



HESSISCHER LANDTAG

17. 08. 2021

Kleine Anfrage

Dr. Dr. Rainer Rahn (AfD) vom 16.02.2021

Corona-Pandemie – Störungen des Online-Unterrichts durch Externe und Cyberkriminelle

und

Antwort

Kultusminister

Vorbemerkung Fragesteller:

Distanzunterricht und Beschulung in Form von Homeschooling sind seit einiger Zeit für hessische Schüler normaler Alltag. Neben rein technischen Problemen wie der temporären Unerreichbarkeit von Lernplattformen tritt zunehmend das Problem der Störung des Unterrichts durch Externe und Cyberkriminelle in Erscheinung. Dabei wird über Teilnahme von nicht befugten Personen am Online-Unterricht berichtet, die diesen teilweise massiv stören oder behindern – etwa durch Einspielen von Störgeräuschen. In einem Fall wurde über die Einspielung pornografischer Materials in die Plattform einer Grundschule berichtet. Teilweise werden auch Unterrichtsinhalte aufgezeichnet und in den sozialen Medien in Form von Parodien aufgearbeitet und wiedergegeben. Die Teilnahme von unbefugten Personen am Online-Unterricht scheint vielfach relativ einfach zu sein, da der Zugang zu den entsprechenden Plattformen entweder völlig offen ist oder Links und entsprechende Passwörter an Unbefugte weitergegeben werden oder im Netz kursieren. Auch scheint die Kontrolle der teilnehmenden Personen durch die Lehrkräfte – soweit eine solche überhaupt erfolgt – vielfach lückenhaft zu sein.

Vorbemerkung Kultusminister:

Das Hessische Kultusministerium unterstützt die Schulen fortlaufend mit Hinweisen zum Umgang mit virtuellen Besprechungen. Zum Beispiel wurden die Schulen im Jahr 2020 darauf aufmerksam gemacht, dass beim Einsatz von Videokonferenzsystemen ein erhöhtes Risiko durch den Beitritt unerwünschter Personen besteht. Einzelne Vorfälle dieser Art wurden Anfang des Jahres 2021 bekannt, woraufhin das Hessische Kultusministerium umgehend weitere Informationen an alle Schulen versandt hat, damit die Schulen mit diesen Situationen im schulischen Alltag sensibel umgehen können. Diese Informationen beinhalten unter anderem Handlungsempfehlungen des Hessischen Landeskriminalamts und des Hessen CyberCompetenceCenter (Hessen3C) des Hessischen Ministeriums des Innern und für Sport.

Darüber hinaus bereitet das Hessische Kultusministerium aktuell die Einführung einer datenschutzkonformen landesweiten Videokonferenzlösung einschließlich technischem Support für die Schulen vor. Mit dem Landessystem wird den spezifischen Anforderungen für den Schulbetrieb und dem Datenschutz in besonderer Weise Rechnung getragen. Es wird in enger Abstimmung mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit aufgebaut. Mit der Erarbeitung einer landesweiten Videokonferenzlösung reagiert die Hessische Landesregierung auf die datenschutzrechtlichen Unwägbarkeiten, die mit den vorhandenen Videokonferenzangeboten verbunden sind.

Diese Vorbemerkung vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit der Ministerin für Digitale Strategie und Entwicklung sowie dem Hessischen Minister des Innern und für Sport wie folgt:

Frage 1. Wie viele Fälle von Störungen des Online-Unterrichts an hessischen Schulen sind der Landesregierung bekannt?

Dem Kultusministerium wurden über die Staatlichen Schulämter insgesamt vier Fälle gemeldet, die sich als gravierende Störung („Zoombombing“) verursacht durch fremde Personen einordnen lassen.

Frage 2. Über welche Arten der Störungen wurde bei den unter 1. aufgeführten Fällen berichtet?

In zwei Fällen handelte es sich um das Zeigen von pornographischen Darstellungen beziehungsweise Bildern. In zwei weiteren Fällen handelte es sich um grobe Beschimpfungen mit sexistischen Ausdrücken.

Frage 3. Konnten in den unter 1. aufgeführten Fällen die Täter bzw. Tatverdächtigen ermittelt werden?

Frage 4. Falls 3. zutreffend: Konnten die unter 2. aufgeführten Täter bzw. Tatverdächtigen entsprechend zivil-, ordnungsrechtlich oder strafrechtlich verfolgt werden?

Die Fragen 3 und 4 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Zu den konkreten Ermittlungsergebnissen kann aktuell noch keine abschließende Aussage getroffen werden.

Frage 5. Gibt es Vorgaben der Landesregierung an die Schulen über die Ausgestaltung des Online-Unterrichts hinsichtlich der Sicherheit des Zugangs bzw. der Kontrolle und Identifizierung der teilnehmenden Personen?

Frage 6. Falls 5. zutreffend: Welche Vorgaben hat die Landesregierung den Schulen hierzu gemacht?

Frage 7. Falls 5. unzutreffend: plant die Landesregierung, entsprechende Vorgaben zu machen, um einen störungsfreien Online-Unterricht zu gewährleisten?

Die Fragen 5 bis 7 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Auf die Vorbemerkung wird verwiesen. Darüber hinaus ist darauf hinzuweisen, dass grundsätzlich kein vollständiger technischer Schutz vor Angriffen von Dritten möglich ist. Dennoch können geeignete Maßnahmen umgesetzt werden, um das Risiko unautorisierter Zugriffe zu minimieren. Auf diese Maßnahmen hat das Hessische Kultusministerium die Schulen mit dem in der Vorbemerkung genannten Schreiben hingewiesen.

Entscheidend für die Abwehr von Zugriffen von Dritten ist hierbei vor allem der Konferenzzugang. Bei den meisten angebotenen Lösungen erstellt die Lehrkraft einen sogenannten virtuellen Konferenzraum und verschickt hierzu Einladungen oder Identifikationsnummern, sogenannte „Meeting-IDs“. Diese Zugänge sollten niemals öffentlich verteilt oder kommuniziert werden. Die Schülerinnen und Schüler müssen deshalb sensibilisiert werden, mit diesen Zugängen entsprechend vorsichtig und verantwortungsvoll umzugehen. Die Lehrkraft sollte außerdem zu jeder Zeit die Kontrolle über den Zugang zur Videokonferenz haben. Hierzu eignen sich Maßnahmen wie zum Beispiel das Vergeben eines Passwortes oder einer PIN oder auch das Einrichten von Zugangsräumen, über die dann die Teilnehmerinnen und Teilnehmer erst zugelassen werden, wenn man sie eindeutig identifizieren kann. Die Lehrkraft sollte darüber hinaus während der Videokonferenz sicherstellen, dass sie in der Lage ist, Teilnehmende oder unerwünschte Inhalte aus der Konferenz zu entfernen. Konferenzsysteme, in denen es keine explizite Rolle als Administratorin beziehungsweise Administrator für die Lehrkraft gibt, sind nicht zu empfehlen.

Unterstützung steht den Schulen und Lehrkräften über die Fachberatungen für Medienbildung an den Staatlichen Schulämtern sowie die regionalen Medienzentren zur Verfügung. Um mehr Sicherheit im Umgang mit Videokonferenzsystemen zu gewinnen, bietet die Hessische Lehrkräfteakademie Lehrkräften zudem verschiedene Online-Fortbildungen an, die auch die Vermeidung potentiellen Missbrauchs zum Inhalt haben. Darüber hinaus steht Lehrkräften das e-Learning-Angebot „Grundlagenwissen zur Informationssicherheit“ des Hessischen Ministeriums des Innern und für Sport zur Verfügung.

Außerdem sind folgende grundsätzliche Vorkehrungen gemäß Hessen3C zu empfehlen:

- Um auf Sicherheitsvorfälle adäquat reagieren zu können, sind schulinterne Meldekettens einzurichten.
 - Meldungen haben unverzüglich zu erfolgen.
 - Die Schulleitung und im Fall von Videokonferenzsystemen, die durch den Schulträger betrieben werden, die Informationssicherheitsbeauftragte beziehungsweise der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte beziehungsweise der Datenschutzbeauftragte des Schulträgers sind zu informieren.
- Um im Klassenverband zeitnah auf entsprechende Vorfälle reagieren zu können, wird empfohlen, einen einheitlichen E-Mail-Verteiler der jeweiligen Klasse durch die Klassenlehrkraft einzurichten und diesen stets aktuell zu halten. Der Versand von E-Mails durch Lehrkräfte darf ausschließlich über E-Mail-Adressen des Landes oder der Schulträger erfolgen. Darüber hinaus können an der Schule alternative Kommunikationswege genutzt werden.
- Es wird empfohlen, für den Online-Unterricht einen geschlossenen Teilnehmerkreis zu nutzen und die Benutzernamen der Schülerinnen und Schüler so festzulegen, dass eine eindeutige

Identifikation des jeweiligen Gruppenmitglieds möglich ist. Unberechtigte können so schnell identifiziert und aus dem Meeting entfernt werden.

- Die Teilnehmenden sollten darauf hingewiesen werden, dass die zur Einwahl in den Onlineunterricht verwendeten mobilen Endgeräte vor einem unberechtigten Zugriff geschützt sein sollten. Zum Beispiel sollte bei einer Abwesenheit vom Endgerät die Teilnehmende beziehungsweise der Teilnehmende dahingehend sensibilisiert werden, dass sie ihr mobiles Gerät sperren.

Neben den allgemeinen Verhaltensregeln für ein strukturiertes Kommunizieren, die auch außerhalb einer Videokonferenz gelten, gibt es bei Videokonferenzen noch einige zusätzliche Aspekte zu beachten, auf die die Teilnehmenden hingewiesen werden sollten, wie zum Beispiel, dass das Teilen von unangemessenen Inhalten verboten ist oder die Bildschirmfreigabe grundsätzlich deaktiviert sein sollte und nur durch die Lehrkraft freigegeben werden kann. Sofern es trotz der vorgenannten Maßnahmen zu einem Zwischenfall und einer schwerwiegenden Störung kommen sollte, werden von der Polizei unter anderem folgende Maßnahmen empfohlen:

- Sofern es sich um strafrechtlich relevante Sachverhalte handelt, sollten umgehend Screenshots zur Beweissicherung angefertigt und Anzeige bei der zuständigen Polizeidienststelle erstattet werden.
- Nicht eingeladene Personen sollten umgehend aus dem Meeting entfernt werden.
- Bei Zwischenfällen mit Schülerinnen und Schülern sollte die Sitzung umgehend beendet und neue Zugangsdaten mit einem neuen Passwort zur Verfügung gestellt werden.

Im Bereich der kriminalpolizeilichen Prävention stehen in jedem Polizeipräsidium Ansprechpersonen für die Bereiche Jugendkoordination, Prävention Cybercrime und Opferschutz für entsprechende Beratungen bei einem Vorfall oder im Vorfeld zu präventiven Aspekten zur Verfügung. Die Übersicht aller Ansprechpersonen ist im Internet abrufbar. Das Hessen3C berät die Schulträger rund um alle Fragen zur IT-Sicherheit und unterstützt bei Sicherheitsvorfällen.

Wiesbaden, 11. August 2021

Prof. Dr. R. Alexander Lorz