Handreichung zu Zoom

Stellungnahme der IT-Sicherheitsbeauftragten und der Datenschutzbeauftragten

Zoom ist eine Cloud-Lösung, d.h. die Software wird beim Anbieter betrieben. Die Universität Regensburg (UR) hat mit diesem Anbieter aber einen Vertrag zur Auftragsdatenverarbeitung abgeschlossen. Dadurch ist sichergestellt, dass die Einhaltung der Datenschutzregelungen der DSGVO gewahrt ist. Zusätzlich werden durch die Administratoren des Rechenzentrums (RZ) entsprechende Einstellungen vorgenommen, die das Datenschutzniveau der Software im Vergleich zu den Standardeinstellungen weiter erhöhen.

Durch die hohe Popularität, die Zoom durch die Corona-Krise bekommen hat, steht der Dienst stark im Fokus der Öffentlichkeit, auch im Hinblick auf den Datenschutz. Dies bedeutet auf der einen Seite, dass Missbrauchsversuche (wie etwa das mutwillige Stören von Videokonferenzen) zunehmen, auf der anderen Seite werden so aber auch mögliche Schwachstellen der Software schneller erkannt und können durch den Hersteller schneller behoben werden. S hat Zoom in letzter Zeit sehr schnell auf Kritik und Hinweise reagiert und mögliche Schwachstellen geschlossen. Insbesondere die Version 5.0 hat wesentliche neue Sicherheitsfeatures bekommen, u.a. eine sehr starke Verschlüsselung mit 256-Bits. Der Anbieter hat die hohe Bedeutung des Themas gerade für europäische Nutzer*innen mittlerweile erkannt und bemüht sich durch zahlreiche Maßnahmen um eine verbesserte Transparenz und das Vertrauen der Nutzer*innen.

Wir halten die Nutzung von Zoom über die UR-Lizenz aus folgenden Gründen für vertretbar:

- Vertrag zur Auftragsdatenverarbeitung zwischen UR und Zoom garantiert DSGVO-Konformität
- Zahlreiche potenziell kritische Funktionen durch IT-Administration des RZ deaktiviert (z.B. Anmeldung mittels Facebook)
- Meetings sind transportverschlüsselt und lassen sich durch zahlreiche Zoom-Features (Passwort, Warteraumfreigabe, geheime Raum-ID usw.) vor Missbrauch (sog. Zoombombing) schützen
- IT-Sicherheitsbeauftragte hat Zugriff auf die „90 Tage Sicherheitsplan" - Fortschrittsberichte
- Zoom bessert bekannte Schwachstellen schnell nach und konzentriert sich in den nächsten Monaten ausschließlich auf Sicherheitsfeatures

Die Datenschutzerklärung für die Nutzung von Zoom an der UR finden Sie unter folgendem Link: Datenschutzerklärung zu Zoom

Wir möchten in diesem Zusammenhang auch auf die wirklich umfangreichen Informationen der am RZ der Universität Würzburg beheimateten Stabsstelle IT-Recht für die bayerischen staatlichen Hochschulen und Universitäten zum Thema Zoom hinweisen: Zoom - Stellungnahme zu Schwachstellen .

Es stimmt auch, dass in jüngster Vergangenheit tatsächlich viele Schwachstellen entdeckt wurden. Zoom hat diese Fehler zeitnah geschlossen und setzt nach eigenen Angaben nun mehr Entwicklerressourcen für die Verbesserung der Sicherheit und Datenschutz ein. Für alle, die aus diesem Grund Bedenken hinsichtlich der Nutzung von Zoom haben, bietet das RZ verschiedene Alternativen an, die vom RZ selbst oder dem DFN betrieben werden. Diese unterscheiden sich jedoch im Hinblick auf Funktionsumfang und Qualität von Zoom und eignen sich daher eher für Besprechungen mit wenigen Teilnehmern.

Neben Zoom bietet das RZ auch Alternativen an: DFNconf und Jitsi

Wir empfehlen Zoom (wie bereits in der Vergangenheit geschrieben) für die Lehre, empfehlen allerdings auch, kritische Informationen (Personalangelegenheiten, Dienstgeheimnisse etc.) nicht über Zoom zu verbreiten. Hierfür stehen andere Plattformen (z.B. DFN Conf, aktuell mit Skalierungsschwierigkeiten innerhalb der Peak-Zeiten) zur Verfügung.

Handlungsempfehlung: Sicherheitseinstellungen & -funktionen

Um die Sicherheit Ihres Zoom-Meetings zu erhöhen, sollten Sie beim Planen und Durchführen des Meetings je nach Einsatzgebiet (z.B. Vorlesung oder kleine Besprechung) folgende Einstellungen und Funktionen nutzen:

- *Passwortschutz:* Ein Passwort ist für jedes Meeting zwingend erforderlich. Es wird automatisch generiert.
- *Zugangsdaten:* Geben Sie die Meeting-URL, die häufig auch das Passwort enthält, nicht weiter. Geben Sie die Zugangsdaten direkt an die Teilnehmer*innen weiter; veröffentlichen Sie die Zugangsdaten nicht auf anderem Weg.
- *Warteraumfreigabe:* Wenn Sie ein Meeting mit kleiner Gruppengröße planen, können Sie unter "Erweiterte Optionen" die Warteraumfreigabe aktivieren. Sie müssen nun jedem*jeder Teilnehmer*in den Zutritt zum Meeting manuell erlauben. Auf diese Weise verhindern Sie den Beitritt unerwünschter Personen. Sie können den Warteraum auch direkt im Meeting in der unteren Menüleiste unter "Sicherheit" aktivieren.
- *Meeting sperren:* Wenn Sie ein Meeting mit kleiner Gruppengröße durchführen, können Sie das Meeting für weiteren Zutritt sperren, sobald alle Teilnehmer*innen anwesend sind. Sie finden die Option in der unteren Menüleiste unter "Sicherheit". Auf diese Weise verhindern Sie den Beitritt unerwünschter Personen zum Meeting sowie zum Warteraum, falls Sie diesen aktiviert haben.
- *Unerwünschte Teilnehmer*innen entfernen:* Unerwünschte Teilnehmer*innen können Sie in der unteren Menüleiste über "Teilnehmer verwalten" aus dem Meeting entfernen. Ein erneuter Beitritt durch diese*n Teilnehmer*in ist dann nicht mehr möglich.
- *Bildschirmfreigabe durch Teilnehmer*innen deaktivieren:* Grundsätzlich sollten Sie die Bildschirmfreigabe durch eine*n Teilnehmer*in nur ermöglichen, wenn Sie tatsächlich benötigt wird (bspw. für Präsentationen durch Studierende). Deaktivieren Sie die Funktion anschließend wieder, um zu verhindern, dass Personen unerwünschte Inhalte zeigen. Die relevanten Einstellungsoptionen finden Sie in der unteren Menüleiste unter "Bildschirm freigeben".
- *Bildschirmfreigabe - Annotierung deaktivieren:* Bei einer Bildschirmfreigabe können andere Teilnehmer*innen standardmäßig Anmerkungen auf den Bildschirm schreiben. Falls Sie die Funktion nicht benötigen, sollten Sie sie bei jeder Freigabe deaktivieren. Sobald Sie Ihren Bildschirm freigegeben haben, können Sie die Funktion über die Buttons "Sicherheit" oder "Mehr" deaktivieren.
- *Chat deaktivieren:* Für den Fall, dass Teilnehmer beispielsweise unpassende Witze, Werbung, Beleidigungen oder Verleumdung über den Chat veröffentlichen, kann dieser vom Host deaktiviert werden. Sie finden die Option in der unteren Menüleiste unter "Sicherheit".
- *Virtueller Hintergrund:* Zum Schutz Ihrer Privatsphäre können Sie bei Bedarf den virtuellen Hintergrund in den Einstellungen oder direkt im Meeting in den Videoeinstellungen aktivieren. So ist Ihre Umgebung für die anderen Teilnehmer*innen nicht sichtbar.

Handlungsempfehlung: Datenschutz

Bitte beachten Sie auch die folgenden datenschutzrechtlichen Empfehlungen:

- *Aufzeichnung der Vorlesung:* Soweit ein Zoommeeting aufgezeichnet werden soll, beispielsweise, um es im Anschluss in der Mediathek zur Verfügung zu stellen, ist aus Gründen der Transparenz darauf zu achten, dass alle Teilnehmer darüber informiert sind, ggf. ist eine Einwilligung einzuholen, wenn Daten, Bilder, Tonaufnahmen oder Videos von Studierenden oder Dritten veröffentlicht werden sollen. Eine Einwilligung kann auch mündlich im Rahmen der Zoomkonferenz erteilt werden. Aus Gründen der Datenminimierung und Rechtmäßigkeit der Datenverarbeitung ist darauf zu achten, dass keine weiteren Teilnehmer eingeblendet werden oder personenbezogene Daten genannt werden, soweit dies nicht erforderlich ist und/oder die betroffenen Personen nicht eingewilligt haben. Beim Einstellen in die Mediathek ist dabei darauf zu achten, dass nur der Personenkreis darauf Zugriff hat, für den es erforderlich ist (bspw. nur für in einen GRIPS- Kurs eingeschriebene Studierende).
- *Sensible Daten Dritter:* Es ist darauf zu achten, dass keine sensiblen Daten Dritter zu sehen sind, soweit es hierfür keine Rechtsgrundlage gibt (z.B. Einwilligung), beispielsweise Patientendaten in medizinischen Vorlesungen.
- *Zuschaltung der Kamera:* Soweit es nicht für die konkrete Zoom-Konferenz erforderlich ist, sollte das Zuschalten der Kamera (insbesondere im häuslichen Bereich) den Teilnehmern freigestellt werden. Ggf. kann auf die Option des virtuellen Hintergrundes hingewiesen werden.
- *Hinweis auf die Datenschutzerklärung zu Zoom:* Mit der Einladung zu einer Zoom-Konferenz oder der Ankündigung auf der Homepage o.ä. sollte auf die o.g. Datenschutzerklärung zu Zoom der Universität Regensburg hingewiesen werden, um die Informationspflichten nach Art. 13 DSGVO zu erfüllen.
- *Statusanzeige:* Über die Zoom-Anwendung erfolgt eine Statusanzeige ("abwesend", "nicht stören", "online", "in einem Zoommeeting"). Der Status kann manuell geändert werden. Eine automatische Anzeige als "abwesend" erfolgt nur, wenn man sich abmeldet. Das Schließen des Fensters alleine reicht nicht aus. Die Abfrage des Status darf ausschließlich für legitime Zwecke (z.B. spontane Einladungen zu Meetings) genutzt werden.

Ihre IT-Sicherheitsbeauftragte
Elena Maria Kellinghaus

Ihre Datenschutzbeauftragte
Susanne Stingl