Deutscher Bundestag **Drucksache 21/2408**

21. Wahlperiode 27.10.2025

Kleine Anfrage

der Abgeordneten Tobias Matthias Peterka, 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, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Dr. Christina Baum, Dr. Maximilian Krah, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Joachim Bloch, Marc Bernhard, 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 Forschung, Technologie und Raumfahrt

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/).

Angriffe auf interne IT-Infrastrukturen des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) könnten nicht nur vertrauliche Forschungs- und Entwicklungsdaten gefährden, sondern auch sicherheitsrelevante Auswirkungen auf strategische Zukunftstechnologien und die Raumfahrt haben. Gleichzeitig ist der Schutz im Austausch mit Unternehmen, Hochschulen, internationalen Partnern und Raumfahrtorganisationen essenziell, um Datenabflüsse und Manipulationen zu verhindern.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMFTR aktuell, und wie viele davon erfüllen nachweislich die geltenden Mindeststandards für IT-Sicherheit?

2. Welche dieser Rechenzentren verfügen über eine funktionsfähige Notstromversorgung, die auch längerfristige (über mehrere Stunden oder Tage) Krisenlagen abdecken kann?
3. An welchen Standorten des BMFTR sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMFTR 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 BMFTR in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder durch unabhängige Dienstleister) durchführen lassen, und mit welchen Ergebnissen?
6. Wie wird die Europäische Weltraumorganisation (ESA) in die Cybersicherheitsstrategie des BMFTR eingebunden?
7. Welche organisatorischen Zuständigkeiten für Cybersicherheit bestehen innerhalb des BMFTR (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
8. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMFTR ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
9. Welche Maßnahmen hat das BMFTR seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren (vgl. Vorbemerkung der Fragesteller)?
10. In welcher Form arbeitet das BMFTR mit nationalen und internationalen Partnern im Bereich Forschung, Technologie und Raumfahrt zusammen, um gemeinsame Sicherheitsstandards gegen Cyberbedrohungen zu etablieren?
11. Welche Verfahren bestehen, um den vertraulichen Austausch mit Hochschulen, Forschungsinstituten, Technologieunternehmen und Raumfahrtorganisationen vor Cyberangriffen zu schützen?
12. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMFTR registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Vorfälle aufschlüsseln)?
13. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage durch Cyberangriffe auf das BMFTR, insbesondere in Bezug auf hochsensible Forschungs- und Raumfahrtdaten?
14. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMFTR seit 2020 durchgeführt?
15. Welche konkreten Schritte plant das BMFTR, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?
16. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMFTR (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?
17. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMFTR seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?

18. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMFTR abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
19. Wie viele dieser möglichen Stellen (vgl. Frage 18) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
20. Welche besonderen Schwierigkeiten sieht die Bundesregierung ggf. bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMFTR, und welche Maßnahmen werden ggf. ergriffen, um diese Herausforderungen zu bewältigen?
21. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMFTR, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?
22. Welche Maßnahmen ergreift das BMFTR ggf., um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
23. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMFTR 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