Deutscher Bundestag **Drucksache 21/5573**

21. Wahlperiode 23.04.2026

Kleine Anfrage

der Abgeordneten Sascha Lensing, Dr. Gottfried Curio, Dr. Christian Wirth, Dr. Bernd Baumann, Christopher Drößler, Jochen Haug, Martin Hess, Steffen Janich, Markus Matzerath, Arne Raue und der Fraktion der AfD

Sicherheitsrisiken staatlicher Überwachungssysteme und cloudbasierter IT-Lösungen

Nach übereinstimmenden Medienberichten sollen ausländische Nachrichtendienste in 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 cloudbasierte 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 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 cloudbasierter Lösungen unterstreicht.

Wir fragen die Bundesregierung:

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 Angreifern und wenn ja, welche ist dies?

2. Welche Rolle spielen nach Kenntnis der Bundesregierung externe Dienstleister (einschließlich Cloud-Anbieter) beim Betrieb, der Speicherung und der Auswertung von Daten aus öffentlichen Überwachungs- und Sensorsystemen?
3. Inwieweit sieht die Bundesregierung beim Einsatz cloudbasierter Kommunikations- und Kollaborationsdiensten 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?
4. Welche Erkenntnisse liegen der Bundesregierung ggf. über Schwachstellen oder bereits erfolgte Angriffe auf die in den vorherigen Fragen genannten Systemen in Deutschland 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?
6. Welche Abstimmungen erfolgen ggf. zwischen Bund, Ländern und Kommunen zur Sicherstellung einheitlicher Sicherheitsstandards bei öffentlichen Überwachungs- und IT-Systemen?
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?
8. In welchen Bereichen der Bundesverwaltung bestehen ggf. Abhängigkeiten von ausländischen Software- oder Cloudanbietern, und wie kritisch bewertet die Bundesregierung diese im Hinblick auf die Funktionsfähigkeit staatlicher IT-Systeme?
9. Wie bewertet die Bundesregierung vor dem Hintergrund, dass im Zuge der durch die NSA-Affäre 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: 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, dem Menschenrechtsaktivisten Ahmed Mansoor, dem indischen 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://se

curitylab.amnesty.org/case-study-the-pegasus-project/), und wie rechtfertigt die Bundesregierung vor diesem Hintergrund, dass deutsche Sicherheitsbehörden Pegasus Spyware einsetzen?

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?

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?

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?

Berlin, den 22. April 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

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