

Umgang mit Störungen in Zoom

Inhalt

1. Prävention von Störungen	01
Rechte verwalten	01
Zweite Person (Co-Host)	02
Wartezimmer	02
Bereitstellung von Zugangsdaten	03
Authentifizierung	03
Registrierung	03
Webinar	03
2. Aktiv eingreifen bei Störungen	03
3. Nachbereitung: Störungen kommunizieren	04

Trotz ihrer zahlreichen Vorteile können während der Durchführung von Online-Veranstaltungen technische oder kommunikative Störungen auftreten, die den Lehrfluss beeinträchtigen. Dieses Handout bietet einen Überblick über typische Störungen in Zoom und zeigt praxisnahe Methoden auf, wie Lehrende diesen gezielt begegnen können.

1. Prävention von Störungen

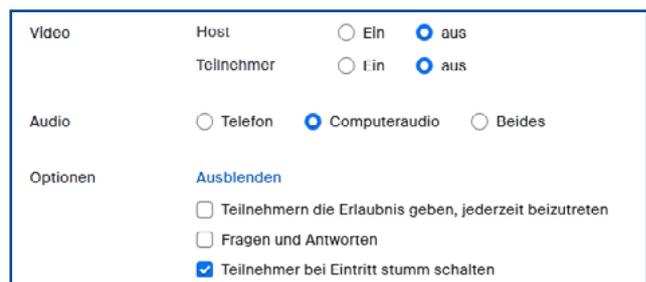
Der beste Umgang mit Störungen ist es, sie gar nicht erst entstehen zu lassen. Durch eine vorausschauende Planung und klare Kommunikation lassen sich viele potenzielle Probleme in Zoom-Veranstaltungen von vornherein vermeiden.

Rechte verwalten

Prüfen Sie zunächst, welche Rechte die Teilnehmer*innen in Ihrem Meeting benötigen und deaktivieren Sie „überflüssige“ Rechte. Auf diese Weise können Sie bereits im Vorfeld das Risiko für unangebrachte Störungen durch Teilnehmende eingrenzen.

Da jedes Meeting unterschiedlich ist, empfiehlt es sich, die Anpassungen nicht auf Kontoebene vorzunehmen, sondern für jedes Meeting individuell.

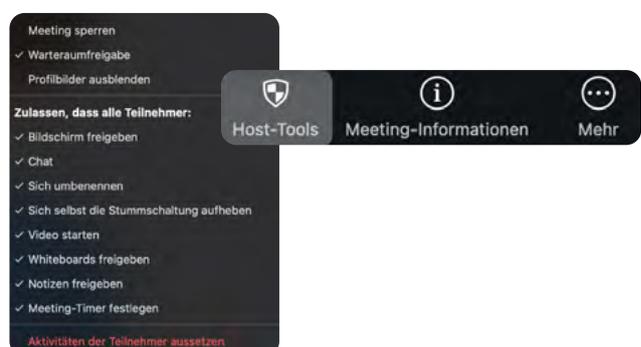
Bereits bei der Erstellung des Meetings, können Sie festlegen, dass Teilnehmende ohne Kamerabild und stummgeschaltet beitreten:



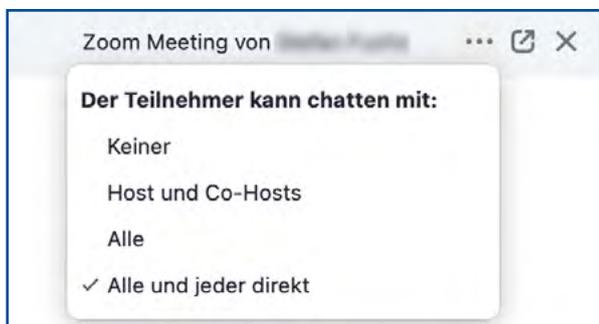
Im Meeting selbst sollten Sie vor Eintritt der Teilnehmenden die **Host-Tools in der Menüleiste** öffnen. Dort können Sie zum Beispiel folgende weitere Rechte für Teilnehmende verwalten:

- Bildschirmfreigabe
- Chat
- Sich umbenennen
- Aufhebung der Stummschaltung
- Video starten
- Whiteboards freigeben
- Notizen freigeben
- Meeting-Timer festlegen

Schalten Sie alle Funktionen aus, die die Teilnehmenden nicht benötigen.



Für den Chat können Sie auch gezielt einstellen, ob und mit wem Teilnehmende chatten dürfen. Öffnen Sie hierzu den Chat im Meeting und öffnen Sie dort das „...“-Menü und wählen Sie aus, ob Teilnehmende mit keinem, mit allen, mit allen und per Direktnachricht oder nur mit Host und Co-Host chatten dürfen.



Achtung: Bitte beachten Sie, dass die Einstellungen, die Sie im Meeting in den Host-Tools und im Chat vornehmen, nur für das laufende Meeting gelten. Sie werden nicht für nachfolgende Meetings oder einen Neustart des aktuellen Meetings gespeichert. Sollten Sie Einstellungen für all Ihre Meetings festlegen wollen, loggen Sie sich bitte im Fernuni-Zoom-Portal (<https://fernuni-hagen.zoom-x.de/>) in Ihr Konto ein und wählen Sie dort „Mein Konto“, „Einstellungen“, „Meeting“ aus.

Tipp: Rechte können auch situationsbedingt an einzelne Personen im Meeting vergeben werden. Wenn eine teilnehmende Person beispielsweise für eine Wortmeldung die Hand hebt, können Sie über die Teilnehmendenliste oder über die jeweilige Videokachel die Funktion „**Bitten Ton einzuschalten**“ auswählen. Die Stummschaltung wird dann für diese Person aufgehoben, bis sie selbst das eigene Mikro stummschaltet oder von Host oder Co-Host stummgeschaltet wird.

Bitten Ton einzuschalten



Sollten Sie einer einzelnen teilnehmenden Person kurzzeitig oder für das gesamte Meeting erweiterte Rechte geben wollen, können Sie diese Person für diesen Zeitraum zum Co-Host ernennen.

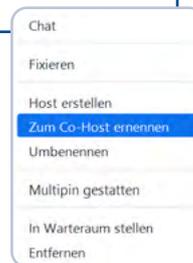
Zweite Person (Co-Host)

Es ist empfehlenswert, eine zweite Person als Co-Host im Zoom-Meeting einzubeziehen, um im Falle von Störungen flexibel und schnell reagieren zu können. Der*die Co-Host kann beispielsweise technische Probleme der Teilnehmenden betreuen, den Chat moderieren oder bei Unterbrechungen durch unbefugte Personen unterstützend eingreifen. Die bereits genannten Host-Tools stehen auch für Co-Host in der Menuleiste zur Verfügung. So bleibt der Fokus der Lehrperson auf der inhaltlichen Gestaltung der Veranstaltung erhalten.

Diese Person kann beispielsweise ein*e Kolleg*in aus dem Lehrgebiet oder auch eine ELFe (<https://e.feu.de/elfen>) aus dem ZLI sein. Sprechen Sie mit dieser Person ab, welche Aufgaben anfallen (könnten) und wer welche Zuständigkeiten übernimmt. Vergeben Sie idealerweise bereits vor dem Meeting Co-Host-Rechte an die betreffende Person, indem Sie diese als **alternativen Host** in das Zoom-Meeting eintragen.

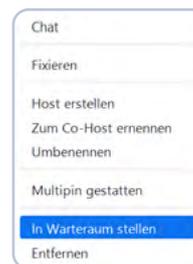


Sollte eine spontane Zuteilung erforderlich sein, zum Beispiel weil es sich um eine externe Person ohne Fernuni-Zoom-Konto handelt, können Sie diese auch während des Meetings zum Co-Host ernennen.



Wartezimmer

Die Aktivierung des Warteraums in Zoom bietet eine effektive Möglichkeit, Störungen bereits vor Beginn des Meetings zu vermeiden. Sie ermöglicht es der Lehrperson oder dem*der Co-Host, Teilnehmende gezielt einzulassen (zum Beispiel bei kleinen/bekannteren Gruppen) und unbefugten Zugriff frühzeitig zu erkennen und zu verhindern. Gerade bei öffentlich zugänglichen Links ist der Wartezimmer ein wichtiger Schutzmechanismus für einen sicheren und kontrollierten Start der Veranstaltung.



Kommt es während der Veranstaltung zu einer Störung durch eine bestimmte Person, so kann diese auch zunächst in den Wartezimmer geschoben werden bis eine Klärung stattgefunden hat.

Der Wartezimmer kann auch als abgeschwächte Form der Authentifizierung verwendet werden: Personen, die nicht in ein Konto eingeloggt sind, werden nicht vom Meeting ausgeschlossen, landen aber im Wartezimmer. Dies hat jedoch zum Nachteil, dass der Wartezimmer nicht mehr dazu verwendet werden kann, um im laufenden Meeting Absprachen unter (Co-)Hosts zu führen. Die Einstellung kann im Fernuni-Zoom-Portal unter „Einstellungen“ im Reiter „Meeting“ vorgenommen werden.



Meeting sperren

Sofern bereits alle Teilnehmer im Meeting sind oder Sie allgemein nach dem offiziellen Beginn des Meetings keine weiteren Teilnehmer im Meeting wünschen, können Sie über die bereits genannten Host-Tools auch das „Meeting sperren“. Das hat keine Auswirkungen auf die Teilnehmenden, die sich bereits im Meeting befinden. Es können aber keine weiteren, potentiell störenden Teilnehmenden mehr hinzukommen. *Bitte beachten Sie aber, dass dann auch Personen, die das Meeting kurzzeitig verlassen (aktiv oder durch Verbindungsprobleme) das Meeting nicht erneut betreten können.*

Bereitstellung von Zugangsdaten

Zugangsdaten zu Zoommeetings sollten nicht auf öffentlichen Websites veröffentlicht werden, da sie so sehr leicht von potenziellen Angreifer*innen gefunden und verwendet werden können.

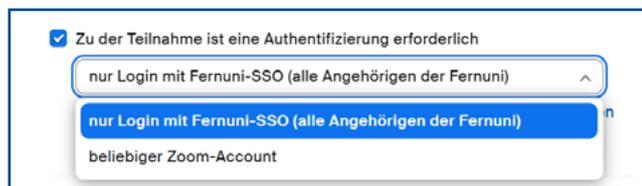
Zugangsdaten sollten nach Möglichkeit nur den Personen zur Verfügung gestellt werden, die auch teilnehmen sollen. Zum Beispiel über einen Moodle-Kurs oder auf einer internen Website, die einen Login erfordert oder über einen E-Mail-Verteiler.

Tip: Sie können mit der Aktivität „Zoom“ auch direkt in Moodle ein Meeting in Ihrem Kurs anlegen.

Authentifizierung

Die Aktivierung der Authentifizierung in Zoom sorgt dafür, dass je nach Einstellung nur dann eine Teilnahme am Meeting möglich ist, wenn ein Zoomkonto an der Fernuni oder generell ein Zoomkonto vorhanden ist und sich die Person zur Teilnahme in ihr Konto eingeloggt hat. Dadurch wird das Risiko von Störungen durch unbefugte Dritte deutlich reduziert. Insbesondere bei sensiblen Inhalten ist diese Einstellung ein wirksames Mittel, um die Sicherheit und Vertraulichkeit der Veranstaltung zu gewährleisten.

Dies wird beim Erstellen des Meetings unter dem Punkt „Sicherheit“ eingestellt:



Der Vorteil: nach der Veranstaltung kann über die Berichte nachvollzogen werden, wer genau im Meeting anwesend war, da neben dem Namen auch die Mailadresse übertragen wird (außer bei Gästen). Dies eignet sich zum Beispiel für Veranstaltungen mit Anwesenheitspflicht. Da Studierende bei dieser Einstellung zwingend ein Zoomkonto benötigen, sollten Sie als Veranstalter*in darüber informieren und ergänzend eine Anleitung zur Registrierung bereitstellen. Diese findet sich im Helpdeskwiki (<https://e.feu.de/zoom-registrierung>).

Registrierung

Sie können Ihr Meeting auch so einstellen, dass eine Registrierung erforderlich ist. In diesem Fall verteilen oder veröffentlichen Sie nicht den Teilnahmelink zum Meeting, sondern einen Registrierungslink. Meeting-Interessierte müssen dann auf der Registrierungsseite Namen und E-Mail-Adresse hinterlassen und erhalten einen personalisierten Teilnahmelink an die angegebene E-Mail-Adresse. Sie können selbst definieren, ob der Teilnahmelink automatisch verschickt wird oder ob Sie manuell entscheiden wollen, welche registrierten Teilnehmer zugelassen werden, und welche nicht.

Hinweis: Wenn sowohl die Authentifizierung als auch die Registrierung erforderlich ist, müssen sich die Teilnehmenden bereits bei der Registrierung authentifizieren – also wahlweise mit einem Fernuni-Account oder mit einem beliebigen Zoom-Account registrieren.

Webinar

Die Nutzung des Zoom-Webinars eignet sich besonders für Veranstaltungen mit größerem Publikum oder einem klaren Rollenverhältnis zwischen Vortragenden und Zuhörenden. Da Teilnehmende standardmäßig weder ihre Kamera noch ihr Mikrofon aktivieren können, wird das Risiko spontaner Störungen deutlich minimiert. Für Veranstaltungen mit wenig Interaktion kann das Webinar-Format daher eine hilfreiche Alternative zum klassischen Meeting sein.

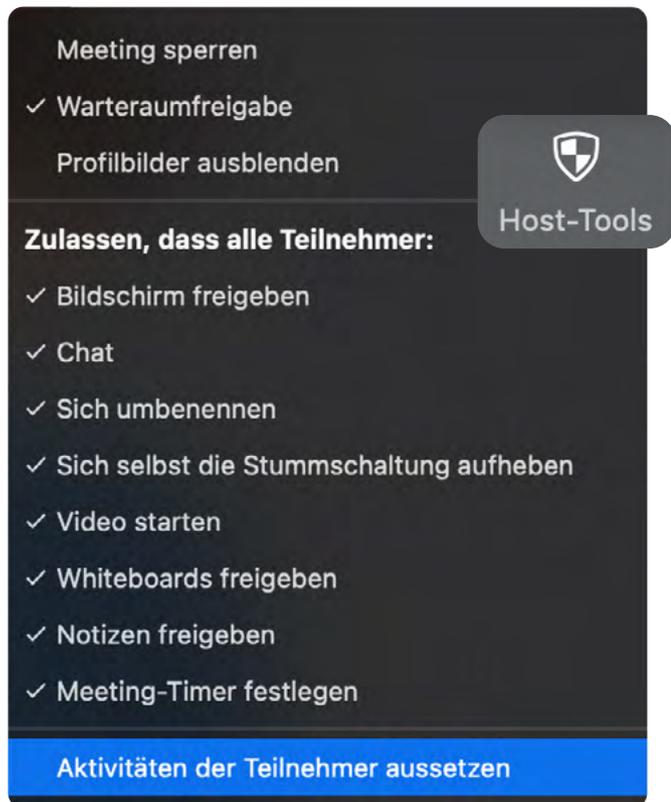
- Teilnehmende sind reine Zuhörerschaft, eine Interaktion unter den Teilnehmenden ist nicht möglich. Eine Beteiligung an der Veranstaltung kann über verschiedene Funktionen ermöglicht werden (Q&A-Funktion, Wortmeldungen, Umfragen, Chat, Whiteboard lesend).
- Das Webinar benötigt eine gesonderte Lizenz (mehrere 500er und 1x 3000er vorhanden), die über <https://e.feu.de/zoom-large-meeting> (500er für ganzes Semester) beantragt werden kann.

2. Aktiv eingreifen bei Störungen

Während einer Störung haben Sie folgende Möglichkeiten, um diese ad hoc im Zoommeeting zu unterbinden:

- Über die Host-Tools können Sie wie in Kapitel 1 beschrieben auch im laufenden Meeting die Rechte für den Chat, die Umbenennung, die Aufhebung der Stummschaltung, den Start des Videos, den Meeting-Timer, sowie für die Freigabe von Bildschirm, Whiteboard und Notizen, den Teilnehmenden entziehen.
- Über die Teilnehmendenliste können Sie gezielt einzelnen Personen Rechte entziehen/vergeben, diese in den Warteraum schieben oder aus dem Meeting entfernen (Achtung: bei letzterer Option ist ein erneuter Beitritt für diese Person nicht möglich).

Lässt sich die Störquelle nicht identifizieren, können Sie über die Host-Tools auch alle „Aktivitäten der Teilnehmer aussetzen“, sodass mit einem Klick alle Rechte entzogen werden (zunächst auch von Host und Co-Host).



3. Nachbereitung: Störungen kommunizieren

Bitte versuchen Sie nach der Veranstaltung die Störung so gut wie möglich zu dokumentieren:

- Basisinformationen zum Meeting (Meeting-ID, Datum, Uhrzeit, in wessen Konto wurde das Meeting angelegt, Titel des Meetings)
- Beschreibung der Störung (was ist passiert, wann ist das passiert (Uhrzeit/Situation), wer war involviert)
- ggfs. Rückmeldungen von betroffenen Studierenden aufnehmen

Leiten Sie die Störung an Ihre*n Fachmediendidaktiker*in und das ZLI weiter (zli@fernuni-hagen.de oder via Ticket an den Helpdesk). Gravierende Störungen sollten zusätzlich im eigenen Zoom-Konto auch über „Berichte“, „Aktivitätsbericht des Benutzers“, „Gemeldete Teilnehmer“ direkt an das Trust and Safety-Team von Zoom gemeldet werden.

FernUniversität in Hagen
Zentrum für Lernen und Innovation (ZLI)

Universitätsstr. 21
58097 Hagen

www.fernuni-hagen.de/zli/