Deutscher Bundestag **Drucksache 21/9092**

21. Wahlperiode 11.11.2026

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Robin Jünger, Ruben Rupp, 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

Erkenntnisstand des Bundes zu privilegierten Zugängen beim Cyberangriff auf die Berliner Landesverwaltung

Im August 2026 wurden informationstechnische Systeme der Berliner Landesverwaltung Ziel eines schwerwiegenden Cyberangriffs. Betroffen waren insbesondere zwei Senatsverwaltungen. Nach den öffentlich bekannt gewordenen Angaben wurden umfangreiche Datenbestände aus den betroffenen Systemen kopiert und später veröffentlicht. Die Aufarbeitung des Vorfalls umfasst sowohl die technische Rekonstruktion des Angriffs als auch die Bewertung der abgeflossenen Daten und möglicher Sicherheitsfolgen (www.berlin.de/cyberangriff/informationen-fuer-buergerinnen-und-buerger/ und www.berlin.de/rbmskzl/aktuelles/pressemitteilungen/2026/pressemitteilung.1707289.php).

Die Bundesregierung hat am 7. September 2026 erklärt, dass neben den zuständigen Sicherheitsbehörden des Landes Berlin insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt und das Bundesamt für Verfassungsschutz die Aufarbeitung unterstützen. Die beim Bund und beim Land gewonnenen Erkenntnisse würden unter anderem im Nationalen Cyber-Abwehrzentrum zusammengeführt. Zugleich erklärte das Bundesministerium des Innern, die Gruppierung Rhysida werde grundsätzlich als kriminell und finanziell motiviert eingeschätzt (www.bundesregierung.de/breg-de/aktuelles/regierungspressekonferenz-vom-7-september-2026-2451640).

In ihrer Antwort auf eine schriftliche Einzelfrage teilte die Bundesregierung am 10. September 2026 ergänzend mit, das BSI, das Bundeskriminalamt und das Bundesamt für Verfassungsschutz unterstützten die ermittlungsführenden Behörden in beratender Funktion. Dabei würden auch Sicherheitsinteressen des Bundes berücksichtigt. Die Prüfung einer möglichen Betroffenheit solcher Interessen dauerte zu diesem Zeitpunkt noch an (Antwort auf Frage 29 – https://dserver.bundestag.de/btd/21/079/2107980.pdf),

Für die Fragesteller ist bei der weiteren Aufklärung insbesondere die technische Fragestellung von Bedeutung, auf welche Weise die Angreifer nach einem erfolgreichen Zugang Zugriff auf weitere Systeme und Datenbestände erlangen konnten. Nach einem initialen Eindringen kann sich ein Angreifer innerhalb einer Infrastruktur unter anderem durch die Verwendung kompromittierter Zugangsdaten, die technische Ausweitung von Berechtigungen oder die Nutzung bereits bestehender privilegierter Konten zwischen weiteren Systemen bewegen. Von besonderer Sicherheitsrelevanz wäre dabei ein Zugriff auf zentrale Verzeichnisdienste, Administrationssysteme, Virtualisierungsmanagementsyste-

me oder Hypervisoren, über die mehrere virtuelle IT-Systeme gesteuert werden können.

Ein solcher privilegierter Zugriff erlaubt für sich genommen keinen belastbaren Schluss auf einen bestimmten Täterkreis oder auf eine interne Mitwirkung. Denkbar sind unterschiedliche technische Ursachen, darunter der Diebstahl legitimer Administrationszugangsdaten, eine technische Rechteausweitung nach dem initialen Eindringen, die Ausnutzung einer Schwachstelle, eine Fehlkonfiguration oder der Missbrauch bereits bestehender Zugriffsrechte durch eine zuvor berechtigte Person. Das BSI berücksichtigt die Gefährdung durch Personen mit autorisiertem Zugang in seinen Sicherheitskonzepten grundsätzlich als eigenes Bedrohungsszenario. Zugleich sollen privilegierte Rechte auf den erforderlichen Umfang begrenzt werden (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=6).

Wir fragen die Bundesregierung:

1. Welche eigenen technischen Erkenntnisse liegen der Bundesregierung, insbesondere dem BSI, dazu vor, ob die Angreifer beim Cyberangriff auf Teile der Berliner Landesverwaltung für die Bewegung zwischen unterschiedlichen Informationssystemen oder für den Zugriff auf weitere Datenbestände Benutzer-, Administrations-, Service- oder sonstige privilegierte Konten verwendeten, die bereits vor Beginn des Angriffs regulär eingerichtet und mit entsprechenden Berechtigungen versehen waren?
2. Welche eigenen technischen Erkenntnisse liegen der Bundesregierung beziehungsweise dem BSI dazu vor, ob die Angreifer Zugriff auf zentrale Verzeichnisdienste, Administrationssysteme, zentrale Virtualisierungsmanagementsysteme, über die mehrere virtuelle Server gesteuert werden, Hypervisoren oder Backup-Infrastrukturen erlangten, und welche dieser Zugriffskategorien sind nach dem bisherigen technischen Erkenntnisstand bestätigt, nicht bestätigt oder noch nicht abschließend bewertbar?
3. Welchen jeweiligen technischen Erkenntnisstand haben die beteiligten Bundesbehörden hinsichtlich der möglichen Erklärungen, dass weitreichende Berechtigungen durch
   a) eine technische Schwachstelle oder Fehlkonfiguration,
   b) den Diebstahl beziehungsweise die Kompromittierung bereits vorhandener Zugangsdaten,
   c) eine nach dem initialen Eindringen erfolgte technische Rechteausweitung oder
   d) die missbräuchliche Nutzung von bereits zuvor bestehenden berechtigten Zugriffsrechten erlangt wurden, und welche dieser Möglichkeiten konnten aufgrund bereits vorliegender eigener technischer Erkenntnisse bestätigt, ausgeschlossen oder bislang weder bestätigt noch ausgeschlossen werden?
4. Hat das BSI in den ihm im Rahmen seiner Unterstützung zugänglich gewordenen technischen oder forensischen Informationen Anhaltspunkte dafür festgestellt, dass eine bereits vor Beginn des Cyberangriffs zum Zugriff berechtigte natürliche Person den unbefugten Zugriff vorsätzlich oder fahrlässig ermöglicht oder erleichtert haben könnte, und falls bislang keine entsprechenden Anhaltspunkte festgestellt wurden, beruht dies nach Kenntnis der Bundesregierung auf einer insoweit abgeschlossenen technischen Prüfung oder ist dieser Aspekt der technischen Analyse noch offen?

Vorabfassung - wird durch die lektorierte Version ersetzt.

5. Welche konkreten zusätzlichen technischen oder organisatorischen Schutzmaßnahmen für die Bundesverwaltung hat das BSI aufgrund bereits gewonnener Erkenntnisse aus dem Berliner Cyberangriff empfohlen, veranlasst oder in bestehende Sicherheitsvorgaben einbezogen, insbesondere hinsichtlich der Trennung von Administrations- und Produktivumgebungen, des Schutzes privilegierter Konten, der Mehrfaktorauthentisierung, der Überwachung atypischer Administrationshandlungen sowie der Absicherung von Virtualisierungs- und Hypervisor-Managementsystemen?
6. Hat das BSI aufgrund der beim Berliner Cyberangriff gewonnenen technischen Erkenntnisse Bundesbehörden oder zentrale IT-Dienstleister des Bundes veranlasst, eigene Informationssysteme gezielt auf vergleichbare Angriffsmuster, kompromittierte privilegierte Konten, ungewöhnliche administrative Zugriffe oder vergleichbare Bewegungen zwischen Systemen zu überprüfen, und welche aggregierten Ergebnisse dieser Überprüfungen liegen der Bundesregierung vor, soweit deren Mitteilung ohne Offenlegung operativ nutzbarer Sicherheitsdetails möglich ist?

Berlin, den [

Dr. Alice Weidel, Tino Chrupalla und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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