Deutscher Bundestag **Drucksache 21/5046**

21. Wahlperiode 26.03.2026

Kleine Anfrage

der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Martin Hess, Sascha Lensing und der Fraktion der AfD

Schutzmaßnahmen zur Abschirmung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben

Der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Digitalfunk BOS) stellt eine zentrale Kommunikationsinfrastruktur für einsatzkritische Lagen dar. Als bundesweit einheitliches, hochverfügbares Funknetz für Sprach- und Kurzdatenkommunikation ist er für den Schutz von Leib, Leben und öffentlichen Gütern in Polizei, Feuerwehr, Rettungsdienst und Katastrophenschutz von erheblicher Bedeutung (www.bdbos.bund.de/DE/Aufgaben/DigitalfunkBOS/DigitalfunkBOSimUeberblick/digitalfunkbosimueberblick_node.html?). Aus dem Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben ergibt sich, dass die Bundesanstalt den Digitalfunk BOS aufzubauen, zu betreiben und weiterzuentwickeln hat (www.gesetze-im-internet.de/bdbosg/BDBOSG.pdf?).

Die Diskussion um „Abschirmung“ des Digitalfunks BOS betrifft dabei nicht einen singulären Aspekt, sondern einen Maßnahmenverbund aus IT-Sicherheitsarchitektur, Betriebsorganisation, Lieferketten- und Beschaffungssteuerung, Zertifizierung sowie Resilienz- und Krisenmanagement. Hierzu gehören unter anderem kryptographische Verfahren (einschließlich Ende-zu-Ende-Verschlüsselung), die Absicherung von Übergängen in andere Netze, die Härtung zentraler Komponenten, die Detektion und Abwehr von Cyberangriffen, der Schutz vor Sabotage und Störung sowie die Begrenzung von Abhängigkeiten von Dritten. In behördlichen Betriebsvorgaben der Länder wird etwa ausdrücklich auf die Nutzung von Ende-zu-Ende-Verschlüsselung im Digitalfunk BOS hingewiesen und zugleich beschrieben, dass bestimmte Kommunikationsdienste nicht durchgängig Ende-zu-Ende verschlüsselt sind (https://bks-portal.rlp.de/system/files/organisationen/1842-autorisierte-stelle-digitalfunk-bos/dokumente/betriebshandbuch_digitalfunkbos_rp_0.pdf? Kapitel 5.2.4). Solche technischen Randbedingungen sind in den Augen der Fragesteller für die Frage relevant, wie die Bundesregierung die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit über das Gesamtsystem hinweg praktisch sicherstellt.

Die Notwendigkeit nachvollziehbarer und überprüfbarer Schutzmaßnahmen wird zudem durch externe Befunde unterstrichen. So hat der Bundesrechnungshof im Kontext der Objektfunkversorgung im Digitalfunk BOS die bundesrechtliche Aufgabenstellung der Bundesanstalt nach dem BDBOS-Gesetz herausgestellt und Prüfmaßstäbe an Wirtschaftlichkeit, Steuerung und Umsetzung formuliert (www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2020/objektfunkversorgung-im-digitalfunk-volltext.pdf?__blob=publicationFile&v=1; S. 5). Daneben berichten Fachmedien über neu diskutierte Schwach-

stellen und Forschungsbefunde zur TETRA-Verschlüsselung, die unabhängig von einer abschließenden sicherheitstechnischen Bewertung im Einzelfall die Bedeutung transparenter Härtungs-, Audit- und Migrationsstrategien für sicherheitskritische Funknetze verdeutlichen (www.heise.de/news/Digitaler-Behoerdenfunk-Neue-Schwachstellen-bei-Tetra-Verschluesselung-versagt-10515157.html?).

Wir fragen die Bundesregierung:

1. Welche konkreten Zuständigkeiten nimmt das Bundesministerium für Digitales und Staatsmodernisierung im Rahmen der „Steuerung der Cybersicherheit des Bundes“ in Bezug auf den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben wahr?
2. Welche Aufgaben nimmt das Bundesministerium für Digitales und Staatsmodernisierung über das Referat „Netze“ sowie über das Referat „Sicherheit und Resilienz digitaler Infrastrukturen“ im Hinblick auf Vorgaben, Standards oder Koordinierung zur Absicherung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben wahr (bitte jeweils einzeln benennen)?
3. Welche bundeseinheitlichen Sicherheitsanforderungen, Sicherheitsleitlinien oder Mindeststandards gelten nach Kenntnis der Bundesregierung aktuell für den Betrieb des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben?
4. Welche Maßnahmen hat die Bundesregierung seit dem 1. Januar 2023 ergriffen, um die Wirksamkeit der kryptographischen Absicherung im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben zu überprüfen oder fortzuentwickeln (bitte um Aufschlüsselung nach Maßnahmen und ausführender Bundesbehörde)?
5. Welche regelmäßigen Sicherheitsüberprüfungen (z. B. Audits, Penetrationstests, Red-Team-Übungen, Krisenübungen) werden nach Kenntnis der Bundesregierung für zentrale Komponenten und Betriebsprozesse des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben durchgeführt (bitte um Aufschlüsselung nach Bundesbehörde)?
6. Welche Rolle hat das Bundesamt für Sicherheit in der Informationstechnik bei Zertifizierung, Anerkennung oder Kontrolle von sicherheitsrelevanten Produkten und Dienstleistungen im Zusammenhang mit dem Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (bitte um Aufschlüsselung der Rechtsgrundlagen und der konkreten Verfahren)?
7. Welche zertifizierten oder anerkannten IT-Sicherheitsdienstleister werden nach Kenntnis der Bundesregierung in Verfahren zur sicherheitstechnischen Prüfung von Endgeräten oder Komponenten für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben?
8. Welche Anforderungen gelten nach Kenntnis der Bundesregierung für Hersteller, Lieferketten und Wartungsdienstleister sicherheitskritischer Komponenten im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben?
9. Welche Maßnahmen hat die Bundesregierung seit dem 1. Januar 2023 ggf. ergriffen, um Abhängigkeiten von einzelnen Herstellern oder proprietären Sicherheitsmechanismen im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben zu reduzieren (bitte Maßnahmen und Stand der Umsetzung angeben)?
10. Welche Vorhaben, Programme oder Projekte unterstützt oder koordiniert die Bundesregierung ggf. zur technologischen Weiterentwicklung des Di-

gitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben in Richtung breitbandiger einsatzkritischer?

11. Welche Sicherheitsanforderungen stellt die Bundesregierung bei Modernisierungsvorhaben (z. B. Einbindung von LTE/5G-fähigen Diensten) an die Trennung, Übergänge oder Kopplung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben zu anderen Netzen (bitte technische und organisatorische Maßnahmen benennen)?

12. Welche Vorkehrungen bestehen nach Kenntnis der Bundesregierung zur Detektion, Meldung und Behandlung sicherheitsrelevanter Vorfälle im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (bitte Meldewege, Zuständigkeiten, Eskalationsstufen und Berichtspflichten angeben)?

13. Welche Erkenntnisse liegen der Bundesregierung ggf. zu Ursachen, Auswirkungen und Abhilfemaßnahmen bei bundesweiten oder großflächigen Störungen des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben seit dem 1. Januar 2023 vor (bitte nach Ereignisdatum und Hauptursache aufschlüsseln)?

14. Welche Abstimmungen führt die Bundesregierung mit den Ländern zur Sicherstellung einer einheitlichen Sicherheitsarchitektur und Resilienz im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben durch, und welche Ergebnisse dieser Abstimmungen liegen nach Kenntnis der Bundesregierung vor (bitte Gremien, Termine und Beschlüsse/Arbeitsergebnisse benennen)?

Berlin, den 9. März 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