

## **Kleine Anfrage**

**der Abgeordneten Tobias Matthias Peterka, Peter Bohnhof, 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, Marc Bernhard, Dr. Christina Baum, Carolin Bachmann, Stefan Keuter, Dr. Maximilian Krahl, 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 Arbeit und Soziales**

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/pressemitteilung/n/angespannt-bis-kritisch-die-cybersicherheitslage-in-deutschland#:~:text=Lagebericht%20des%20BSI:%20Cybersicherheit%20in%20Deutschland%20](http://www.tuev-verband.de/pressemitteilung/n/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-6baacf5-2e6b-4e8b-a64b-e10d9cf2585e](http://www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacf5-2e6b-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/](http://www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/)).

Das Bundesministerium für Arbeit und Soziales (BMAS) arbeitet mit großen Mengen personenbezogener Daten. Insbesondere beim sog. Bürgergeld ist ein hohes Maß an IT-Sicherheit erforderlich, um Missbrauch, Manipulation oder Datenabfluss zu verhindern. Angriffe auf die IT-Infrastruktur des BMAS oder auf Schnittstellen zwischen Bundesministerium, Jobcentern und Leistungsempfängern können die Auszahlung existenzsichernder Leistungen gefährden. Durch gezielte Cyberangriffe können Datenbestände verändert, Leistungsansprüche verfälscht oder Zahlungen an unberechtigte Empfänger umgeleitet werden. Die Möglichkeit, interne Abläufe des BMAS oder bei seinen nachgeordneten Behörden gezielt zu stören oder zu missbrauchen, eröffnet ein erhebliches Schadenspotenzial für die öffentliche Hand.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMAS 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 BMAS sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMAS 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 BMAS 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 BMAS (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMAS ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
8. Welche Maßnahmen hat das BMAS 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 BMAS 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 BMAS und der mit dem Bürgergeld befassten Jobcenter?
11. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMAS seit 2020 durchgeführt?
12. Welche konkreten Schritte plant das BMAS, 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 BMAS (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?
14. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMAS seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?
15. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMAS abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
16. Wie viele dieser Stellen sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?

17. Welche besonderen Schwierigkeiten sieht die Bundesregierung bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMAS, und welche Maßnahmen werden ergriffen, um diese Herausforderungen zu bewältigen?
18. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMAS, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?
19. Welche Maßnahmen ergreift das BMAS ggf., um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
20. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMAS mittelfristig auszubauen, und wenn ja, mit welchem zeitlichen Horizont?

Berlin, den 22. Oktober 2025

**Dr. Alice Weidel, Tino Chrupalla und Fraktion**

