LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/21331**

10.09.2026

Kleine Anfrage 8752

des Abgeordneten Sven W. Tritschler AfD

Cyberangriffe auf Energieversorger und Netzbetreiber über externe Dienstleister – Was tut die Landesregierung?

Am 16. Juli 2026 berichtete die Hamburger Morgenpost, dass Hamburger Energienetze jüngst Opfer von Cyberkriminellen wurden.[1] Auch Netze BW und Stuttgart Netze gerieten ins Visier von Cyberkriminellen.[2] Der Angriff erfolgte nicht auf die Betreiber selbst, sondern auf externe Dienstleister, im Fall der Hamburger Energienetze auf das Unternehmen Enseco, das Zähler- und Montagedaten verarbeitet. Medienberichten zufolge waren bis zu 117.050 Kundendatensätze betroffen, darunter Namen, Anschriften, Zählernummern und Termindaten.[3] Im Fall von Netze BW und Stuttgart Netze soll ein Montage-Dienstleister aus dem Raum München angegriffen worden sein, wodurch Daten tausender Haushalte abgeflossen sein sollen.[4]

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) ist am 6. Dezember 2025 in Kraft getreten.[5] Es verpflichtet Unternehmen, die dem Wirkungsbereich der NIS2-Richtlinie unterliegen, als sogenannte KRITIS-Betreiber nach § 30 BSIG die Sicherheit ihrer Lieferkette einschließlich unmittelbarer Dienstleister als Teil ihrer Risikomanagementmaßnahmen zu gewährleisten. Die direkte Aufsicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) richtet sich jedoch nur gegen die regulierten Einrichtungen selbst.

Externe Dienstleister, die nicht selbst als besonders wichtige oder wichtige Einrichtungen eingestuft sind, unterliegen keiner unmittelbaren BSI-Aufsicht. Ihre Bindung an KRITIS-relevante Sicherheitsstandards entsteht allein mittelbar über vertragliche Verpflichtungen und Kontrollpflichten der Auftraggeber.

Diese Strukturschwäche zeigt sich auch in Nordrhein-Westfalen: Am 28. Juni 2026 wurden die Gemeinschaftsstadtwerke Kamen, Bönen und Bergkamen Opfer eines Cyberangriffs. Rund 60.000 Kunden waren betroffen; interne Netzwerke, das Kundenportal sowie der Zahlungsverkehr wurden erheblich beeinträchtigt.[6] Die ZAC NRW ermittelt wegen des Verdachts der Computersabotage. Ob ältere Kundendaten abgeflossen sind, war zum

[1] https://www.mopo.de/hamburg/hamburger-energienetze-betroffen-kundendaten-bei-cyberangriff-gestohlen/4886082
[2] https://www.swr.de/swraktuell/baden-wuerttemberg/stuttgart/hackerangriff-netze-bw-tipps-verbraucherzentrale-100.html
[3] https://www.solarserver.de/2026/08/20/hacker-erbeuten-kundendaten-bei-smart-meter-dienstleistern/
[4] https://www.drweb.de/netze-bw-datenleck-zaehler-dienstleister/
[5] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html
[6] https://gsw-kamen.de/unternehmen/presse/pressemitteilungen/detailansicht/cyberangriff-bei-den-gsw---alle-hellip:258854

Datum des Originals: 10.09.2026/Ausgegeben: 21.09.2026

Zeitpunkt der Anfrage noch offen. Bereits im Februar 2024 war PSI Software SE, ein zentraler Software- und Netzleitsystemanbieter für Energieunternehmen, Opfer eines Cyberangriffs geworden und das mit mittelbarem Risiko für verbundene Betreiber.[7]

Nordrhein-Westfalen verfügt über eine dichte Energieinfrastruktur: Übertragungsnetzbetreiber, Verteilernetze (u. a. Westnetz, Thyssengas), kommunale Stadtwerke und zahlreiche Dienstleister bilden ein verflochtenes System. Das Landeskriminalamt NRW und die ZAC NRW übernehmen strafrechtliche Ermittlungen; die Cybersicherheitsagentur NRW und DIGITAL.SICHER.NRW bieten Beratung und Prävention. Eine eigenständige landesrechtliche Meldepflicht für Cybervorfälle bei privaten oder kommunalen Energieversorgern, getrennt von den bundesrechtlichen Pflichten nach dem BSIG, ist im geltenden NRW-Recht nicht belegt. Damit besteht eine mögliche Transparenz- und Koordinationslücke gegenüber der Öffentlichkeit.

Die Bedrohungslage verschärft sich weiter: Am 21. August 2026 warnte die US-Regierung ausdrücklich vor Angriffen auf Siemens-Industriesteuerungen, die auch in der deutschen Energieinfrastruktur eingesetzt werden. In Berlin legten Cyberangriffe am 18. und 20. August 2026 zwei Senatsverwaltungen lahm.

Der Bundesrechnungshof kritisierte zuletzt die fehlende Wirkungskontrolle beim BSI. In diesem Umfeld stellen dienstleistervermittelte Angriffe eine qualitativ neue Herausforderung dar, denn die Sicherheit der kritischen Infrastruktur hängt zunehmend von Akteuren ab, die selbst nicht reguliert sind.

Ich frage daher die Landesregierung:

1. Welche konkreten Erkenntnisse hat die Landesregierung über Cyberangriffe auf Energieversorger sowie Netzbetreiber in Nordrhein-Westfalen, bei denen der Erstzugang nachweislich oder mutmaßlich über externe Dienstleister erfolgte?

2. Nach welchem festgelegten Verfahren erfolgt die behördliche Koordination zwischen der Cybersicherheitsagentur NRW, dem Landeskriminalamt, der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen sowie dem Bundesamt für Sicherheit in der Informationstechnik bei Cybervorfällen in der Energieversorgung?

3. Welche konkreten Maßnahmen zur Gefahrenabwehr sowie Schadensbegrenzung hat die Landesregierung als Reaktion auf den Cyberangriff auf die Gemeinschaftsstadtwerke Kamen, Bönen und Bergkamen vom 28. Juni 2026 ergriffen?

4. Welche über die bundesrechtlichen Vorgaben des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik hinausgehenden Meldepflichten für Cybervorfälle bei privaten oder kommunalen Energieversorgern existieren im nordrhein-westfälischen Landesrecht?

5. Welche Initiativen auf Bundes- oder Landesebene plant die Landesregierung, um Kontroll- sowie Regulierungslücken bei nicht unmittelbar BSI-regulierten Dienstleistern kritischer Energieinfrastrukturen zu schließen?

Sven W. Tritschler

[7] https://www.handelsblatt.com/unternehmen/energie/psi-software-hacker-legen-wichtigen-dienstleister-fuer-energieunternehmen-lahm/100015519.html