

Kurzbericht

öffentlicher Teil

11. Sitzung – Kultuspolitischer Ausschuss

26. Februar 2025 – 19:54 bis 20:47 Uhr

Anwesend:

Vorsitz: Kerstin Geis (SPD)

CDU

Patrick Appel
Sabine Bächle-Scholz
Hans Christian Göttlicher
Thomas Hering
Anna-Maria Schölch
Sebastian Sommer (Hochtaunus)
Frank Steinraths
Christian Wendel
Christin Ziegler (Schwalm-Eder)

AfD

Andreas Lobenstein
Lothar Mulch
Pascal Schleich
Heiko Scholz

SPD

Nina Heidt-Sommer
Sebastian Sack
Turgut Yüksel

BÜNDNIS 90/DIE GRÜNEN

Julia Herz
Torsten Leveringhaus
Daniel May
Katrin Schleenbecker

Freie Demokraten

Moritz Promny


Fraktionsassistentinnen und -assistenten:

CDU: Philipp Breiner
 AfD: Nils Krüger
 SPD: Anja Kornau
 BÜNDNIS 90/DIE GRÜNEN: Inga Winterberg

Landesregierung, Rechnungshof, etc.:

Name (bitte in Druckbuchstaben)	Amtsbezeichnung	Ministerium, Behörde
Julia Spohn	StR 'in	HMKB
Pascal Graf	ROR	HMKB
Stefan Steinseher	Wd. Dir.	LA
Christian Mecker	StD	LA
Benjamin Nabali	ROR	HMKB
Anja Reul	MR	HMKB
Christian Mahest	MR	HMKB

Armin Schwarz
 Dr. Manuel Lösel
 Nils Hektor

Minister
 Staatssekretär
 ROR

HMKB
 HMKB
 HKMB

Protokollierung: Hanns Otto Zinßer

1. Dringlicher Berichts Antrag
Fraktion BÜNDNIS 90/DIE GRÜNEN
Hinweise auf Datensicherheitsmängel beim Hessischen Schulportal
– Drucks. [21/1685](#) –

Minister **Armin Schwarz** teilt mit, er wolle Folgendes voranstellen. Das Schulportal Hessen sei die zentrale pädagogische Lern- und Arbeitsplattform des Landes Hessen, die allen Schulen zur Verfügung stehe. Aktuell seien mehr als 1,1 Millionen aktive Nutzerinnen und Nutzer aus über 1.800 Schulen registriert. Das zeige, dass sich das Schulportal Hessen einer sehr großen Beliebtheit erfreue.

Der modulare Aufbau des Schulportals biete eine Vielzahl an Funktionen, die den Schulalltag aus organisatorischer Sicht erheblich erleichterten. Dazu gehörten unter anderem das Lernmanagementsystem „SchulMoodle“, Kommunikationsmöglichkeiten sowie die Verwaltung der Unterrichtsinhalte, der Noten, der Anwesenheiten und vieles mehr. Beispielsweise könnten Lehrkräfte Raumbuchungen vornehmen, mit den Eltern kommunizieren sowie Klassenlisten erstellen. Diese standardisierten Prozesse würden dazu beitragen, dass den Lehrkräften mehr Zeit für die pädagogische Arbeit mit den Schülerinnen und Schülern bleibe.

Darüber hinaus vereinfache das Schulportal aus pädagogischer Sicht die Individualisierung des Unterrichts durch die Bereitstellung von Tools wie „Mein Unterricht“ und „SchulMoodle“. So werde eine individuelle Lernbegleitung beispielsweise durch individualisierte Lehrmaterialien in „SchulMoodle“ gefördert und eine gezielte Unterstützung der Schülerinnen und Schüler ermöglicht.

Was den Kern der Fragestellungen des Dringlichen Berichtsantrags anbelange, wolle er klarstellen, dass es grundsätzlich nicht problematisch sei, wenn eine externe App wie die sogenannte Lanis-Mobile-App auf das Schulportal zugreifen könne. Das sei ein weit verbreiteter technischer Vorgang. Es sei davon auszugehen, dass die Mehrheit der hier anwesenden Personen im Alltag vergleichbare Anwendungen regelmäßig verwendeten.

Hierzu gehörten zum Beispiel die sogenannten Multi-Banking-Apps, die mehrere Konten von unterschiedlichen Banken bündelten. Vergleichbar seien auch Mailprogramme, die den gleichzeitigen Zugang zu verschiedenen Mailadressen ermöglichten. Auch gebe es Apps, die mehrere Social-Media-Konten verschiedener Anbieter miteinander verknüpften und darstellten.

Die App Lanis-Mobile, die den Zugang zum Schulportal ermögliche, sei mit den vorgenannten Anwendungen vergleichbar. Zudem erfülle die App Lanis-Mobile klassische Aufgaben zur Anmeldung in einer Webanwendung, wie es auch bei einem gebräuchlichen Internet-Browser der Fall sei. Die App ersetze gewissermaßen den Zugang über Google Chrome, Mozilla Firefox oder Microsoft Edge.

Auch Aussagen zu dem Portal GitHub, auf das sich eine der nachfolgenden Fragen beziehe, wolle er eingangs kurz einordnen. Das Schulportal Hessen sei vollständig per HTTPS abgesichert. HTTPS sei ein Protokoll beziehungsweise der Weg, mit dem Nachrichten im Internet von A nach B übermittelt würden. Das sei ein internationaler, äußerst sicherer und auch der einzige Standard, der in äußerst sensiblen Bereichen wie dem Online-Banking genutzt werde.

Die Lanis-Mobile-App greife wie alle anderen Browser auch über HTTPS auf das Schulportal zu. Dementsprechend sei die Darstellung auf GitHub hinsichtlich der Verschlüsselung von HTTPS nicht korrekt, da die App bereits die Zugangsdaten von den Nutzerinnen und Nutzern bekommen habe, und zwar freiwillig, da die App bewusst genutzt werde.

Nicht korrekt sei außerdem die Darstellung, dass einige Inhalte des Schulportals durch eine Verschlüsselung abgesichert seien, während andere Elemente auch ohne Verschlüsselung zugänglich seien. Korrekt sei, dass alle Elemente des Schulportals per HTTPS verschlüsselt seien. Das bedeute, dass die in der Vormerkung der Fragesteller dargestellten angeblichen Sicherheitslücken und Schwachstellen des Schulportals nicht bestünden.

Diese Vorbemerkungen vorangestellt, berichte er im Einzelnen Folgendes:

Aufgrund des Sachzusammenhangs beantworte er die Fragen 1 bis 5 gemeinsam. Das Schulportal Hessen erfülle die erforderlichen datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung und gewährleiste höchste Standards der Informationssicherheit – insbesondere den BSI-IT-Grundschutz.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, kurz HBDI, komme in seinem 52. Tätigkeitsbericht bei der datenschutzrechtlichen Bewertung des Schulportals zu dem Ergebnis, das Schulportal Hessen sei ein gelungenes Beispiel dafür, wie digitale Souveränität praktiziert werden könne. Das Schulportal verfüge über ein Datenschutzkonzept, das durch den HBDI im Jahr 2023 umfassend geprüft und grundsätzlich positiv bewertet worden sei. Darüber hinaus sei eine Datenschutz-Folgenabschätzung nach Artikel 35 Datenschutz-Grundverordnung vorgenommen worden. In diesem Zusammenhang weise er darauf hin, dass es nicht den Datenschutz-Grundverordnung-Standard bzw. die eine Zertifizierung gebe.

Der HBDI sei seit mehreren Jahren eng in die Umsetzung der Anforderungen zum Datenschutz und der IT-Sicherheitsarchitektur des Schulportals eingebunden. Im Rahmen dieses Prozesses seien durch den HBDI in verschiedenen Stellungnahmen wichtige Hinweise und Bewertungen an das Ministerium herangetragen worden. Laut HBDI würden demnach im Zusammenhang mit dem Schulportal die datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung im Rahmen der Verarbeitung personenbezogener Daten erfüllt. Der HBDI sehe hier lediglich punktuelle Verbesserungsbedarfe. Zu keinem Zeitpunkt habe er inhaltlich-technische Kritik geäußert.

Lediglich bei der Dokumentation der komplexen Strukturen des Schulportals habe die Aufsichtsbehörde auf Anpassungsbedarfe hingewiesen. Da gehe es etwa um die Vereinheitlichung von

Begrifflichkeiten wie „Lehrkräfte“ und „Lehrerin bzw. Lehrer“ oder „Lernende“ und „Schülerinnen und Schüler“.

Die Dokumentation werde im Rahmen eines kontinuierlichen und fachgerechten Revisionsprozesses angepasst. Zudem sollte nach Auffassung des HBDI bei der Umsetzung einzelner Datenverarbeitungsprozesse noch nachgesteuert werden. Beispielsweise sollte das Löschkonzept, das angebe, welche Daten zu welchem Zeitpunkt aus der Anwendung gelöscht würden, detaillierter sein. Schwachstellen hinsichtlich der Sicherheit der Verarbeitung personenbezogener Daten seien nicht ersichtlich gewesen.

Die Entwicklung und der Betrieb des Schulportals werde vom IT-Sicherheitsbeauftragten des HMKB begleitet. Aufgrund der Größe und der Wichtigkeit des Systems für die hessische Schullandschaft sei im letzten Jahr zudem die Stelle eines eigenen BSI-zertifizierten IT-Sicherheitskoordinators für das Schulportal in der Hessischen Lehrkräfteakademie besetzt worden.

Darüber hinaus werde die Fortentwicklung und der Betrieb des Schulportals dauerhaft durch eine IT-Sicherheitskoordinierungsgruppe, bestehend aus Mitarbeiterinnen und Mitarbeitern der Lehrkräfteakademie mit BSI-IT-Grundschutz- und EU-DSGVO-Zertifizierungen, begleitet. Außerdem sei die Stelle einer Datenschutzkoordinatorin in der Lehrkräfteakademie geschaffen worden, die mit einer Volljuristin besetzt worden sei. Die Sicherheitskoordinierungsgruppe bewerte die IT-sicherheits- und datenschutzrelevanten Änderungen im Schulportal und stelle so die Einhaltung des BSI-Standards sowie des Datenschutzes sicher. Sie werde von der Datenschutzkoordinatorin des Schulportals und dem IT-Sicherheitskoordinator gemeinsam geleitet.

Hinsichtlich der Überprüfung des Schulportals wolle er mitteilen, dass das Schulportal aus zahlreichen verschiedenen Anwendungen bestehe, die unter einem Dach gebündelt seien. Bei den Systemen und bei der Entwicklung fänden bei jeder Änderung automatisiert Sicherheitsüberprüfungen statt. Begleitend dazu werde der Betrieb dauerhaft überwacht. Aufgrund der Modularität des Schulportals sei diese Vorgehensweise am zielführendsten, da somit vornehmlich die Bereiche, in denen Anpassungen vorgenommen würden, getestet würden.

Der letzte Pen-Test habe vor diesem Hintergrund im Jahr 2019 für den Teil des Bildungsservers im Schulportal stattgefunden. Er habe nur 13 nicht kritische Sicherheitslücken aufzeigen können, die danach umgehend geschlossen worden seien. Das sei ein Penetrationstest, der zeige, wie weit man vordringen könne. Damit könne man möglicherweise vorhandene Schwachstellen identifizieren.

An dieser Stelle sei zu betonen, dass das Auffinden von Sicherheitslücken im Rahmen von Pen-Tests nichts Ungewöhnliches sei. Gerade dafür würden diese Tests schließlich durchgeführt. Außerdem habe keiner der vier Fälle in einem Zusammenhang mit der thematisierten Lanis-Mobile-App gestanden. Pen-Tests würden immer nur eine Momentaufnahme darstellen. Es gebe auch keine rechtliche Verpflichtung zur Durchführung.

Zu Frage 6 teilt der Minister mit, das Personal im Sachgebiet II.3-1 der Lehrkräfteakademie könne im Sinne der Fragestellung wie folgt aufgeschlüsselt werden: Fünf Mitarbeiterinnen und Mitarbeiter hätten ein informationstechnisches Lehramt. Sie würden in einem Umfang von insgesamt 196,5 Wochenstunden arbeiten. 22 Mitarbeiterinnen und Mitarbeiter mit einem informationstechnischen Lehramt würden auf Abordnungsbasis 409 Wochenstunden arbeiten.

Vier Mitarbeiterinnen und Mitarbeiter hätten tätigkeitsbegleitende Fortbildungen durchlaufen oder hätten eine Zertifizierung im IT-Bereich wie die BSI-IT-Grundschutz- oder die ITIL-Zertifizierung. Sie arbeiteten 141,8 Wochenstunden. 24 Mitarbeiterinnen und Mitarbeiter mit einer dieser Qualifikationen arbeiteten auf Abordnungsbasis 433,6 Wochenstunden. Auch die Personen mit informationstechnischem Lehramt würden an Fortbildungen oder Zertifizierungen teilnehmen.

Aufgrund des Sachzusammenhangs beantworte er die Fragen 7 bis 10 gemeinsam. Das Schulportal Hessen sei eine Anwendung im World Wide Web, die mit jedem Browser aufgerufen und genutzt werden könne, wenn sich die Nutzerinnen und Nutzer mit ihren persönlichen Zugangsdaten einloggen. Auf diese Weise stünden den Lehrkräften, den Schülerinnen und Schülern sowie den Eltern die für den Lehr- und Lernprozess erforderlichen Informationen jederzeit zur Verfügung, sowohl in der Schule als auch zu Hause.

Mittlerweile verfüge jedes Land über ein zentrales pädagogisches Portal, das in vergleichbarer Weise bereitgestellt werde. Jede Programmiererin und jeder Programmierer könne eine App entwickeln, mit der beliebige Internetseiten nach dem entsprechenden Log-in genutzt werden könnten. Bei der Nutzung könne die App grundsätzlich auf alle Daten zugreifen, die die Nutzerin oder der Nutzer bei einem Log-in über einen Browser auch sehen oder bearbeiten könnten. Das sei auch bei der hier diskutierten Lanis-Mobile-App der Fall, Die Nutzerinnen und Nutzer hätten in diesem Fall eigenverantwortlich ihre Log-in-Daten in die App eingegeben.

Die Daten könnten in der App aufbereitet und den Nutzenden auf dem mobilen Endgerät dargestellt werden. Nur die Entwicklerinnen und Entwickler der App könnten beeinflussen, wohin die Daten der Nutzenden abfließen. Log-in-Daten sollten von den Nutzerinnen und Nutzern daher nicht in die Apps eingegeben werden, wenn sie sich nicht sicher seien, was mit ihren Daten geschehe. Er verweise insofern auf seine Vorbemerkung.

Die genannte Lanis-Mobile-App sei von einer Privatperson entwickelt worden. Der Zeitpunkt des Entwicklungsbeginns der App sei in seinem Haus nicht bekannt.

Kenntnis, dass diese App auf das Schulportal Hessen zugreife, habe die Hessische Lehrkräfteakademie seit dem 21. Februar 2024, was seinem Haus am 23. Februar 2024 gemeldet worden sei. Eine Prüfung in seinem Haus habe ergeben, dass von externen Apps allgemein keine Sicherheitsgefahr für das Schulportal ausgehe.

Aufgrund des Sachzusammenhangs beantworte er die Fragen 11 und 12 gemeinsam. Das Staatliche Schulamt für den Landkreis Groß-Gerau und den Main-Taunus-Kreis stehe seit August 2024 mit dem Entwickler, einem Schüler, in Kontakt. Um die besondere Informatikleistung des Schülers zu würdigen, habe das Staatliche Schulamt, ergänzend zur internen Einschätzung hinsichtlich

der Praktikabilität, der Sicherheit und der Nutzbarkeit, die Erprobung der App an vier Schulen ermöglicht, um so Rückmeldungen zum einfachen Zugriff auf zentrale und häufig genutzte Funktionen des Schulportals zu erhalten. Daran seien eine Lehrkraft in ihrer Funktion als Medienfachberater und der Datenschutzkoordinator am Staatlichen Schulamt beteiligt gewesen.

Im Rahmen der Erstellung der Antwort auf den Dringlichen Berichtsantrag habe man zu diesem Vorhaben weitere Informationen vom Staatlichen Schulamt angefordert. Diese werte man jetzt aus. Hierzu zählten beispielsweise die Prüfkriterien des Staatlichen Schulamts und ob weitere datenschutzrechtliche Dokumente erforderlich seien sowie ob angemessene IT-Sicherheitsstandards gewährleistet seien. Dazu stehe sein Haus im engen Austausch mit dem Staatlichen Schulamt.

Grundsätzlich wolle er an dieser Stelle darauf hinweisen, dass der Einsatz der App im eigenen Ermessen und auf freiwilliger Basis der jeweiligen Nutzerinnen und Nutzer erfolge. Es gebe in keiner Weise eine Verpflichtung zur Nutzung. Das Schulportal sei vollumfänglich ohne die in Rede stehende App nutzbar. Durch den Einsatz der App bestehe kein Risiko für den Betrieb des Schulportals.

Aufgrund des Sachzusammenhangs beantworte er die Fragen 13 und 14 gemeinsam. In den gängigen App-Stores gebe es eine Vielzahl an Apps, die den Nutzerinnen und Nutzern Daten von Internetseiten nach dem Login zur Verfügung stellten.

Die Verantwortung für die Datenverarbeitung von externen Apps könne nicht vom HMKB übernommen werden. Die Nutzerinnen und Nutzer würden in eigener Verantwortung entscheiden, welche Apps sie auf ihren mobilen Endgeräten installierten und welche Daten, insbesondere Login-Daten, sie diesen Apps zur Verfügung stellten. Derzeit prüfe man jedoch die Einführung einer Nutzungsvereinbarung zum Schulportal, bei der man allgemeine Hinweise und potenzielle Risiken bei der Nutzung externer Apps, zum Beispiel hinsichtlich der Weitergabe von Zugangsdaten, im Blick habe.

Zu Frage 15 teilt der Minister mit, sein Haus habe seit dem 5. Februar 2025 Kenntnis davon, dass der Entwickler der App vermeintliche Schwachstellen oder Sicherheitslücken beim Schulportal entdeckt zu haben glaube. Im Übrigen verweise er auf die Vorbemerkung.

Aufgrund des Sachzusammenhangs beantworte er die Fragen 16 und 17 gemeinsam. Datensicherheitskritische Vorfälle seien solche, bei denen ein Risiko für die Rechte und Freiheiten natürlicher Personen nicht ausgeschlossen werden könne. Solche Vorfälle seien entsprechend Artikel 33 Absatz 1 der Datenschutz-Grundverordnung der zuständigen Datenschutzaufsichtsbehörde zu melden.

Ein potenzielles Risiko des Schutzes personenbezogener Daten im Zusammenhang mit dem Schulportal sei am 3. November 2023 zunächst vorsorglich dem HBDI gemeldet worden. Die ausführliche Nachmeldung sei im Anschluss an die abschließende Klärung und Bewertung sämtlicher Umstände am 6. November 2023 erfolgt. Es seien unverzüglich technische und organisatorische Maßnahmen ergriffen worden, um die fehlerhaften Zugriffsmöglichkeiten abzustellen.

Aufgrund des Sachzusammenhangs beantworte er die Fragen 18 bis 20 gemeinsam. Es seien zwei Fälle aus dem Oktober und dem November 2024 bekannt, die im Zusammenhang mit der Nutzung der Lanis-Mobile-App stehen würden. Bei dem ersten Fall sei dem Ministerium von dem schulischen Administrator über den Support mitgeteilt worden, dass eine Nachricht fälschlicherweise an nicht beabsichtigte Empfängerinnen und Empfänger gesendet worden sei. Bei dem zweiten Fall sei eine Nachricht fälschlicherweise nicht beabsichtigt an Eltern einer Schulklasse gesendet worden. Beide Fälle seien dem Support mit der Bitte um Löschung der Unterhaltung übermittelt worden. Die Löschung sei umgehend vorgenommen worden.

Hinsichtlich der Frage 21 verweise auf seine Antwort zu den Fragen 16 und 17.

Zu Frage 22 teilt Minister Armin Schwarz mit, die Lehrkräfte könnten im Schulportal im Modul „Mein Unterricht“ Noten nur an die entsprechenden Schülerinnen und Schüler zur Ansicht freigeben, die mit dieser Note verknüpft seien. Eine Einsicht in diese Noten sei auch über die Lanis-Mobile-App möglich. Da Noten anders als Nachrichten jedoch nicht versendet würden, sei ein fehlerhafter Empfängerkreis im Sinne der Fragen 18 bis 20 ausgeschlossen.

Zu Frage 23 führt der Minister aus, jeder Betriebs- oder Sicherheitsvorfall im Schulportal, unabhängig davon, ob per automatischer Überwachung oder manuell gemeldet worden sei, bedinge immer eine erste, kurze Einschätzung durch das technische Betriebsteam. Nach dieser werde kurzfristig ein sogenanntes Incident-Meeting unter Beteiligung des Programmbüros Schulportal Hessen im HMKB, der zuständigen Sachgebietsleitung in der Lehrkräfteakademie, dem IT-Sicherheitskoordinator, der Datenschutzkoordinatorin sowie den betroffenen technischen Teamleitungen einberufen, um direkt die erforderlichen Maßnahmen zu ergreifen.

Oberstes Ziel sei auch hierbei der Schutz der personenbezogenen oder personenbeziehbaren Daten. Daher werde auch eine Einschätzung vorgenommen, ob solche Daten bei einem etwaigen Vorfall betroffen seien und ob es sich damit um einen meldepflichtigen Datenschutzvorfall handeln könnte. In einem solchen Fall finde zuerst örtlich eine weitergehende Betrachtung mit dem Datenschutzbeauftragten des HMKB statt. Sollte es sich um einen IT-Sicherheitsvorfall handeln, würden je nach Situation in Folgeschritten die IT-Sicherheitsbeauftragten des HMKB, aber auch beispielsweise das Hessen CyberCompetenceCenter vom HMKB involviert.

Durch die Überwachung der Vorfälle könnten bei Bedarf unter anderem Maßnahmen im Zuge der Nachbereitung ergriffen werden. Das könnten zum Beispiel Maßnahmen der automatisierten Überwachung sein.

Abgeordneter **Lothar Mulch** teilt mit, Minister Armin Schwarz habe sinngemäß gesagt, durch die Nutzung der App bestehe keine Gefahr für die Funktionalität des Schulportals. Er halte das für eine steile These. Seiner Auffassung nach funktioniere das Schulportal noch, weil es kein sonderlich interessantes Angriffsziel sei. Da sei mit Ransomware nichts zu holen. Deswegen bestehe kein Interesse daran, das Schulportal zu infiltrieren.

Seiner Auffassung nach sei es nur eine Frage der Zeit, bis das Schulportal angegriffen werde. Da müsse die vorgeschaltete App sicher sein. Da sei die Frage, wie ein Schüler auf das Portal zugreifen könne, ohne offiziell beauftragt worden zu sein, berechtigt.

Minister **Armin Schwarz** antwortet, totale Sicherheit werde es bei der Datenverarbeitung nicht geben. Die Systeme würden ständig angegriffen. Der Deutsche Bundestag und der Hessische Landtag hätten ständig damit zu tun, die IT-Sicherheit zu erhöhen, um Angriffe abzuwehren.

Ein **Vertreter** der Landesregierung teilt mit, die Frage habe aus mehreren Teilen bestanden. Angriffe auf das Schulportal würden ständig stattfinden. In den letzten Monaten habe es DDoS-Attacken gegen das Schulportal in einem Ausmaß gegeben, wie man es im Land Hessen noch nicht erlebt habe. Die HZD sei nicht in der Lage gewesen, dem zu begegnen. Man habe externe technische Dienstleister eingeschaltet, um die Sicherheit des Schulportals zu gewährleisten. Man müsse sich zu jeder Zeit verteidigen können.

Der Zugriff über die App stelle kein Sicherheitsrisiko dar. Das weise man weit von sich. Das Schulportal sei eine Online-Plattform. Über den Browser könne man mit seinem Log-in auf die Daten des Schulportals zugreifen. Eine wie von dem Schüler verwendete App mache nichts anderes als ein Browser. Die Sicherheit für das Schulportal bestehe zu jedem Zeitpunkt, weil der Nutzer sich mit der App dort genauso bewegen könne, wie wenn er einen Browser verwenden würde. Es gebe keine darüber hinaus gehenden Nutzungen oder Aktionen, die man mit der App im Schulportal ausführen könne.

StDir **Christian Mehler** führt aus, die Kernidee des Internets sei, dass man über definierte Protokolle Inhalte zur Verfügung stellen könne. Das könne sowohl vor als auch nach dem Log-in geschehen. Es handele sich um offene und standardisierte Protokolle. Ob man da mit einem Browser oder irgendetwas anderem zugreife, sei unerheblich, denn Endpunkt und Start seien definiert.

Als Beispiel wolle er einen Gartenschlauch anführen, der im Garten liege. Auf der einen Seite habe man den Wasserhahn. Da sei es unerheblich ob man mit dem anderen Ende Blumen gieße oder sein Auto wasche. Für den Schlauch als Übertragungsprotokoll sei es genau dieselbe Aktion.

In dem vorliegenden Fall gehe es um die Frage, ob es Auswirkungen habe, wenn man nicht mit einem Browser, sondern mit einer App zugreife. Das spiele keine Rolle, weil man verschiedene Absicherungsmechanismen habe, also Systeme, die bei zu vielen oder fehlerhaften Zugriffen funktionierten. Es würden immer dieselben Abwehrmechanismen greifen. Es gebe also keine Einschränkungen in Bezug auf die IT-Sicherheit.

Abgeordneter **Torsten Leveringhaus** legt dar, seiner Auffassung nach bestehe ein Unterschied zwischen einer Landes-Mobile-App und einer Banking- oder Mail-App. Denn keiner wolle, dass ein fremdes Mailkonto auf seine Mail zugreifen könne. Das gelte insbesondere beim Banking.

Darum gehe es bei dem Dringlichen Berichts Antrag. Man habe zum Beispiel gehört, dass E-Mails falsch verschickt worden seien. Es seien Daten genutzt worden, auf die die Personen eigentlich keinen Zugriff haben sollten.

Der Minister habe ausgeführt, dass es 2019 den letzten Pen-Test gegeben habe. Die Lanis-Mobile-App gebe es vermutlich bereits seit 2021. Die App habe also vermutlich zugegriffen, ohne dass es einen Pen-Test gegeben habe. Er bitte, mitzuteilen, warum kein weiterer Test erfolgt sei. Gerade in der Software gebe es erhebliche Fortschritte. Da könne es möglich sein, dass es inzwischen Angriffswege gebe, die es 2019 noch nicht gegeben habe.

Der Minister habe des Weiteren berichtet, dass das Schulportal aus verschiedenen Anwendungen und verschiedenen Modulen bestehe. Er könne sich gut vorstellen, dass sich bei der Verknüpfung verschiedener Module, die unterschiedlich programmiert worden seien, Angriffsmöglichkeiten ergäben, die ausgenutzt werden könnten.

Es sei gesagt worden, dass man die Session-ID auslesen könne und dass das HTTPS-Verfahren deshalb gar nicht so wirksam sei. Es gebe verschiedene Möglichkeiten, auf die Daten einer Website trotz HTTPS zuzugreifen. Man könne einen Man-in-the-Middle-Angriff starten. Man könne mit Cross-Site-Scripting auf Daten zugreifen, wenn der Datenaustausch zwischen den verschiedenen Modulen nicht abgesichert sei. Er bitte, mitzuteilen, wie das beim Schulportal geregelt sei.

Es gehe auch um die Frage, ob das Schulportal weiterhin genutzt werden könne. Diese Frage sei auch vom Vertreter der AfD-Fraktion gestellt worden. Er, so Abgeordneter Torsten Leveringhaus sei der Auffassung, man könne es auch weiterhin nutzen. Man müsse aber berücksichtigen, was im Hintergrund geschehe. Es gehe um die Frage, welche Datenabflüsse es gebe.

In der Antwort auf die Fragen 16 und 17 habe Minister Armin Schwarz mitgeteilt, am 3. November 2023 sei es zu einem Vorfall gekommen, der dem HBDI mitgeteilt worden sei. Er bitte, genauer mitzuteilen, was da geschehen sei. Der Minister habe berichtet, dass E-Mails an die falschen Adressaten verschickt worden seien. Seiner Auffassung nach, so Abgeordneter Torsten Leveringhaus, handele es sich dabei um einen datenschutzrelevanten Vorfall. Er bitte, mitzuteilen, ob es eine Meldung an die Aufsichtsbehörde gegeben habe. Falls es diese Meldung gegeben habe, bitte er, mitzuteilen, wie die Reaktion ausgefallen sei.

Der Minister habe in der Antwort zu Frage 22 mitgeteilt, dass Noten nur die Schülerinnen und Schüler einsehen könnten, die sie betreffen. Er, so der Abgeordnete, bitte, mitzuteilen, ob ausgeschlossen werden könne, dass bei einem Zugriff mit der App auch Menschen zugreifen könnten, die dazu keine Berechtigung hätte.

Minister **Armin Schwarz** antwortet, der nächste Pen-Test werde in Abstimmung mit der HZD gerade geplant. Der nächste Pen-Test für ein Teilsystem solle Ende 2025 erfolgen. Aktuell arbeite man daran, selbst Pen-Tests durchführen zu können. Damit einher gehe die Anschaffung einer entsprechenden Software-Lizenz. Man teste so viel, dass man im laufenden Betrieb die Sicherheit gewährleisten könne.

Zu der Antwort auf die Frage 17 könne er ausführen, dass ein potenzielles Risiko des Schutzes personenbezogener Daten im Zusammenhang mit dem Schulportal bestehen könnte. Das sei am 3. November 2023 dem HBDI vorsorglich mitgeteilt worden. Die ausführliche Meldung sei dann nach abschließender Klärung und Bewertung sämtlicher Umstände am 6. November 2023 erfolgt. Es seien unverzüglich technische und organisatorische Maßnahmen ergriffen worden, um die fehlerhaften Zugriffsmöglichkeiten abzustellen.

Damals habe ein White-Hat-Hacker eine Sicherheitslücke im Schulportal aufgezeigt, durch die es potenziell möglich gewesen wäre, Benutzerdaten des Schulportals einzusehen. Es seien unverzüglich technische und organisatorische Maßnahmen ergriffen worden, um die fehlerhaften Zugriffsmöglichkeiten abzustellen. In einer öffentlichen Sitzung könne man dazu keine technischen Details nennen.

Ein **Vertreter** der Landesregierung teilt mit, wenn man Software entwickle, würden schon Tests geschrieben, die automatisiert zur Anwendung kämen. Bevor die Software eingesetzt werde, würden manuelle und automatisierte Tests angewendet. So schaue man zum Beispiel, wie die Software sich im Austausch mit anderer verhalte.

Ein wichtiger Aspekt sei die dauerhafte Stabilisierung und Überwachung der Systeme. Regelmäßig würden dabei bestimmte Daten abgefragt. Es gehe darum, ob sich die Software korrekt verhalte. Dabei würden mehrere automatisierte Überwachungssoftwares eingesetzt, die automatisch warnen würde, wenn sich das System nicht korrekt verhalte.

Das Schulportal bestehe aus verschiedenen Modulen, die verschiedene Sprachen und verschiedene Entwicklungsumgebungen hätten. Sie würden sogar über Rechenzentren hinweg miteinander kommunizieren. Das sei aber keine schwierige Aktion mehr. Dort bestünden kaum Angriffsmöglichkeiten, weil man die regulären Standards einhalte.

Das Session-Cookie könne eingesehen werden, weil man eine offene Kommunikation habe. Man könne einsehen, was der Browser sende und was er als Antwort erhalte. Es gehe dabei nicht um eine Man-in-the-Middle-Aktion, sondern darum, dass einer der Endpunkte von der App übernommen worden sei. Der Endpunkt könne alle Daten mitlesen, die er versende und erhalte.

Berichte über Ausfälle seien zutreffend. Das hänge auch damit zusammen, dass auf die hessischen Landessysteme Angriffe in einem Ausmaß gefahren worden seien, wie es sie zuvor nicht gegeben habe. Das Hauptziel beim Schulportal sei gewesen, die Verfügbarkeit einzuschränken, damit niemand mehr damit arbeiten könne. Da müsse man Gegenmaßnahmen ergreifen und

müsse gegebenenfalls noch eine weitere Schicht davor schalten, damit das System funktionsfähig bleibe.

MinR **Christian Meinert** führt aus, er sei der Datenschutzbeauftragte des Ministeriums für Kultus, Bildung und Chancen. Seit mehreren Jahren begleite er die Datenschutzkonzeptionen des Schulportals. Mit dem HBDI bestehe ein reger Austausch. Man habe seinerzeit die Meldung gemacht, weil man Transparenz haben wollte. Es handele sich dabei um eine Meldung gemäß Artikel 33 Datenschutz-Grundverordnung. Damit werde der Aufsichtsbehörde die Möglichkeit gegeben, den Sachverhalt unabhängig zu prüfen.

Der Minister habe bereits ausgeführt, dass es Hinweise auf potenzielle Sicherheitsrisiken gegeben habe, denen man umgehend entgegengewirkt habe. Das habe der HBDI dokumentiert bekommen. Er sei mit den Maßnahmen, die getroffen worden seien, zufrieden gewesen und habe den Vorgang geschlossen.

Minister **Armin Schwarz** teilt mit, hinsichtlich einer unberechtigten Einsicht in die Noten könne er auf seine Antwort zu Frage 22 verweisen.

Abgeordneter **Daniel May** legt dar, es habe einen Vorfall im Herbst 2023 und dann noch einmal einen im Herbst 2024 gegeben. Er bitte, mitzuteilen, wie seinerzeit vorgegangen worden sei.

Abgeordneter **Torsten Leveringhaus** bemerkt, er bitte, zusätzlich mitzuteilen, ob bei den beiden Vorfällen auch die Aufsichtsbehörde, also der HBDI, einbezogen worden sei.

MinR **Christian Meinert** antwortet, man habe ein ganzes Team, das aus Technikern und Fachleuten bestehe. Dem gehöre er als Volljurist und Datenschutzbeauftragter auch an. Das Ganze sei dann entsprechend den eigenen internen Meldeprozessen behandelt worden. Dabei sei schnell klar geworden, dass kein erhebliches Risiko hinsichtlich einer unrechtmäßigen Nutzung der personenbezogenen Daten vorgelegen habe. Man habe dann die in Frage stehenden Daten einfach gelöscht. Eine Meldung an den HBDI sei nicht erforderlich gewesen.

Abgeordneter **Daniel May** führt aus, seine Fraktion habe den Hinweis erhalten, dass es beim Schulportal eine Schwachstelle geben könnte. Da es ihnen wichtig gewesen sei, dass das Schulportal sicher laufe, habe man, bevor man den Dringlichen Berichtsantrag eingereicht habe, die Landesregierung vertraulich darüber informiert.

Stützig mache ihn, dass die Hinweise, die es auf Schwachstellen im System gegeben habe, nicht einschlägig sein sollten. Es habe beim Schulportal Probleme gegeben. Insofern würde er begrüßen, wenn man die Zusage des Ministers erhalten würde, dass der Kultuspolitische Ausschuss informiert werde, falls es beim Schulportal noch einmal zu sicherheitsrelevanten Vorfällen komme.

Minister **Armin Schwarz** antwortet, er wolle sich zunächst einmal herzlich dafür bedanken, dass man diese Hinweise erhalten habe. Das sei auch eine Frage des Teamworks. Er gehe davon aus, dass alle gemeinsam ein Interesse daran hätten, dass das Schulportal gut und sicher laufe.

Man nehme solche Vorfälle sehr ernst. Er hoffe, es sei deutlich geworden, mit welcher Professionalität in einem Team daran gearbeitet werde, das Ganze so sicher wie nur möglich zu machen. Er sei für das dankbar, was die Kolleginnen und Kollegen dort leisteten.

Er halte viel von Transparenz. Man wolle nichts verheimlichen. Wenn jemand der Auffassung sei, dass irgendetwas nicht stimme, sei er dankbar, wenn sein Haus im Sinne eines kollegialen Miteinanders eine Mitteilung erhalten würde.

Wenn es gewünscht werde, könne sei Haus den Kultuspolitischen Ausschuss ein- oder zweimal im Jahr über den Stand beim Schulportal unterrichten. Wenn etwas ganz Außergewöhnliches geschehen sei, könne man sich sicher sein, dass er darüber informieren werde. Er wolle die Vorfälle nicht bagatellisieren. Aber es fänden permanent Angriffe statt. Man werde nicht über jede Kleinigkeit berichten können. Wenn es aber zu gravierenden Vorfällen kommen sollte, würde er darüber berichten.

Beschluss:

KPA 21/11 – 26.02.2025

Der Dringliche Berichts Antrag gilt mit der Entgegennahme des mündlichen Berichts im Kultuspolitischen Ausschuss als erledigt.

(einvernehmlich)

Zu Beginn der Sitzung kam der Kultuspolitische Ausschuss einvernehmlich überein, den Dringlichen Berichts Antrag in öffentlicher Sitzung zu beraten.

Wiesbaden, 23. April 2025

Protokollierung:

Vorsitz:

Hanns Otto Zinßer

Kerstin Geis