LANDTAG RHEINLAND-PFALZ
17. Wahlperiode

Drucksache 17/14373
zu Drucksache 17/14121
zu Drucksache 17/14122
29. 01. 2021

Antwort

des Ministeriums für Bildung

auf die Kleinen Anfragen der Abgeordneten Anke Beilstein (CDU)

Fehlstart des Fernunterrichts zum Jahresbeginn 2021
– Drucksache 17/14121 –

Fehlstart des Fernunterrichts zum Jahresbeginn 2021
– Drucksache 17/14122 –

Die **Kleinen Anfragen – Drucksachen 17/14121/14122 –** vom 5. Januar 2021 haben folgenden Wortlaut:

Drucksache 17/14121
Seit Beginn der Corona-Pandemie, spätestens aber seit der von den Schulen verlangten Vorbereitung auf möglichen Wechsel-, Hybrid- oder Fernunterricht war klar, dass im weiteren Verlauf der Pandemie die faktische Umsetzung dieser Unterrichtsformen erforderlich werden könnte. Rheinland-Pfalz hat sich trotz vieler Hinweise auf Bedenken bezüglich einer reibungslosen Nutzung für den landesweiten Einsatz von Moodle und BigBlueButton entschieden. Spätestens seit Mitte Dezember war klar, dass zum Schulstart am 4. Januar 2021 die Voraussetzungen für landesweiten Fernunterricht in Rheinland-Pfalz hätten gegeben sein müssen. Statt eines reibungslosen Digitalunterrichts erlebten Lehrkräfte, Schülerinnen/Schüler und Eltern landesweit einen ausgeprägten Fehlstart. Das Bildungsministerium spricht von technischen Problemen „auch“ durch einen Hackerangriff. Man habe „in den vergangenen Wochen“ und „bis zur letzten Sekunde“ daran gearbeitet, die Serverinfrastruktur zu stärken. Bildschirmfotos von diesem Tag belegen die Anzeige „Serverfehler“ mit dem Hinweis: „Die Kapazitäten des Systems (5 000 gleichzeitige Konferenzen, 100 000 Teilnehmerinnen/Teilnehmer ist erreicht! Bitte versuchen Sie es später erneut.“
Ich frage die Landesregierung:
1. Auf welche Kapazitäten (wie viele gleichzeitige Konferenzen und wie viele Teilnehmerinnen/Teilnehmer) war das System jeweils ausgelegt zu den Terminen 1. April 2020, 1. August 2020, 1. November 2020, 15. Dezember 2020 und 4. Januar 2021?
2. Welche Kapazität (wie viele gleichzeitige Konferenzen und wie viele Teilnehmerinnen/Teilnehmer) ist für eine flächendeckende und reibungslose landesweite Nutzung erforderlich?
3. Wie wurde diese Kapazität berechnet?
4. Wann soll die nach Ziffer 2 erforderliche Kapazität erreicht sein?
5. Welche Schutzvorrichtungen sind für solche DDoS-Angriffe möglich?
6. Ist das Landesrechenzentrum in der Lage, diese verlässlich einzurichten?
7. Wer sonst ist in der Lage, solche Schutzvorrichtungen vorzunehmen und sicherzustellen?

Drucksache 17/14122
Seit Beginn der Corona-Pandemie, spätestens aber seit der von den Schulen verlangten Vorbereitung auf möglichen Wechsel-, Hybrid- oder Fernunterricht war klar, dass im weiteren Verlauf der Pandemie die faktische Umsetzung dieser Unterrichtsformen erforderlich werden könnte. Rheinland-Pfalz hat sich trotz vieler Hinweise auf Bedenken bezüglich einer reibungslosen Nutzung für den landesweiten Einsatz von Moodle und BigBlueButton entschieden. Spätestens seit Mitte Dezember war klar, dass zum Schulstart am 4. Januar 2021 die Voraussetzungen für landesweiten Fernunterricht in Rheinland-Pfalz hätten gegeben sein müssen. Statt eines reibungslosen Digitalunterrichts erlebten Lehrkräfte, Schülerinnen/Schüler und Eltern landesweit einen ausgeprägten Fehlstart. Das Bildungsministerium spricht von technischen Problemen „auch“ durch einen Hackerangriff. Man habe „in den vergangenen Wochen“ und „bis zur letzten Sekunde“ daran gearbeitet, die Serverinfrastruktur zu stärken. Bildschirmfotos von diesem Tag belegen die Anzeige „Serverfehler“ mit dem Hinweis: „Die Kapazitäten des Systems (5 000 gleichzeitige Konferenzen, 100 000 Teilnehmerinnen/Teilnehmer) ist erreicht! Bitte versuchen Sie es später erneut.“
Ich frage die Landesregierung:
1. Welchen „Anteil“ am Fehlstart hatte der in der Pressemitteilung genannte Hackerangriff, bzw. wäre ohne diesen Hackerangriff die flächendeckende und reibungslose Nutzung landesweit gesichert gewesen?
2. Gab es im Vorfeld des 4. Januar 2021 seit Beginn der Corona-Pandemie Hinweise auf die Erwartbarkeit technischer Probleme und/oder möglicher Hackerangriffe?

Druck: Landtag Rheinland-Pfalz, 25. Februar 2021

3. Für den Fall, dass Frage 2 bejaht wird: Wie ist man damit umgegangen?
4. Aus welchen Gründen hat man sich bei der grundsätzlichen Entscheidung für Moodle/BigBlueButton als Open-Source-Software und gegen eine Closed-Source-Software entschieden?
5. Wurde eine finanzielle Vergleichsberechnung zwischen der Open-Source- und der Closes-Source-Variante im Vorfeld vorgenommen?
6. Hat die Vergleichsberechnung auch die Kosten für eine mögliche Schutzabwehr gegen Angriffe beinhaltet?
7. Wie war das Ergebnis der Vergleichsberechnung?

Das **Ministerium für Bildung** hat die Kleinen Anfragen namens der Landesregierung mit Schreiben vom 28. Januar 2021 wie folgt beantwortet:

Vorbemerkung:

Bei dem Angriff auf die Lernplattform Moodle am 4. Januar 2021 handelte es sich um eine Distributed-Denial-of-Service-(DDoS)-Attacke, d. h. eine absichtliche Überlastung der Server durch Anfragen von außen. Ein Eindringen in das System war damit nicht verbunden.

Von diesen Angriffen waren nicht nur rheinland-pfälzische Server betroffen. Entsprechende Attacken gab es auch in anderen Ländern.

Drucksache 17/14121:

Zu Frage 1:

BigBlueButton wird auf einem Server-Cluster betrieben, das auch für andere Zwecke genutzt wird. Dementsprechend können die Kapazitäten dynamisch nach Bedarf erhöht werden und werden nicht zu unterschiedlichen Zeitpunkten erfasst.

In Vorbereitung des Fernunterrichts wurde ein zusätzliches Server-Cluster bei einem deutschen Dienstleister angemietet, das das Videokonferenzsystem an der Johannes Gutenberg-Universität Mainz unterstützt.

Damit stehen nach Aussagen des Zentrums für Datenverarbeitung der Johannes Gutenberg-Universität Mainz (ZDV) bei maximaler Auslastung der Rechner Kapazitäten von 100 000 bis 150 000 gleichzeitige Teilnahmen (über direkte Weitergabe von Links zu Konferenzen) und nach Aussage der Open Source Company auf den extern angemieteten Rechnern Kapazitäten für 120 000 bis 150 000 gleichzeitige Teilnahmen (vermittelt durch Moodle) zur Verfügung, insgesamt also bei optimaler Verteilung auf die beiden Cluster Kapazitäten im Bereich zwischen 220 000 und 300 000 gleichzeitigen Teilnahmen.

Zu den Fragen 2 bis 4:

Welche Anzahl an Konferenzen bzw. Teilnehmenden erforderlich ist, hängt von den Nutzungsszenarien ab. Die pädagogischen Konzepte, wie beispielsweise in der Handreichung „Lehren und Lernen im Präsenz- und Fernunterricht“ dargelegt, empfehlen eine Unterrichtsgestaltung, bei der sich – insbesondere ältere Schülerinnen und Schüler – didaktisch aufbereitete Inhalte zunächst selbstständig erarbeiten und dann in Plenumsphasen per Videokonferenz besprechen.

Das entspricht dem pädagogischen Instrument des „Flipped Classrooms“, das von Pädagoginnen und Pädagogen und Fachdidaktikerinnen und Fachdidaktikern empfohlen wird, um das eigenständige und selbstverantwortliche Arbeiten der Schülerinnen und Schüler zu fördern. Dementsprechend wird in aller Regel das Unterrichtsgeschehen aus der Präsenzzeit nicht „eins zu eins nach Stundenplan“ als Videokonferenz abgebildet.

Der Kapazitätsschätzung liegt ein Modell zugrunde, bei dem an den weiterführenden Schulen pro Klasse und Woche mindestens zehn Stunden Videokonferenzzeit gewährleistet sein sollen. Der Bedarf bei den Grundschulen unterscheidet sich davon. Es ist gewährleistet, dass die jüngeren Schülerinnen und Schüler in regelmäßigem Kontakt – bei Bedarf täglich – mit ihrer Klassenlehrkraft stehen können.

Die hierfür erforderlichen Kapazitäten stehen bereits jetzt zur Verfügung, wobei auch „Pufferkapazitäten“ wegen möglicher ungleichmäßiger Belastung mit eingerechnet sind. Auf die Beantwortung von Frage 1 wird verwiesen.

Zu den Fragen 5 bis 7:

Die hier betroffenen Systeme liegen nicht beim Landesbetrieb Daten und Information (LDI), sondern – der besseren Internetanbindung und der schnellen Verfügbarkeit eines Hochleistungs-Clusters wegen – am Zentrum für Datenverarbeitung.

Ein DDoS-Angriff kann nicht durch die Betreuer der angegriffenen Systeme verhindert werden, weil der Angriff aus anderen Systemen heraus erfolgt, auf die diese Betreuer keinerlei Einfluss haben.

Da der Angriff selbst nicht beeinflusst werden kann, haben die Systembetreuer Abwehrmaßnahmen ergriffen, um die Konsequenzen eines potenziellen Angriffs auf die Systeme so gering zu halten, dass ein effizienter Gesamtbetrieb weiterhin gewährleistet bleibt. Solche Maßnahmen bestehen insbesondere darin, durch möglichst passgenaue Filterung auf verschiedenen Ebenen legitime Zugriffe von illegitimen Zugriffen automatisiert und mit hoher Geschwindigkeit zu unterscheiden. Das Zentrum für Datenverarbeitung prüft derzeit in Verhandlungen mit spezialisierten Dienstleistern, wie ein noch umfassenderer Schutz vor DDoS-Attacken gewährleistet werden kann.

Drucksache 17/14122:

Zu Frage 1:

Die technischen Schwierigkeiten beim System BigBlueButton waren ausschließlich durch den DDoS-Angriff begründet. Vor dem Angriff und nach Abwehr dessen lief das System stabil. Laufende Webkonferenzen waren nicht gestört.

Die technischen Schwierigkeiten bei Moodle zu Beginn des Fernunterrichts Anfang Januar waren nicht ausschließlich durch den DDoS-Angriff begründet. Daneben gab es Probleme in der Konfiguration der verschiedenen Teilsysteme, die erst unter extrem hoher Belastung zutage getreten sind.

Wie bei jedem komplexen IT-System lässt sich das Systemverhalten unter deutlich erhöhter Last nicht im Vorfeld theoretisch voraussagen; hier musste vor dem Hintergrund sorgfältiger und gleichzeitig zeitnaher Analyse des realen Betriebs unter hoher Belastung gezielt nachjustiert werden.

Zu den Fragen 2 und 3:

Alle Beteiligten wussten, dass sich bei hoher Belastung komplexer technischer Systeme unvorhergesehene Effekte ergeben können. Auch gab es nach Aussagen des Zentrums für Datenverarbeitung der Johannes Gutenberg-Universität (ZDV) im Jahr 2020 bereits Cyber-Attacken geringeren Ausmaßes auf die dortige Infrastruktur, auf die reagiert wurde. Deshalb wurde bis zuletzt an der Erhöhung der Ressourcen gearbeitet. So wurden die Lernplattform Moodle im vergangenen Sommer in das Zentrum für Datenverarbeitung umgezogen und rund 600 000 Euro für Serverinfrastruktur, Internetbandbreite und Support investiert. Zu Fragestellungen der Systemkonfiguration wurde externe Expertise eingeholt.

In Vorbereitung des Fernunterrichts wurde zum Jahreswechsel 2020/21 ein zusätzliches Server-Cluster mit 300 Videokonferenz-Servern bei einem deutschen IT-Dienstleister hinzugebucht, um eine Überlastung möglichst zu vermeiden (vgl. Kleine Anfrage – Drucksache 17/14121 – Frage 1).

Die am 4. Januar 2021 konkret aufgetretenen technischen Probleme waren im Vorfeld nicht absehbar, sondern zeigten sich insbesondere durch die Doppelbelastung durch starke legitime Nutzung einerseits und DDoS-Attacke andererseits.

Zu Frage 4:

Bei der Auswahl des Webkonferenzsystems wurden zahlreiche Kriterien berücksichtigt. Bei dem ausgewählten System BigBlueButton handelt es sich um ein in vielen Regionen der Welt im Bildungsbereich eingesetztes Produkt, das genau hierfür konzipiert wurde. BigBlueButton hat bezüglich seiner pädagogischen Verwendbarkeit sowie unter den Aspekten Datenschutz und Datensicherheit überzeugt.

Es bietet eine Reihe von pädagogischen und technischen Möglichkeiten, die bei anderen Systemen teilweise erst später implementiert wurden. Dazu gehört beispielsweise die Entbehrlichkeit einer Softwareinstallation durch die Lauffähigkeit in aktuellen Internetbrowsern, die Möglichkeit zum gemeinsamen Arbeiten an Präsentationen, die Möglichkeit, sogenannte Breakout-Räume für die Arbeit in Kleingruppen zu eröffnen, sowie gemeinsam genutzte „Klassenräume“.

Mit dem Betrieb einer Open-Source-Software auf landeseigenen Servern haben rheinland-pfälzische Schulen den höchsten Standard in puncto Datenschutz und Datensicherheit: Der Betrieb der Server unterliegt – im Gegensatz zu den Servern US-amerikanischer Unternehmen unabhängig vom ihrem physischen Standort – in transparenter Weise allein bundesdeutschem bzw. europäischem Recht. Die Verwendung von Open-Source-Software zeichnet sich dadurch aus, dass der Programmcode von einer breiten Gemeinschaft von Benutzern daraufhin untersucht werden kann, inwiefern er einen Abfluss von Benutzerdaten an Dritte vorsieht. Auch eine Untersuchung auf Sicherheitslücken wird so vereinfacht. Dies ist bei Closed-Source-Produkten per Konstruktion so nicht der Fall. Hinzu kommt, dass die Serviceanbieter von kommerziellen Produkten in der Regel die Software auf eigenen Servern betreiben und sich dieser Betrieb damit der Kontrolle des Auftraggebers entzieht. Durch den Betrieb von BigBlueButton auf eigenen Servern kann langfristig sichergestellt werden, dass die Anforderungen des Datenschutzes erfüllt werden. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit befürwortet diese Lösung ausdrücklich. Viele andere Bildungseinrichtungen nutzen deshalb ebenfalls BigBlueButton.

Während andere Länder sich aktuell noch mit ihren Datenschutzbeauftragten auseinandersetzen, welche Systeme erlaubt werden können, hat sich das Ministerium für Bildung schon während des ersten Lockdowns für diesen sicheren Weg entschieden und durch die frühzeitige Kommunikation Planungssicherheit gegeben. Diese Entscheidung wird durch Rückmeldungen von Lehrkräften, Personalvertretungen und Eltern bestätigt.

Zu den Fragen 5 bis 7:

Nein. Ausschlaggebend waren die Anforderungen an die pädagogischen Funktionen und den Schutz der Daten der Teilnehmerinnen und Teilnehmer, keine Kostenargumente.

In Vertretung:
Hans Beckmann
Staatssekretär