Deutscher Bundestag **Drucksache 21/7707**

21. Wahlperiode 25.08.2026

Kleine Anfrage

der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Dr. Michael Kaufmann, Micha Fehre, Beatrix von Storch, Ronald Gläser, Peter Bohnhof, Thomas Ladzinski, Sascha Lensing und der Fraktion der AfD

Digitale Resilienz unter Beschuss – Aufklärung der Cyberangriffe von Russland gegen Deutschland

Die Sicherheit der Informationstechnik und der Schutz kritischer Infrastrukturen bilden das Rückgrat eines funktionsfähigen Staates und sind elementare Voraussetzungen für die digitale Souveränität Deutschlands. In einer zunehmend vernetzten Welt sind staatliche Stellen, Energieversorger, Verkehrsunternehmen und Gesundheitseinrichtungen wachsenden Bedrohungen durch hochprofessionelle Cyberakteure ausgesetzt. Die Resilienz dieser Systeme gegenüber Sabotage und Spionage ist daher nicht nur eine technologische Herausforderung, sondern eine Kernfrage der nationalen Sicherheit.

Anlass der vorliegenden Kleinen Anfrage sind die schwerwiegenden Cyberangriffe auf staatliche Stellen und kritischen Infrastrukturen in Deutschland, die am 13. Juli 2026 öffentlich bekannt wurden. Nach Angaben der Bundesregierung und internationaler Partner wurden dabei gezielte Sabotageakte gegen lebensnotwendige Versorgungsstrukturen verübt und eine Kompromittierung gesicherter Regierungsnetzwerke vollzogen (www.tagesschau.de/ausland/cyberangriffe-russland-sanktionen-botschafter-100.html). Die Bundesregierung machte für diesen Angriff russische Geheimdienste verantwortlich und zog mit der Einbestellung des russischen Botschafters sowie der Ankündigung weiterer Sanktionen diplomatische Konsequenzen (www.consilium.europa.eu/de/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystemtargeting-the-eu-its-member-states-and-international-partners/pdf/).

Diese aktuelle Angriffswelle verdeutlicht erneut die Verwundbarkeit der staatlichen IT-Landschaft und die strategische Bedeutung einer modernen Cyberabwehr. Die offizielle Zurechnung dieser Angriffe zu staatlich gesteuerten Akteuren unterstreicht das Ausmaß der Bedrohung für kritische Infrastrukturen und Regierungsnetzwerke (www.tagesschau.de/ausland/cyberangriffe-russland-sanktionen-botschafter-100.html). Dies wirft dringende Fragen nach dem Stand der IT-Sicherheit in der Bundesverwaltung, der Wirksamkeit der Früherkennungssysteme des Bundesamtes für Sicherheit in der Informationstechnik sowie der allgemeinen Krisenfestigkeit der deutschen Digitalinfrastruktur auf.

Trotz zahlreicher Ankündigungen zur Stärkung der Cybersicherheit im Rahmen der Staatsmodernisierung offenbaren Vorfälle dieser Größenordnung regelmäßig strukturelle Defizite in der behördlichen Sicherheitsarchitektur. Es ist für die parlamentarische Kontrolle von entscheidender Bedeutung, zu erfahren, welche konkreten Behörden und Infrastrukturbereiche betroffen waren, welcher

Schaden entstanden ist und inwieweit die bestehenden Schutzkonzepte des Bundes den aktuellen Bedrohungslagen noch gewachsen sind.

Wir fragen die Bundesregierung:

1. Welche Erkenntnisse liegen der Bundesregierung zum Umfang, zur Zielsetzung und zur Schwere der Cyberangriffe vom Juli 2026 vor?
2. Wann und auf welchem Weg wurde die Bundesregierung erstmals über die Angriffe informiert?
3. Welche konkreten Bundesbehörden, Regierungsnetzwerke oder Einrichtungen der kritischen Infrastruktur waren von den Angriffen direkt betroffen?
4. Welche Ziele verfolgten die Angreifer nach Einschätzung der Bundesregierung primär: Spionage, Sabotage oder die Vorbereitung künftiger Angriffe?
5. Wurden bei den Angriffen nach Kenntnis der Bundesregierung sensible Daten abgezogen oder wurden in die Infrastruktur Schadfunktionen eingeschleust, um künftige Sabotageakte zu ermöglichen?
6. Welche Rolle spielte das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der Identifikation und Abwehr dieser Angriffe, ab welchem Zeitpunkt wurde die Behörde tätig, und wie bewertet die Bundesregierung rückblickend die Leistungsfähigkeit der eingesetzten Früherkennungssysteme?
7. Inwieweit waren die betroffenen IT-Systeme der Bundesverwaltung zum Zeitpunkt des Angriffs auf dem aktuellen Stand der Sicherheitsupdates, und welche Rolle spielten sogenannte Legacy-Systeme bei der Infiltration?
8. Welche Rolle spielten nach Kenntnis der Bundesregierung beim Erstzugriff externe IT-Dienstleister, Cloud-Lösungen oder Wartungszugänge, die die internen Sicherheitsmechanismen der Bundesverwaltung möglicherweise umgangen haben?
9. Inwieweit verfügt die Bundesregierung über ein zentrales, echtzeitfähiges digitales Lagebild der IT-Sicherheit aller Bundesressorts, und wie wird der Informationsfluss zwischen dem BSI und den IT-Sicherheitsbeauftragten der Bundesministerien technisch koordiniert?
10. Welchen Stellenwert nimmt das Sicherheitskonzept „Zero Trust“ bei der Absicherung der Regierungsnetzwerke ein, und inwieweit hat dies bei den betroffenen Systemen bereits Anwendung gefunden?
11. Welche Konsequenzen zieht die Bundesregierung aus den Vorfällen für die IT-Architektur des Bundes, insbesondere hinsichtlich Netztrennung sowie Härtung der digitalen Infrastruktur, und welche Maßnahmen sind bis zum Jahr 2030 geplant?
12. Inwieweit plant die Bundesregierung eine Aufwertung des BSI zu einer stärkeren operativen Zentralstelle, um die IT-Sicherheit in allen Bundesressorts nach einheitlichen und verbindlichen Standards durchzusetzen?
13. Welche Auswirkungen haben diese Angriffe auf die aktuelle Budgetplanung für IT-Sicherheit und den notwendigen Personalaufbau in den Cyberabwehrzentren des Bundes?
14. Welche Abhängigkeiten von ausländischer Hard- oder Software haben nach Einschätzung der Bundesregierung zur Anfälligkeit der angegriffenen Systeme beigetragen?

15. Wie bewertet die Bundesregierung die Resilienz der deutschen Energie- und Kommunikationsnetze gegenüber den nun bekannt gewordenen Angriffs- und Sabotagemethoden?
16. Erfolgte die Kommunikation über die Angriffe an die betroffenen KRITIS (Kritische Infrastrukturen)-Betreiber rechtzeitig, und gibt es Hürden beim Austausch von Angriffssignaturen zwischen Staat und Privatwirtschaft?
17. Wie bewertet die Bundesregierung das Risiko durch KI-gestützte, automatisierte Schwachstellensuche durch staatliche Akteure, und welche eigenen KI-Verteidigungssysteme werden derzeit entwickelt?
18. Inwieweit führt die Bundesregierung eine Intensivierung der Zusammenarbeit mit europäischen Partnern durch, um eine gemeinsame, proaktive Cyberabwehr gegen russische Hackergruppen aufzubauen?
19. Welche Lehren zieht die Bundesregierung für die digitale Souveränität Deutschlands, um die Angriffsfläche für fremde Geheimdienste systematisch zu verringern?

Berlin, den 24. August 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