Deutscher Bundestag **Drucksache 21/7929**

21. Wahlperiode 08.09.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/7707 –

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

Vorbemerkung der Fragesteller

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.

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

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

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.

Vorbemerkung der Bundesregierung

Die Bundesregierung weist darauf hin, dass die von der Fraktion der AfD zitierte Attribuierung vom 13. Juli 2026 durch die Hohe Vertreterin der Europäischen Union (EU) im Rahmen einer gemeinsamen Attribuierung der EU und ihrer Mitgliedstaaten vorgenommen wurde. Die zitierten Cyberangriffe betreffen eine Vielzahl von EU-Mitgliedstaaten, die in unterschiedlicher Weise von den Angriffen betroffen waren. Zu den Zielen zählten Regierungsinstitutionen und kritische Infrastrukturen. In diesem Zusammenhang wurde der russische Botschafter in das Auswärtige Amt einbestellt. Der Wortlaut der Erklärung der Hohen Vertreterin ist abrufbar unter: www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/

Nach sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass die erbetenen Informationen zu den Fragen 1 bis 5, 7, 8 und 14 nicht – auch nicht in eingestufter Form – zur Verfügung gestellt werden können. Die erbetenen Informationen zielen auf den nachrichtendienstlichen Kenntnisstand der Nachrichtendienste des Bundes und können Rückschlüsse auf Einsatzbereitschaft, Arbeitsschwerpunkte, die Erkenntnislage und die konkrete Ausgestaltung der nachrichtendienstlichen Vorfallbearbeitung einschließlich etwaiger Aufklärungsfähigkeiten ermöglichen. Hierdurch können fremde Nachrichtendienste zu einer Einschätzung der Kapazitäten der Cyberspionageabwehr und ihren operativen Möglichkeiten gelangen. Eine Preisgabe der Informationen könnte somit schwere Nachteile für die Arbeitsfähigkeit und Aufgabenerfüllung der Nachrichtendienste des Bundes mit sich bringen. Unbefugte Dritte könnten daran ihre eigenen Maßnahmen zum Nachteil der Bundesrepublik Deutschland ausrichten. Daraus können erhebliche negative Folgewirkungen für die Sicherheitslage in der Bundesrepublik Deutschland entstehen.

Selbst eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde im vorliegenden Fall nicht ausreichen, um ihrer besonderen Sensibilität im Hinblick auf die Bedeutung der nachrichtendienstlichen Aufklärung und Abwehr von Cyberspionage und -sabotage für die Aufgabenerfüllung der Nachrichtendienste des Bundes sowie der Sicherheit der Bundesrepublik Deutschland ausreichend Rechnung zu tragen. Ein Bekanntwerden der Informationen würde diesen die weitere Aufklärung geheimdienstlicher Aktivitäten in und gegen die Bundesrepublik Deutschland erheblich erschweren. Das Risiko, dass derart sensible Informationen bekannt werden, kann unter keinen Umständen hingenommen werden, da eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern dem dargelegten Schutzbedürfnis nicht Rechnung tragen würde. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

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?

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?

14. Welche Abhängigkeiten von ausländischer Hard- oder Software haben nach Einschätzung der Bundesregierung zur Anfälligkeit der angegriffenen Systeme beigetragen?

Die Fragen 1 bis 5, 7, 8 und 14 werden gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Die Sensorik und Signaturen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden laufend an neue Angriffsmuster angepasst. Bei Meldungen, die über die Meldestellen eingehen, erfolgt die Unterstützung des BSI auf Bitten der und nach Absprache mit der betroffenen Institution.

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?

Das BSI erzeugt kontinuierlich ein Lagebild für die Bundesregierung, entwickelt die daraus abgeleiteten und verteilten Lageprodukte zudem stetig weiter und passt diese an die sich ändernden Bedürfnisse der Empfänger (z. B. IT-Sicherheitsbeauftragte der Bundesministerien) und Rahmenbedingungen an.

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?

Grundsätzlich sind Zero-Trust-Ansätze ein nützliches Mittel zur Absicherung von Netzen und werden ergänzend zu vielen anderen mitigierenden Maßnahmen in den Regierungsnetzen eingesetzt.

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?

Netztrennung ist ein Kernelement der Absicherung in aktuellen Regierungsnetzen. Die Bundesregierung setzt sich dafür ein, zeitgemäße Maßnahmen nach Stand der Technik zur Netztrennung und Härtung der eingesetzten Systeme in den aktuellen und zukünftigen Regierungsnetzen zu realisieren. Bis 2030 soll in dem neu geplanten Netz der Bundesregierung Zero Trust, wo möglich, verstärkt implementiert werden.

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?

Zur Stärkung der Cybersicherheit in der Bundesverwaltung wurde mit Beschluss des NIS2-Umsetzungsgesetzes die Rolle des Koordinators für Informationssicherheit (Chief Information Security Officer des Bundes (CISO Bund), ausgeübt durch die Präsidentin des BSI) eingeführt und eine neue Governance-Struktur für die Informationssicherheit des Bundes festgelegt. Das Programm CyberGovSecure wurde in diesem Jahr als ressortübergreifendes Programm konzipiert, das zentral durch die CISO Bund unter Einbeziehung der Ressorts gesteuert wird. Dieses Programm ist ein Beitrag für den Schutz und die digitale Wehrhaftigkeit Deutschlands und stellt eine gemeinsame prioritäre Aufgabe aller Ressorts dar.

13. Welche Auswirkungen haben diese Angriffe auf die aktuelle Budgetplanung für IT-Sicherheit und den notwendigen Personalaufbau in den Cyberabwehrzentren des Bundes?

Die Ausgabenplanung für IT-Sicherheit berücksichtigt immer die aktuelle Sicherheitslage und wird bei Bedarf entsprechend angepasst. Gleiches gilt für die Personalausstattung z. B. des Nationalen Cyber-Abwehrzentrums. In diesem Zusammenhang wird auf den Auftrag aus dem Koalitionsvertrag (Z. 2679f) verwiesen: „Das Nationale Cyber-Abwehrzentrum entwickeln wir fort und intensivieren den Informationsaustausch.

15. Wie bewertet die Bundesregierung die Resilienz der deutschen Energie- und Kommunikationsnetze gegenüber den nun bekannt gewordenen Angriffs- und Sabotagemethoden?

Grundsätzlich ist von Betreibern Kritischer Infrastrukturen gemäß dem BSI-Gesetz (BSIG) eine geeignete Absicherung umzusetzen, durch die die Erfolgswahrscheinlichkeit derartiger Angriffe reduziert wird. In Bezug auf Energie-

netze sowie Telekommunikationsnetze gibt es langjährig Anforderungen im Energiewirtschaftsgesetz (EnWG) sowie im Telekommunikationsgesetz (TKG).

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?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert die Betreiber Kritischer Infrastrukturen rechtzeitig über seine Lageprodukte. Das BSI macht zudem Informationen geschlossenen Nutzerkreisen (wie Bundesbehörden und KRITIS-Betreibern) zugänglich. In der UP-KRITIS erfolgt ein regelmäßiger Austausch zwischen BSI und KRITIS-Betreibern zur Bedrohungslage. Dieser kooperative Ansatz vermeidet die Entstehung von möglichen Hürden.

17. Wie bewertet die Bundesregierung das Risiko durch KI-gestützte, automatisierte Schwachstellensuche durch staatliche Akteure, und welche eigenen KI-Verteidigungssysteme werden derzeit entwickelt?

Die Bundesregierung bewertet das Risiko durch KI-gestützte und automatisierte Schwachstellensuche durch staatliche Akteure als hoch und dynamisch ansteigend. Um diesen Bedrohungen wirksam zu begegnen, entwickeln u. a. das BSI und die Cyberagentur geeignete Abwehrsysteme. Bei allen genannten Entwicklungen wird strikt darauf geachtet, dass die menschliche Kontrolle gewahrt bleibt, was durch die Implementierung des sogenannten Human-in-the-Loop-Prinzips sichergestellt wird.

18. Inwieweit führt die Bundesregierung eine Intensivierung der Zusammenarbeit mit europäischen Partnern durch, um eine gemeinsame, proaktive Cyberabwehr gegen russische Hackergruppen aufzubauen?

Die Bundesregierung pflegt bereits eine vertrauensvolle und intensive Zusammenarbeit mit europäischen und internationalen Partnern, um im bestehenden gesetzlichen Rahmen gegen Cyberangriffe vorzugehen. Der von der Bundesregierung Ende Mai 2026 verabschiedete Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (Bundestagsdrucksache 21/6585) sieht zusätzliche Befugnisse zur verbesserten Prävention, Detektion und Reaktion auf Cyberangriffe vor.

19. Welche Lehren zieht die Bundesregierung für die digitale Souveränität Deutschlands, um die Angriffsfläche für fremde Geheimdienste systematisch zu verringern?

Die Bundesregierung verfolgt ein Bündel an Maßnahmen, mit dem klaren Ziel: mehr Eigenständigkeit und Sicherheit durch europäische Kooperation, durch Investitionen in Schlüsseltechnologien und eine Stärkung der europäischen Digitalindustrie sowie durch Absicherung außereuropäischer Produkte mit Hilfe technischer Kontrollschichten.

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