

Stellungnahme zum Einsatz der Videokonferenz-App ZOOM für das „Homeschooling“ im Rahmen von (teilweisen) Schulschließungen

Motivation

Für den Einsatz von Videokonferenzen im Rahmen des „Homeschoolings“ gibt es eine Reihe guter Gründe:

- Videokonferenzen erlauben einen persönlicheren, direkteren Sozialkontakt in einer Gruppe als es mit E-Mails möglich ist. Sie können helfen, der gefühlten oder tatsächlichen Isolation während der Kontaktbeschränkungen entgegenzuwirken.
- Viele Fragen lassen sich in einem Gespräch leichter stellen und leichter klären, oft reicht schon eine kurze Bemerkung aus. Durch ein Gespräch in der Gruppe sind diese Klärungen außerdem erheblich effizienter als in vielen einzelnen Mails.
- In der E-Mail-Kommunikation fehlen Informationen wie die Betonung, Mimik und Gestik und lassen so nicht so leicht erkennen, wie bestimmte Aussagen aufgenommen wurden oder ob z. B. eine Nachfrage angebracht wäre.
- In einer Videokonferenz kann der Lehrer/die Lehrerin mittels „Bildschirmfreigabe“ (o.ä.) Inhalte wie Arbeitsblätter, Lösungen, Tafelbilder vom eigenen Gerät aus allen SchülerInnen zeigen, ggf. können auch SchülerInnen ihre Lösungen für alle sichtbar demonstrieren. Die gemeinsame Arbeit an einem „Tafelbild“ ist ebenfalls möglich. Manche Systeme unterstützen auch klassische Gruppenarbeiten durch die zeitweilige Aufteilung in Teilgruppen, zu denen der Lehrer/die Lehrerin hinzugerufen werden kann. Somit erlauben solche Videokonferenz-Apps die Abbildung typischer Unterrichtsmethoden.

Darüber hinaus gibt es auch Argumente gegen die Nutzung von Videokonferenzen:

- Nicht jeder Schüler, jede Schülerin hat zu Hause einen hinreichend schnellen Internetzugang, manche auch kein geeignetes Endgerät (oder eins, das nur zeitweise zur Verfügung steht). Eventuell vorhandene Smartphones sind für reine Videochats zwar oft ausreichend, bei Videokonferenzen mit Bildschirmübertragung wird es aufgrund der Displaygröße schwierig.
Die Hilfsangebote der Schule hinsichtlich der Ausstattung anzufragen oder zu nutzen, bedeutet für viele eine große Hemmschwelle. Somit kann sich die soziale Kluft durch Videokonferenzen vergrößern.
- Manche empfinden Videokonferenzen als fremd und unangenehm – nicht zuletzt überträgt man Daten (Video, Audio, eigene Antworten, ...) über das Internet.

Der letzte Punkt ist hierbei nicht von der Hand zu weisen: Die Nutzung von Videokonferenz-Software berührt auch Fragen des Datenschutzes, weshalb die Auswahl von Videokonferenzen als Kommunikationsform an sich sowie die Wahl der passenden Software gut überlegt sein sollte.

Für das Gymnasium der Benediktiner gilt: Die Schulleitung empfiehlt grundsätzlich auch den Einsatz von Videokonferenzen als ergänzende Kommunikationsform, auch wenn für die Zusendung von Aufgaben, die Rückübermittlung von Schülerlösungen und für die Zusendung von Feedback durch den Lehrer einerseits lo-net²-Mails und andererseits lo-net²-Dateiablagen zentral bleiben.

Zur Auswahl der Software

Für Videokonferenzen gibt es am Markt sehr viele Angebote. Eine zentrale Beschaffung einer Softwarelösung hat bislang nicht stattgefunden, wohl aber eine laufende Auseinandersetzung mit dem am Markt befindlichen bekannteren Systeme: Neben den „großen“ wie Zoom, WebEx, Teams und Skype gehören dazu Discord, Jitsi, GoToMeeting, Adobe Connect, (Teamviewer) Blizz und Big Blue Button.

Der Funktionsumfang im Hinblick auf die schulische Nutzung variiert dabei gar nicht so sehr, viele Angebote sind für Schulen zur Zeit sogar kostenlos nutzbar. Hinsichtlich der Stabilität, der Einfachheit der Bedienung, der möglichen Anzahl der Teilnehmer und nicht zuletzt unter Datenschutzaspekten gibt es deutliche Unterschiede, die hier nicht im Einzelnen aufgeführt werden sollen.

Derzeit nutzen etliche Kolleginnen und Kollegen den Dienst Zoom für Videokonferenzen. Vorteile dieses Dienstes sind die sehr einfache Bedienung von Schülerseite, die hohe Verfügbarkeit und Stabilität sowie der Funktionsumfang. Im Gegensatz zu vielen anderen Diensten ist bei Zoom auch keine Registrierung der Teilnehmer notwendig, d.h. die Schüler müssen keine Mailadresse o.ä. preisgeben – sie nutzen den Dienst anonym. Für Schulen bietet Zoom den Dienst derzeit (auch über die sonst vorgesehene 40-Minuten-Beschränkung hinaus) kostenfrei an.

Kritik an Zoom

Vor allem Mitte/Ende März 2020 gab es allerdings verschiedene kritische Berichte zu Zoom. Zum einen gab es ein Rechtsgutachten des Datenschutzbeauftragten der Kasseler Universität, Prof. Dr. Roßnagel, vom 23.03.20, auf das sich die meisten mir bekannten Presseveröffentlichungen beriefen. Auch ich habe dieses gelesen, meinerseits am 30.03. die Vorwürfe gegenüber Zoom nachzuvollziehen versucht – und konnte die Vorwürfe beim besten Willen nicht nachvollziehen. Der Grund war, dass Zoom bereits mit einer komplett überarbeiteten Datenschutzerklärung am 29.03. reagiert hatte, die viele Vorwürfe entkräftete. In einem zweiten Gutachten vom 01.04.20 kommt Prof. Dr. Roßnagel denn auch zu dem Fazit, dass Zoom nun auch an der Uni Kassel genutzt werden darf:

„8. Zusammenfassend ist für die Nutzung von Zoom-Diensten durch die Universität Kassel zu beachten, dass Zoom nicht alle Anforderungen der Datenschutz-Grundverordnung erfüllt. Dennoch ist die Nutzung von Zoom-Diensten nach den neuen Datenschutzrichtlinien vertretbar, wenn die Universität
a) alle zentral einstellbaren Konfigurationsmöglichkeiten zugunsten des Datenschutzes nutzt und

b) die einzelnen Nutzer über die individuellen datenschutzgerechten Konfigurationsmöglichkeiten informiert.“

Auch hinsichtlich der Voreinstellungen hat Zoom inzwischen reagiert, so dass diese im Sinne der Forderungen weitgehend so gestaltet sind, dass das Gebot der Datensparsamkeit eingehalten ist. Das sogenannte „Zoom-Bombing“, das Stören eines öffentlichen (!) Meetings durch nicht eingeladene Nutzer, wurde hierdurch ebenfalls wirksam verhindert.

Zoom wurde darüber hinaus für die falsche Behauptung einer Ende-zu-Ende-Verschlüsselung kritisiert. Dass Zoom zunächst angegeben hatte, dass man eine solche einsetze, ist kritikwürdig. Dass sie nicht eingesetzt wird, aber nicht so sehr: Eine Bitraten- und Auflösungsregulierung, wie sie vorgenommen wird, damit auch Nutzer mit schwächeren Anbindungen den Dienst nutzen können bzw. bei vielen Nutzern nur verkleinerte Videobilder übertragen werden, wäre sonst gar nicht möglich, und folgerichtig bieten auch die anderen von uns in Erwägung gezogenen Dienstleister bzw. Softwareplattformen diese nicht an (WebEx warb damit, hat die Werbung inzwischen aber auch zurückgezogen).

Der Bundesbeauftragte für Datenschutz, Ulrich Kelber, hat seinerseits in einem Interview vom 24.05.2020 mit dem Handelsblatt deswegen davon abgeraten, Zoom zu verwenden, man solle stattdessen auf Anbieter mit einer Ende-zu-Ende-Verschlüsselung ausweichen. Welche Anbieter dieses in einer für Schulen verfügbaren Weise anbieten, hat er leider auch auf Nachfrage nicht mitgeteilt.

Bitte bedenken Sie: Wenn man fordert, dass die Kommunikation zwischen Lehrern und Schülern grundsätzlich Ende-zu-Ende-verschlüsselt erfolgt, so darf man weder das Telefon benutzen noch Mails in der herkömmlichen Weise versenden. Sowohl bei der Telefonie als auch bei E-Mails erfolgt nur der Transport der Inhalte verschlüsselt (wie bei den Videokonferenzdienstleistern auch), beteiligte Dienstleister haben aber technisch grundsätzlich die Möglichkeit, auf die Inhalte zuzugreifen. (Das dürfen diese aber dank DSGVO bzw. (in den USA) EU-US-Privacy Shield nicht ohne Weiteres, wobei die Schwelle hierfür in den USA bekanntermaßen faktisch deutlich niedriger ist.)

Dass darüber hinaus in den vergangenen Jahren vereinzelt weitere Sicherheitsprobleme aufgrund von Softwarefehlern bei Zoom bekannt worden sind, ist sicherlich nicht erfreulich – zugleich gibt es diese Meldungen über etliche Anbieter. Bemerkenswert ist aber, dass Zoom nicht nur Sicherheitslücken unverzüglich stopfte, sondern bei den datenschutzrechtlichen Vorwürfen unmittelbar reagierte, was die „Großen“ der Branche typischerweise nicht oder erst nach gravierenden Interventionen machen. (Software ohne Sicherheitslücken gibt es leider i.W. nicht – nicht zuletzt deswegen muss man ja seine Software regelmäßig aktualisieren...)

Zu einer im April 2020 gemeldeten angeblichen Sicherheitslücke gibt es die Stellungnahme des Unternehmens, dass es sich hier mutmaßlich um „Credential-Stuffing-Angriffe“ handelte, die zunächst einmal wenig mit Sicherheitslücken von Zoom zu tun haben, wie auch durch Fachzeitschriften bestätigt wurde.

Zur Erläuterung: Viele Internetnutzer benutzen für die Anmeldung bei verschiedenen Diensten ihre (immer gleiche) Mailadresse und häufig auch eines von nur sehr wenigen

unterschiedlichen Kennworten (oder gar immer das gleiche). Wenn nun bei einzelnen dieser Dienste aufgrund von Sicherheitslücken Daten abgegriffen werden, werden diese automatisiert für weitere Angriffe ausgenutzt – wie hier zum Beispiel zur Anmeldung bei Zoom – und bei Erfolg ggf. weiterverkauft oder anderweitig ausgenutzt.

Im Übrigen führte auch das Schulministeriums Zoom anfangs in seinen Unterstützungsangeboten für das Homeschooling auf, und selbst unsere Landesregierung bot Mitte April an, dass man sich per Zoom z.B. dem Presse-Briefing zuschalten konnte.

Es gab eine Stellungnahme des Berliner Datenschutzbeauftragten, der angegeben hat, dass Zoom, Microsoft Teams und Skype nicht datenschutzgerecht seien – aber leider begründete dieser das in keiner Weise inhaltlich, was mehrere Anwälte/Jurablogs in ihren Veröffentlichungen wiederum kritisieren. Als Stand der Kritik des Berliner BfD war der 2. April 2020 angegeben. Mittlerweile wurde der Berliner Datenschutzbeauftragte von Microsoft wegen der rufschädigenden Behauptungen abgemahnt, seine Kritik war zunächst nicht mehr auf seiner Webseite veröffentlicht. Am 25.05.20 veröffentlichte er eine neue Fassung. Auch hierin gibt er an, dass Zoom nicht datenschutzgerecht sei – leider nach wie vor ohne jegliche Begründung und somit in keiner Weise nachvollziehbar.

Es gibt etliche – teilweise sehr ausführlich begründete und mit Quellenverzeichnissen belegte – Stellungnahmen behördlicher Datenschutzbeauftragten, die den Einsatz von Zoom für datenschutzrechtlich zulässig halten (u.a. die DSB der HU Berlin, der TU Darmstadt, des Hessischen Datenschutzbeauftragten, der Uni Würzburg, der Uni Bielefeld).

Darüber hinaus gibt es auch anderslautende Stellungnahmen, die weitaus weiter gehen – am weitesten geht dabei der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in der Beantwortung einer Anfrage zur Nutzung der Microsoft-Clouddienste: „empfiehlt BfDI für den Einsatz von Windows 10 die Trennung vom Internet“, d.h. nach dessen Empfehlung sollten Windows 10-Rechner grundsätzlich nicht mit dem Internet verbunden sein.

Fazit

Vor der Empfehlung, Zoom für Unterrichtseinheiten im Rahmen des „Homeschooling“ einzusetzen, habe ich mich im Rahmen meiner Möglichkeiten recht ausführlich damit auseinandergesetzt – Stand heute würde ich meine Empfehlung bekräftigen, und die positiven Rückmeldungen der KollegInnen, die das bereits einsetzen, bestärken mich in der Auffassung, dass meine Abwägung hier klar zugunsten dieses Dienstleisters ausfällt.

Dass langfristig eine Lösung zu bevorzugen ist, bei der man es mit einem europäischem Anbieter, der der Datenschutzgrundverordnung direkt unterliegt, zu tun hat, oder eventuell auch eine „in-house“-Lösung, bei der man auf keine externen Anbieter angewiesen ist, liegt auf der Hand. Für ein möglichst zügig umsetzbares „Homeschooling“ erscheint die Abwägung zugunsten Zoom aber angemessen.

*Joachim Deckers, 25.05.2020
aktualisiert 29.05.2020*