Landtag von Baden-Württemberg **Drucksache 18 / 325**

18. Wahlperiode **16.7.2026**

Mitteilung

des Rechnungshofs

Jahresbericht 2026 zur Haushaltsrechnung 2024 (vgl. Drucksache 18/300)

hier: Beitrag Nr. 25 – Informationssicherheit an den Hochschulen in Baden-Württemberg (Kapitel 1426 bis 1464, 1468 und 1470 bis 1477)

Anlage zum Schreiben des Rechnungshofs vom 16. Juli 2026, Az.: RHP3-0451.1-25/3/3:

Die Hochschulen des Landes waren in den vergangenen Jahren mehrfach Ziel von Cyberangriffen. Zur Abwehr bedarf es wirksamer Informationssicherheitsmanagementsysteme. Die überwiegend dezentralen Strukturen der Hochschul-IT sind nur bedingt geeignet, diesen Anforderungen gerecht zu werden. Mit einer stärkeren Zentralisierung insbesondere von IT-Basisdiensten und mehr Kooperation sowohl zwischen den Hochschulen als auch mit anderen Akteuren der Informationssicherheit könnte den wachsenden Herausforderungen begegnet werden.

25.1 Ausgangslage

Die Bedrohungslage für die IT-Systeme des Landes hat sich in den vergangenen Jahren erheblich verschärft – dies gilt auch für die Hochschulen. Angreifer agieren heute hochgradig professionalisiert, arbeitsteilig und werden in zunehmendem Maß durch staatliche oder staatsnahe Akteure aus dem Ausland unterstützt. Hochschulen stehen als Zentren für Spitzenforschung und Innovation besonders im Fokus.

Die Hochschulen in Baden-Württemberg verarbeiten zahlreiche sensible Daten, z. B. Forschungsinhalte oder personenbezogene Daten von Studierenden oder Mitarbeitenden. In jüngster Vergangenheit gab es bei den Hochschulen mehrere durch Cyberangriffe verursachte Sicherheitsvorfälle. Bei diesen Sicherheitsvorfällen mussten die wissenschaftlichen Institutionen teilweise über Wochen hinweg

Eingegangen: 16.7.2026 / Ausgegeben: 12.8.2026

vollständig vom Netz genommen werden. Es kam zu starken Beeinträchtigungen der Aufgabenwahrnehmung der Hochschulverwaltung sowie in der Forschung und Lehre. Zur Wiederaufnahme des Dienstbetriebs musste teilweise die komplette IT-Infrastruktur neu aufgebaut werden.

Die Prüfung des Rechnungshofs erstreckte sich auf die Duale Hochschule, die Pädagogischen Hochschulen, die Hochschulen für angewandte Wissenschaften sowie die Musik- und Kunsthochschulen. Die Universitäten waren nicht Gegenstand der Prüfung.

25.2 Prüfungsergebnisse

25.2.1 Informationssicherheitsmanagementsysteme an Hochschulen

Informationssicherheit ist eine Daueraufgabe. Geänderte Aufgaben und Prozesse, ein Wandel der gesetzlichen Rahmenbedingungen, neue Technik, aber auch bislang unbekannte Schwachstellen und daraus erwachsende Gefährdungen stellen immer wieder neue Anforderungen an die Informationssicherheit dar. Sie ist insoweit ein Prozess, der kontinuierlich überprüft und angepasst werden muss.

Für den Schutz von Informationen in den behördlichen Strukturen des Landes ist die Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) von besonderer Bedeutung. Mit ihr wurde 2017 ein wesentlicher Grundstein gelegt, um ein umfassendes Informationssicherheitsmanagementsystem (ISMS) in der Landesverwaltung zu etablieren. Sie definiert Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen für einen Informationssicherheitsmanagementprozess und verpflichtet die Landesbehörden, ihre Prozesse im Hinblick auf die Informationssicherheit zu überprüfen, anzupassen und das ISMS an den IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auszurichten.

Die Hochschulen des Landes wenden die VwV Informationssicherheit an. Um den steigenden Anforderungen an die Resilienz und Compliance gerecht zu werden, bauten sie in den vergangenen Jahren wesentliche Strukturen eines ISMS auf. Allerdings unterscheiden sich Hochschulen in ihren gesetzlichen Aufgaben und mit Blick auf die Freiheit von Forschung und Lehre wesentlich von anderen Landesbehörden in Baden-Württemberg. Sie verfügen nur teilweise über klassische behördliche Strukturen und Hierarchien, was die Etablierung eines ISMS erheblich erschwert. Die ISMS der Hochschulen sind deshalb noch nicht durchgehend wirksam; in den Bereichen Strategie, Personal, Sicherheitskonzeption sowie in der Detektion und Reaktion auf Sicherheitsvorfälle bestehen Verbesserungspotenziale.

25.2.2 Einsatz von Personal aus Forschung und Lehre innerhalb der Informationssicherheit

Das BSI definiert als Basis-Anforderung an ein ISMS, dass Informationssicherheitsbeauftragte zu benennen sind. Der Haushaltsgesetzgeber hat dem Wissenschaftsressort 58 Stellen in der Entgeltgruppe 13 bereitgestellt, um Beauftragte für Informationssicherheit an den Hochschulen bestellen zu können. Darin enthalten sind 12 Stellen für ein „Kernteam“, das an den Standorten in Reutlingen (für die Hochschulen) und in Heidelberg (für die Universitäten) zentrale Maßnahmen der Informationssicherheit durchführt.

Nach einer Umfrage des Rechnungshofs werden an neun Hochschulen zusätzlich Personen aus Forschung und Lehre eingesetzt, um Aufgaben und Funktionen des ISMS zu erfüllen. Diese Hochschulen gewähren dafür eine Ermäßigung auf das Lehrdeputat. In mindestens einem Fall erfolgt die Übernahme der Funktion des Informationssicherheitsbeauftragten durch Lehrpersonal.

Eine dauerhafte Übernahme von Aufgaben sowie Funktionen innerhalb des ISMS durch Lehrpersonen kann problematisch sein, wenn dadurch die Aufgabenerfüllung in Forschung und Lehre beeinträchtigt wird. Die Wahrnehmung dieser Funktion sollte grundsätzlich durch die dafür zur Verfügung stehenden Stellen abgedeckt werden.

25.2.3 Sicherheitsvorfälle

Ein Sicherheitsvorfall ist nach der Verordnung des Innenministeriums zur Verbesserung der Cybersicherheit in Baden-Württemberg (Cybersicherheitsverordnung – CSVO) „ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder Dienste, die über Informationstechnik angeboten werden oder zugänglich sind, beeinträchtigt." In der Umfrage gaben mehr als zwei Drittel der Hochschulen an, seit 2022 von mindestens einem Sicherheitsvorfall gemäß der Begriffsbestimmung der CSVO betroffen gewesen zu sein.

Am häufigsten traten Malware-Infektionen auf, die mittels Phishing verbreitet wurden. In einigen Fällen kam es zu gezielten Hackerangriffen, über die Ransomware eingeschleust wurde. An einigen Hochschulen wurde dadurch der komplette Datenbestand inklusive Backup verschlüsselt. In einem Fall haben Angreifer im Darknet Zugangsdaten zu einer Hochschule erworben, die durch einen Phishing-Angriff abgegriffen wurden, und erlangten dadurch Zugriff auf das Campusnetz.

Teils meldeten sich die Angreifer anschließend bei den betroffenen Hochschulen und boten gegen Lösegeldzahlungen in Kryptowährungen die Herausgabe des Schlüssels bzw. die Entschlüsselung des Datenbestandes an. In einigen Fällen führten die Angriffe zum Totalverlust des Datenbestandes, was einen kompletten Neuaufbau der IT-Infrastruktur erforderlich machte. Dem Rechnungshof ist kein Fall bekannt, bei dem die Hochschulen auf Forderungen nach Lösegeld eingegangen sind.

25.2.4 Kooperationsverbund bwInfoSec

Um den steigenden Anforderungen an die Informationssicherheit gerecht zu werden, entwickelten Hochschulen und Wissenschaftsministerium 2018 gemeinsam das „Rahmenkonzept Informationssicherheit". Die dort definierten Maßnahmen sollen zu einer wesentlichen und dauerhaften Verbesserung der Informationssicherheit an den Hochschulen führen. Dazu gehört unter anderem die Gründung des Kooperationsverbundes „bwInfoSec", der Synergien im Hochschulbereich erzeugen und die Cyber-Resilienz der akademischen Einrichtungen festigen soll.

Der Kooperationsverbund besteht im Wesentlichen aus Vertretern des Wissenschaftsministeriums und der Hochschulen. Operatives Zentrum der bwInfoSec ist das Kernteam Informationssicherheit. Dieses bündelt zentrale Aufgaben für die Hochschulen, stellt Dienste wie beispielsweise das ISMS-Tool zur Dokumentation und Abbildung des ISMS bereit und bietet entsprechende Beratungen an.

25.2.5 Cybersicherheitsagentur Baden-Württemberg

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) wurde mit Inkrafttreten des Cybersicherheitsgesetzes am 17. Februar 2021 gegründet und ist seit dem 1. Januar 2022 als eigenständige Landesoberbehörde tätig. Zum 1. Juli 2022 hat sie das Computer Emergency Response Team (CERT BWL) von der Landesoberbehörde IT Baden-Württemberg (BITBW) übernommen. Die CSBW nimmt mit dem CERT BWL eine Schlüsselrolle in der Cybersicherheit im Land ein; sie bietet u. a. einen Warn- und Informationsdienst an und gibt Handlungsempfehlungen.

Die Hochschulen sind an den Warn- und Informationsdienst der CSBW angebunden. In Krisenfällen ist das CERT BWL eine der ersten Anlaufstellen für betroffene Dienststellen. Darüber hinaus bietet die CSBW den Hochschulen

diverse präventive Angebote an. In den vergangenen Jahren hat die CSBW mit dem CERT BWL die Hochschulen bei der Behandlung von Sicherheitsvorfällen und sicherheitskritischen Ereignissen unterstützt.

Die Rolle und das Vorgehen der CSBW bei der Vorfallbehandlung wird bei den betroffenen Hochschulen durchweg positiv bewertet. Die CSBW konnte schnell und wirksam Erstmaßnahmen einleiten und dadurch die Hochschulen unterstützen. Die Zusammenarbeit mit der CSBW und weiteren Beteiligten (u. a. Landeskriminalamt, Landesamt für Verfassungsschutz) während der Krisensituation habe, so die übereinstimmende Meinung der Hochschulen, gut funktioniert.

Das Cybersicherheitsgesetz Baden-Württemberg definiert die Aufgaben der CSBW und regelt die Zusammenarbeit mit den öffentlichen Stellen. In § 2 Absatz 2 Satz 2 sieht das Gesetz vor, dass für Stellen des Landes mit Sonderstatus – zu denen die Hochschulen gehören – einvernehmlich gesonderte Vereinbarungen zwischen der CSBW und der jeweils zuständigen obersten Landesbehörde getroffen werden. Der Abschluss einer solchen Vereinbarung, mit der die Zusammenarbeit auf operativer, strategischer und taktischer Ebene ausgestaltet werden sollte, war für 2024 vorgesehen, ist aber bislang nicht erfolgt.

Zur klaren Abgrenzung der Aufgaben und Befugnisse sollte diese Vereinbarung schnellstmöglich geschlossen werden. Dann könnten Doppelarbeiten vermieden und das Hochschul-ISMS zielgerichtet weiterentwickelt werden. Zudem könnte geregelt werden, ob die Hochschulen weitere Leistungen der CSBW, beispielsweise bei der Netzwerküberwachung, nutzen können.

25.2.6 Schatten-IT

Bei rund 70 % der Hochschulen ist bekannt oder zumindest wahrscheinlich, dass es IT-Systeme, Software oder Cloud-Dienste gibt, die von Fakultäten oder Instituten ohne Wissen oder Freigabe der zentralen IT-Abteilung eingesetzt werden. Diese sogenannte „Schatten-IT“ stellt eine erhebliche Gefahr für die Informationssicherheit an Hochschulen dar.

Schatten-IT entsteht oft, weil IT-Lösungen nicht schnell genug bereitgestellt werden können oder deren Funktionsumfang unzureichend ist. Diese Anforderungen können die Hochschulen angesichts eines in der Regel dezentralen IT-Betriebs jedoch häufig nicht erfüllen. Ein breiteres Produktportfolio und schnellere Bereitstellungszeiten könnten erreicht werden, wenn Hochschulen stärker kooperieren und IT-Dienste zentralisiert werden.

25.2.7 Stärkung der Informationssicherheit durch zentrale IT-Dienste

Die IT-Infrastruktur an den Hochschulen in Baden-Württemberg ist sehr heterogen. Zwar werden teilweise Dienste von einer Hochschule bereitgestellt und von mehreren Hochschulen genutzt. Dies gilt beispielsweise für E-Mail-Services. Beim Identitätsmanagement[1] und bei der Bereitstellung und Nutzung von Infrastrukturdiensten[2] gibt es ebenfalls bereits Kooperationen zwischen den Hochschulen und den Universitäten, die vom Wissenschaftsministerium unterstützt werden.

Derzeit betreiben fast alle Hochschulen weitere ressourcenintensive Basis-Dienste, kritische Fachanwendungen und Endgeräte in Eigenregie, d. h. fragmentiert in der Verantwortung der jeweiligen Hochschule. Dies bindet hochqualifiziertes Personal unnötig an Administrationsaufgaben. Vor allem aber können die dezentralen IT-Strukturen der Hochschulen den wachsenden Anforderungen der Informationssicherheit nicht mehr gerecht werden. Einzelne Hochschulen verfügen weder

[1] https://www.bwidm.de/.

[2] https://bwcloud-os.de/.

über die personellen Ressourcen noch über das spezialisierte Know-how, um mit der technologischen Entwicklung auf Seiten der Angreifer Schritt zu halten. In Gesprächen mit Vertretern der Hochschulen zeigte sich mehrfach der Wunsch nach einer stärkeren Zentralisierung und hochschulübergreifenden Zusammenarbeit bei der IT.

Eine stärkere Zentralisierung der IT-Infrastruktur steht nicht im Widerspruch zur Hochschulautonomie. Im Gegenteil: Eine stärkere Zentralisierung und die damit einhergehende Professionalisierung des IT-Betriebs würde die Freiheit von Forschung und Lehre im digitalen Zeitalter fördern. Die vom Grundgesetz und durch § 3 LHG geschützte akademische Freiheit bezieht sich insbesondere auf Wissenschaft, Forschung, Kunst, Lehre und die inhaltliche Gestaltung des Studiums. Der Betrieb von IT-Basisdiensten (wie beispielsweise E-Mail-Servern, Netzwerk-Backbones, Speichersystemen oder dem Patch-Management von Betriebssystemen) ist lediglich eine administrative Unterstützungsleistung. Stärker zentralisierte IT-Dienste könnten dazu beitragen, die Hochschul-IT wirtschaftlicher zu gestalten und den Wissenschaftsbetrieb besser vor existenzgefährdenden Cyber-Risiken zu schützen.

25.3 Empfehlungen

25.3.1 Informationssicherheitsmanagementsystem weiterentwickeln

Die Hochschulen sollten ihre ISMS regelmäßig überprüfen und gezielt weiterentwickeln. Insbesondere durch Maßnahmen in den Bereichen Strategie, Personal, Sicherheitskonzeption sowie in der Detektion und Reaktion auf Sicherheitsvorfälle sollte der Reifegrad der ISMS gesteigert werden.

Die Hochschulen sollten Lehrpersonen nur dann dauerhaft für Aufgaben oder Funktionen des ISMS (beispielsweise als Informationssicherheitsbeauftragte) einsetzen, wenn die Aufgabenwahrnehmung in Forschung und Lehre dadurch nicht beeinträchtigt wird.

Das Wissenschaftsministerium sollte mit den Hochschulen und der CSBW eine Vereinbarung im Sinne des § 2 Absatz 2 Satz 2 des Cybersicherheitsgesetzes abschließen, um die Zusammenarbeit auf operativer, strategischer und taktischer Ebene zu konkretisieren.

25.3.2 Informationssicherheit durch zentrale IT-Dienste stärken

Das Wissenschaftsministerium sollte gemeinsam mit den Hochschulen und in Abstimmung mit dem Innenministerium (BITBW, CSBW) eine stärkere Zentralisierung der Hochschul-IT anstoßen. Hierzu sollte für die staatlichen Hochschulen – unter Berücksichtigung der bestehenden Angebote der IT der Landesverwaltung – eine übergreifende IT- und Rechenzentrumsstrategie entwickelt werden.

Mit Blick auf die operative Umsetzung sollte der Aufbau einer zentralen Einheit oder der Ausbau einer bestehenden Einheit für den zentralen IT-Betrieb erwogen werden.

Basis-Dienste wie Kommunikationslösungen (E-Mail, Messenger, Videokonferenz), Speicher- und Betriebssysteme sollten – unter Berücksichtigung der jeweils spezifischen Anforderungen – so umfassend wie möglich zentralisiert werden.

25.4 Stellungnahme des Ministeriums

Das Wissenschaftsministerium begrüßt die Empfehlungen des Rechnungshofs zur Weiterentwicklung der ISMS der Hochschulen und zur Stärkung der Informationssicherheit durch eine Zentralisierung von IT-Diensten.

Das Wissenschaftsministerium stimmt mit dem Rechnungshof darin überein, dass die Hochschulen als Zentren für Spitzenforschung und Innovation im besonderen Fokus von Cyberangriffen stehen. Daraus resultiere die Notwendigkeit, die Informationssicherheit der Hochschulen als stetig zu optimierende Daueraufgabe zu begreifen, auch wenn die besonderen Strukturen und Hierarchien an Hochschulen die Etablierung eines ISMS erschweren würden. Das Wissenschaftsministerium werde die Hochschulen zur kontinuierlichen Verbesserung des Reifegrads ihrer ISMS anhalten.

Das Wissenschaftsministerium stimmt mit dem Rechnungshof auch darin überein, dass eine dauerhafte Übernahme von Aufgaben sowie Funktionen innerhalb des ISMS durch Lehrpersonen nur dann möglich ist, wenn die Aufgaben in Forschung und Lehre dadurch nicht beeinträchtigt werden. Es sei allerdings darauf hinzuweisen, dass es bei einem Einsatz von wissenschaftlichen Fachvertreterinnen und -vertretern in der Informationssicherheit einer Hochschule zu sehr positiven Wechselwirkungen kommen könne.

Das Wissenschaftsministerium werde sich erneut darum bemühen, mit der Cybersicherheitsagentur eine Kooperationsvereinbarung abzuschließen und hoffe auf eine entsprechende Bereitschaft auf Seiten des Innenministeriums und der Cybersicherheitsagentur.

Darüber hinaus werde das Wissenschaftsministerium in Abstimmung mit dem Innenministerium eine stärkere Zentralisierung der Hochschul-IT anstoßen und die dazu notwendigen Diskussionen und Konzepte in den Hochschulgremien initiieren. Dabei werde genau zu prüfen sein, welche Dienste sich für eine Zentralisierung eignen und ob es Bereiche gibt, in denen eine Heterogenität der Ausgestaltung die Resilienz vor Angriffen stärker erhöht als eine Zentralisierung.

Neben der Prüfung des Aufbaus einer zentralen Einheit für den IT-Betrieb werde das Wissenschaftsministerium die Einrichtung eines Security Operation Center für den Hochschulbereich weiterverfolgen.