Einsatz von Zoom an der JLU

Konfiguration von Zoom zur Datensparsamkeit

Stand: 31. August 2020

Damit personenbezogene Daten bestmöglich geschützt sind, haben die Fachbereiche und zentrale Einrichtungen der JLU Zoom in allen Funktionsbereichen so zu konfigurieren, dass nur ein Minimum an Daten übertragen und gespeichert wird. Alle Voreinstellungen sind so zu wählen, dass den Nutzenden bestmögliche Kontrolle über die Preisgabe von Daten erlaubt wird. Im Einzelnen sind die folgenden Konfigurationen vorzunehmen.

1. Voreinstellungen für die Teilnahme an Meetings

- Alle Meetings beginnen mit abgeschaltetem Teilnehmervideo. Das Videobild kann von den Teilnehmenden aktiv eingeschaltet werden.
- Teilnehmende sind bei Betreten des Meetings stumm geschaltet.
- Die Anzeige von E-Mail-Adressen per Wasserzeichen ist unterbunden.
- Für alle Meetings wird standardmäßig ein Passwort gesetzt.
- Feedbacks an Zoom am Ende eines Meetings sind deaktiviert.
- Die Fernsteuerung über die Bildschirmfreigabe ist deaktiviert.
- Die Kamera-Fernsteuerung ist deaktiviert.
- Teilnehmende können an Meetings direkt über den Browser teilnehmen, ohne den Zoom-Client zu installieren. Wir empfehlen hierzu den Browser Chrome, da andere Browser nicht alle Features von Zoom unterstützen. Informationen zum Thema Zoom-Client vs. Zoom per Browser finden Sie hier: https://support.zoom.us/hc/en-us/articles/360027397692

2. Technische Einstellungen

- Verschlüsselung aller Daten zwischen dem Zoom-Client und dem Zoom Room ist aktiviert.
- Wenn sich nur zwei Personen in einem Meeting befinden, wird eine Peer-to-Peer-Verbindung aufgebaut.
- Schnappschuss in der iOS-Aufgabenumschaltfunktion wird weichgezeichnet, um eventuelle vertrauliche Informationen von der Momentaufnahme des Zoom Hauptfensters auszublenden. Diese Momentaufnahme wird als Vorschaubildschirm in der iOS Aufgabenumschaltfunktion angezeigt, wenn mehrere Apps offen sind.

3. Datenaustausch mit anderen Diensten
- Datenaustausch mit Office 365 ist deaktiviert.
- CDN-Nutzung ist deaktiviert.

4. Speicherung von Meeting-Inhalten
- **Aufzeichnung von Meetings in der Zoom-Cloud ist deaktiviert.**
- **Lokale Aufzeichnung von Meetings ist deaktiviert.**
- **Automatische Aufzeichnung bei Meetings-Beginn ist generell deaktiviert.**
- Eine Speicherung der Chat-Kommunikation ist für Teilnehmer unterbunden.
- Die automatische Speicherung der Chat-Kommunikation für den Host ist unterbunden.
- Die automatische Speicherung von Whiteboard-Inhalten ist unterbunden.

5. Generelle Hinweise
- Es besteht die Möglichkeit, Zoom nicht direkt unter dem eigenen Nutzerkonto auf dem Computer zu installieren, sondern unter einem zweiten privilegierten Nutzerkonto. Ggfs. kann Zoom auch auf einem separaten Gerät installiert werden. Das reduziert den möglichen Schaden bei Sicherheitslücken erheblich.
- Auf mobilen Geräten sollte Zoom möglichst unter einem separaten Nutzerkonto installiert werden, bei dem Nutzer nicht mit ihrem Google-/Facebook/... Accounts eingeloggt sind.
- Beim Registrieren für Zoom darf niemals die Möglichkeit verwendet werden, den eigenen Google-/Facebook-/...-Account zu benutzen.
- Zur weiteren Steigerung des Sicherheitsniveaus können Meeting-IDs für Zoom unmittelbar vor dem Veranstaltungstermin z.B. auf ILIAS oder Stud.IP bekanntgegeben werden. In diesem Fall empfiehlt es sich, die Meeting-IDs für jeden Veranstaltungstermin zu ändern. Auf diese Weise vermeidet man das (relativ geringe) Risiko, dass sich Bots oder Unbeteiligte störend dazugesellen.