LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/21401**

15.09.2026

Kleine Anfrage 8781

des Abgeordneten Marcel Hafke FDP

Hackerangriff auf Berliner Verwaltung – Sind auch sicherheitsrelevante Daten aus Nordrhein-Westfalen im Darknet gelandet?

Zwischen dem 7. und 12. August 2026 haben mutmaßlich Cyberkriminelle umfangreiche Datenbestände aus Teilen der Berliner Verwaltung entwendet. Nach Angaben der Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden bei dem Angriff Daten in erheblichem Umfang kopiert und anschließend öffentlich zugänglich gemacht. Betroffen sind insbesondere Bereiche der Berliner Senatsverwaltungen für Stadtentwicklung, Bauen und Wohnen sowie für Mobilität, Verkehr, Klimaschutz und Umwelt. Aufgrund des Umfangs der abgeflossenen Daten dauert deren vollständige Auswertung weiterhin an.

Medienberichten[1] zufolge handelt es sich um rund 1,4 Millionen Dateien mit einem Datenvolumen von mehreren Terabyte. Besondere sicherheitspolitische Bedeutung erhält der Vorfall dadurch, dass sich unter den veröffentlichten Dateien offenbar auch umfangreiche Informationen über kritische Infrastrukturen befinden. Berichtet wird unter anderem über Daten zu Heizkraftwerken, Tanklagern, Notstromanlagen, Umspannwerken, Wasserwerken, Gefängnissen und Rüstungsunternehmen sowie über Gebäude- und Sicherheitsplanungen.

Der „Tagesspiegel“ berichtete am 5. September 2026[2] darüber hinaus unter Berufung auf den Vorsitzenden der Linksfraktion im Berliner Abgeordnetenhaus, Tobias Schulze, dass sich unter den veröffentlichten Informationen auch Pläne kritischer Infrastruktur samt Kriseneinsatzplänen anderer Bundesländer befinden sollen. Welche Länder hiervon betroffen sind, ist bislang öffentlich nicht abschließend bekannt.

Der Vorgang hat damit möglicherweise Auswirkungen weit über das Land Berlin hinaus. Informationen über Aufbau, Sicherheitsvorkehrungen oder Schwachstellen kritischer Infrastrukturen sowie über staatliche Reaktionsplanungen können nach ihrer Veröffentlichung dauerhaft für kriminelle, extremistische oder nachrichtendienstliche Akteure verfügbar sein. Das Bundesamt für Sicherheit in der Informationstechnik weist im Zusammenhang mit dem Berliner Vorfall darauf hin, dass Informationen zu kritischen Infrastrukturen, Unternehmen und Organisationen eine Erhöhung der Bedrohungslage bewirken können. Die Berliner Behörden

[1] Vgl. etwa: „Welche Gefahren drohen durch die Datenveröffentlichung“, Tagesschau vom 05.09.2026, abrufbar unter: https://www.tagesschau.de/inland/faq-hackerangriff-berlin-folgen-100.html (letzter Abruf: 15.09.2026).
[2] Latz, Christian, Pohl, Dennis und Sturm Daniel Friedrich, „Bundesregierung vermutet Zusammenhang mit Berlin-Wahl“, in: Tagesspiegel vom 05.09.2026, abrufbar unter: https://www.tagesspiegel.de/berlin/berliner-hackerangriff-beschaftigt-jetzt-auch-die-bundeswehr-fuhrung-linken-politiker-sieht-schwersten-it-sicherheitsfall-in-der-geschichte-der-bundesrepublik-16021348.html (letzter Abruf: 15.09.2026).

Datum des Originals: 15.09.2026/Ausgegeben: 21.09.2026

haben angekündigt, sicherheitskritische Behörden und Einrichtungen bei entsprechenden Erkenntnissen unverzüglich zu kontaktieren.

Der Vorfall wirft daher auch für Nordrhein-Westfalen die Frage auf, ob sich Daten nordrhein-westfälischer Behörden, Einrichtungen oder Betreiber kritischer Infrastrukturen unter den veröffentlichten Beständen befinden. Darüber hinaus stellt sich unabhängig von einer konkreten Betroffenheit die Frage, wie das Land mit der dauerhaften Kompromittierung sicherheitsrelevanter Informationen umgeht. Ein einmal veröffentlichter Krisenplan, Gebäudeplan oder eine bekannt gewordene Schwachstelle kann nicht durch eine bloße technische Bereinigung des angegriffenen IT-Systems wieder geheim gemacht werden. Vielmehr kann eine Neubewertung der Gefährdungslage sowie gegebenenfalls eine Anpassung von Schutzmaßnahmen, Planungen und Verfahren erforderlich werden.

Mit dem zum Jahresbeginn in Kraft getretenen Informationssicherheitsgesetz Nordrhein-Westfalen wurden die Anforderungen an die Informationssicherheit der Landesverwaltung neu geregelt. Daneben bestehen insbesondere für Verschlusssachen besondere Vorgaben des Geheimschutzes. Der Berliner Vorfall wirft die Frage auf, ob diese Regelungen auch dem Risiko Rechnung tragen, dass sicherheitsrelevante Informationen Nordrhein-Westfalens nicht aus nordrhein-westfälischen Systemen selbst, sondern bei Behörden anderer Länder, des Bundes oder sonstigen Stellen abfließen, denen diese zuvor im Rahmen notwendiger Zusammenarbeit übermittelt wurden.

Vor diesem Hintergrund frage ich die Landesregierung:

1. Welche Erkenntnisse liegen der Landesregierung über nordrhein-westfälische Daten, Dokumente oder Informationen vor, die im Zuge des Cyberangriffs auf die Berliner Verwaltung abgeflossen oder veröffentlicht worden sind?

2. Welche Maßnahmen hat die Landesregierung seit Bekanntwerden der Veröffentlichung ergriffen, um eine mögliche Betroffenheit nordrhein-westfälischer Behörden, kritischer Infrastrukturen sowie von Sicherheits-, Krisen- oder Einsatzplanungen festzustellen?

3. Nach welchen Verfahren bewertet und behandelt die Landesregierung Fälle, in denen Informationen über kritische Infrastrukturen, bestehende Schwachstellen oder staatliche Krisen- und Einsatzplanungen Nordrhein-Westfalens infolge eines Datenlecks öffentlich bekannt und damit dauerhaft kompromittiert worden sind?

4. Welche technischen, organisatorischen und geheimschutzrechtlichen Vorkehrungen bestehen in Nordrhein-Westfalen zum Schutz von Informationen über kritische Infrastrukturen, deren Schwachstellen sowie Krisen- und Einsatzplanungen vor unberechtigtem Zugriff und Datenabfluss?

5. Welche Anforderungen gelten bei der Übermittlung sicherheitsrelevanter Informationen Nordrhein-Westfalens an Behörden des Bundes, anderer Länder oder sonstige externe Stellen hinsichtlich der Prüfung ihrer Schutzbedürftigkeit, ihrer Einstufung, der Beschränkung des Empfängerkreises sowie des Schutzes vor einem Datenabfluss?

Marcel Hafke