Rechercheauftrag
Projekt digitale Hochschule
Prof. Thomas Hoeren

Bearbeiter wiMi Julian Albrecht
30.04. - 02.05.20

Fragestellung:

a) Was ist Zoom auf tatsächlicher Ebene, wer betreibt es, wo stehen die Server u.Ä.

b) Datenschutzrechtliche Kritik

c) Wie Zoom darauf reagiert hat

d) Erste Einschätzung zur Möglichkeit einer rechtlich zulässigen Nutzung von Zoom durch Universitäten

e) Bebilderung einiger Einstellungsmöglichkeiten bei Zoom, etwa wie Teilnehmer aus Konferenzen ausgeschlossen werden können, um die Konferenz bei Störungen zu schützen

Hintergrund:

Die Uni Münster hat sich für Zoom als flächendeckendes Video-Konferenz-System entschieden und mit Zoom einen Lizenzvertrag geschlossen (WWUZoom[1]). Dabei wurde unter anderem ein Auftragsverarbeitervertrag (AVV) geschlossen. Erste andere Universitäten fragen an, ob und wie Münster Zoom datenschutzrechtskonform seinen Mitarbeitern und Studierenden anbieten kann. Einige Datenschutzaufsichtsbehörden haben sich allgemein kritisch zur Nutzung kommerzieller, amerikanischer Videokonferenzsoftwaresystemen gezeigt.

Eine Stellungnahme hierzu und Handreichung zur datenschutzrechtskonformen Nutzung der Software wäre als erste wichtige Aufgabe des neu anlaufenden Drittmittelprojektes Digitale Hochschule zu sehen.

[1] https://www.uni-muenster.de/IT/services/kommunikation/wwuzoom/index.html

Kurzzusammenfassung

Die starke Verbreitung des Dienstes Zoom seit Beginn der Corona-Pandemie (200 Mio. tägliche Konferenzteilnehmer) hat durch den Fokus in IT-Sicherheitskreisen zu dem Bekanntwerden verschiedener Datensicherheitslücken sowie anderer datenschutzrechtlicher Mängel geführt. Zoom Inc. hat auf die Kritik ungewöhnlich schnell reagiert und legt spätestens seit dem 01.04.20 den Fokus auf die Verbesserung der Daten- und IT-Sicherheit, zunächst für 90 Tage seit dem 01.04.

Viele Mängel wurden mit kleineren Patches innerhalb weniger Tage nach Bekanntwerden behoben. Mit der neuen Programmversion Zoom 5.0, abrufbar seit 27.04.20, werden weitere Mängel behoben. Sofern man von grundsätzlicher zoomunabhängiger Kritik an Datenverarbeitung in den USA (welche durch das sog. Privacy Shield geregelt wird) absieht, erscheint spätestens mit Zoom 5.0 eine DSGVO-konforme Nutzung durch öffentliche Stellen wie Universitäten z.B. in Online-Vorlesungen ohne weiteres möglich. Es kann argumentiert werden, dass bereits zuvor eine DSGVO-konforme Nutzung möglich war.
Dies lässt sich durch eine anlassbezogene, auf das Erforderliche beschränkte Nutzung von Zoom (nur bei nötigen synchronen Lehrelementen) sowie datenschutzfreundliche Voreinstellungen erreichen. Auf der sicheren Seite wäre man, böte man für kleinere, sowie datenschutzsensiblere synchrone Sitzungen ein alternatives, datenärmeres, „on premises“ betriebenes Konferenzsystem an.

Zu beachten ist, dass für das Eingreifen einige der Neuerungen von Zoom 5.0 (insb. der höhere Transport-Verschlüsselungs-Standard nach dem Stand der Technik) *alle Teilnehmer* einer Konferenz das Update installiert haben müssen, damit sie eingreifen. Dies umzusetzen erscheint bei Vorlesungen mit über 100 Teilnehmern praktisch unmöglich. Ab dem 30.05.20 wird man Zoom nur noch in Versionen ab 5.0 nutzen können.

a) Was ist Zoom auf tatsächlicher Ebene, wer betreibt es, wo stehen die Server?

Allgemeine Infos

- Videokonferenzsoftware
- Betreiberin: Zoom Video Communications, Inc. (Amerikanische Corporation) mit Sitz in San José, Kalifornien, USA
- Ca. 2300 Mitarbeiter
- 2011 gegründet, 2013 Launch der Software, Börsengang 2019
- Selbstverständnis: „Marktführer für reine Videokonferenzen“
- Company mission: Make video communications frictionless
- Kernmerkmale: easy-to-use, scalable, interoperable
    - Besonders einfach zu benutzen, da für Teilnehmer keine Anmeldung nötig ist vor Teilnahme, lediglich eine schnelle Installation des Clients
    - Besonders viele Teilnehmer sind möglich
    - Große Interoperabilität mit Betriebssystemen und Integrationen in andere Apps
- Nutzerzahlen von 10 Mio pro Monat im 12/2019 auf 200 Mio. pro Monat in 03/2020
- Serverstandorte in Australien, China, Europa, Indien, Japan/Hongkong, Kanada, Lateinamerika und den USA.

Funktionen des Kernprodukts ZoomMeetings

- Videokonferenzen
- Bildschirm teilen, auch mehrere Teilnehmer gleichzeitig oder nacheinander

- „Verschlüsselung für alle Meetings, rollenbasierte Benutzersicherheit, Passwortschutz, Warteräume, und Teilnehmer in Warteschleife stellen."
- Aufzeichnen möglich
- Team Chat
- „Breakup-Sessions" sind möglich, dh. zB von 100 Teilnehmer-Konferenz in 10 Breakup-Sessions á 10 Teilnehmern
- Virtueller Hintergrund ist möglich
- Umfragen sind möglich
- Teilen von Inhalten ist möglich

b) Datenschutzrechtliche Kritik
c) Wie Zoom Inc. darauf reagiert hat

Datum	**Kritik**	**Behoben nach meiner Einschätzung?**
Mitte März	Funktion, die es Konferenz-Host ermöglicht, zu prüfen, ob Teilnehmer Zoom im Vordergrund laufen haben	(+) Global deaktiviert, 02.04.20[2]
26.03.20	Zoom übermittelt personenbezogene Daten an bestimmte Unter-Auftragsverarbeiter, die in den Datenschutzbestimmungen nicht ausgewiesen werden[3]	(+) Datenschutzhinweise am 30.03.20 überarbeitet und auch eine Liste von Subprocessors veröffentlicht[4]
23.03.20	Datenschutzerklärung genügt nicht den Anforderungen der Art. 13 ff. DSGVO[5]	(+), dito
26.03.20	Zoom schickt bei der iOS Anwendung heimlich Daten an Facebook, auch wenn nicht ein Facebook-Login verwandt wird[6]	(+), das kritische Facebook-SDK wurde aus dem iOS Client entfernt[7] am 27.03.
31.03.20	Zoom erweckt den Eindruck eine End-to-End-Verschlüsselung leisten zu können, tut dies aber tatsächlich nicht. Fremde können nicht auf die Kommunikationsinhalte zugreifen, Zoom allerdings schon[8]	(+) was den Eindruck und die Kommunikation angeht; Zoom hat die angewandte Verschlüsselung erklärt[9]

[2] https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking
[3] https://www.kuketz-blog.de/Zoom-uebermittelt-personenbezogene-daten-an-drittanbieter/
[4] https://zoom.us/de-de/subprocessors.html; https://zoom.us/de-de/subprocessors.html
[5] Stellungnahme von Prof. Roßnagel, CIO der Uni Kassel, 23.03.20, abzurufen unter https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjPs7G5-JLpAhVJxhoKHcRnDV0QFjABegQIBBAB&url=https%3A%2F%2Fwww.uni-kassel.de%2Feinrichtung%2Findex.php%3FeID%3DdumpFile%26t%3Df%26f%3D1092%26token%3D0568e4e5bd9f740baf69bf375411bb6c8bd2e37a&usg=AOvVaw1VG7a1WDYCnWvd0Kxo1E-S
[6] https://www.heise.de/mac-and-i/meldung/Bericht-Zoom-App-fuer-iOS-reicht-Daten-heimlich-an-Facebook-weiter-4691613.html
[7] https://blog.zoom.us/wordpress/de/2020/03/27/die-verwendung-des-facebook-sdk-im-ios-client/
[8] https://theintercept.com/2020/03/31/zoom-meeting-encryption/
[9] https://blog.zoom.us/wordpress/de/2020/04/01/die-fakten-rund-um-zoom-und-die-verschluesselung-fuer-meetings-webinare/

31.03.20	Es wird keine echte End-to-End-Verschlüsselung geleistet, dh. Zoom selbst kann auf die Konferenzinhalte zugreifen	(-) technisch schwierig aber möglich (vgl. Facetime) Keine Lösung, auch nicht mit 5.0, indes nach Einschätzung vieler für Art. 32 DSGVO im Regelfall Transportverschlüsselung nach dem Stand der Technik ausreichend
03.04.20	Es wird ein alter, nicht hinreichender Verschlüsselungsstandard (128-AES Schlüssel im ECB-mode) verwandt[10]	(+) mit Version 5.0 wird branchenüblicher 256-AES Standard verwandt, **sofern alle Teilnehmer einer Konferenz 5.0 installiert haben**
März	Sog. Zoombombing ist relativ einfach möglich, dh. Störung von Konferenzen durch Fremde, die sich durch erratene Passwörter oder öffentlich gepostete Zugangslinks ohne weitere Zugangsbeschränkungen Zugang verschaffen zu Konferenzen und dann anstößiges, beleidigendes, diskriminierendes usw. Material teilen	(+) Konferenz-Host selbst kann hinreichende Schutzmaßnahmen treffen, zB: - Passwort vorsehen - Warteraum einrichten - Bildschirm nur von Host zu teilen als Voreinstellung - Raum abschließen vgl. hierzu Blogpost[11]
01.04.20	Rendering und Anklickbarmachen von UNC Links[12]	(+) am 01.04. durch Patch
	Privacy Shield nicht ausreichend	(+/-) Ist generelle Frage, losgelöst von Zoom. Gegenstand eines Verfahrens vor dem EuGH[13] und viel kritisiert; momentan aber noch wirksamer EU-Rechtsakt (Angemessenheitsbeschluss der Kommission) und Grundlage sämtlicher Datenverarbeitungen von US-Softwareunternehmen[14]
Weitere Verbesserungen mit Zoom 5.0, teilweise erst wirksam, sofern alle Teilnehmer einer Konferenz nachgerüstet haben; dies ist spätestens mit systemweiten obligatorischen Update am 30.05. der Fall:	• AES 256-bit GCM encryption (s.o.) • Report a User feature (gegen Zoombombing) • Encryption icon zur Kontrolle der aktuellen Verschlüsselung • Auswahlmöglichkeit der data-centers, die das eigene Meeting hosten – wobei das US-data	

[10] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
[11] https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/
[12] https://www.tomsguide.com/news/zoom-password-malware-flaw
[13] http://curia.europa.eu/juris/fiche.jsf?id=T;738;16;RD;1;P;1;T2016/0738/P&lgrec=de&language=de
[14] https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165de.pdf

		center vorausgewählt und nicht änderbar ist; zB aber China muss nicht angesteuert werden • Enhanced profile picture control for the host • Passwort security

Einschätzung der Datensicherheitsbemühungen von Zoom Inc.

Mit Pressemitteilung vom 1.04.20[15] verspricht der CEO von Zoom Eric S. Yuan, dass sich das Unternehmen in den nächsten 90 Tagen auf Daten- und IT-Sicherheit sowie Datenschutzthemen fokussiert. Unter anderem folgende Maßnahmen sollen umgesetzt werden und sind Stand jetzt bereits teilweise umgesetzt:

- Keine Entwicklung neuer Funktionen mehr, sondern Konzentration aller Ingenieurs-Kapazitäten auf die Sicherheitsthemen
- Gründung eines Chief Information Security Officers-Boards, indem sich verschiedene CISOs verschiedener großer Unternehmen der Softwarebranche austauschen über Standards und best practices
- Reporting zu ihm als CEO zu den genannten Themen
- Transparente Kommunikation nach außen mit einem regelmäßigen schriftlichen Bericht und wöchentlichen Webinaren
- Beauftragung von Sicherheitsexperten und Hackern, die Sicherheitslücken identifizieren sollen

Nach meinem ersten Eindruck und nach Lektüre einiger Artikel von Experten[16] ist der Umgang des Unternehmens mit den immer neu auftauchenden Problemen vorbildlich und nicht selbstverständlich. Der proklamierte Fokus auf die Verbesserung der Sicherheit erscheint angesichts schneller Fehlerbeseitigungen glaubhaft. Der Fokus erscheint auch plausibel und im Eigeninteresse des Unternehmens zu liegen mit Blick auf die stark steigenden Nutzerzahlen und Geschäftschancen auch mit öffentlichen Stellen (Schulen, Universitäten etc.) und auf dem europäischen Markt. In diesen beiden Bereichen gilt ein gutes Datenschutzniveau als Verkaufsargument.

d) erste Einschätzung zur Möglichkeit einer rechtlich zulässigen Nutzung durch Universitäten

(teilweise graue) Literatur:

- *Stoklas, Jonathan*, Datenschutz in Zeiten von Corona, ZD-Aktuell 2020, 07093
- *John, Nicolas,* Corona is calling – Datenschutzrechtliche Probleme bei der Auswahl und Benutzung von Videokonferenzprogrammen für den Arbeits- und Hochschulalltag
- *Piltz, Carlo/Hessel, Stefan*, Berliner Datenschutzaufsicht: Stellungnahme und Checkliste zum Datenschutz bei Videokonferenzen, abzurufen unter https://www.reuschlaw.de/news/berliner-datenschutzaufsicht-stellungnahme-und-checkliste-zum-datenschutz-bei-videokonferenzen/
- *Hansen-Oest, Stephan,* Hilfe…ist „Zoom" etwa eine Datenschleuder?, abzurufen unter https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder/#update16

[15] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[16] https://medium.com/@0xamit/zoom-isnt-malware-ae01618e2046; https://www.cs.columbia.edu/~smb/blog/2020-04/2020-04-06.html; https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder/

- *Berliner Datenschutzbeauftragte Maja Smoltczyk*, Zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, 08.04.20, abzurufen unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf
- *Berliner Datenschutzbeauftragte Maja Smoltczyk,* Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen, 08.04.20, abzurufen unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf
- Pressestelle des Landesbeauftragten für Datenschutz BaWü Stefan Brink, Datenschutzfreundliche technische Möglichkeiten der Kommunikation, 17.04.20, abzurufen unter https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/
- Schröter, Nico/Zöllner, Lukas, Videokonferenz mit Zoom und Co. – Denn sie wollen wissen, was sie tun (dürfen), 15.04.2020, abzurufen unter https://www.lto.de/recht/hintergruende/h/datenschutz-behoerden-dsgvo-zoom-videokonferenz-unsicherheit/
- *Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Dieter Kugelmann*, Einsatz von videogestützter Kommunikationstechnik zu Zwecken des Schulunterrichts während der Corona-Krise, abzurufen unter https://www.datenschutz.rlp.de/de/themenfelder-themen/videogestuetzte-kommunikationstechnik/
- Prüfung verschiedener Dienste durch den Datenschutzbeauftragten des Kantons Zürich, abzurufen unter https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/digitale-zusammenarbeit.html
- *Lukaß, Tom,* Videochats & Datenschutz – Heute: „Zoom", 6.04.20, letztes Update am 29.04.20, abzurufen unter https://www.datenschutz-notizen.de/videochats-datenschutz-heute-zoom-4325330/
- *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,* Datenschutz: Plötzlich Videokonferenzen – und nun?, abrufbar unter https://www.datenschutzzentrum.de/uploads/it/ULD-Ploetzlich-Videokonferenzen.pdf
- *Schwenke, Thomas*, DSGVO-sicher? Videokonferenzen, Onlinemeetings und Webinare (mit Anbieterübersicht und Checkliste), 16.04.20, abrufbar unter https://datenschutz-generator.de/dsgvo-video-konferenzen-online-meeting/#Fazit

Nach einer ersten Einschätzung ist eine datenschutzrechtskonformen Nutzung von Zoom jedenfalls nach dem Upgrade auf Version 5.0 durch alle Teilnehmer möglich, etwa durch eine Universität im Rahmen interaktiver Online-Vorlesungen. Selbstgehostete datenärmere Alternativen wie etwa Jitsi Meets oder BigBlueButton bieten offenbar nicht einen ähnlichen Funktionsumfang und eine vergleichbare Performanz für große synchrone Meetings. Die Datenschutzbehörden *empfehlen* einstimmig solche OpenSource-Lösungen, welche „on premises" auf unieigenen Servern gehostet werden. Gleichwohl sind sie – soweit Stellungnahmen veröffentlicht sind – mehrheitlich wohl nicht der Rechtsauffassung, dass ein Auftragsverarbeitung durch Zoom *per se* unzulässig ist.

Für eine rechtskonforme Nutzung muss eine Uni einen AVV mit Zoom Inc. schließen, welche diesen vorformuliert zur Verfügung stellt[17]. Noch besser wäre es, einzelne Klauseln nachzuverhandeln. Inwieweit dies für größere institutionelle Kunden möglich ist, ist noch unbekannt. Die Datenverarbeitung in den USA, welche sich auch mit der neuen Funktion der Version 5.0 zur Auswahl der data centers nicht vermeiden lässt, ist nach geltender Rechtslage zulässig, da ein entsprechender Angemessenheitsbeschluss der europäischen Kommission (das sog. Privacy Shield) in Kraft und Zoom insoweit zertifiziert ist.

Das größte Risiko aus datenschutzrechtlicher Perspektive sehe ich nach ersten Recherchen in der fehlenden echten Ende-zu-Ende-Verschlüsselung der Kommunikation, welche technisch zwar schwer, aber doch möglich zu sein scheint (vgl. Facetime von Apple). Im Hinblick auf Art. 32 DSGVO verdient dieser Aspekt noch einer genaueren Untersuchung. Indes scheint die Einschätzung verbreitet, dass eine Transport-Verschlüsselung nach dem Stand der Technik ausreichend und eine Ende-zu-Ende-Verschlüsselung nur für besonders sensible Datenkategorien erforderlich ist.

[17] https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf

Für eine datenschutzrechtskonforme Nutzung wären meines Erachtens folgende Dinge zu beachten:

- Neben Zoom für Elemente der synchronen Lehre wird ein anderes datenärmeres Programm zur asynchronen Lehre verwandt:

  Im Sinne des Grundsatzes der Datenminimierung, welcher bereits bei der Auswahl der verwendeten Videokonferenz-Software zu berücksichtigen ist, darf Zoom nicht flächendeckend für den Lehrbetrieb eingesetzt werden, sondern nur soweit erforderlich, dh. insoweit *synchrone Lehre* mit einer großen Anzahl an Teilnehmern im Lehrkonzept des jeweiligen Lehrenden vorgesehen ist. Für asynchrone „Videokonserven" stehen indes leistungsfähige und datenärmere Alternativprogramme zur Verfügung.
  Nach den Empfehlungen etwa des Zentrums für digitale Lehre Münster bietet es sich aus pädagogischer Perspektive an, Vorlesungen mit einem Nebeneinander eines asynchronen und eines synchronen Elements zu digitalisieren. Im asynchronen Element findet in einem längeren Block „frontale Lehre" ohne Interaktion statt, welches Studierende je nach Präferenz zeitlich flexibel abrufen können und etwa auch pausieren und zurückspulen können. In dem synchronen Element werden die Studierenden einbezogen, es können Fragen gestellt werden, es wird diskutiert usw. Dieses Element kann durch den Hinweis und das Zurverfügungstellen von Materialien im Vorhinein vorbereitet werden.

  In diesem Konzept könnte der asynchrone Teil in Münster bspw. über eLectures aufgezeichnet werden. Der synchrone Teil könnte in einem großen Zoom-Meeting ohne Aufzeichnung durchgeführt werden.

- Neben Zoom wird ein datenärmeres Programm für synchrone Videokonferenzen mit kleinerem Teilnehmerkreis verwandt, insbesondere bei Erwartung besonders sensibler Daten wie zB Prüfungsgespräche, Beratungen u.Ä.:
  Für ein konsequent datenarmes Konzept wäre nach einer ersten Einschätzung eine differenzierte Nutzung eines anderen weniger performanten und funktionalen, für kleinere Gruppen aber hinreichend leistungsfähigen Programms wie etwa Jitsi Meet (nach Angaben des ZIV Münster für bis 10 Teilnehmer), BigBlueButton oder DFNconf[18] angezeigt.
  Inwieweit die „Reibungsverluste" durch das Eingewöhnenmüssen verschiedener Akteure mit mehr als einem Programm in eine Abwägung eingestellt werden können, bedarf einer vertieften Recherche.

  vgl. etwa den Pilotbetrieb gleich vier versch. Videokonferenzsysteme der TU Dresden, welche eine nach Sensibilität und Größe des Teilnehmerkreises differenzierte Nutzung vorschlägt, Frank Schulze in einer Email an die edu-coordination-Mailliste, eingerichtet vom DFN:

  „Die TU Dresden hat mit Beginn der Krise gleich vier Systeme parallel aufgebaut, die jetzt im Einsatz sind:

  - Jitsi für kleine Gruppen bis sechs Personen
  - Big Blue Button für die Lehre und vertrauliche Sitzungen mit max. 25 Kameras und insgesamt max. 100 Teilnehmern
  - GoToMeeting für Seminare und Vorlesungen mit max. 25 Kameras und insgesamt bis zu 250 Teilnehmern
  - GoToWebinar für Seminare und Vorlesungen mit max. 6 Kameras und insgesamt bis zu 1.000 Teilnehmern

[18] Vgl. für Münster https://www.uni-muenster.de/IT/services/kommunikation/videokonferenz/.

- Zoom für Seminare ohne sensible Daten mit max. 49 Kameras und bis zu 300 Teilnehmern“[19]

- Bei der Verwendung von Zoom müssen die Unis als Verantwortliche datenschutzfreundliche Voreinstellungen treffen (zB, Ton- und Videoübertragungen der Studierenden nicht als default, Anzeige der Profilbilder nicht als default usw.) und ggfs. manche Einstellungsmöglichkeiten für einzelne Konferenz-Hosts (zB Seminarleiter) blockieren, Art. 25 DSGVO.
- Ein Zwang zur Audio- oder Videoübertragung durch Teilnehmer jedenfalls bei nicht anwesenheitspflichtigen Veranstaltungen ist nicht zulässig.

Sonstiges

Es sei darauf hingewiesen, dass unter anderem folgende Bildungseinrichtungen Zoom zumindest als Teil des Toolkits zur digitalen Lehre nutzen: HS Mainz; TH Köln; Uni Marburg; Uni Bielefeld; Uni Lüneburg; Uni Potsdam; Schulen München; TU Darmstadt; HS Bochum.

[19] Genauer und inkl. Bewertung des Datenschutzniveaus: https://tu-dresden.de/zih/dienste/videokonferenz.

e) Bebilderung einiger Einstellungsmöglichkeiten bei Zoom, etwa wie Teilnehmer aus Konferenzen ausgeschlossen werden können, um die Konferenz bei Störungen zu schützen

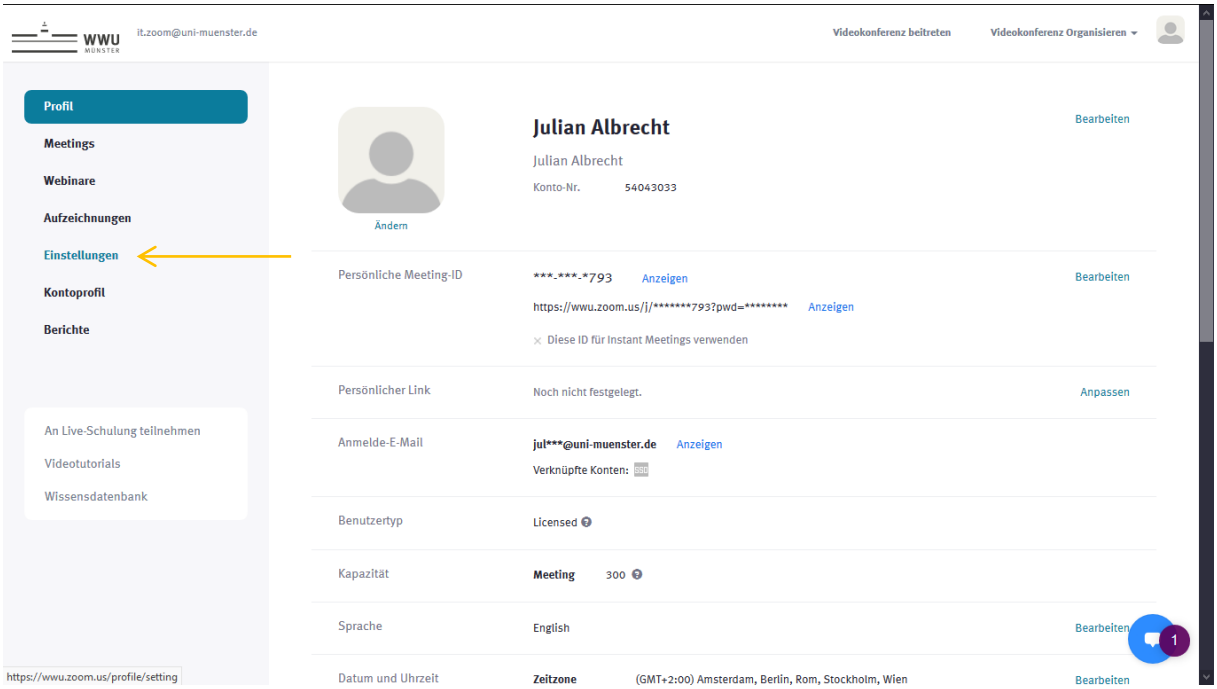

Abb.1: Jeder Videokonferenz-Host kann vor Starten einer Konferenz recht umfangreiche Einstellungen treffen, welche teilweise auch datenschutzrechtlich relevant sind. Man gelangt in dieses Menü zB bei WWUZoom, wenn man sich unter wwu.zoom.us anmeldet, statt direkt eine Konferenz startet oder an einer solchen teilnimmt.

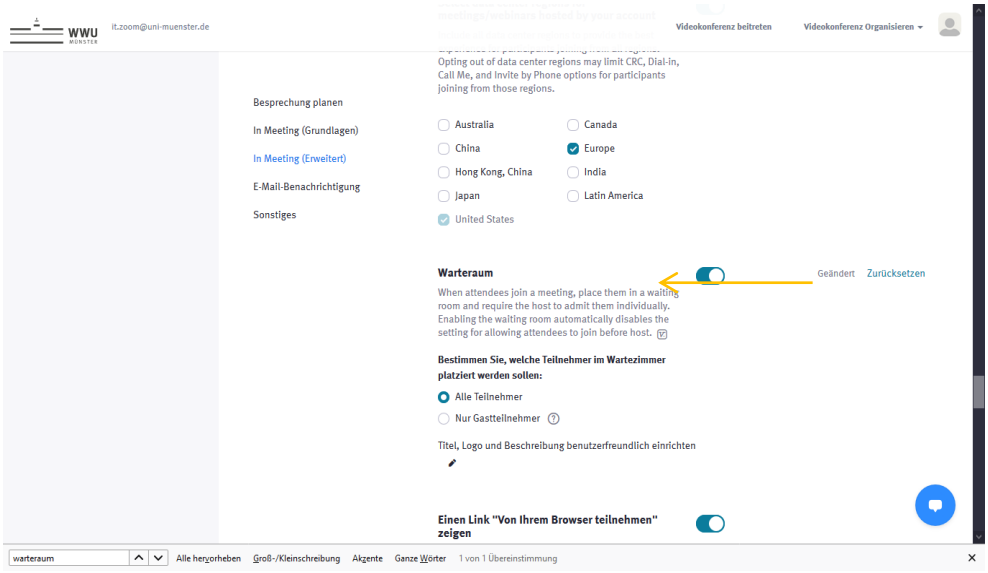

Abb. 2: Jeder Videokonferenz-Host kann recht umfangreiche Einstellungen treffen vor Erstellung einer Konferenz, welche auch datenschutzrechtlich relevant sind. Der Verantwortliche iSd DSGVO (zB eine Uni), welche mit Zoom Inc. einen AVV abgeschlossen hat und institutioneller Kunde ist, kann teilweise die default-Einstellungen treffen und dabei etwa den Grundsatz der Datenschutzfreundlichkeit und Datenminimierung gem. Art. 5, 25 DSGVO beachten.

Eine Abwahl der USA als Standort eines verarbeitenden data centers ist aktuell nicht möglich.

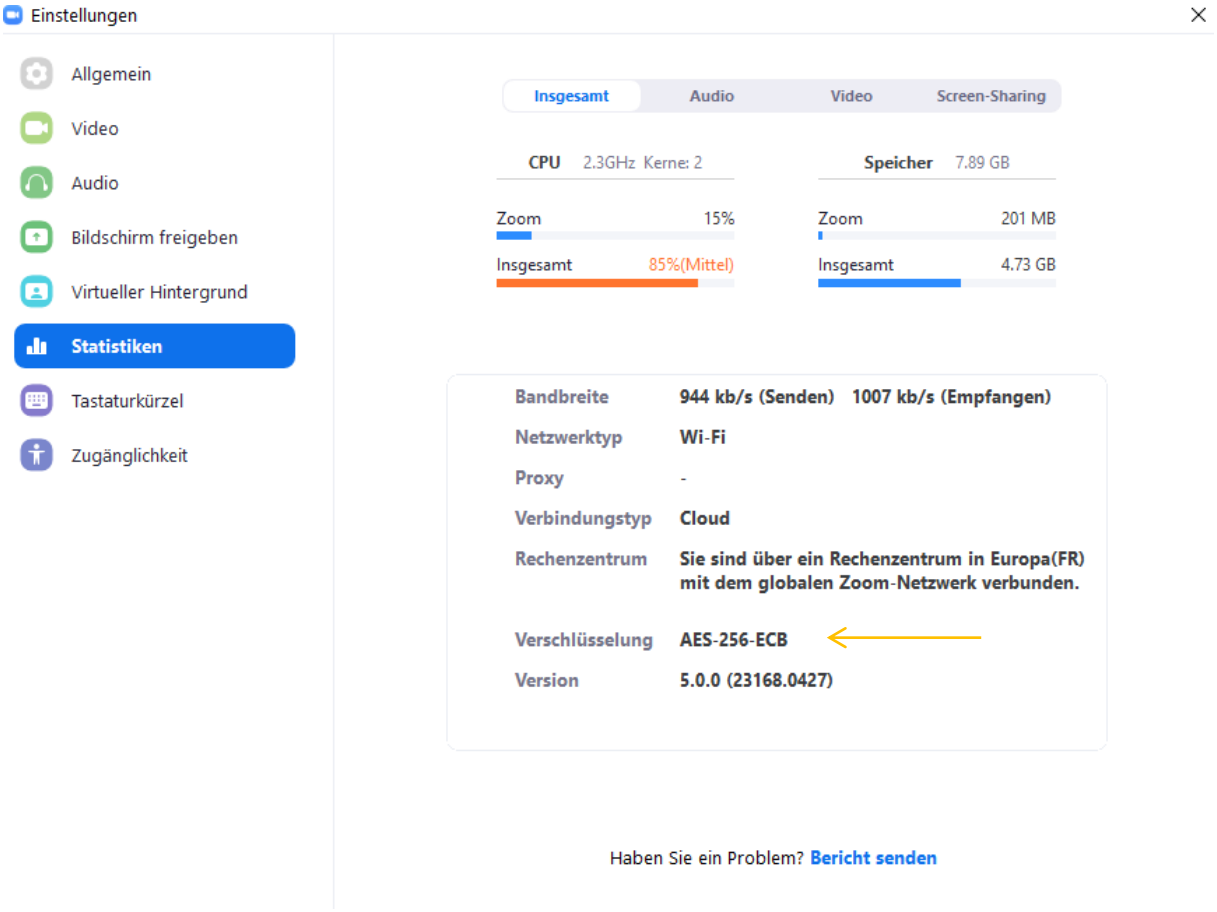

Abb. 3: Während einer Konferenz kann man leicht überprüfen, ob die Konferenz mit dem neuen Standard AES-256-ECB transport-verschlüsselt wird (weil bereits alle Teilnehmer eine Version ab 5.0 nutzen) oder noch der alte Standard zur Anwendung kommt.

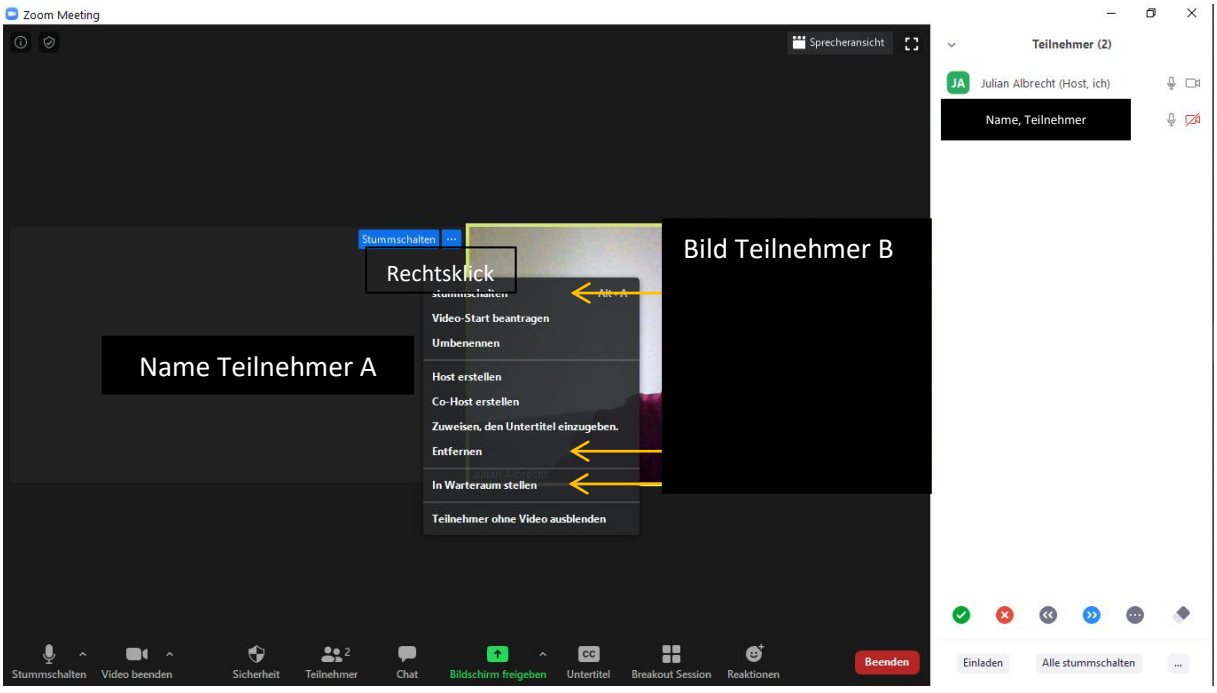

Abb.4: Bei entsprechender Voreinstellung kann der jeweilige Host Teilnehmer zentral stummschalten, deren Videoübertragung ausschalten, sie in den Warteraum stellen oder ganz entfernen (dann je nach Voreinstellung kein Wiedereintritt möglich). Dies sind wichtige Mittel, um sich Zoombombings zu erwehren.