Landtag von Baden-Württemberg **Drucksache 18 / 665**

18. Wahlperiode **8.10.2026**

Kleine Anfrage

des Abg. Daniel Lindenschmid AfD

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Europa

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

Kleine Anfrage

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 abgeflossen 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?

Eingegangen: 8.10.2026 / Ausgegeben: 12.11.2026

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

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.

Antwort

Mit Schreiben vom 5. November 2026 Nr. IM4-0141.0-6/4/27 beantwortet das Ministerium des Inneren, für Digitalisierung und Europa im Einvernehmen mit dem Staatsministerium, dem Ministerium für Finanzen, dem Ministerium für Kultus, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Handwerk und Tourismus, dem Ministerium für Soziales, Arbeit und Gesundheit, dem Ministerium der Justiz und für Migration, dem Ministerium für Verkehr, dem Ministerium für Ländlichen Raum, Landwirtschaft und Heimat und dem Ministerium für Landesentwicklung und Wohnen die Kleine Anfrage wie folgt:

1. Welche Erkenntnisse aus dem im August 2026 bekannt gewordenen Cyberangriff auf die Berliner Landesentwicklung 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 Behören, Beschäftigten oder Einrichtungen Baden-Württembergs abgeflossen sind?

Die Fragen 1, 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Unmittelbar nach Bekanntwerden des Vorfalls am 17. August 2026 wurden auf Veranlassung des Innenministeriums die IT Baden-Württemberg (BITBW) und die Cybersicherheitsagentur Baden-Württemberg (CSBW) in Rufbereitschaft versetzt, um im Falle einer zu diesem Zeitpunkt nicht auszuschließenden Ausbreitung des Angriffs über die Netze des Bundes entsprechende Schutzmaßnahmen zu jeder Zeit umsetzen zu können. Das technische Monitoring der Netzknoten und Firewalls durch die BITBW wurde ausgeweitet.

Parallel dazu wurden vonseiten des Innenministeriums und in Koordination mit der CSBW umfassende, rechenzentrumsübergreifende technische Überprüfungen im Landesverwaltungsnetz initiiert. Diese wurden fortlaufend – auch über die Wochenenden – wiederholt und entsprechend neu eingegangener technischer Indikatoren angepasst. Die Rechenzentrumsbetreiber, zuvorderst die BITBW und das Landeszentrum für Datenverarbeitung (LZfD), erstatteten laufend Bericht über den Status der Untersuchungen. Zu keinem Zeitpunkt lagen Anzeichen vor, dass die Systemlandschaft der Landesverwaltung Baden-Württemberg von dem Angriff betroffen ist. Weitergehende Informationen zu den technischen Überprüfungen können nicht mitgeteilt werden, da diese potentiellen Angreifern Rückschlüsse auf die in der Landesverwaltung eingesetzten Schutzmaßnahmen und Technologien ermöglichen können.

Die CSBW hat im Verlauf des Vorfalls stetig das Cyber-Lagebild fortgeschrieben und mögliche Risiken für Baden-Württemberg bewertet. Dabei stand sie im stetigen Austausch mit dem Nationalen Cyber-Abwehrzentrum (NCAZ) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Diese Bewertung umfasste neben technischen Aspekten auch Risiken im Zusammenhang mit gemeinsam genutzten Daten und Zugriffsberechtigungen vor dem Hintergrund der im Zuge des Angriffs abgeflossenen und veröffentlichten 1,4 Millionen Dateien aus den Berliner Systemen.

Da nicht ausgeschlossen werden konnte, dass in den veröffentlichten Daten auch Bezüge zu Baden-Württemberg enthalten sind, wurden allen Ressorts von der CSBW erste Handlungsempfehlungen und Sensibilisierungsinformationen für die Mitarbeitenden übermittelt. Zur Bewertung der abgeflossenen Daten und möglicher Implikationen für Baden-Württemberg steht die CSBW in engem Austausch mit dem BSI. Bisher konnten eine zweistellige Zahl an Dateien identifiziert und heruntergeladen werden, die Hinweise darauf geben, dass auch Informationen mit Bezug zu Baden-Württemberg beinhaltet sind. Die CSBW informierte umgehend die jeweils zuständigen Landesministerien und bot ihre Unterstützung für weitere erforderliche Schritte an. Außerdem übermittelte die CSBW den Datei-Index sowohl dem Landeskriminalamt Baden-Württemberg (LKA) als auch dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV) für eigene Auswertungen.

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?

Die Fragen 4 und 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Gemäß den Vorgaben der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) steuern die Ressorts in eigener Verantwortung die Prozesse ihrer jeweiligen Informationssicherheitsmanagementsysteme (ISMS).

In der folgenden Tabelle sind die von den Ressorts in eigener Hoheit und unabhängig von der BITBW durchgeführten Informationssicherheitsüberprüfungen aufgeführt. Einzelne Meldungen, dass keine „unabhängigen“ Prüfungen stattfinden, schließen nicht aus, dass intern eigenverantwortete Prüfungen erfolgen.

Bei der BITBW selbst werden regelmäßig verschiedene Audits und Überprüfungen nach Maßgabe der Standards des BSI durchgeführt. Dies auch vor dem Hintergrund, dass wesentliche Betriebsabschnitte der BITBW Teil von BSI-zertifizierten Verbünden sind. Diese Überprüfungen entfalten unmittelbar Wirkung auf die an das Landesverwaltungsnetz angeschlossenen Stellen und damit auf die Ressorts der Landesverwaltung. Neben Informationssicherheitsprüfungen werden bei der BITBW regelmäßig technische Prüfungen durchgeführt, die auch die CSBW begleitet.

Ressort	**Durchgeführte unabhängige Informationssicherheitsprüfungen**
Staatsministerium	Das Staatsministerium nutzt die Dienste der BITBW und führt daher in diesem Bereich keine zusätzlichen Informationssicherheitsprüfungen durch. Soweit ein Verfahren nicht bei der BITBW betrieben wird, wurden bereits separate Sicherheitsprüfungen durchgeführt.
Ministerium des Inneren, für Digitalisierung und Europa	Im Geschäftsbereich des Innenministeriums werden seit 2024 fortlaufend Audits nach BSI IT-Grundschutz durch unabhängige externe Auditoren durchgeführt. Als Anschlussstelle an die Infrastruktur der Bundesverwaltung wird die BITBW jährlich zusätzlich gesondert für die Netze des Bundes auditiert. Die Polizei führt eigene Audits in allen 17 Polizeidienststellen und Einrichtungen durch. Außerdem finden jährliche Audits der EU-Zahlstellen in den Regierungspräsidien statt.
Ministerium für Finanzen	Im Geschäftsbereich des Finanzministeriums in der Oberfinanzdirektion Baden-Württemberg (OFD BW) wurden seit dem 1. Januar 2024 14 interne Audits durchgeführt. Dabei wurde der Umsetzungsstand der Anforderungen des BSI von einem beauftragten unabhängigen Auditor geprüft. Die OFD BW erbringt außerdem Dienstleistungen für die EU-Zahlstelle BW. Im Rahmen der Zertifizierung der EU-Zahlstelle BW nach ISO 27001 auf der Basis von IT-Grundschutz wurden auch die von der OFD BW erbrachten Dienstleitungen im Rahmen der jährlichen Zertifizierungs- bzw. Überwachungsaudits geprüft. Es fanden ebenfalls jährliche Dienstleisteraudits des Landwirtschaftsministeriums bei der OFD BW statt.
Ministerium für Kultus	Unabhängige Informationssicherheitsprüfungen (= Third-Party Security Assessments oder externe Audits) wurden in der Kultusverwaltung bisher nicht durchgeführt.
Ministerium für Wissenschaft, Forschung und Kunst	Sowohl das Wissenschaftsministerium als auch die Einrichtungen der unmittelbaren Landesverwaltung im Geschäftsbereich des Wissenschaftsministeriums setzen den BSI IT-Grundschutz gemäß den Vorgaben der VwV Informationssicherheit um. Innerhalb dieses Rahmenwerks werden IT-Systeme und Verfahren fortlaufend – teilweise auch unabhängig – geprüft.
Ministerium für Umwelt, Klima und Energiewirtschaft	Im Geschäftsbereich des Umweltministeriums (Ministerium, Landesanstalt für Umwelt Baden-Württemberg und Nationalpark Schwarzwald) wurden interne (durch die jeweiligen Dienststellen-CISO oder durch die Ressort-CISO) und externe Informationssicherheitsüberprüfungen durchgeführt.
Ministerium für Wirtschaft, Handwerk und Tourismus	Das Wirtschaftsministerium nutzt die Dienste der BITBW. Im Wirtschaftsministerium wurden keine von der BITBW unabhängigen Informationssicherheitsprüfungen durchgeführt.
Ministerium für Soziales, Arbeit und Gesundheit	Das Sozialministerium nutzt hauptsächlich die Dienste der BITBW und führt daher in diesem Bereich keine eigenen Informationssicherheitsprüfungen durch. Informationssicherheitsüberprüfungen werden für alle anderen Fachverfahren durch einen externen Dienstleister durchgeführt.

Ressort	Durchgeführte unabhängige Informationssicherheitsprüfungen
Ministerium der Justiz und für Migration	Im Geschäftsbereich des Justizministeriums wurden seit dem 1. Januar 2024 unabhängige Informationssicherheitsprüfungen durchgeführt, die ressortweite Dienste und somit alle Justizbehörden des Ressorts betrafen.
Ministerium für Verkehr	Im Verkehrsministerium wurden keine von der BITBW unabhängigen Informationssicherheitsprüfungen durchgeführt.
Ministerium für Ländlichen Raum, Landwirtschaft und Heimat	Im Landwirtschaftsministerium selbst erfolgt seit 2016 eine jährliche Auditierung/Rezertifizierung der EU-Zahlstelle BW nach ISO 27001 auf Basis BSI IT-Grundschutz. Im Geschäftsbereich des Landwirtschaftsministeriums (Ministerium und nachgeordneten Dienststellen) werden die folgenden unabhängigen Prüfungen durchgeführt: • Seit 2022 wird kontinuierlich ein Webcheck der aus dem Internet erreichbaren Anwendungen im MLR-Ressort durchgeführt. • Seit 2024 werden alle in Entwicklung und Betrieb befindlichen Apps für iOS und Android kontinuierlich überprüft. • Entsprechend eines Prüfplans werden regelmäßig ausführliche Pen-Tests der IT-Fachverfahren durch Externe im Ressortbereich durchgeführt.
Ministerium für Landesentwicklung und Wohnen	Das Ministerium für Landesentwicklung und Wohnen nutzt die Dienste der BITBW und führt daher in diesem Bereich keine zusätzlichen Informationssicherheitsprüfungen durch. Soweit ein Verfahren nicht bei der BITBW betrieben wird, werden separate Sicherheitsüberprüfungen durchgeführt.

Landesbehörden außerhalb des Betriebs der BITBW, die IT-Systeme selbst oder durch externe Dienstleister betreiben, sind, soweit sie im Geschäftsbereich der jeweiligen Landesministerien liegen, unter obenstehender Tabelle subsumiert. Auch sie unterliegen den Landes-Vorgaben an Informationssicherheit und müssen daher entsprechende Maßnahmen umsetzen.

Generell wird in der Landesverwaltung im Falle von Beauftragungen externer Dienstleister das Einhalten der vorgegebenen Sicherheitsanforderungen über vertragliche Regelungen im Rahmen der Beauftragung als auch durch die Forderung zur Vorlage eines BSI-konformen Informationssicherheitskonzeptes für das extern betriebene IT-System kontrolliert. Der Nachweis eines entsprechenden BSI-Zertifikats und die Durchführung von Audits wird ebenfalls regelmäßig zur Kontrolle der Einhaltung der Sicherheitsanforderungen verwendet. Eine weitere Maßnahme, die von den Ressorts und von der CSBW zur Absicherung extern betriebener IT-Systeme genutzt wird, ist die Durchführung von Pen-Tests und Schwachstellen-Scans (OSINT-Scans).

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)?

Informationen zu der Absicherung externer Zugriffe auf Systeme im Landesverwaltungsnetz durch Mehrfaktor-Authentifizierung, auch in kumulierter Form, können nicht zur Verfügung gestellt werden, da diese potenziellen Angreifern Rückschlüsse auf die in der Landesverwaltung eingesetzten Schutzmaßnahmen ermöglichen können.

Generell ergibt sich über die Umsetzung der Vorgaben der VwV Informationssicherheit und damit der Standards des BSI IT-Grundschutz über den Baustein „ORP.4 Identitäts- und Berechtigungsmanagement“ die Anforderung, Benutzerkennungen mit weitreichenden Berechtigungen mit einer Mehrfaktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token abzusichern. Hierzu zählen auch administrative externe Zugänge.

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?

Zeitkritische Verwaltungsverfahren der Ressorts werden in der Regel bei der BITBW betrieben. Bei der BITBW erfolgen Datensicherungen und Wiederherstellungsübungen nach den Vorgaben des relevanten BSI IT-Grundschutz-Bausteins „CON.3 Datensicherungskonzept“. Dieser Baustein enthält die grundlegenden Vorgaben zur Planung, Durchführung und Kontrolle von Datensicherungen, wie Datensicherungspläne, sichere Aufbewahrung getrennt von den gesicherten IT-Systemen, Schutz der Datensicherungen vor unbefugtem Zugriff und unbeabsichtigtem Überschreiben und auch Übungen zur Wiederherstellung. Ressorts, die eigenverantwortlich zeitkritische Verwaltungsverfahren betreiben, unterliegen denselben Vorgaben.

8. Für welche zeitkritischen Verwaltungsleistungen, insbesondere die Bewilligung und Auszahlung existenzsichernder Leistungen, bestehen nach ihrer Kenntnis erprobte Ersatzverfahren für einen mehrtägigen IT-Ausfall?

Im Geschäftsbereich des Ministeriums für Finanzen sind die für die Auszahlung erforderlichen Systeme des Rechnungswesens und des Zahlungsverkehrs redundant vorgehalten. Sollte es trotz aller umfangreichen Sicherheitsmaßnahmen zu mehrtägigen Ausfällen dieser Systeme kommen, besteht über die Landesoberkasse Baden-Württemberg (LOK BW) die Möglichkeit, Zahlungen manuell zu veranlassen.

Im Geschäftsbereich des Ministeriums für Landesentwicklung und Wohnen erfolgt die Bearbeitung von Wohngeldanträgen durch die kommunalen Wohngeldbehörden samt Bewilligungsbescheid und Veranlassung der Auszahlung an die berechtigten Haushalte landeseinheitlich im IT-Fachverfahren beim kommunalen IT-Dienstleister Komm.ONE. Die Auszahlung selbst erfolgt wiederum über eine IT-Schnittstelle zur LOK BW. Um die Funktionsfähigkeit des Wohngeldfachverfahrens auch bei einem mehrtägigen IT-Ausfall aufrechterhalten zu können, wurden nach Auskunft von Komm.ONE entsprechende Notfallkonzepte und Verfahrensweisen etabliert und erfolgreich erprobt. Die Daten für das wohngeldrechtliche Fachverfahren DiWo – inklusive der Online-Antragstellung, der Wohngeldberechnung und der Schnittstelle zur LOK BW für die Auszahlungen – werden permanent und mehrfach gesichert. Sie liegen vollständig redundant vor. In Übereinstimmung mit den vertraglichen Vereinbarungen mit dem Land führt die Komm.ONE als Fachverfahrensbetreiberin zudem regelmäßig Testzahlläufe durch. Die bestehenden Sicherungskonzepte garantieren insbesondere in Bezug auf die Schnittstelle zur LOK BW die fortlaufende Auszahlung des Wohngeldes für Bestandsfälle. Für die Durchführung der Zahlläufe und die Übertragung der Zahlungsdaten zur LOK BW hält die Komm.ONE mehrere voneinander getrennte Systeme vor.

Der Online-Wohngeldantrag ist in Baden-Württemberg auf unterschiedlichen Plattformen implementiert. Eingehende Anträge werden sicher gespeichert und im Schadensfall zu einem späteren Zeitpunkt weitergeleitet und verarbeitet. Für Neuanträge besteht bei den Wohngeldbehörden die Möglichkeit der formlosen und vom Onlineantrag losgelösten Antragstellung. Damit wird die Frist zur rückwirkenden Wohngeldauszahlung nach Bewältigung eines etwaigen Cyberangriffs vollumfänglich gewahrt.

Über das Wohngeldfachverfahren „DiWo“ hinaus greifen im Falle eines Cyberangriffs die allgemeinen Betriebskonzepte und das Krisenmanagement des IT-Dienstleisters Komm.ONE.

Im Bereich der Leistungen nach dem SGB II unterscheidet sich die Handhabung und Ausgestaltung bei einem mehrtägigen IT-Ausfall grundlegend nach der jeweiligen Organisationsform der Jobcenter – den zugelassenen kommunalen Trägern (zkT) und den gemeinsamen Einrichtungen (gE).

Die Sicherstellung zeitkritischer Verwaltungsleistungen im Rahmen des SGB II – insbesondere die Bewilligung und unterbrechungsfreie Auszahlung existenzsichernder Leistungen zur Sicherung des Lebensunterhalts sowie der Bedarfe für Unterkunft und Heizung – besitzt in beiden Organisationsformen im Fall von IT-Störungen höchste Priorität. Die IT-Infrastruktur der zkT liegt im Rahmen der Organisationhoheit eigenverantwortlich bei den Stad- und Landkreisen bzw. deren kommunalen IT-Dienstleistern. Hiervon unabhängig sind die Systeme der Bundesagentur für Arbeit. Für den Fall eines IT-Ausfalls in den gE gelten die zentralen Notfall- und Katastrophenschutzkonzepte der Bundesagentur für Arbeit.

Der Bereich der Sozialhilfe nach dem SGB XII und der Eingliederungshilfe nach Teil 2 des SGB IX liegt ebenfalls eigenverantwortlich in der Organisationhoheit der Stadt- und Landkreise bzw. deren kommunalen IT-Dienstleistern.

Überdies bestehen seitens der Landesministerien keine weiteren zeitkritischen Verwaltungsleistungen zur Bewilligung und Auszahlung existenzsichernder Leistungen im Sinn der Fragestellung.

9. Welche verbindlichen Verfahren bestehen, um bei einem vermuteten Datenabfluss betroffene Personen zu identifizieren und zu informieren?

Gemäß Artikel 34 DSGVO besteht für Verantwortliche die Pflicht, bei hohem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen diese unverzüglich über den Vorfall zu informieren. In den Ressorts sind entsprechende Verfahren nach den Vorgaben des Artikels 34 DSGVO etabliert. Danach wird eine Verletzung des Schutzes personenbezogener Daten unverzüglich und innerhalb der gesetzlichen Fristen der zuständigen Aufsichtsbehörde gemeldet und in Fällen mit hohem Risiko zusätzlich die betroffenen Personen benachrichtigt.

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?

Der in Drucksache 18/325 enthaltene Auszug aus dem Jahresbericht 2026 zur Haushaltsrechnung 2024, Beitrag 25, bezieht sich auf Empfehlungen des Rechnungshofs zur Informationssicherheit der Hochschulen in Baden-Württemberg. Diese waren Gegenstand von Beratungen des Ausschusses für Finanzen vom 24. September 2026. In der Sitzung des Finanzausschusses wurde der Anregung des Rechnungshofs für eine Beschlussempfehlung des Ausschusses an das Plenum einstimmig zugestimmt. Sie sieht u. a. eine Berichtspflicht des Wissenschaftsministeriums zum 30. September 2027 vor. Vorbehaltlich der noch ausstehenden Entscheidung des Landtags geht das Wissenschaftsministerium davon aus, dass ihm eine Berichtspflicht bis zum 30. September 2027 obliegt.

Das Wissenschaftsministerium wird dem Landtag innerhalb der von ihm gesetzten Frist berichten, welche Konsequenzen aus den Empfehlungen des Rechnungshofs gezogen wurden, auch in Hinblick auf die vom Rechnungshof angeregte Vereinbarung mit der CSBW.

In Vertretung

Kemmer

Ministerialdirektorin