Deutscher Bundestag **Drucksache 21/2419**

21. Wahlperiode 27.10.2025

Kleine Anfrage

der Abgeordneten Tobias Matthias Peterka, Alexis L. Giersch, Ulrich von Zons, Lukas Rehm, Manfred Schiller, Tobias Teich, Gerold Otten, Dr. Rainer Kraft, Jan Wenzel Schmidt, Thomas Korell, Dr. Paul Schmidt, Robin Jünger, Dr. Malte Kaufmann, Dr. Daniel Zerbin, Mirco Hanker, Reinhard Mixl, Dr. Michael Blos, Dr. Christina Baum, Dr. Maximilian Krah, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Marc Bernhard, Joachim Bloch, Udo Theodor Hemmelgarn, Stefan Henze, Uwe Schulz, Sascha Lensing, Rocco Kever, Volker Scheurell, Otto Strauß, Tobias Ebenberger und der Fraktion der AfD

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Verkehr

Die Cybersicherheitslage in Deutschland wird von der Bundesregierung und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) regelmäßig als „angespannt bis kritisch“ beschrieben (www.tuev-verband.de/pressemitteilungen/angespannt-bis-kritisch-die-cybersicherheitslage-in-deutschland#:~:text=Lagebericht%20des%20BSI:%20Cybersicherheit%20in%20Deutschland%20).

Auch der Bundesrechnungshof warnt vor eklatanten Sicherheitslücken in den Rechenzentren und Netzen des Bundes (www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacfe5-2e6b-4e8b-a64b-e10d9cf2585e). Unter anderem bemängelt der Bundesrechnungshof, dass weniger als 10 Prozent der mehr als 100 Bundesrechenzentren die Mindeststandards erfüllen, dass die Notstromversorgung in Krisenlagen vielfach unzureichend ist und dass kritische IT-Dienste oft nicht georedundant verfügbar sind (s. o.). Nach aktuellen Berichten hat die Bundesregierung im Bereich IT-Sicherheit Stellen abgebaut (www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/).

Das Bundesministerium für Verkehr (BMV) trägt eine besondere Verantwortung für die sichere und verlässliche Gestaltung der Verkehrsinfrastrukturen in Deutschland. Mit der zunehmenden Digitalisierung im Bereich Verkehr – etwa durch intelligente Verkehrssysteme, digitale Steuerungstechnologien im Schienen- und Luftverkehr oder vernetzte Fahrzeuge – wächst zugleich die Abhängigkeit von stabilen und sicheren IT-Systemen. Cyberangriffe auf die behördeninterne IT oder auf Schnittstellen zu Infrastrukturbetreibern können die Sicherheit im Straßen-, Schienen-, Luft- und Schiffsverkehr gefährden. Vor allem im Hinblick auf die Verkehrssicherheit sind Ausfälle oder Manipulationen digitaler Systeme von erheblicher Tragweite, weil sie direkte Auswirkungen auf die Sicherheit von Millionen Verkehrsteilnehmern haben können. Das BMV steht zudem in engem Austausch mit Unternehmen, Betreibern kritischer Infrastrukturen und internationalen Partnern, die darauf vertrauen können müssen, dass ihre Kommunikation mit dem BMV sicher vor dem Zugriff Dritter ist.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMV aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?
2. Welche dieser Rechenzentren (vgl. Frage 1) verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?
3. An welchen Standorten des BMV sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMV in den Jahren von 2022 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?
5. In welchem Umfang hat das BMV in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder durch unabhängige Dienstleister) durchführen lassen, und mit welchen Ergebnissen?
6. Welche organisatorischen Zuständigkeiten für Cybersicherheit bestehen innerhalb des BMV (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMV ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
8. Welche Maßnahmen hat das BMV seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren (vgl. Vorbemerkung der Fragesteller)?
9. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMV registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Vorfälle aufschlüsseln)?
10. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage durch Cyberangriffe auf die IT-Systeme des BMV mit Blick auf mögliche Auswirkungen auf die Verkehrssicherheit?
11. Welche Vorkehrungen bestehen, um Manipulationen oder Ausfällen in digitalisierten Verkehrssteuerungssystemen (z. B. Schienenverkehr, Luftverkehr, intelligente Verkehrsnetze) vorzubeugen?
12. Welche Notfall- und Reaktionspläne existieren, um im Falle eines Cyberangriffs schnellstmöglich die Funktionsfähigkeit kritischer Verkehrsinfrastrukturen wiederherzustellen?
13. Welche internen Notfall- und Reaktionspläne bestehen im BMV für den Fall von Cyberangriffen auf zentrale Verwaltungsprozesse?
14. Inwiefern sind Betreiber kritischer Verkehrsinfrastrukturen in die Cybersicherheitsstrategie des BMV eingebunden?
15. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMV seit 2020 durchgeführt?
16. Welche konkreten Schritte plant das BMV, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen (vgl. Vorbemerkung der Fragesteller)?

17. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMV (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?
18. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMV seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?
19. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMV abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
20. Wie viele dieser Stellen (vgl. Frage 19) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
21. Welche besonderen Schwierigkeiten sieht die Bundesregierung bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMV, und welche Maßnahmen werden ergriffen, um diese Herausforderungen zu bewältigen?
22. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMV, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?
23. Welche Maßnahmen ergreift das BMV, um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
24. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMV mittelfristig auszubauen, und mit welchem zeitlichen Horizont?

Berlin, den 22. Oktober 2025

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