Deutscher Bundestag **Drucksache 21/2380**

21. Wahlperiode 22.10.2025

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, Marc Bernhard, Dr. Malte Kaufmann, Dr. Daniel Zerbin, Mirko Hanker, Reinhard Mixl, Dr. Michael Blos, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Dr. Christina Baum, Achim Köhler, Edgar Naujok, Dr. Maximilian Krah, 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 Wohnen, Stadtentwicklung und Bauwesen

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 Prozent22angespannt,f%C3 ProzentBCr%20Cyberangriffe%20durch%20Transparenz%20sch%C3 ProzentA4rfen%20und%20Cyber).

Auch der Bundesrechnungshof warnt vor eklatanten Sicherheitslücken in den Rechenzentren und Netzen des Bundes (https://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 (ebd.). Nach aktuellen Berichten hat die Bundesregierung im Bereich IT-Sicherheit Stellen abgebaut (www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/).

Mit der Digitalisierung von Verwaltungsverfahren im Bau- und Wohnungswesen entstehen für Bund, Länder und Kommunen neue Chancen, aber auch erhebliche Risiken. Digitale Bauantragsverfahren, die Wohnraumförderungsdatenbank, Building Information Modeling (BIM) in Planungs- und Bauprozessen sowie die internen Kommunikations- und Verwaltungsplattformen des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) sind zunehmend integraler Bestandteil staatlicher Kernaufgaben. Diese Verfahren haben bereits heute eine Schlüsselfunktion für die Umsetzung zentraler politischer Ziele – vom sozialen Wohnungsbau über Stadtentwicklungsprogramme bis hin zu Planungsprozessen für große Infrastrukturprojekte. Sie müssen daher im weiteren Sinne als Teil der kritischen Infrastruktur betrachtet werden. Ein

erfolgreicher Cyberangriff auf diese Systeme könnte schwerwiegende Folgen haben: Blockaden oder Verzögerungen bei Bauanträgen könnten die Umsetzung von Bauvorhaben erheblich verzögern, Manipulationen an der Wohnraumförderungsdatenbank könnten Förderentscheidungen verfälschen und das Vertrauen in staatliche Programme untergraben, Angriffe auf BIM-Verfahren könnten Bau- und Infrastrukturprojekte stören oder Fehlplanungen verursachen, Störungen in internen Verwaltungs- und Kommunikationssystemen könnten den Behördenbetrieb erheblich einschränken und die Zusammenarbeit mit Ländern und Kommunen gefährden.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen 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 BMWSB 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 BMWSB sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMWSB in den Jahren 2020 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?
5. In welchem Umfang hat das BMWSB in den vergangenen fünf Jahren Sicherheitsüberprüfungen (z. B. durch das BSI oder unabhängige Dienstleister) durchführen lassen, und mit welchen Ergebnissen?
6. Welche organisatorischen Zuständigkeiten für Cybersicherheit bestehen innerhalb des BMWSB (z. B. eigenes CERT (Community Emergency Response Team), IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMWSB für die Sicherung der digitalen Bauantragsverfahren, Wohnraumförderungsdatenbank, BIM-Verfahren und internen Kommunikations- und Verwaltungsplattformen?
8. Welche Maßnahmen hat das BMWSB 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 BMWSB registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr, Anzahl der Zwischenfälle aufschlüsseln)?
10. Welche Bedrohungsanalysen zu Cyberangriffen auf die genannten digitalen Verfahren liegen dem BMWSB vor?
11. Welche spezifischen Gefahren bestehen für die Verfügbarkeit und Integrität der Wohnraumförderungsdatenbank, Sicherheit der digitalen Bauantragsverfahren, Manipulationssicherheit bei BIM-Prozessen, interne Kommunikation und Datenverwaltung im BMWSB?

12. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um die genannten Verfahren gegen Cyberangriffe abzusichern?
13. Welche zusätzlichen Maßnahmen sind in Planung, um die digitale Bauverwaltung als kritische Infrastruktur künftig zu stärken bzw. zu erhöhen?
14. Welche konkreten Schritte plant das BMWSB, um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanten Systemen) sicherzustellen?
15. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMWSB (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?
16. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMWSB seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?
17. Wurden in den Jahren 2020 bis 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMWSB abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
18. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMWSB ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
19. Wie viele dieser Stellen sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
20. Welche spezifischen Qualifikationen (z. B. IT-Sicherheit in Verwaltungsverfahren, Schutz kritischer Datenbanken, OT (Operational Technology)-Sicherheit in Bauprozessen) werden bei der Besetzung von Stellen gefordert oder bevorzugt berücksichtigt?
21. Welche Schulungen und Fortbildungen wurden für Beschäftigte des BMWSB und seiner nachgeordneten Behörden im Bereich IT-Sicherheit seit 2018 durchgeführt (bitte nach Jahr und Art der Fortbildung aufschlüsseln)?
22. Welche Kooperationen bestehen mit anderen Ressorts, den Ländern, Kommunen oder internationalen Organisationen zur Stärkung der Resilienz gegen Cyberangriffe?
23. Welche Maßnahmen ergreift das BMWSB, um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
24. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMWSB mittelfristig auszubauen, mit welchem zeitlichen Horizont?
25. Inwieweit bewertet die Bundesregierung die digitalen Verwaltungs- und Planungsverfahren des BMWSB als kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes, und welche Konsequenzen ergeben sich daraus für die Cybersicherheitsstrategie?

Berlin, den 30. 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