 priorisiert Open-Source und souveräne, europäische Lösungen, um die Abhängigkeit von ausländischen Anbietern zu minimieren und die Datensicherheit zu erhöhen. Durch die Förderung von Open-Source-Lösungen und die Auswahl von Anbietern, die strenge Sicherheits- und Datenschutzstandards erfüllen, wird die Sicherheit der Daten und Systeme der Bundesverwaltung gewährleistet. Diese Strategie stärkt die technologische Souveränität und Unabhängigkeit der EU und minimiert die Risiken im Zusammenhang mit dem Einsatz ausländischer Technologien.

Im Übrigen wird auf die Antwort zu Frage 11 verwiesen.

11. Welche konkreten technischen und organisatorischen Schutzmaßnahmen werden getroffen, um Endgeräte von Mitgliedern der Bundesregierung gegen derartige, in Frage 1 dargestellte Überwachungs- und Ausspähmaßnahmen zu schützen, über welche forensischen Fähigkeiten verfügt die Bundesregierung, um entsprechende Kompromittierungen festzustellen, und in welchen regelmäßigen Abständen werden entsprechende Prüfungen durchgeführt?

Die Fragen können aus Gründen des Staatswohls nicht- auch nicht eingestuft – abschließend beantwortet werden. Ein Bekanntwerden der konkreten technischen und organisatorischen Schutzmaßnahmen, um gegen die in Frage 1 dargestellten Überwachungs- und Ausspähmaßnahmen zu schützen, würde ein schwerwiegendes Sicherheitsrisiko für die gesamte Bundesregierung darstellen. Eine Offenlegung der angefragten Informationen zu technischen und organisatorischen Schutzmaßnahmen birgt die Gefahr, dass diese von Dritten zu einer Umgehung der Schutzmaßnahmen und in der Folge zu einer Kompromittierung der von der Bundesregierung eingesetzten Systeme genutzt werden.

Der konkrete technische Schutz der eingesetzten IT-Systeme, Cloud-Dienste, Kommunikationsinfrastruktur, einschließlich der Endgeräte der Mitglieder der Bundesregierung, ist für das Staatswohl von überragender Bedeutung.

Selbst die Bekanntgabe der erbetenen Informationen unter Wahrung des Geheimschutzes durch Übermittlung an die Geheimschutzstelle des Deutschen Bundestages birgt das geringfügige Risiko des Bekanntwerdens, das unter keinen Umständen hingenommen werden kann. Ein Bekanntwerden von Information von konkreten technischen und organisatorischen Schutzmaßnahmen bergen ein hoch problematisches Angriffsszenario. Das Bekanntwerden von Einzelheiten zu sensiblen Informationen wäre ein schwerwiegendes Sicherheitsrisiko für die gesamte Bundesregierung. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, aufgrund derer das Staatswohl gegenüber dem parlamentarischen In-

formationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

12. Welche technischen Stellen haben die eingesetzte Pegasus-Spyware daraufhin validiert, ob wirksame Mechanismen zur Verhinderung missbräuchlicher Nutzung implementiert sind, und über welche konkret nachprüfbaren technischen Garantien wird sichergestellt, dass erhobene Daten ausschließlich unter Kontrolle deutscher Behörden verbleiben und nicht an Hersteller oder sonstige Dritte im Ausland übermittelt werden können?

Auf die Antwort zu Frage 9 wird verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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.bundesanzeiger-verlag.de
ISSN 0722-8333