

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, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Dr. Maximilian Krah, Dr. Christina Baum, 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 der Justiz und für Verbraucherschutz

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-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/).

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) ist als Träger hochsensibler Daten – etwa in Bezug auf das Gesetzgebungsverfahren, die Registersysteme und internationale Justizkooperation – in besonderem Maße auf eine verlässliche und sichere IT angewiesen.

Wir fragen die Bundesregierung:

1. Über wie viele Rechenzentren verfügt das BMJV 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 BMJV sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMJV 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 BMJV 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 BMJV (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche Maßnahmen hat das BMJV seit 2020 ggf. ergriffen, um auf die Kritikpunkte des Bundesrechnungshofes im Bereich IT-Sicherheit zu reagieren?
8. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMJV registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Vorfälle aufschlüsseln)?
9. Welche Schulungs- und Sensibilisierungsmaßnahmen zum Thema Cybersicherheit wurden für Mitarbeiter des BMJV seit 2020 durchgeführt?
10. Welche konkreten Schritte plant das BMJV ggf., um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?
11. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMJV (bitte nach Behörden und Besoldungsgruppen aufschlüsseln)?
12. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMJV seit 2020 entwickelt (bitte jährlich angeben und nach Behörden differenzieren)?
13. Wurden in den Jahren 2022, 2023 und 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMJV abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
14. Wie viele dieser möglichen Stellen (vgl. Frage 13) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
15. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMJV ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Justizinfrastrukturen, IT-Forensik)?
16. Welche besonderen Schwierigkeiten sieht die Bundesregierung ggf. bei der Gewinnung von IT-Sicherheitsfachkräften im Geschäftsbereich des BMJV, und welche Maßnahmen werden ggf. ergriffen, um diese Herausforderungen zu bewältigen?
17. Welche Rolle spielt das Informationstechnikzentrum Bund (ITZBund) in Bezug auf die IT-Sicherheit für das BMJV, und wie entwickelt sich dort die Personalausstattung in diesem Bereich?
18. Ist die Justizverwaltung im Hinblick auf ihre IT-Sicherheitskapazitäten durch Fachkräftemangel oder Stellenkürzungen betroffen, und wenn ja, inwiefern?

19. Welche Maßnahmen ergreift das BMJV ggf., um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
20. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMJV mittelfristig auszubauen, und mit welchem zeitlichen Horizont?

Berlin, den 22. Oktober 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

