Deutscher Bundestag **Drucksache 21/5315**

21. Wahlperiode 09.04.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/5046 –

Schutzmaßnahmen zur Abschirmung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben

Vorbemerkung der Fragesteller

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 kryptografische 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 die Störung sowie 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 Bundesrech-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 9. April 2026 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

nungshof im Kontext der Objektfunkversorgung im Digitalfunk BOS die bundesrechtliche Aufgabenstellung der Bundesanstalt nach dem Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOSG) herausgestellt und Prüfmaßstäbe an die 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 Schwachstellen und Forschungsbefunde zur TETRA-Verschlüsselung (TETRA = Terrestrial Trunked Radio), 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?).

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?

Der Organisationserlass des Bundeskanzlers vom 6. Mai 2025 regelt die Geschäftsbereiche der Ressorts. Im Organisationserlass wurden im Rahmen der „Steuerung der Cybersicherheit des Bundes“ keine Zuständigkeiten in Bezug auf den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben übertragen. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) hat daher keine Zuständigkeit in diesem Themengebiet übernommen.

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)?

Das BMDS hat kein Referat mit der Bezeichnung „Netze“. Die Bundesregierung geht davon aus, dass damit das Referat DS I 5 „Kommunikationsinfrastruktur öffentlicher Stellen“ des BMDS gemeint ist. Gemäß Organisationserlass des Bundeskanzlers vom 6. Mai 2025 sind die Aufgaben Netze des Bundes (NdB) und Informationsverbund der öffentlichen Verwaltung (IVÖV) an das BMDS übergegangen. Die Zuständigkeiten für den Digitalfunk sind hingegen vollumfänglich im Bundesministerium des Innern verblieben. Insofern hat das Referat „Kommunikationsinfrastruktur öffentlicher Stellen“ des BMDS keine Aufgaben im Bereich „Vorgaben, Standards oder Koordinierung zur Absicherung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben.

Die Aufgaben des Referats „Sicherheit und Resilienz öffentlicher Telekommunikationsnetze“ ergeben sich aus dem 10. Teil des Telekommunikationsgesetzes. Entsprechend gehört der Digitalfunk BOS nicht zum Aufgabenbereich des vorgenannten Referats.

3. Welche bundeseinheitlichen Sicherheitsanforderungen, Sicherheitsleitlinien oder Mindeststandards gelten nach Kenntnis der Bundesregierung aktuell für den Betrieb des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben?

Für den Betrieb des Digitalfunks BOS gelten: das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) für besonders wichtige Einrichtungen, die Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) i. V. m. dem Sicherheitsüberprüfungsgesetz (SÜG) für lebenswichtige Einrichtungen, der Umsetzungsplan Bund (UP Bund), die Mindeststandards des BSI sowie der IT-Grundschutz-Standard des BSI.

4. Welche Maßnahmen hat die Bundesregierung seit dem 1. Januar 2023 ergriffen, um die Wirksamkeit der kryptografischen Absicherung im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben zu überprüfen oder fortzuentwickeln (bitte nach Maßnahmen und ausführender Bundesbehörde aufschlüsseln)?

Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) nimmt regelmäßig an den relevanten Gremien der internationalen Standardisierung teil. Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) überprüft die BDBOS die kryptographische Absicherung regelmäßig und entwickelt diese fort.

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 nach Bundesbehörde aufschlüsseln)?

Die BDBOS führt regelmäßig Audits und Informationssicherheitsrevisionen (IS-Revisionen) zur Erreichung der Sicherheitsziele und Strategien gemäß der „Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen“ der BDBOS sowie der Richtlinie „Audits und Revisionen in der BDBOS“ zur Erfüllung der Anforderungen der ISO/IEC Norm 27001 ISMS sowie die Umsetzung des darauf aufsetzenden BSI IT-Grundschutz (hier BSI-Standard 200-1 „ISMS“) durch. Sie führt zudem im Bereich Notfallmanagement regelmäßig Revisionen der Notfalldokumente durch. Weiterhin finden regelmäßig mit Bund und Ländern Übungen in diesem Bereich statt, insbesondere jährliche Alarmierungsübungen. Diese werden durch regelmäßige Schulungen sowie die strukturierte Nachbereitung von tatsächlich eingetretenen Ereignissen ergänzt.

6. Welche Rolle hat das Bundesamt für Sicherheit in der Informationstechnik bei der Zertifizierung, Anerkennung oder Kontrolle von sicherheitsrelevanten Produkten und Dienstleistungen im Zusammenhang mit dem Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (bittedie Rechtsgrundlagen und konkreten Verfahren aufschlüsseln)?

Der UP Bund ist die zentrale Leitlinie zur Gewährleistung der Informationssicherheit in der deutschen Bundesverwaltung. Er verpflichtet Bundesbehörden, ein Informationssicherheitsmanagementsystem (ISMS) nach BSI-Standards zu etablieren und verbindliche Sicherheitsmaßnahmen umzusetzen. Das BSI hat hierbei die zentrale Verantwortung entsprechende Vorgaben und Richtlinien zur Verfügung zu stellen.

Das BSI zertifiziert informationstechnische Systeme, Komponenten, Produkte, Schutzprofile, Personen sowie IT-Sicherheitsdienstleister nach § 52 BSI-Gesetz und der Verordnung EU 2019/881 sowie der hiernach erlassenen Umsetzungsrechtsakte. Listen der erteilten Zertifikate sind auf den Webseiten des BSI abrufbar.

Eine Liste der für den Geltungsbereich „BOS Digitalfunk“ zertifizierten IT-Sicherheitsdienstleister ist hier abrufbar:

www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/IT-Sicherheitsdienstleister-im-Digitalfunk-BOS/it-sicherheitsdienstleister-im-digitalfunk-bos_node.html.

Bezüglich des Betriebs des BOS-Digitalfunknetzes wurde ein Zertifikat ISO27001 auf Basis von IT-Grundschutz erteilt:

www.bsi.bund.de/SharedDocs/Zertifikate_GS_ISO27001/Abgeschlossen/BSI-IGZ-0743-2025.html.

Der TETRA-Standard, auf dem der Digitalfunk BOS aufsetzt, verfügt lediglich über eine Verschlüsselung der Luftschnittstelle. Auf Grundlage des damaligen BSI-Gesetzes hat das BSI für den Digitalfunk BOS seit dem Jahr 2000 eine zusätzliche Ende-zu-Ende-Verschlüsselung (E2EE) entwickeln lassen. Diese sichert die Vertraulichkeit und die Integrität der Kommunikation lückenlos zwischen den Kommunikationspartnern ab. Seitdem pflegt und betreibt das BSI die E2EE. Zusätzlich betreibt das BSI gemäß§ 3 Absatz (1) Satz 2 Nr. 12 BSIG die Root-CA und ein Trustcenter zur Bereitstellung der erforderlichen Zertifikate. Die für die Verschlüsselung verwendeten Chipkarten sind gemäß§ 3 Absatz (1) Satz 2 Nr. 8 BSIG nach Common Criteria zertifiziert

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 eingebunden?

Die BDBOS befindet sich bei der sicherheitstechnischen Prüfung in enger Zusammenarbeit und Abstimmung mit dem BSI.

8. Welche Anforderungen gelten nach Kenntnis der Bundesregierung für Hersteller, Lieferketten und Wartungsdienstleister sicherheitskritischer Komponenten im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben?

Es gelten die einschlägigen Richtlinien des BSI IT-Grundschutzes.

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)?

Beim bestehenden TETRA-Digitalfunk wurde auf ein proprietäres System gesetzt. Für den künftigen Digitalfunk der nächsten Generation wird auf Produkte gesetzt werden, die auf offenen Standards der ETSI und 3GPP basieren, um die Abhängigkeit von einem bestimmten Hersteller oder proprietären Produkten zu vermeiden.

10. Welche Vorhaben, Programme oder Projekte unterstützt oder koordiniert die Bundesregierung ggf. zur technologischen Weiterentwicklung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben in Richtung breitbandiger und bzw. oder einsatzkritischer?

Die mit Bund und Ländern abgestimmte Breitbandstrategie sieht einen stufenweisen Aufbau des Digitalfunks der nächsten Generation vor. Die BDBOS hat dafür das Programm Breitband eingerichtet.

11. Welche Sicherheitsanforderungen stellt die Bundesregierung bei Modernisierungsvorhaben (z. B. Einbindung von LTE- bzw. 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)?

Der Digitalfunk der nächsten Generation (DFnG) stützt sich künftig auf LTE/5G-Mobilfunk, wobei hier ein eigenbeherrschtes Kernnetz das Ziel ist. Hier werden neben den bisher geltenden hohen Sicherheitsanforderungen, speziell auch den BSI-Standards, auch die Vorgaben für kritische Komponenten nach § 165 Absatz 4 Telekommunikationsgesetz Berücksichtigung finden. Speziell ein 5G Mobilfunksystem beinhaltet starke Sicherheitsmechanismen, welche auch die Kopplung von Netzen betreffen. Darüber hinaus ist weiterhin der Einsatz eines Security Information and Eventmanagement (SIEM) vorgesehen, welches das Netz kontinuierlich überwacht und Bedrohungen identifiziert. Die Ende-zu-Ende-Verschlüsselung der Sprach- und Datenkommunikation wird dann integraler Bestandteil der 3GPP Mission Critical (MC)-Funktionen sein, welche auf dem LTE/5G-Mobilfunksystem aufsetzen und speziell für Nutzer mit sehr hohen Sicherheitsanforderungen spezifiziert wurden.

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)?

Die BDBOS betreibt im Digitalfunk BOS ein Security Operations Center (SOC), welches sicherheitsrelevante Ereignisse auf technischer Ebene im Digitalfunk überwacht.

Weiterhin hat die BDBOS eine mit Bund und Ländern gemeinsam abgestimmte Richtlinie zum Melden und Behandeln von Sicherheitsvorfällen. In dieser Richtlinie sind folgende fragegegenständliche Regelungen getroffen:

Zuständigkeiten bei Sicherheitsvorfällen: Im Prozess zur Behandlung von Sicherheitsvorfällen im Digitalfunk sind mehrere Akteure involviert. Für die handelnden Akteure ist festgelegt, welche Aufgaben und Kompetenzen diese haben und auf welche Art sie verpflichtet bzw. benachrichtigt werden. Dabei wird nach den Ebenen der Nutzer, der Fachverantwortlichen, des Service Desks, der/des Informationssicherheitsbeauftragte/-n, der/des Verantwortlichen für den Digitalfunk sowie dem Sicherheitsvorfall-Team unterschieden.

Festlegung von Meldewegen für Sicherheitsvorfälle: Sicherheitsvorfälle werden nach den jeweils intern gültigen Prozessvorgaben bearbeitet und bewertet. In jedem Fall wird durch Meldende als auch durch Adressierte der Meldung die potentielle Betroffenheit weiterer Beteiligter am Digitalfunk BOS außerhalb der eigenen Zuständigkeit geprüft. Der Austausch von Informationen zu Sicher-

heitsvorfällen zwischen Bund, Ländern und BDBOS findet primär über die eingerichteten Zuständigen statt.

Eskalationsstrategie für Sicherheitsvorfälle: Damit Sicherheitsvorfälle ohne Zeitverlust von den Verantwortlichen bearbeitet werden können, sind im Vorfeld Eskalationsstrategien und Ansprechpartner bzw. Wege definiert. Eine Liste mit den Erreichbarkeiten ist bei den „Service Desks“ hinterlegt.

Berichtspflichten: Bis zur Beendigung des Sachverhalts und der eingeleiteten Maßnahmen erfolgt in regelmäßigen, geeigneten Abständen eine Aktualisierung der Lage. Meldungen zu Sicherheitsvorfällen werden bei der BDBOS gemeinsam mit den betroffenen Institutionen bearbeitet und ausgewertet. Die hieraus entstehenden Arbeitsergebnisse werden bei Bedarf mit allen am Digitalfunk Beteiligten nachbereitet. Die Ergebnisse der Nachbereitung und Schlussfolgerungen werden den zuständigen Instanzen zur Verfügung gestellt

13. Welche Erkenntnisse liegen der Bundesregierung ggf. zu den 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)?

Ein Beauskunften der hier infragestehenden Informationen kann aufgrund entgegenstehender überwiegender Belange des Staatswohls nur eingestuft erfolgen. Durch eine offene Auskunft darüber, welche Ursachen eine bundesweite oder großflächige Störung des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben zugrunde liegen und welche Auswirkungen konkret entstanden sind, wären Rückschlüsse auf die konkreten technischen Schutzmechanismen des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben und etwaige, sehr spezifische Schwachstellen möglich. Durch eine offene Auskunft über den aktuellen Wissensstand könnten Extremisten oder staatliche Akteure Angriffsstrategien entwickeln und dadurch die Funktionsfähigkeit des Digitalfunks und damit die Aufgabenerfüllung der Behörden mit Sicherheitsaufgaben gefährden oder letztere sogar unmöglich machen. Dies würde einen Nachteil für die Interessen der Bundesrepublik Deutschland bedeuten. Eine offene Beantwortung der Frage ist daher nicht möglich und wird gesondert als VS-Nur für den Dienstgebrauch eingestufte Anlage übersendet.

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 bzw. Arbeitsergebnisse benennen)?

Auf Grundlage von § 5 BDBOS-G wurde bei der BDBOS ein Verwaltungsrat gegründet, in dem der Bund und jedes Bundesland über einen Sitz verfügt. Im Verwaltungsrat der BDBOS beraten der Bund und die Länder laufend über alle relevanten Belange für den Digitalfunk der BOS einschließlich Resilienzmaßnahmen und Fragen der Sicherung der Kommunikation.

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