

Kleine Anfrage

des Abg. Daniel Lindenschmid AfD

Konsequenzen aus dem Cyberangriff auf die Berliner Landesverwaltung für die Informationssicherheit in Baden-Württemberg

Ich frage die Landesregierung:

1. Welche Erkenntnisse aus dem im August 2026 bekannt gewordenen Cyberangriff auf die Berliner Landesverwaltung hat sie bislang auf ihre Bedeutung für Baden-Württemberg geprüft?
2. Welche konkreten Überprüfungen oder Schutzmaßnahmen wurden daraufhin veranlasst (bitte mit Angabe des Datums)?
3. Welche Hinweise liegen ihr darauf vor, dass bei dem Berliner Vorfall auch Daten, Zugangsdaten oder vertrauliche Unterlagen mit Bezug zu Behörden, Beschäftigten oder Einrichtungen Baden-Württembergs abgefließen sind?
4. Bei wie vielen Behörden der unmittelbaren Landesverwaltung wurden seit dem 1. Januar 2024 unabhängige Informationssicherheitsprüfungen durchgeführt (bitte nach Ressort, Einstufung und Dauer seit Feststellung zusammengefasst darstellen, ohne technisch ausnutzbare Einzelheiten offenzulegen)?
5. Wie wird bei IT-Systemen, die Landesbehörden außerhalb des Betriebs der BITBW selbst oder durch externe Dienstleister betreiben lassen, die Einhaltung einheitlicher Sicherheitsanforderungen kontrolliert?
6. Welcher Anteil der administrativen Konten und der für externe Zugriffe auf Verwaltungsnetze vorgesehenen Konten ist durch Mehrfaktor-Authentifizierung geschützt (bitte nach Ressort und Kontenkategorie zusammengefasst darstellen)?
7. Für welchen Anteil der als kritisch eingestuften IT-Dienste der unmittelbaren Landesverwaltung bestehen vom Produktivsystem ausreichend getrennte und gegen nachträgliche Veränderung geschützte Datensicherungen, deren Wiederherstellung innerhalb der vergangenen zwölf Monate erfolgreich praktisch getestet wurde?
8. Für welche zeitkritischen Verwaltungsleistungen, insbesondere die Bewilligung und Auszahlung existenzsichernder Leistungen, bestehen nach ihrer Kenntnis erprobte Ersatzverfahren für einen mehrtägigen IT-Ausfall?
9. Welche verbindlichen Verfahren bestehen, um bei einem vermuteten Datenabfluss betroffene Personen zu identifizieren und zu informieren?
10. Welche Konsequenzen hat sie aus den Feststellungen des Rechnungshofs zur Informationssicherheit an Hochschulen in Drucksache 18/325 gezogen, insbesondere hinsichtlich Datensicherungen und der zum Prüfungszeitpunkt noch ausstehenden Vereinbarung zwischen dem zuständigen Ressort und der Cybersicherheitsagentur?

8.10.2026

Lindenschmid AfD

Begründung

Der im August 2026 bekannt gewordene Cyberangriff auf Teile der Berliner Landesverwaltung führte zur zeitweisen Trennung betroffener Senatsverwaltungen vom Landesnetz und zu Einschränkungen wichtiger Verwaltungsleistungen, darunter der Beantragung und Auszahlung von Wohngeld. Anfang September wurde über die Veröffentlichung gestohlener Verwaltungsdaten berichtet. Der genaue Umfang und die Folgen des Datenabflusses waren weiterhin Gegenstand der Aufklärung. Der Vorfall verdeutlicht, dass sich staatliche Informationssicherheit nicht auf die Wiederherstellung ausgefallener Systeme beschränken darf. Ebenso entscheidend sind die Verhinderung von Datenabflüssen, der Schutz betroffener Personen und die Aufrechterhaltung zeitkritischer Verwaltungsleistungen. Auch in Baden-Württemberg besteht konkreter Prüfbedarf. Der Rechnungshof hat in Drucksache 18/325 für den untersuchten Hochschulbereich Defizite der Informationssicherheit beschrieben. Hierzu zählen Fälle, in denen auch Datensicherungen verschlüsselt wurden, sowie eine zum Prüfungszeitpunkt noch nicht abgeschlossene Vereinbarung zur Zusammenarbeit mit der Cybersicherheitsagentur. Die Kleine Anfrage soll klären, welche überprüfbaren Schutzvorkehrungen bestehen, welche Mängel noch nicht behoben sind und wer deren Beseitigung bis wann verantwortet. Technisch ausnutzbare Angaben zu einzelnen Systemen oder Sicherheitslücken werden nicht begehrt.