Deutscher Bundestag **Drucksache 21/2418**

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, Dr. Christina Baum, Dr. Maximilian Krah, Stefan Keuter, Marc Bernhard, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, 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 Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit

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 Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) trägt eine zentrale Verantwortung für die nukleare Sicherheit in Deutschland. Dazu gehört auch die Aufsicht über den sicheren Betrieb kerntechnischer Anlagen und die Umsetzung internationaler Verpflichtungen. Die Gewährleistung hoher Sicherheitsstandards im Bereich der nuklearen Sicherheit umfasst nicht nur den physischen Schutz kerntechnischer Anlagen, sondern zunehmend auch die Dimension der Cybersicherheit. Angriffe auf kritische Infrastrukturen haben in den vergangenen Jahren zugenommen (www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html#:~:text=Aktuelle%20Trends%20und%20Entwicklungen%20der,Gefahren%20Warnhinweise%20und%20Sonderauswertungen%20heraus), und auch im internationalen Kontext warnen Fachgremien wie die Internationale Atomenergie-Organisation (IAEO) vor steigenden Risiken im Bereich der IT-

und Operational Technology (OT)-Sicherheit nuklearer Einrichtungen (www.heise.de/news/Atomenergie-Organisation-baut-Trainingslager-fuer-Kampf-gegen-Nuklearterrorismus-6135943.html). Neben diesem besonders sicherheitskritischen Bereich unterliegen jedoch auch weitere Zuständigkeiten des BMUKN – wie Umwelt- und Naturschutz – spezifischen Cyberrisiken. So sind etwa Mess- und Überwachungssysteme im Umweltbereich, digitale Infrastrukturen sowie Datenbanken und Verwaltungsprozesse im Naturschutz ebenfalls potenziellen Angriffen ausgesetzt.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des BMUKN integriert sind und wie sich die personelle Ausstattung in den letzten Jahren entwickelt hat.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMUKN 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 BMUKN sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMUKN 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 BMUKN 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 BMUKN (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMUKN für die Cybersicherheit kerntechnischer Anlagen?
8. Welche Maßnahmen hat das BMUKN seit 2020 ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren?
9. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMUKN registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr, Anzahl der Zwischenfälle und Zuständigkeitsbereichen im BMUKN aufschlüsseln)?
10. Welche Bedrohungsanalysen zu Cyberangriffen auf kerntechnische Anlagen liegen dem BMUKN derzeit vor, und wie werden diese in die Aufsichtspraxis integriert?
11. Welche Bedrohungsanalysen zu Cyberangriffen in den Bereichen Umwelt- und Naturschutz, z. B. auf Messnetze, Dateninfrastrukturen oder Steuerungssysteme, liegen dem BMUKN derzeit vor?
12. Welche konkreten Schritte plant das BMUKN, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?

13. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMUKN (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?
14. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMUKN seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?
15. Wie viele Stellen mit Bezug zur IT- und Cybersicherheit waren seit 2020 im Geschäftsbereich des BMUKN vorhanden, die unmittelbar den sicheren Betrieb kerntechnischer Anlagen betreffen (bitte jeweils nach Jahr, Organisationseinheit und Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?
16. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMUKN abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
17. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMUKN ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
18. Wie viele dieser Stellen (vgl. Frage 17) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
19. In welchen Abteilungen oder nachgeordneten Behörden des BMUKN werden Fragen der IT- und Cybersicherheit mit Bezug zur nuklearen Sicherheit bearbeitet?
20. Welche spezifischen Qualifikationen im Bereich Cybersicherheit und Leittechniksicherheit werden bei der Besetzung von Stellen in der nuklearen Aufsicht gefordert oder bevorzugt berücksichtigt?
21. Welche Schulungen und Fortbildungen zur Abwehr von Cyberangriffen auf kerntechnische Anlagen wurden seit 2018 für Beschäftigte des BMUKN und seiner nachgeordneten Behörden durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?
22. In welchem Umfang bestehen Kooperationen mit anderen Ressorts und Behörden, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, sowie mit internationalen Organisationen wie der International Atomic Energy Agency [IAEO], der Organization for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA) oder im Rahmen der EU im Bereich Cybersicherheit kerntechnischer Anlagen sowie in Umwelt- und Naturschutzbereichen?
23. Welche konkreten Vorkehrungen wurden vom BMUKN und von der Bundesregierung getroffen, um Angriffe auf digitale Steuerungs- und Sicherheitssysteme kerntechnischer Anlagen zu verhindern?
24. Welche Maßnahmen ergreift das BMUKN, um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
25. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMUKN mittelfristig auszubauen, und wenn ja, 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