Universität Konstanz

06. Mai 2020

Sicherheit und Datenschutz bei Webkonferenzen

Kontakt:
digitale-lehre@uni-konstanz.de

www.uni-konstanz.de/elearning

1. Allgemeine Empfehlungen für sichere Webkonferenzen

Die Universität Konstanz empfiehlt vier Webconferencing-Tools für unterschiedliche Anwendungsszenarien. Wie sonst üblich, nutzt keines dieser Tools eine Ende-zu-Ende Verschlüsselung (E2EE). Für die kommerziellen und von der Universität lizenzierten Systeme Zoom und Cisco WebEx sind derzeit die datenschutzrechtlich relevanten Dokumente in Abstimmung.

Big Blue Button

- Lokal gehostetes System auf OpenSource-Basis, Server an der Universität Konstanz
- Empfohlen für die Lehre und für Besprechungen mit sensiblen Inhalten, wie etwa personenbezogene Daten
- Auch direkt in ILIAS integrierbar
- Dauerhafter Service des KIM
- Läuft direkt im Browser Ihrer Wahl, keine App
- Login mit Uni-Account

Cisco WebEx

- Kommerzielles System, Server in der Europäischen Union
- Empfohlen für die Lehre und Besprechungen, insbesondere mit hohem Video-Anteil
- Lizenziert für ein Jahr
- Läuft im Browser oder in WebEx-App (bessere Funktionalität)
- Login mit Uni-Account

DFNconf

- Service des Deutschen Forschungsnetzes (DFN), Server in Deutschland
- Empfohlen für Lehre und Besprechungen
- Dauerhafter Service des DFN
- Läuft im Browser Ihrer Wahl
- Login mit Uni-Account

Zoom

- Kommerzielles System; die Universität nutzt für Gesprächsinhalte Server in Deutschland, Österreich und der Schweiz; für Metadaten Server in den USA
- Empfohlen für die Lehre und Besprechungen, insbesondere mit hohem Video-Anteil, unter besonderer Berücksichtigung der Datenschutzhinweise
- Lizenziert für ein Jahr
- Läuft im Browser Ihrer Wahl. Aus Gründen der IT-Sicherheit wird die Zoom-App nach derzeitigem Kenntnisstand nicht empfohlen

– Lizenzen werden zentral über das KIM bereitgestellt (prinzipiell eine Lizenz pro Lehrstuhl).

Es wird generell die Nutzung der Browser Firefox oder Chrome empfohlen.
https://www.kim.uni-konstanz.de/services/forschen-und-lehren/videokonferenzen/

1.1. Empfehlungen für Lehrende

1. Nutzen Sie Videokonferenzsysteme generell nur auf vertrauenswürdigen Geräten. Installieren Sie zusätzliche Software nur, wenn unbedingt erforderlich. Falls möglich, nutzen Sie dafür ein dediziertes Gerät, auf dem keine kritischen Daten verarbeitet werden.

2. Achten Sie darauf, dass jegliche Software auf dem neuesten Stand ist: Betriebssystem, Browser, ggf. App. Beachten Sie aktuelle Hinweise zu Sicherheitslücken (Informationssicherheitsmanagement). Wenn es aktuelle, kritische Sicherheitswarnungen gibt, ist von der Verwendung von Zoom abzusehen, auch wenn dies eine Einschränkung im Betrieb bedeutet.

3. Für jede Konferenz verwenden Sie ein dediziertes, sicheres Passwort (siehe Passworthinweise der Informationssicherheit).

4. Konferenzen nicht wiederverwenden, jede Veranstaltung bekommt einen eigenen Konferenz-Link.

5. Zugangsdaten dürfen nur über sichere und bekannte Kanäle geteilt werden (bspw. als Informationen im Ilias-Kurs).

6. Prüfen Sie vor Beginn der Videokonferenz den sichtbaren Hintergrund im Kameraausschnitt und entfernen Sie persönliche Gegenstände.

7. Überzeugen Sie sich von der Verfügbarkeit der Datenschutzinformation gem. Art. 13 DSGVO und holen Sie u.U. die Einwilligung der Teilnehmenden ein.

8. Beim Durchführen einer Videokonferenz muss die Aufzeichnung von Sprache und Video deaktiviert sein. Aufgezeichnet werden darf nur bei Vorliegen einer Rechtsgrundlage, im Zweifel erfordert dies das explizite und dokumentierte Einverständnis aller Teilnehmenden. In diesem Fall muss eine aktive Aufzeichnung allen Teilnehmenden vorab signalisiert werden. Beachten Sie die Strafbarkeit des unbefugten Abhörens oder Aufzeichnens des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

9. Teilnehmende standardmäßig nur mit deaktiviertem Mikrofon, Kamera und Screensharing lassen. Diese Funktionen müssen explizit freiwillig von Teilnehmenden freigegeben werden. Fragen Sie die Teilnehmenden, ob sie mit Kamerafunktion an der Videokonferenz teilnehmen wollen und zeigen Sie mögliche Alternativen auf.

10. Achten Sie darauf, dass es keine unbefugten Beobachter im Raum gibt.

11. Wenn möglich, nutzen Sie ein LAN-Kabel für die Teilnahme an der Videokonferenz.s

1.2. Empfehlungen für Studierende

1. Nutzen Sie Videokonferenzsysteme generell nur auf vertrauenswürdigen Geräten. Installieren Sie zusätzliche Software nur, wenn unbedingt erforderlich. Falls möglich, nutzen Sie dafür ein dediziertes Gerät, auf dem keine kritischen Daten verarbeitet werden.

2. Geben Sie die erhaltenen Zugangsdaten nicht weiter, diese sind nur für Sie persönlich bestimmt.

3. Wenn Sie Links zu Konferenzen oder Software/Apps erhalten, prüfen Sie die Herkunft und die Ziele sorgfältig (phishing, scamming, hijacking).

4. Achten Sie darauf, Software/Apps nur aus vertrauenswürdigen Quellen zu installieren. Wenn möglich, nutzen Sie bevorzugt den Browser anstatt die App-Versionen. Dies geht ggf. mit Funktionseinschränkungen einher. Nutzen Sie die WebEx-App nur, wenn Sie zwingend bestimmte Funktionen benötigen (wie „Hand heben“, das Whiteboard in der Cisco Desktop-App oder in mobilen App von WebEx bzw. die „Rasteransicht“)

5. Achten Sie beim Beitritt darauf, dass Mikrofon, Kamera und Bildschirmfreigabe ausgeschaltet sind. Aktivieren Sie diese nur, wenn erforderlich. Lassen Sie sich nicht zu irgendeiner Freigabe nötigen.

6. Prüfen Sie vor Beginn der Videokonferenz den sichtbaren Hintergrund im Kameraausschnitt und entfernen Sie persönliche Gegenstände

7. Wenn Sie gar keine persönlichen Informationen preisgeben wollen, empfehlen wir, bei der Angabe einer E-Mail Adresse das Wegwerfadresssystem void.uni-konstanz.de zu verwenden. Hierdurch werden Sie als Mitglied der Universität ausgewiesen, können aber ein Pseudonym verwenden. Erstellen Sie eine neue Wegwerfadresse für jede neue Konferenz.

8. Fertigen Sie keine Mitschnitte, Aufzeichnungen oder Screenshots an (§ 201 StGB - Strafbarkeit der unbefugten Abhörens des nicht-öffentlich gesprochenen Wortes)

9. Eine Aufzeichnung der Videokonferenz erfolgt nur nach Ihrer Information und nach einer Einwilligung durch Sie. Ansonsten findet keine Aufzeichnung durch die Universität statt. Achten Sie dennoch darauf, was sie sagen, schreiben, zeigen.

10. Wenn möglich, nutzen Sie ein LAN-Kabel für die Teilnahme an der Videokonferenz

11. Sollten Sie gegen Ihren Willen zur Herausgabe von persönlichen Informationen oder zur Freigabe von Bild und Video genötigt werden, oder falls Sie einen begründeten Verdacht haben, dass Sie ohne Ihr Einverständnis aufgezeichnet wurden, so setzen Sie sich bitte umgehend mit dem Datenschutzbeauftragten der Universität in Verbindung (datenschutzbeauftragter@uni-konstanz.de).

https://www.kim.uni-konstanz.de/e-mail-und-internet/it-sicherheit/

2. Aufzeichnungen von Videokonferenzen

Aus rechtlicher Sicht ist ein unerlaubtes Aufzeichnen oder Mitschneiden von Videokonferenzen untersagt (§ 201 StGB - Strafbarkeit des unbefugten Abhörens des nicht-öffentlich gesprochenen Wortes). Unerlaubtes Aufzeichnen oder Mitschneiden verletzt sowohl Persönlichkeitsrechte als auch das sog. Recht am eigenen Bild. Bitte machen Sie daher als ModeratorIn eines Web-Meetings Ihre Teilnehmenden unbedingt vor Beginn eines Web-Meetings darauf aufmerksam.

U.a. aus Datenschutzgründen ist daher die Möglichkeit, Videokonferenzen aufzuzeichnen, bei BBB auf unseren Uni-eigenen Servern per default deaktiviert. Da Cisco WebEx und Zoom jedoch kommerzielle Systeme sind, lässt sich das Aufzeichnen/Mitschneiden nicht deaktivieren oder verhindern. Somit bedarf es im Fall eines beabsichtigten Mitschnitts unbedingt **vorher** der Zustimmung **jedes einzelnen** Teilnehmenden – dabei ist es unerheblich, ob der/die ModeratorIn mitschneidet oder eine/r der Teilnehmenden. Gleiches gilt auch für Screencasts.

3. Empfehlungen für das System Zoom

Aus gegebenem Anlass möchten wir Sie auf die Besonderheiten bei der Verwendung von Zoom aufmerksam machen.

Wegen der hohen Nachfrage nach einem stabilen Ausweichsystem hat die Universität Konstanz beschlossen, Lizenzen für Zoom für ein Jahr zu kaufen. Hierbei gibt es allerdings Sicherheitshinweise zu beachten, die zusätzlich zu den Hinweisen für die anderen Systeme gelten:

– Zoom ist eine kommerzielle Software mit Sitz in den USA. Die Meta-Daten (also wer wann mit wem konferiert hat) werden auf weltweiten Servern gespeichert, ohne die in der EU geltende DSGVO zu berücksichtigen.

– Alle Inhalte, die über Zoom per Text, Bild und Video kommuniziert werden, laufen im Rahmen der Lizenz der Universität Konstanz mit dem Anbieter C4V auf Servern in Deutschland, Österreich und der Schweiz. Der Anbieter hat keine DSGVO-Zertifizierung, unterliegt aber den Regeln der DSGVO.

– Im Klartext bedeutet das: Verwenden Sie Zoom nicht für Gespräche, die sensible und/oder personenbezogene Daten beinhalten, wie z.B. Prüfungen, vertrauliche Gespräche oder Sprechstunden. Also: Verwenden Sie Zoom nur für öffentliche Gespräche.

3.1. Hinweise für Lehrende / Moderator/innen

1. Nutzen Sie Videokonferenzsysteme generell nur auf vertrauenswürdigen Geräten. Installieren Sie zusätzliche Software nur, wenn unbedingt erforderlich. Falls möglich, nutzen Sie dafür ein dediziertes Gerät, auf dem keine kritischen Daten verarbeitet werden.

2. Achten Sie darauf, dass jegliche Software auf dem neuesten Stand ist: Betriebssystem, Browser, Zoom-App. Beachten Sie aktuelle Hinweise zu Sicherheitslücken (Informationssicherheitsmanagement). Wenn es aktuelle, kritische Sicherheitswarnungen gibt, ist von der Verwendung von Zoom abzusehen, auch wenn dies eine Einschränkung im Betrieb bedeutet.

3. Für jedes Meeting ein eigenes, individuelles Passwort wählen oder generieren lassen (-> Passworthinweise der Uni)

4. Für jeden Veranstaltungstermin oder zumindest jede Veranstaltung möglichst ein neues Meeting anlegen (neue ID, neue Zugangsdaten) und kein altes Meeting wiederverwenden.

5. Den Link auf das Meeting/Meeting-ID mit dem Passwort über sichere, und vorher kommunizierte Kanäle einer geschlossenen Gruppe bereitstellen. Bspw. In einer ILIAS-Veranstaltung. Zugangsdaten NICHT über öffentliche Kanäle teilen (social Media, öffentliche Webseite)

6. Studierende deutlich und erkennbar dazu anhalten, Zugangsdaten nicht weiterzugeben.

7. Folgende Einstellungen sind standardmäßig für alle Zoom-Meetings vorzunehmen:

- Mikrofone der Teilnehmer*innen sind deaktiviert
- Kameras der Teilnehmer*innen sind deaktiviert
- Kamera-Fernsteuerung ist deaktiviert
- Bildschirmfreigabe der Teilnehmer*innen ist deaktiviert
- die Fernsteuerung über die Bildschirmfreigabe ist deaktiviert
- Remoteunterstützung ist deaktiviert
- Aufmerksamkeitstracking ist deaktiviert
- Aufzeichnungen sind deaktiviert
- Benachrichtigung des Hosts bei Zutritt von Teilnehmer*innen vor dem Host sind
- deaktiviert
- Automatische Benachrichtigung von Teilnehmer*innen bei Absage eines
- Meetings ist deaktiviert
- Versand von E-Mails über die ZOOM-Webseite ist deaktiviert
- Feedbacks an ZOOM am Ende eines Meetings sind deaktiviert

8. Die Teilnehmenden dürfen nicht gegen ihren Willen gezwungen werden, persönliche Informationen herauszugeben oder Audio / Video / Bildschirm freizugeben. Die Veranstaltung darf nur dann aufgezeichnet werden, wenn vorher das explizite Einverständnis aller Teilnehmenden eingeholt und dokumentiert wurde. Ist die Anzahl der Einwilligungen kleiner als die der aktuell Teilnehmenden, darf nicht aufgezeichnet werden.

9. Umgang mit nachträglichem Zutritt zum Meeting-Raum:

- Die Funktion "Warteraum" kann für Nachzügler verwendet werden.
- Die Funktion "Meeting sperren" kann benutzt werden, um weiteren Zugang zu unterbinden, sofern dieses Verhalten gewünscht ist.

10. Teilnehmende sollten nur dann aufgefordert werden, Ihren Namen zu nennen, wenn das für die Veranstaltung notwendig ist.

11. Wenn Teilnehmende negativ auffallen oder zu Störungen führen, schalten Sie deren Audio stumm

12. Wenn der Link zum Raum verschickt wird, empfehlen wir, die URL so umzubiegen, dass eine Teilnahme via Webbrowser angestrebt wird. (https://zoom.us/j/{id} zu https://zoom.us/wc/join/{id}). Wenn der Link nicht manuell verschickt wird (generierte Einladungs-E-Mail), empfehlen wir, die entsprechende Option zu aktivieren, sodass eine Teilnahme via Web-Browser zumindest vorgeschlagen wird.

13. Den Bedarf der Funktionen wie "Dateiübertragung" überlegen und entsprechend konfigurieren.

14. "Beitritt vor Moderator" deaktivieren.

3.2. Hinweise für Studierende / Teilnehmer/innen

- Bei Aufforderung, den Client zu installieren, dies ablehnen und stattdessen auf "treten Sie über Ihren Browser bei" klicken.