Deutscher Bundestag **Drucksache 21/2403**

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. Maximilian Krah, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Dr. Christina Baum, Julian Schmidt, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Joachim Bloch, Udo Theodor Hemmelgarn, Stefan Henze, Uwe Schulz, Sascha Lensing, Rocco Kever, Marc Bernhard, Volker Scheurell, Otto Strauß, Tobias Ebenberger und der Fraktion der AfD

Cybersicherheit und Stellenentwicklung im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums für Landwirtschaft, Ernährung und Heimat

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%).

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/).

Die Landwirtschaft und die Ernährungswirtschaft stehen im Zuge der Digitalisierung vor tiefgreifenden Veränderungen. Systeme des Smart Farmings, digitale Plattformen für Agrar- und Ernährungsdaten, automatisierte Produktionsprozesse in der Lebensmittelwirtschaft sowie komplexe Liefer- und Logistikketten sind zunehmend digital gesteuert.

Damit steigt auch die Anfälligkeit gegenüber Cyberangriffen: Manipulationen an Agrardaten, Unterbrechungen von Lieferketten oder Angriffe auf Steuerungssysteme könnten nicht nur wirtschaftliche Schäden verursachen, sondern auch die Versorgungssicherheit mit Lebensmitteln beeinträchtigen. Besonders in Krisenlagen wie Pandemien und Naturkatastrophen kann eine zusätzliche Gefährdung durch Cyberangriffe gravierende Folgen haben.

Das Bundesministerium für Landwirtschaft, Ernährung und Heimat (BMLEH) trägt die Verantwortung für die Stabilität der landwirtschaftlichen Produktion, die Sicherheit der Lebensmittelversorgung sowie die Stärkung der ländlichen Räume.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, inwieweit Cybersicherheitsaspekte in den Verantwortungsbereich des BMLEH 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 BMLEH 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 BMLEH sind kritische IT-Dienste georedundant verfügbar, und wie wird die Ausfallsicherheit regelmäßig überprüft?
4. Welche Investitionen hat das BMLEH in den Jahren von 2020 bis 2025 konkret für den Ausbau und die Absicherung seiner IT-Infrastruktur (einschließlich Rechenzentren, Netze, Cloudlösungen) getätigt?
5. In welchem Umfang hat das BMLEH 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 BMLEH (z. B. eigenes Computer Emergency Response Team [CERT], IT-Sicherheitsreferate, Zusammenarbeit mit dem BSI)?
7. Welche spezifischen Zuständigkeiten bestehen im Geschäftsbereich des BMLEH für die Abwehr von Cyberangriffen auf digitale Systeme des Smart Farmings, der Produktions- und Verarbeitungseinrichtungen der Ernährungswirtschaft, Liefer- und Logistikketten, Datenplattformen im Bereich Agrar- und Lebensmittelwirtschaft sowie kritischen Infrastrukturen der Lebensmittelversorgung?
8. Welche Maßnahmen hat das BMLEH seit 2020 ggf. 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 BMLEH registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr und Anzahl der Zwischenfälle aufschlüsseln)?
10. Welche Bedrohungsanalysen zu Cyberangriffen auf Lebensmittelversorgungsketten und Agrar- bzw. Ernährungsdaten liegen dem BMLEH vor, und wie fließen diese in die Praxis der IT-Sicherheit ein?
11. Welche technischen und organisatorischen Maßnahmen wurden seit 2018 ergriffen, um Cyberangriffe auf digitale Systeme der Lebensmittel- und Agrarwirtschaft sowie auf Lieferketten abzuwehren?
12. Welche besonderen Vorkehrungen bestehen beim BMLEH für Krisen- und Notlagen, in denen Cyberangriffe die Versorgungssicherheit zusätzlich gefährden könnten?

13. Welche konkreten Schritte plant das BMLEH ggf., um bis spätestens 2030 die vollständige Einhaltung der vom Bundesrechnungshof geforderten Mindeststandards (inklusive Notstromversorgung und georedundanter Systeme) sicherzustellen?
14. Wie viele Stellen im Bereich IT-Sicherheit existieren derzeit im Geschäftsbereich des BMLEH (bitte nach Behörden und Besoldungs- bzw. Entgeltgruppen aufschlüsseln)?
15. Wie hat sich die Zahl der IT-Sicherheitsstellen im BMLEH seit 2018 entwickelt (bitte jährlich angeben und nach Behörden differenzieren sowie nach Besoldungs- bzw. Entgeltgruppe aufschlüsseln)?
16. Wie viele dieser Stellen (vgl. Frage 15) entfallen unmittelbar auf Aufgaben zur Sicherung der Versorgungssicherheit und der Ernährungswirtschaft?
17. Wurden in den Jahren von 2020 bis 2024 Stellen im Bereich IT-Sicherheit im Geschäftsbereich des BMLEH abgebaut, umgewidmet oder neu geschaffen, und wenn ja, in welchem Umfang?
18. Wie viele dieser möglichen Stellen (vgl. Frage 17) sind derzeit unbesetzt, und wie lange bleiben offene Stellen im Durchschnitt vakant?
19. Welche konkreten Aufgabenbereiche decken die IT-Sicherheitsstellen im BMLEH ab (z. B. Netzwerksicherheit, Kryptografie, Incident Response, Schutz kritischer Infrastrukturen, IT-Forensik)?
20. Welche spezifischen Qualifikationen werden bei der Besetzung von Stellen mit Blick auf die Versorgungsketten- und Infrastruktursicherheit gefordert oder bevorzugt berücksichtigt?
21. Welche Schulungen und Fortbildungen wurden für Beschäftigte des BMLEH 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, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, sowie mit europäischen und internationalen Organisationen zur Stärkung der Resilienz von Versorgungsketten gegen Cyberangriffe?
23. Welche Rolle spielen private Unternehmen der Ernährungswirtschaft, Agrarbetriebe und Verbände in den Sicherheitskooperationen des BMLEH?
24. Welche Maßnahmen ergreift das BMLEH ggf., um die Resilienz seiner besonders sensiblen Systeme trotz möglicher Personalknappheit im Bereich IT-Sicherheit sicherzustellen?
25. Inwiefern beteiligt sich das BMLEH an europäischen oder internationalen Organisationen im Hinblick auf den Schutz von Patientendaten?
26. Plant die Bundesregierung, die IT-Sicherheitskapazitäten im BMLEH 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