Leitfaden “ Sicherer Videounterricht”

(Stand: 27.04.2020)

Einleitung

Liebe Kolleg*innen,

die Ausnahmesituation der letzten und wohl noch weiter folgenden Wochen bestimmt das Geschehen in der Schule. Sehr viele Lehrkräfte werden ihre Schüler wohl noch eine ganze Weile nicht im Klassenzimmer begrüßen können. Neben allen Betreuungsmöglichkeiten auf digitalem und telefonischem Weg kommt den Videokonferenzen eine immer größer werdende Bedeutung zu. Durch den rasanten Anstieg der Nutzerzahlen dieser Plattformen sind mögliche Probleme in den Fokus von IT-Sicher-heitsforschern und der Presse gerückt. Einige der Probleme waren und sind technischer Natur und können durch regelmäßige Software-Updates behoben werden. Andere Probleme sind durch eine sachgerechte Bedienung vermeidbar.

Sehr viele Kollegen arbeiten bereits mit Videokonferenzen, die Anfragen und Beratungen in dieser Richtung haben sehr zugenommen. Die Möglichkeit von Lehrkräften, mit der Hilfe von Videokonferenztools auf Schüler zuzugehen, ist einer von vielen Bausteinen einer gelingenden Betreuung.

Die Chancen liegen in einer motivierenden Abwechslung zur Einzelarbeit und der Möglichkeit, Inhalte im Gruppengespräch zu vermitteln. Man kann die Schüler*innen sehen, direkt mit ihnen Kontakt aufnehmen und so einen Eindruck erhalten, wie es ihnen geht. Ferner lassen sich auch Erfahrungen im Einsatz mit digitalen Medien sammeln, die auch in Zukunft genutzt werden können.

Keinesfalls soll es eine Verpflichtung sein, mit Videokonferenzen zu arbeiten. Es muss gewährleistet werden, dass alle Schüler*innen die wichtigen Informationen angemessen (Email, Post etc.) erreichen und technisch nicht angebundene Schüler nicht abgehängt werden.

Die Entscheidung für eine Plattform muss gut überlegt sein und beinhaltet, dass dieses eventuell auch über die Krise hinweg längerfristig verwendbar ist. Der Datenschutz soll vorangestellt (Kriterien: Datenschutzkonformität, Möglichkeiten zur Absicherung von Konferenzen) werden, eine eingehende Beratung übernehmen die Datenschutzbeauftragten und BdB.

Sobald Sie die Plattform nicht mehr verwendet wird, empfehlen wir Ihnen eine Kündigung des Auftragsverarbeitungsvertrages und die Löschung der personenbezogenen Nutzerdaten. Danach sollten die Lehrkräfte das Produkt im schulischen Kontext nicht mehr nutzen. Falls ein Nutzerzugang angelegt wurde, sollte dieser gelöscht werden (Schüler Hilfe anbieten).

Dieser Leitfaden soll Ihnen helfen, das von Ihnen gewählte Tool sicher einzusetzen. Dabei sollen alle gängigen Videokonferenztools verwendbar sei, unter Berücksichtigung der entsprechenden Einstellungen. Manche der Aussagen sind nicht deckungsgleich mit früheren Aussagen und der Tatsache geschuldet, dass sich das Thema sehr dynamisch entwickelt hat. Ziel des Leitfadens ist der adäquate Schutz der persönlichen Daten aller Beteiligten. “Adäquat” heißt in diesem Fall, dass das Restrisiko, welches nach der Absicherung verbleibt, in einem akzeptablen Verhältnis steht zum Nutzen von Videokonferenzsystemen zur Unterstützung von "Lernen zuhause". Bitte informieren Sie sich über die Schulamtshomepage immer über den aktuellen Stand.

Schulamt Oberallgäu-Lindau-Kempten, Berater digitale Bildung, Datenschutzbeauftragte

Inhaltsverzeichnis

Mögliche Probleme mit Videokonferenzsystemen

Wie auch andere IT-Lösungen, die heutzutage im schulischen Umfeld im Einsatz sind, sind Videokonferenzsysteme weder vor technischen Schwachstellen noch von unsachgemäßer Bedienung gefeit, die eine mögliche Verletzung des Datenschutzes nach sich ziehen. Hinzu kommt, dass Situationen entstehen können, die für die Beteiligten verstörend wirken können - Stichwort “Zoombombing” (Unbekannte schaffen sich Zugang zu privaten Meetings - siehe am Ende dieser Seite).

Speicherung und Verarbeitung persönlicher Daten

Videokonferenzsysteme verarbeiten persönliche Daten im Sinne der Datenschutzgrundverordnung (DSGVO). Das bedeutet, dass die Verantwortlichen die Pflicht haben, Vorkehrungen zu treffen, damit diese Daten angemessen geschützt und die Nutzer über ihre Rechte informiert werden. Die DSGVO verlangt u. a., dass persönliche Daten nicht ohne weiteres außerhalb der EU verarbeitet werden. Allerdings ist auch ein Server-Standort innerhalb der EU nicht automatisch DSGVO-konform.

Videokonferenzsysteme speichern in den allermeisten Fällen keine Videos - zumindest nicht, wenn diese Funktion nicht explizit aktiviert wird. Aber auch die Metadaten (z. B. wer wann an welcher Konferenz teilnimmt) sind in vielen Fällen persönliche Daten im Sinne der DSGVO. Manche Systeme ermöglichen den Teilnehmern Chatfunktionen. Auch im Chat können möglicherweise sensible Daten ausgetauscht werden. Keine dieser Anforderungen ist ein unüberwindbares Hindernis. Die DSGVO spricht explizit von “angemessenem” Schutz der persönlichen Daten. Wie wir in diesem Dokument aufzeigen, ist genau dieser angemessene Schutz mit dem meisten Videokonferenzsystemen möglich.

Weiterhin ist die Zustimmung aller Beteiligten notwendig. Dabei ist genau festzulegen, welche Daten verarbeitet werden und für welchen Zweck. Auch hierzu geben wir Tipps.

Unautorisierter Zugriff auf Konferenzen

Ein großes Thema in den Medien ist das sogenannte “Zoombombing”. Um eines klar zu stellen: Dies ist kein Problem des Videokonferenzsystems “Zoom”, sondern betrifft praktisch alle Videokonferenzsysteme.

“Zoombombing” beschreibt den Vorgang, bei dem unautorisierte Personen Zugang zu einer Videokonferenz erhalten und oft verstörendes Material über ihren Videofeed oder Screenshare verbreiten. Dabei ist zu erwähnen, dass auch bereits autorisierte Teilnehmer (Schüler) in ähnlicher Weise Video- oder Bildmaterial teilen können, welches nicht von der Lehrkraft genehmigt wurde.

Der Grund, warum Zoombombing in den meisten Fällen möglich ist nicht, dass eine Konferenz aufwendig “gehackt” wurde. Es bedarf dabei keiner fortgeschrittener technischer Finesse des Angreifers. Die Meeting-IDs der Konferenzen sind oft relativ einfach, z. B. eine 10-stellige Zahl. Die “Angreifer” haben keine bestimmte Konferenz als Ziel, sondern probieren stur alle möglichen Meeting-IDs durch und wenn eine Meeting-ID erfolgreich erraten wird, kann der Angreifer sich in diese Konferenz einwählen.

DSGVO - was ist das und warum sollte keiner Angst davor haben?

Das Ziel der Datenschutzgrundverordung (DSGVO) ist der Schutz persönlicher Daten. Das betrifft sowohl die der Lehrkräfte als auch die der Schüler*innen und Erziehungsberechtigten. Viele der großen Anbieter haben auf ihren Internetseiten Informationen bereitgestellt, die sich mit der Einhaltung der Datenschutzgesetze befassen.

Solche Information finden Sie, indem Sie in einer Suchmaschine nach “<Name des Tools> DSGVO” suchen also z. B. “Webex DSGVO”. Alternativ nach der englischen Abkürzung “GDPR” also z.B. “Webex GDPR”. GDPR steht für “General Data Protection Regulation” - die Datenschutz-Richtlinie der EU die Deutschland als “Datenschutzgrundverordung / DSGVO” umgesetzt hat. Ist eine Lösung “GDPR-compliant” kann davon ausgegangen werden, dass sie auch dem deutschen DSGVO entspricht, da EU-weit der Datenschutz vereinheitlicht wurde.

Zustimmung zur Datenverarbeitung

Die DSGVO schreibt vor, dass in den allermeisten Fällen Daten nur gespeichert und verarbeitet werden können, wenn eine explizite Einwilligung vorliegt (wie beispielsweise die Einwilligungserklärungen zur Datenverarbeitung von Banken, Versicherungen bzw. die “Cookie Banners” auf Internetseiten).

Die Einwilligungen dürfen nicht zu allgemein gehalten sein, d. h. sie müssen ziemlich genau beschreiben, für was die Einwilligung gegeben wird. “Ich erlaube meine Daten zu speichern und verarbeiten.”... ist keine gültige Einwilligung. “Ich erlaube Firma X meine Daten zum Zweck der Kundeninformation zu verarbeiten. Firma X darf meine Daten nicht an Dritte weiterreichen.”... wäre schon besser. Wichtig hier ist auch zu erwähnen, dass Einwilligungen jederzeit ohne Angabe von Gründen widerrufen werden können. Zudem muss auf der Einwilligung die Möglichkeit gegeben werden, nicht zuzustimmen.

Auftragsverarbeitung

Die Auftragsverarbeitung kommt ins Spiel, falls Sie eine Lösung einsetzen, in der die Schule Benutzerkonten für alle Beteiligten (Schüler und/oder Lehrkräfte) selbst verwaltet. Das ist z. B. bei Office 365/Microsoft 365 der Fall, aber auch bei einigen kostenpflichtigen Angebote von z. B. Zoom, GoTo-Meeting und Webex.

Eine der grundlegenden Konzepte ist, dass der Dateneigentümer (also die Schule) einen Auftrag zur Datenverarbeitung mit einem Datenverarbeiter schließen muss. Dies bedeutet, dass die Schule bzw. der Schulträger für die Daten der Schüler und Lehrkräfte verantwortlich ist und damit im Zweifelsfall nachweisen muss, dass die Verarbeitung persönlicher Daten bei einer dritten Partei (hier dem Videokonferenzsystem) ordnungsgemäß beauftragt wurde.

Eine Vereinbarung zur Auftragsverarbeitung ist laut Artikel 28 DSGVO notwendig. So ein Formular finden Sie meist auf der Homepage des kommerziellen Anbieters, bitte schließen Sie so einen Auftragsdatenverarbeitungsvertrag ab.

Individuelle Benutzerkonten

Einige Anbieter ermöglichen es, dass Nutzer einzelne Konten anlegen, die nicht von der Schule selbst verwaltet werden. Mit diesen Konten ist es möglich an Konferenzen teilzunehmen oder auch Konferenzen zu starten. Beispiele solcher Lösungen sind Webex oder Zoom. Bei vielen Tools ist auch die Teilnahme ganz ohne Anlegen von Benutzerkonten möglich. Auch hier sind Lösungen wie GoToMeeting, Webex, Zoom zu nennen. In diesem Fall ist der Abschluss einer Vereinbarung zur Auftragsverarbeitung nicht notwendig - und oft auch gar nicht möglich.

WICHTIGER HINWEIS

Ein Einsatz von individuellen Benutzerkonten befreit Sie nicht von der Einhaltung der Datenschutzgrundverordnung. Es muss ein Videokonferenzsystem eingesetzt werden, das DSGVO-konform ist.

Tipps für eine sichere Videokonferenz

Videokonferenzsysteme können sicher eingesetzt werden und in vielen Schulen ist das auch schon der Fall. Oft besteht aber noch Verbesserungsbedarf. Ein unsicherer Einsatz erfolgt meist aus Unwissen und nicht aus Absicht.

Sicherheit ist kein Ausstattungsmerkmal einer Lösung wie es z. B. eine Klimaanlage bei einem Auto ist. Sicherheit ist eine Kombination aus technischen Funktionen und organisatorischen Maßnahmen. Verschiedene Systeme bieten unterschiedliche Lösungsansätze an, aber das alleine reicht nicht aus. Auch die Anwendung und Verwaltung ist Teil des Sicherheitskonzepts und mindestens ebenso wichtig wie eine technische Funktion der Software an sich. Hier nun ein paar Tipps zum sicheren Einsatz von Videokonferenzsystemen.

Welches Tool?

Viele bekannte und verbreitete Videokonferenzsysteme können sicher betrieben werden. Tatsache ist, dass praktisch alle unsicher betrieben werden können und somit gegen die DSGVO verstoßen.

Opensource Lösungen

Opensource Lösungen - hier sind besonders Jitsi und BigBlueButton (BBB) zu nennen - sind nicht automatisch DSGVO-konform. Bei beiden Lösungen ist ein DSGVO-konformer Betrieb praktisch nur über einen Server, der selbst gehostet ist, zu gewährleisten. Frei verfügbare Jitsi/BBB Instanzen - auch wenn diese in der EU betrieben werden - sind nicht DSGVO-konform, solange die Betreiber nicht die notwendigen technischen und organisatorischen Bedingungen erfüllen.

Auch eine selbst gehostete Jitsi oder BBB Instanz ist nicht zwingend DSGVO-konform. Dazu ist mehr Aufwand notwendig, als diese Instanz selbst zu installieren und am Laufen zu halten. Sollte Ihre Schule die technischen und organisatorischen Voraussetzungen für einen sicheren Betrieb eines Servers erfüllen, spricht nichts dagegen, diese Lösung einzusetzen.
Sollten Eltern selbst eine Instanz betreiben und der Schule zur Verfügung stellen, ist dieses Engagement zwar zu begrüßen, aber nicht zu empfehlen, solange diese Instanz nicht nachweislich DSGVO-konform betrieben wird. Es ist allerdings möglich, dass auch Privatpersonen als Datenverarbeiter auftreten und damit eine Vereinbarung zur Datenverarbeitung mit der Schule abschließen können. Sollte in der Vereinbarung der DSGVO-konforme Betrieb zugesichert werden und die Rechte und Pflichten beider Parteien im Einklang mit Artikel 28 DSGVO festgelegt werden, ist auch diese Variante ein gangbarer Weg.

Firmangebote wie z. B. Webex, Zoom, GoToMeeting, Microsoft Teams, Whereby etc.

Sollten Sie ein Tool eines kommerziellen Anbieters verwenden, achten Sie darauf, dass der Anbieter einen DSGVO-konformen Betrieb ermöglicht und zusichert.

Informationen rund um den DSGVO konformen Betrieb und Nutzung liefern u.a. folgende Internetseiten der Hersteller:
https://help.webex.com/de-de/weov2i/Cisco-Webex-Support-for-GDPR
https://support.logmeininc.com/de/gotomeeting/help/is-gotomeeting-gdpr-compliant-g2m800019
https://support.office.com/de-de/article/datenschutzgrundverordnung-dsgv-und-teams-free-bdf2e378-da6b-48d9-a13d-44917c6ee90a
https://zoom.us/de-de/privacy.html
https://whereby.helpscoutdocs.com/article/334-data-storage-security

Selbstverständlich bedingt der Einsatz eines Systems, dass der jeweilige Hersteller eine DSGVO-konforme Bedienung anbietet. Als Beispiel sei hier die Aufzeichnung von Konferenzen zu nennen. Diese ist für den Einsatzzweck „Schule zuhause“ nicht ratsam und sollte - wenn überhaupt - nur mit ausdrücklicher Genehmigung aller Beteiligten erfolgen. Ansonsten würde damit ein Verstoß gegen die DSGVO erfolgen.

Zustimmung der Erziehungsberechtigten

Die schriftliche Zustimmung der Erziehungsberechtigten zum Videounterricht ist notwendig. Im Anhang finden Sie ein Beispiel, wie solch eine Zustimmung formuliert werden kann. Wichtig hierbei ist, dass die Zustimmung freiwillig erfolgt, jederzeit widerrufen werden kann und genau festgelegt, für welchen Zweck die Einwilligung erfolgt. Hierin sollte auch erwähnt werden, dass eine Teilnahme an der Videokonferenz auch möglich ist, wenn man die Kamera selbst ausgeschaltet hat.

WICHTIGER HINWEIS
Falls noch keine Einverständniserklärung vorliegt, muss diese dringend eingeholt werden.

Einladungen für Konferenzen

Einladungs-Links oder Meeting-IDs sollten niemals über soziale Medien wie Facebook oder Twitter verteilt werden, da dort die Gefahr besteht, diese Information unbeabsichtigt mit einem unerwünschten Personenkreis zu teilen. Es kann von Vorteil sein, die Meeting-ID unverändert zu lassen, um den Schülern einen einfacheren Zugang zu ermöglichen und unnötige Verzögerungen zu vermeiden.

Absicherung von Konferenzen

Gerade gleich bleibende Meeting-IDs müssen besonders gut gesichert werden, aber auch alle anderen Arten von Konferenzen bedürfen Schutzmechanismen. Welche das sind hängt von der eingesetzten Software ab.

Zutrittskontrolle

Mindestens eine der unten aufgeführten Optionen muss verwendet werden.

Passwörter

Die meisten Videokonferenzsysteme bieten neben der Meeting-ID die Möglichkeit an, ein Passwort festzulegen. Ohne dieses Passwort ist eine Teilnahme an der Konferenz nicht möglich. Je nach System ist es möglich, das Passwort als Teil der Meeting-URL den Teil-nehmern bekannt zu geben oder dieses Passwort separat zu kommunizieren. Auch wenn ein separat kommuniziertes Passwort sicherer ist, ist auch eine komplexere Meeting-URL aus-reichend, um “Zoombombing” zu verhindern. (immer vorausgesetzt die Meeting-URL oder das Passwort werden von niemandem einer breiteren Öffentlichkeit bekannt gemacht.)

Warteraum / Lobby

Weiterhin ermöglichen es einige Systeme als Alternative zu Passwörtern - oder als Zusatz - eine Meeting-Lobby einzurichten. Das ist ein virtueller Warteraum, der vom Meeting Host (= der Lehrkraft) überwacht wird. Die Teilnehmer müssen in der Meeting Lobby warten, bis die Lehrkraft sie in das eigentliche Meeting eintreten lässt. Hierbei ist zu beachten, dass die Lehrkraft anhand z. B. der Namen der Teilnehmer erkennt, wer in der Lobby ist. Hilfreich ist deswegen die Regel, Klarnamen (z. B. nur Vornamen) für alle Teilnehmer zu verwenden.

Weitere Verwaltung von Teilnehmern

Zutritt ohne Moderator/Host

Je nach Einstellung kann es möglich sein, dass Teilnehmer an einer Konferenz teilnehmen können, ohne dass der Moderator/Host bereits in der Konferenz ist. Diese Funktion sollte wenn möglich über die Einstellungen unterbunden werden.

Beenden der Konferenz durch den Moderator/Host

Stellen Sie sicher, dass alle Teilnehmer die Konferenz verlassen oder (falls möglich) beenden Sie die Konferenz für alle Teilnehmer.

Sperren

Manche Systeme erlauben es eine Konferenz zu sperren, wenn alle Teilnehmer “angekommen” sind. Sowohl im Warteraum als auch in der gesperrten Konferenz muss sichergestellt sein, dass die Lehrkraft ein Auge auf Schüler hat, die aus technischen Gründen die Konferenz verlassen müssen, z.B. weil deren Internetverbindung unterbrochen wird. Dadurch kann es passieren, dass diese Schüler wieder im Warteraum landen und auf “Abholung” angewiesen sind.

Teilnehmer entfernen

Unliebsame Teilnehmer aus der Konferenz zu entfernen ist technisch meist möglich. Ob dies im Falle von Schülern pädagogisch sinnvoll ist, darf im Einzelfall geklärt werden.

Teilen von Inhalten blockieren

Screenshare, Bildschirm teilen

Einige Systeme erlauben es, nur dem Host (Lehrkraft) Inhalte zu teilen. Das betrifft z. B. den Bildschirm oder ein Applikationsfenster. Andere Systeme erlauben das anfänglich jedem Teilnehmer, aber der Host kann dies unterbinden. Auch von dieser Funktion sollte Gebrauch gemacht werden. Achten Sie darauf, was geteilt wird. Beschränken Sie das Teilen wenn möglich auf ein bestimmtes Fenster oder stellen Sie sicher, dass keine sensitiven Daten auf keinem Teil des Bildschirms zu sehen sind. Dies gilt auch, wenn Sie mehrere Bildschirme haben - achten Sie hier darauf, nur einen (und den richtigen) Bildschirm zu teilen.

Chat blockieren

Falls das System ein Chat zwischen den Teilnehmern ermöglicht, ist ggf. das Unterbinden dieser Funktion ratsam. Teil der Chatfunktion ist oft auch die Möglichkeit, jede Art von Dateien und Links zu senden - je nach Inhalt der Datei bzw. Ziel des Links kann das z. B. urheberrechtliche Probleme nach sich ziehen. Ob das Blockieren des Chats für mehr Aufmerksamkeit sorgt, weil die Teilnehmer weniger Ablenkung haben sei dahingestellt. Genauso einfach können die Teilnehmer über andere Applikationen chatten.

Videos der Teilnehmer

Eine Möglichkeit der Teilnehmer (unerwünschte) Inhalte zu teilen, ist das entsprechende Objekt in die Kamera zu halten. Das kann bei manchen Systemen verhindert werden, indem nur das Moderatorenvideo sichtbar ist und/oder die Teilnehmer sich gegenseitig nicht per Video sehen können. Allerdings ist ja gerade das einer der großen Vorteile einer Videokonferenz, Bitte die Videofunktion mit Bedacht (zeitlich begrenzt und die Kamerafunktion mit einem virtuellen Hintergrund) zu wählen bzw. die Sichtbarkeit innerhalb der Konferenz verändern.

Ende der Nutzung

Nach Wiederaufnahme des regulären Unterrichtsbetriebs (Ende des Schuljahres, Ende der Nutzung des Tools) wird eine Kündigung des Auftragsverarbeitungsvertrages mit einer Löschung der personenbezogenen Nutzerdaten empfohlen. Die Lehrkräfte sollen angewiesen werden, dass sie die Plattform nicht mehr verwenden und Nutzeraccounts gelöscht werden (ggf. Schüler dabei helfen).

Nicht-technische Maßnahmen und Etiquette

Zugangsdaten teilen

Ob mit oder ohne Passwort: Zugangsdaten zu Videokonferenzen sind prinzipiell leicht zu verteilen. Genau das kann zu Problemen führen. Das beste zusätzliche Meeting-Passwort nützt nichts, wenn es mitsamt der Meeting ID unautorisiert geteilt wird. Es muss klar geregelt sein, dass die Zugangsdaten nicht außerhalb der Klassengemeinschaft geteilt werden.

Keine unerlaubten Aufzeichnungen

Das Recht am eigenen Bild ist nicht aufgehoben, nur weil die Zustimmung zu einer Video-konferenz vorliegt. Aufzeichnungen jeglicher Art sollten klar verboten sein, solange nicht alle (!) Beteiligten zugestimmt haben. Es ist zu beachten, dass eine Aufzeichnung nicht nur über die Videokonferenz-Software erfolgen kann, sondern auch über Screenshots oder im einfachsten Fall per Handy-Foto vom Bildschirm.

Chatprotokolle nicht außerhalb der Klasse teilen

Einige Tools ermöglichen es, den Chatverlauf zu speichern. Aber selbst wenn diese Funktion abgeschaltet ist, wäre es möglich, den Text während der Konferenz zu kopieren oder ein Foto davon zu erstellen. Es muss klar geregelt sein, dass der Chatverlauf in keinster Weise verbreitet wird und damit die Privatsphäre anderer verletzt wird.

Freiwilligkeit

Die Teilnahme an der Videokonferenz ist freiwillig. Dem Schüler werden wichtige Inhalte zum Unterrichtsstoff auch ohne Video-Konferenz zugänglich gemacht (E-Mail o. ä.). Die Zustimmung für die Teilnahme am Videounterricht bedingt nicht, dass die Schüler auch ihre Kamera aktivieren. Da in einigen Fällen Einblick in den persönlichen Lebensbereich möglich ist, ist es nachzuvollziehen, dass einige dies nicht möchten. Dies sollte von allen Beteiligten respektiert werden.

Anhang

Sicherheit von Zoom

Auch wenn dieser Leitfaden nicht auf eine bestimmte Videokonferenzlösung abzielt, ist die enorme mediale Aufmerksamkeit hinsichtlich des Tools “Zoom” bzw. “Zoom.us” und die daraus resultierende Unsicherheit bzgl. der Nutzung einen eigenen Abschnitt wert. Wie schon erwähnt, kann Zoom, wie jedes der erwähnten anderen Tools, datenschutzkonform eingesetzt werden. Im Gegenzug dazu kann Zoom auch in einer Art und Weise eingesetzt werden, die nicht datenschutzkonform ist - dies liegt in der Hand des Nutzers, nicht des Anbieters.

Zoom hatte und hat, wie praktisch jede andere Software auch, sicherheitsrelevante Fehler und Unzulänglichkeiten. Es ist zwingend notwendig, diese im Zusammenhang mit der Art der Nutzung zu bewerten. Angreifer mit finanziellen Interessen beschränken sich auf lohnende Ziele und haben dafür nur einen kurze Zeitspanne zur Verfügung da die Hersteller bestrebt sind, Lücken schnellstmöglich zu schließen. Weitere Gruppen von Angreifern sind sogenannte Hacktivists (meist mit politischem Motiv) oder Anarchisten die meist ohne eigentliches Motiv Angriffe starten. Bei beiden ist eher unwahrscheinlich, dass „Schule zuhause“ ein attraktives Angriffsziel darstellt. Bleiben sogenannte “Nation States”-Angreifer, die praktisch über unbegrenzte Ressourcen verfügen. Sie sind von Regierungen direkt oder indirekt gefördert. Selbst für diese Art von Angreifern ist „Schule zuhause“ ein eher unattraktives Ziel - auch unter dem Gesichtspunkt, dass die zu verwendeten Angriffstechniken besser auf andere Ziele wie z. B. Regierungsorgane, Verteidigungsindustrie etc. angewendet werden, da hier der Abgriff von hochsensitiven Daten eine wesentlich höhere Rendite erzielt.

“Zoombombing” war und ist kein exklusives Problem von Zoom und kann durch die oben genannten Tipps verhindert werden. Die Tatsache, dass der Name eines Produktes in dem Namen des “Angriffs” vorkommt ist der weiten Verbreitung von Zoom zu verdanken und nicht Schwachstellen, die nur Zoom betreffen. Die Firma “Zoom.us” geht seit Wochen offen mit den Anschuldigungen um, hat viele Schwachstellen beseitigt, neue Sicherheitsfunktionen implementiert und bereits vorhandene sichtbarer gemacht. So findet z. B. eine DSGVO-konforme Ent- und Wiederverschlüsselung beim Anbieter statt. Weiterführende Betrachtungen bzgl. der Sicherheit von Zoom (auf Englisch)

https://www.computerweekly.com/news/252482048/Zoom-to-roll-out-fresh-cyber-security-updates
https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/
https://www.entrepreneur.com/article/349653
https://medium.com/@0xamit/zoom-isnt-malware-ae01618e2046

Anlage 1 – Vorschlag Einverständniserklärung Video-Unterricht

Einverständniserklärung Video-Unterricht

Ich bin damit einverstanden, dass mein Kind an Video-Konferenzen als unterstützende Maßnahme für die Unterrichtsgestaltung an der Schule ABCDE teilnehmen darf.
Mein Kind kann mit oder ohne aktivierte Videokamera an den Video-Konferenzen teilnehmen.

Mir ist bekannt, dass die Stimme und ggf. ein Video meines Kindes mit der Lehrkraft und den anderen Kindern der Klasse geteilt wird. Es ist möglich, dass sich andere Personen aus dem Umfeld der anderen Kinder in den Videos befinden können und ggf. auch das Video meines Kindes sehen können.

Die Video-Konferenzen werden von der Lehrkraft nicht aufgezeichnet oder veröffentlicht. Ich oder mein Kind werden auch selbst keinerlei Aufzeichnungen der Video-Konferenzen vor-nehmen.

Für die Absicherung und Software-Aktualisierung der Endgeräte (Computer, Tablets, Smartphones) bin ich selbst verantwortlich und ich leite die Zugangsdaten der Video-Konferenzen an niemanden außerhalb der Klassengemeinschaft weiter. Ich kann diese Einverständniserklärung jederzeit widerrufen. Die Einwilligung ist freiwillig. Aus der Nichteinhaltung oder dem Widerruf der Einwilligung entstehen keine Nachteile.

O Ich bin damit einverstanden, dass mein Kind an der Video-Konferenz teilnimmt
O Ich bin nicht damit einverstanden, dass mein Kind an der Video-Konferenz teilnimmt

_____ _____
Name des Kindes Klasse des Kindes

_____
Namen der Erziehungsberechtigten

_____ _____
Ort, Datum Unterschrift der/des Erziehungsberechtigten

_____
ab dem 14. Geburtstag zusätzlich: Unterschrift der Schülerin / des Schülers

Mögliche Ergänzung: Ich bin über das zu verwendete Tool XY zur Video-Konferenz, auch über mögliche Risiken, informiert worden.
Anmerkung: Wenn dieser Satz enthalten ist, müssen Informationen z. B. über einen Elternbrief zwingend gegeben werden.

Anlage 2 - Informationsschreiben an die Erziehungsberechtigten zum Video-Unterricht

Vorschlag 1

Sehr geehrte Eltern und Erziehungsberechtigte!

Aufgrund der aktuellen Situation, können wir Ihr Kind leider nicht wie gewohnt persönlich unterrichten. Trotzdem ist uns als Schule der persönliche Kontakt zu Ihrem Kind wichtig, diesen möchten wir gerne aufrechterhalten. Die Nutzung einer Video-Konferenz soll uns helfen, den sozialen Kontakt zwischen Ihrem Kind und der Lehrkraft aufrechtzuerhalten.
(ggf. weitere Beweggründe/Vorteile nennen)

Für die Umsetzung der Video- Konferenz haben wir uns für XYZ (Tool nennen) entschieden. Informationen finden Sie auch unter www…...com (Internetseite verlinken)

(Einloggen/ Zugang erklären, technische Voraussetzungen oder auf gesonderte E- Mail- Anleitung verweisen.)

Die Schule/ Lehrkraft hat die Einstellungen der Video- Konferenz geprüft. Die Schule/Lehrkraft legt allein fest, wer an der Konferenz teilnimmt. Sie lädt die Teilnehmer (Mitschüler) passwortgeschützt ein. Keine fremde Person wird eingeladen werden. Die Konferenz wird nur im gewohnten Kurs/Klassenverband stattfinden. Ihr Kind muss in keinem Fall seine Kamera und/oder Ton einschalten. Ein Zuhören/Schreiben reicht aus.

Die Teilnahme an dieser Video- Konferenz ist für Ihr Kind ein freiwilliges Angebot. Wenn Ihr Kind nicht an der Video- Konferenz teilnimmt, wird ihm kein Nachteil im Zugang zum Lernstoff entstehen.

Vorschlag 2: “Mein Kind bekommt Videounterricht!”

Liebe Eltern und Erziehungsberechtigte,

Ihr Kind hat nun die Möglichkeit am Videounterricht teilzunehmen. Sicher haben Sie in den verschiedenen Medien über diverse Probleme mit Videokonferenzsystemen gehört oder gelesen. Dieses Schreiben liefert Ihnen einige Informationen über mögliche Risiken und wie wir diesen begegnen. Ihr Kind wird nicht nur einen interessanten und lehrreichen Videounterricht erhalten, sondern auch einen sicheren Videounterricht.

1. Mögliche Risiken

a) Zoombombing

Ein großes Thema in den Medien ist das sogenannte “Zoombombing”. Das ist kein Problem des Videokonferenzsystems “Zoom”, sondern betrifft praktisch alle Videokonferenzsysteme.
“Zoombombing” beschreibt den Vorgang, bei dem unautorisierte Personen Zugang zu einer Videokonferenz erhalten und oft verstörendes Material verbreiten. Der Grund, warum Zoombombing möglich ist, ist in den meisten Fällen nicht, dass eine Konferenz aufwendig “gehackt” wurde. Falls die Videokonferenz ohne weitere Absicherungen erstellt wurde, bedarf es dabei keiner fortgeschrittenen technischen Finesse des Angreifers. Die Meeting-IDs der Konferenzen sind oft relative einfach z. B. eine 10-stellige Zahl. Die “Angreifer” haben keine bestimmte Konferenz als Ziel, sondern probieren stur alle möglichen Meeting-IDs durch und wenn eine Meeting ID erfolgreich erraten wird, kann der Angreifer sich in diese Konferenz einwählen.

b) Probleme mit dem Datenschutz

Die Datenschutz-Grundverordnung (DSGVO) fordert von uns als Schule, dass wir mit den persönlichen Daten aller Personen, mit der wir als Schule in Kontakt stehen sicher umgehen. Dazu gehören die persönlichen Daten Ihres Kindes aber auch Ihre persönliche Daten und natürlich auch die aller Lehrkräfte.

Videokonferenzsysteme verarbeiten persönliche Daten aller Teilnehmer - also auch die Ihres Kindes. Die Verarbeitung besteht u. a. in der Weiterleitung der Videodaten an die anderen Teilnehmer, Protokollierung der IP Adresse. Eine unautorisierte Weitergabe dieser Daten wäre ein Verstoß gegen die DSGVO.

Andere Teilnehmer (d.h. die Lehrkraft und Mitschüler aus der eigenen Klasse) können Ihr Kind hören und ggf. sehen. Damit ist es ggf. möglich, dass die Teilnehmer Einblicke in ihre Privatsphäre erhalten da außer Ihrem Kind vielleicht noch Teile des Raumes sichtbar sind. Möglicherweise sind aber auch Sie oder andere Familienmitglieder für die anderen Teilnehmer sichtbar.

2. Wie wir die Risiken minimieren

a) Freiwilligkeit

Die Teilnahme am Videounterricht ist absolut freiwillig. Wenn daran teilgenommen wird, ist die Verwendung einer Kamera ebenfalls freiwillig d.h. Ihr Kind kann an der Videokonferenz teilnehmen ohne selbst gesehen zu werden. Jedes Kind kann sich (und soll sich in den meisten Fällen) auch stumm schalten - also das Mikrofon ausschalten - solange es von der Lehr-kraft nicht aufgefordert wird zu sprechen.

b) Zutrittsbeschränkungen

Um Zoombombing zu verhindern sichern wir die einzelnen Videokonferenzen ab mit:

[Bitte die nicht verwendete Sicherheitsmaßnahme aus der untenstehenden Liste löschen! Daran denken: mindestens eine der Maßnahmen muss verwendet werden!]

• Einem zusätzlichen Passwort. Dadurch ist das Durchprobieren aller Meeting-IDs durch einen Angreifer, um unautorisiert an einer Konferenz teilzunehmen, nicht mehr von Erfolg gekrönt.
• Einen virtuellen Warteraum. Die Lehrkraft muss alle Teilnehmer erst einzeln Einlass gewähren. Unbekannte Teilnehmer werden dadurch am Zutritt gehindert.

c) Verwendung eines sicheren Videokonferenzsystems
Wir verwenden ein Videokonferenzsystem das den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entspricht. Da wir als Schule für die persönlichen Daten, die wir speichern und verarbeiten, verantwortlich sind, ist es selbstverständlich, dass wir Software und Dienstleistungen nur einsetzen, wenn diese ebenfalls DSGVO-konform betrieben werden.

Wir haben uns bewusst für [TOOL XZY] entschieden, da es nicht nur die Anforderungen der Datenschutz-Grundverordnung erfüllt, sondern auch von den Funktionen und der Nutzerfreundlichkeit für uns die beste Wahl ist.
Wir bitten Sie die Einwilligungserklärung sorgfältig zu lesen, bevor Sie diese unterschreiben.