Zoom gegen Unterbrechungen absichern

Jede Web-/Videokonferenz ist potenzielles Ziel für Störungen. Wann immer Zugangsdaten veröffentlicht werden, können diese von Personen genutzt werden, um Veranstaltung mit unerwünschten Beiträgen zu torpedieren. Um Ihre Konferenz gegen solche Attacken abzusichern können Sie auf verschiedene Taktiken zurückgreifen. Nutzen Sie die nachfolgenden Links, um zu den Themen zu springen, die für Sie relevant sind.

1 - Richtiger Umgang mit Zugangspasswörtern

Wenn Sie ein Zoom-Meeting erstellen, wird standardmäßig ein zufälliges Raumzugangspasswort gesetzt. Die Verwendung solch eines Passworts ist ausdrücklich empfohlen und dient dazu, den Raum gegen unbefugten Zugang abzusichern. Der Schutz kann aber nur dann greifen, wenn diese Daten ausschließlich einem geschlossenen Kreis bekanntgemacht wird. Oftmals werden die Zugangsdaten auf öffentlichen Plattformen wie bspw. Twitter verbreitet, wo sie dann von jedem, auch automatisierten Bots, einsehbar sind. Das führt den Schutzmechanismus ad absurdum. Folgende Methoden können angewandt werden, um das Risiko zu vermindern.

- Nutzen Sie zur Veröffentlichung der Zugangsdaten keine öffentlich zugänglichen Plattformen. Anbieten würden sich stattdessen zum Beispiel der Hörsaal, Element, E-Mails oder Moodle.
- Wenn es unbedingt doch eine öffentliche Plattform sein muss, überlegen Sie, ob Sie zumindest das Passwort gesondert bekanntgeben können. Wenn ja:
    - Entfernen Sie manuell den Passwort-Parameter aus dem Zugangslink.
        - **Beispiel:** Aus *https://hu-berlin.zoom.us/j/67731316437?pwd=RkxtL2hnOUxBaGFVdmlNVmgxQkRGUT09* wird *https://hu-berlin.zoom.us/j/67731316437*
    - *Oder* stellen Sie lediglich die Raum-ID zur Verfügung.
        - **Beispiel:** 677 3131 6437.

Dieses Vorgehen schützt natürlich nicht davor, dass jemand aus dem Kreis der Wissenden die Daten Unbefugten zur Verfügung stellt. Im Mindesten aber wird dem automatisierten Abgreifen der Zugänge durch Bots vorgebeugt.

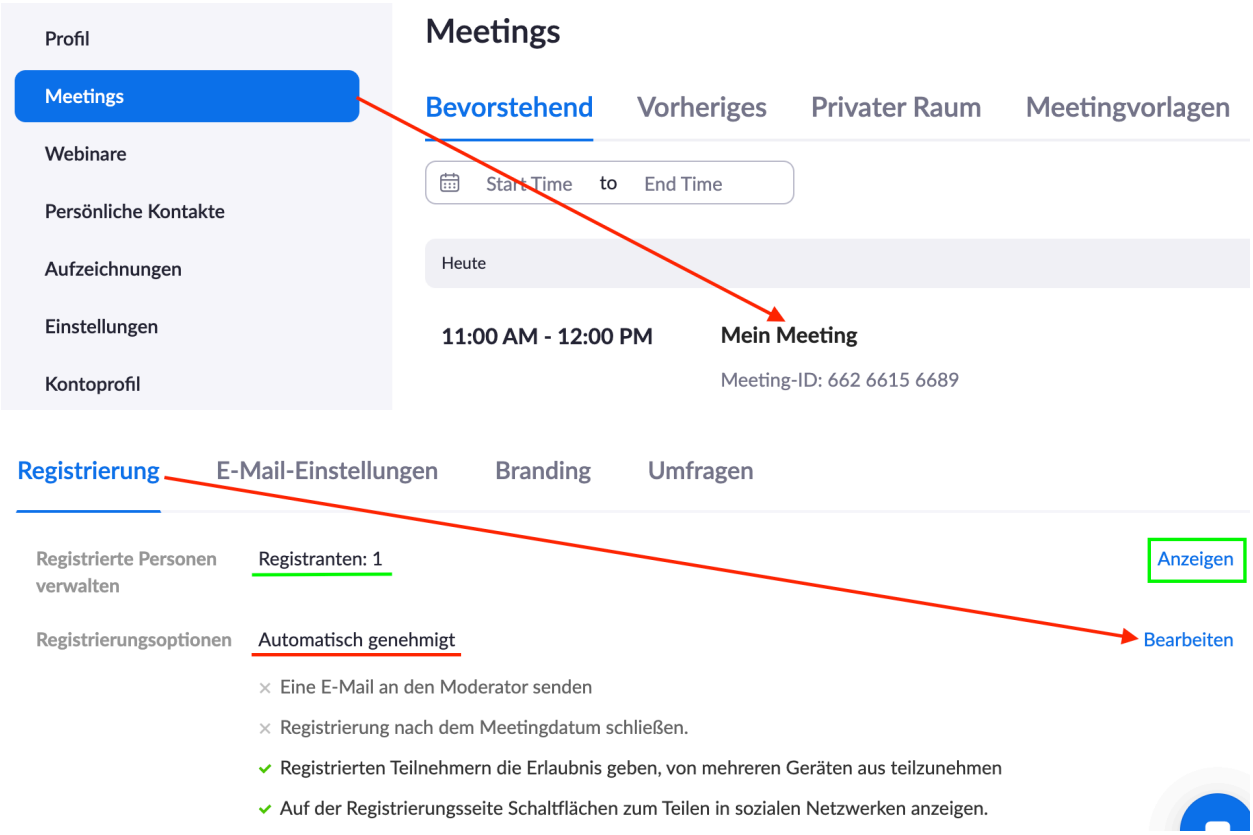
2 - Registrierung nutzen

Bei der Erstellung eines Meetings können Sie eine Registrierung für die Veranstaltung einrichten. Teilnehmende müssen sich dann im Vorfeld der Veranstaltung mit ihren Namen und E-Mail-Adressen registrieren, um einen Zugang zur Konferenz zu erhalten. Diese Methode hat eine starke Schutzwirkung, kommt allerdings mit Nachteilen in Form von Aufwand und Datenschutz. So müssen Sie sicherstellen, dass jeder Eintrag auch wirklich berechtigt ist, an Ihrer Sitzung teilzunehmen und Sie müssen dafür sorgen, dass die Liste der Personen nicht an Unbefugte weitergereicht wird. Rechnen Sie hierbei auch mit Anfragen Teilnehmender zum Datenschutz!

Um die Registrierung zu aktivieren, gehen Sie wie folgt vor:

- Loggen Sie sich unter **https://hu-berlin.zoom.us** ein.
- Legen Sie ein neues Meeting an oder bearbeiten Sie ein bestehendes.
- In der Rubrik „**Registrierung**“ setzen Sie einen Haken bei „**Erforderlich**“.
- **Speichern** Sie das Meeting, nachdem Sie Ihre gewünschten Einstellungen vorgenommen haben.

Standard gemäß werden Teilnehmende die sich registrieren vom System automatisch freigeschaltet und mit den Zugangsdaten versorgt. Sie können dieses Verhalten ändern, indem Sie im Browser, in Ihrer Meeting-Übersicht, auf den Namen des Meetings klicken, im Anschluss runter scrollen und die Registrierungsoptionen bearbeiten. Siehe folgende Abbildungen.



Hier sehen Sie auch, wieviele Personen sich bereits registriert haben und können sich diese anzeigen lassen. Die daraufhin dargestellte Liste sollte nun von Ihnen durchgegangen werden. Markieren Sie alle Einträge die unbekannt sind oder nach Fake-Daten aussehen und stornieren Sie die Registrierung.

Das hindert Teilnehmende nicht daran sich mit einem neuen Eintrag anzumelden und Mehrarbeit für Sie zu generieren. Daher bietet es sich an, den Prozess von „Automatisch genehmigen" auf „**Manuell genehmigen**" umzustellen.

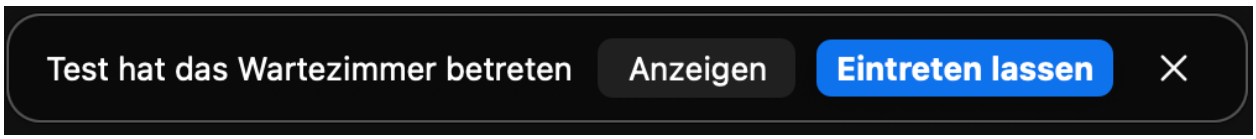
3 - Warteraum nutzen

Mit einem Warteraum sorgen Sie dafür, dass Teilnehmende nach Einwahl zunächst in einem gesonderten Bereich der Konferenz landen, in welchem sie keinen Schaden anrichten können – quasi wie eine Schleuse. Teilnehmende müssen dann einzeln oder in einem Schwung vom Host des Meetings zugelassen werden. Der Vorteil eines Warteraums ist die bessere Randbedingung was den Datenschutz anbelangt. Der Warteraum benötigt keine vorherige Registrierung und läuft in Echtzeit sobald die Konferenz gestartet wird.

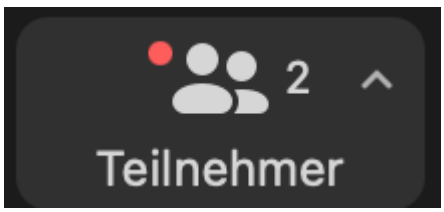
Um einen Warteraum einzurichten, gehen Sie wie folgt vor.

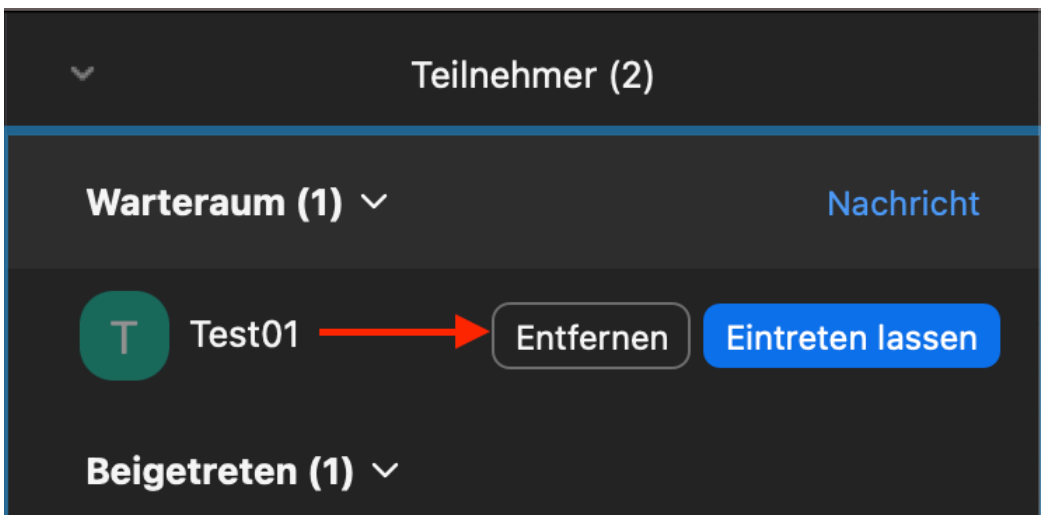
- Loggen Sie sich unter **https://hu-berlin.zoom.us** ein.
- Legen Sie ein neues Meeting an oder bearbeiten Sie ein bestehendes.
- In der Rubrik „**Sicherheit**“ setzen Sie einen Haken bei „**Warteraum**“.
- **Speichern** Sie das Meeting, nachdem Sie Ihre gewünschten Einstellungen vorgenommen haben.

Innerhalb einer laufenden Sitzung bekommen Sie nun einen Hinweis, wann immer jemand den Raum betreten möchte. Klicken Sie auf „Eintreten lassen“ damit die Person das eigentliche Meeting betreten kann. Klicken Sie auf „Anzeigen“, um sich die wartenden Personen zunächst auflisten zu lassen.



Sollte Ihnen die Meldung verlustig gehen, können Sie auch ganz einfach den Schalter „**Teilnehmer**“ verwenden. Der Warteraum wird in der aufgeklappten Seitenleiste gesondert erfasst. Klicken Sie auf „Entfernen“, wenn Sie unberechtigte oder verdächtige Teilnehmende entdecken. Über die **Teilnehmendenliste** und die Schaltfläche „**Mehr**“, neben den Namen, können Sie Personen auch wieder zurück in den Warteraum verschieben.





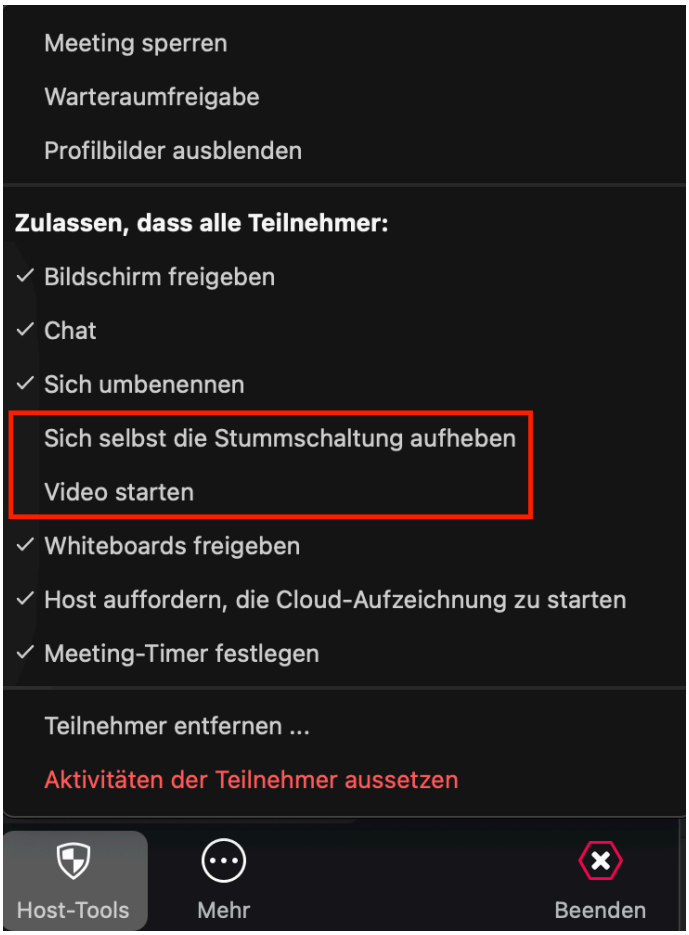
Der Nachteil dieser Methode ist, dass Sie während Ihrer Konferenz ggf. immer wieder prüfen müssen wer rein darf und wer nicht. Es bietet sich daher an, diese Aufgabe an eine Hilfskraft abzutreten. Bitte beachten Sie, dass die Hilfe die Host-Rolle (nicht Co-Host) in der Sitzung haben muss!

4 - Einstellungen in der laufenden Konferenz

Zusätzlich zu den oben beschriebenen Methoden, haben Sie in einer laufenden Sitzung jederzeit die Möglichkeit die Sicherheit zu erhöhen. Hierbei handelt es sich um optionale reaktive Maßnahmen, die im Zusammenspiel mit den o.g. proaktiven Maßnahmen Anwendung finden können, ggf. sollten.

Sperren der Audio- und Videoübertragungen

Um Teilnehmenden die Rechte für die Audio- und Videoübertragung zu nehmen, klicken Sie in einer laufenden Sitzung auf den Schalter „Host-Tools“. Hier finden Sie verschiedene Optionen, welche die Teilnehmendenrechte einschränken. Entfernen Sie die Haken bei „**Sich selbst die Stummschaltung aufheben**“ und „**Video starten**“.



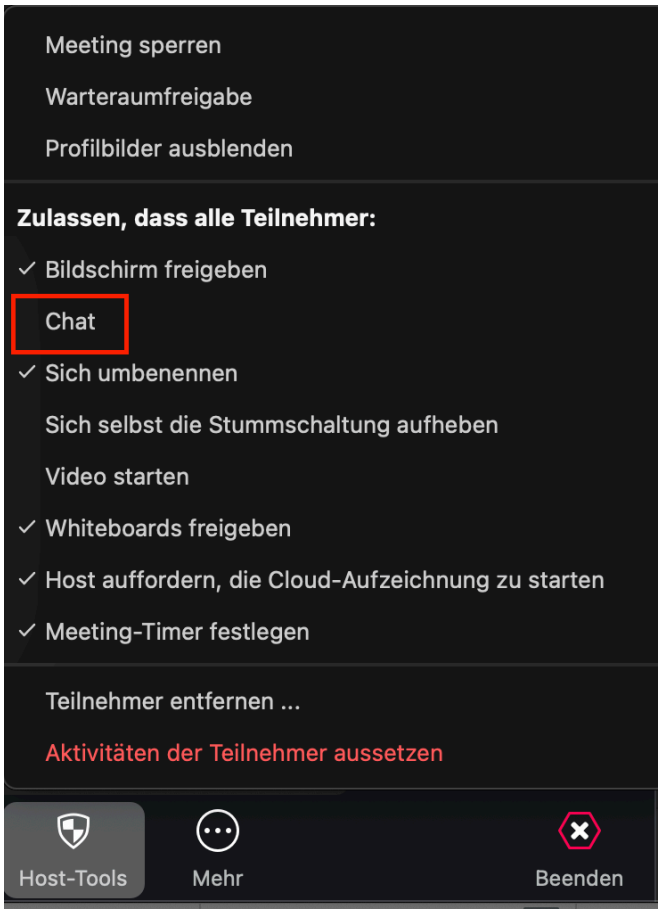
Beachten Sie, dass diese Einstellungen nur für Teilnehmende gelten, nicht für Hosts und Co-Hosts. Das heißt auch, dass gleichzeitig alle Teilnehmenden betroffen sind. Eine solche Einstellung für einzelne Teilnehmende gibt es derzeit nicht. Ungeachtet dessen, handelt es sich bei diesem Vorgehen um eines der effektivsten, um Störungen zu unterbinden.

Der Nachteil ist, dass auch die Interaktion mit den Lehrkräften eingeschränkt wird. Es können hierbei allerdings weiterhin der Chat und virtuelle Meldungen verwendet werden. Der Host hat auch die Möglichkeit explizit einzelne Teilnehmende um die Aktivierung des Mikrofons zu bitten. Öffnen Sie dazu die **Teilnehmendenliste** und wählen Sie „**Bitten Ton einzuschalten**“, neben dem Namen einer Person.

Die betroffene Person bekommt daraufhin eine entsprechende Meldung im eigenen Zoom-Fenster und muss diese Bestätigen. Eine solche Funktion bezogen auf die Videoübertragung gibt es derzeit nicht. Um diesen Umstand zu umgehen, können Sie allerdings dieselbe Person über den Knopf „**Mehr**“ die Co-Host-Rolle zusprechen, woraufhin auch die Kamera aktiviert werden kann. Überlegen Sie bitte gut, wem Sie diese Rolle geben, denn mit ihr einher gehen Rechte die Konferenz zu steuern und Sicherheits-einstellungen zu ändern.

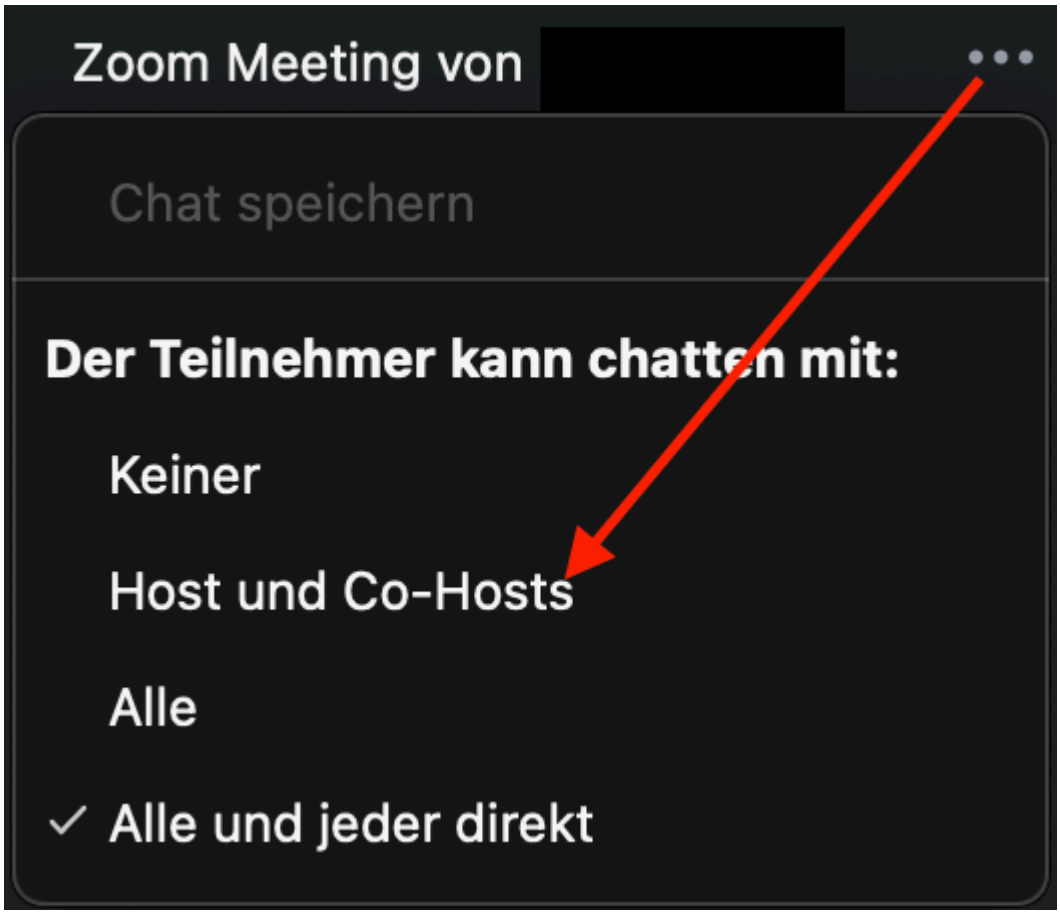
Sperren des Chats

Wenn Sie bemerken, dass der Chat missbräuchlich verwendet wird oder Sie einfach nur die volle Konzentration auf Ihren Vortrag lenken möchten, können Sie das ebenfalls in den schon oben erwähnten Sicherheitseinstellungen beeinflussen. Entfernen Sie dafür einfach den Haken bei „**Chat**“. Auch hier gilt wieder, diese Einstellung betrifft nur Teilnehmende, nicht Hosts und Co-Hosts.



Bonus: Direkt darunter finden Sie die Option das **Umbenennen** für Teilnehmende zu unterbinden. Denken Sie daran, Namen könnten als Text auch missbräuchlich verwendet werden. Weiter oben finden Sie „**Profilbilder ausblenden**“, was ähnlich hilfreich sein kann.

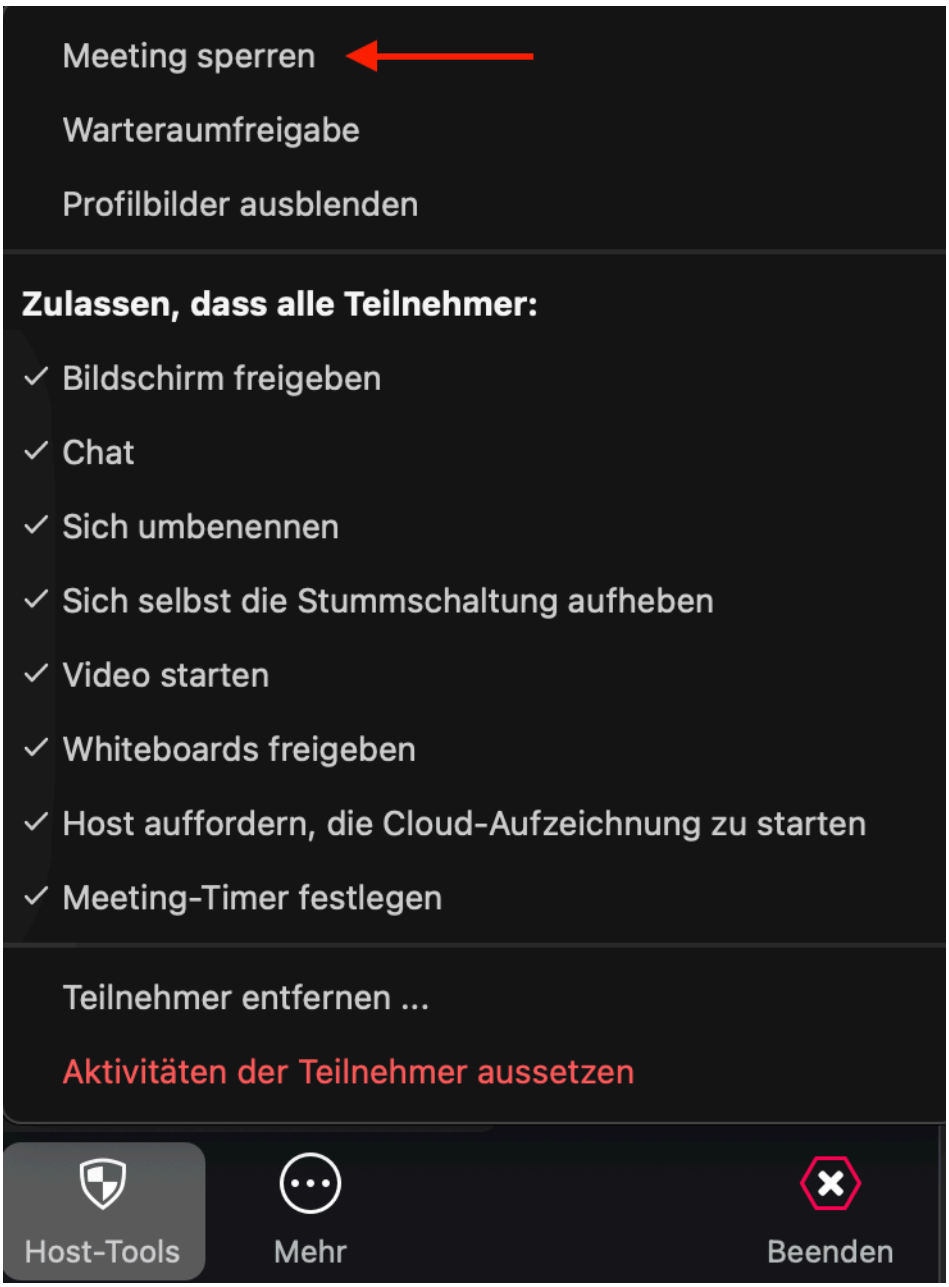
Im Chatfenster finden Sie die Schaltfläche „**Mehr**“. Hier können Sie einstellen, dass nur Hosts und Co-Hosts private Chatnachrichten gesendet werden können. Die angeschriebenen Personen können darauf eine Antwort verfassen.



Meeting sperren

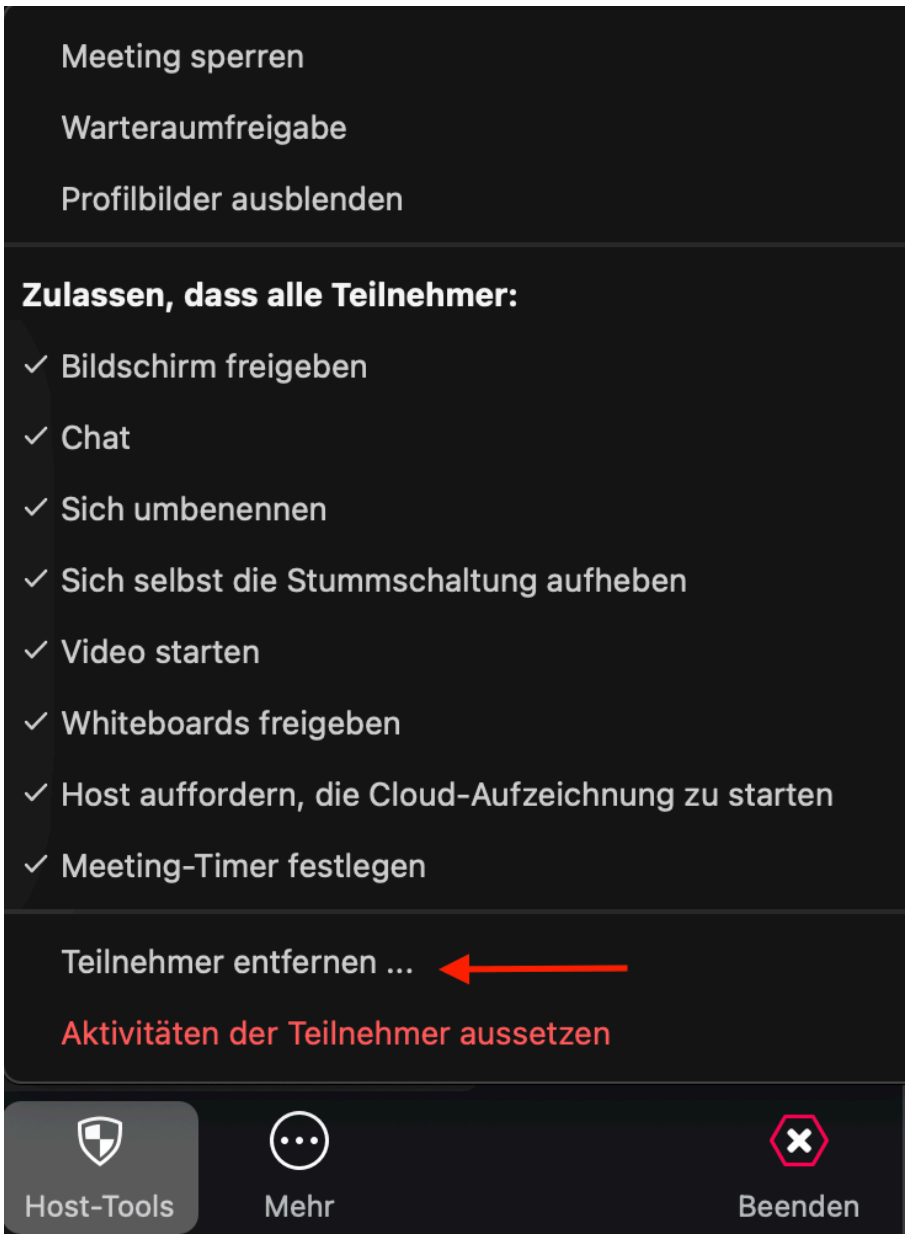
Wenn Sie weder die Registrierung noch den Warteraum nutzen möchten oder können, haben Sie die Möglichkeit das Meeting - zum Beispiel bei Erreichen einer bestimmten Teilnehmendenzahl oder Anwesenheit aller Ihnen bekannter Personen - das Meeting zu sperren. Das ist vergleichbar zu einem Hörsaal den Sie abschließen. Es kommt niemand mehr rein und es bleibt bei den derzeit Anwesenden. Der Nachteil ist, dass Sie bei Nachzüglern den Raum wieder entsperren und anschließend erneut sperren müssten. Gleiches gilt für Teilnehmende, die aufgrund von Internetproblemen o.Ä. kurzzeitig aus der Sitzung fallen. Hier könnte es zu Überblicksproblemen kommen, die durch Hinweise Teilnehmender oder einer gesonderten Hilfskraft umgangen werden können.

Wählen Sie unter der Schaltfläche „**Host-Tools**“ die Option „**Meeting sperren**“.

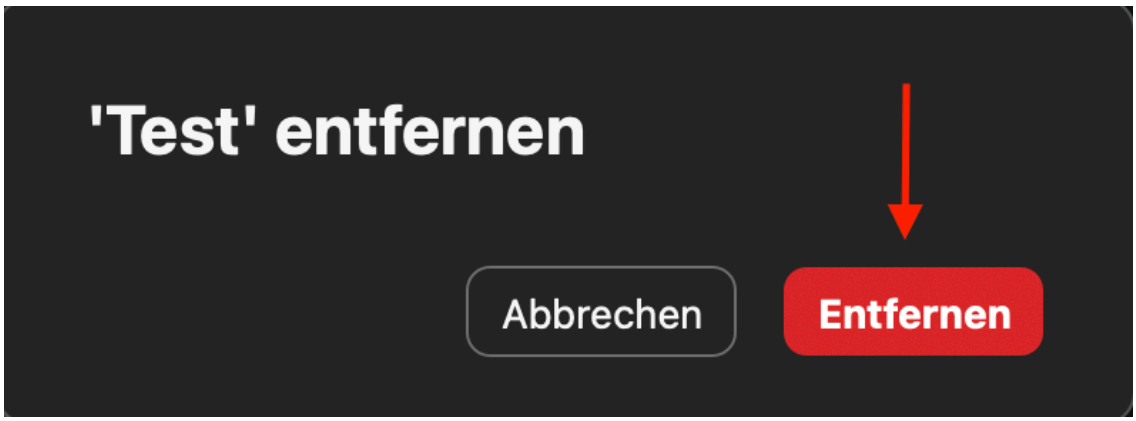


Teilnehmende entfernen

Sollten Sie störende Teilnehmende identifiziert haben, können Sie diese jederzeit entfernen. Auch hier klicken Sie wieder auf die Schaltfläche „**Host-Tools**“ und anschließend auf „**Teilnehmer entfernen ...**“. Eine Seitenleiste mit den Namen der Teilnehmenden öffnet sich. Klicken Sie auf den Schalter „**Entfernen**“, neben dem Namen der störenden Person. Im darauffolgenden Dialogfenster haben Sie auch gleich die Möglichkeit die Person an Zoom zu melden. Das kann in der Sperrung des betroffenen Accounts resultieren.



Teilnehmendenliste:

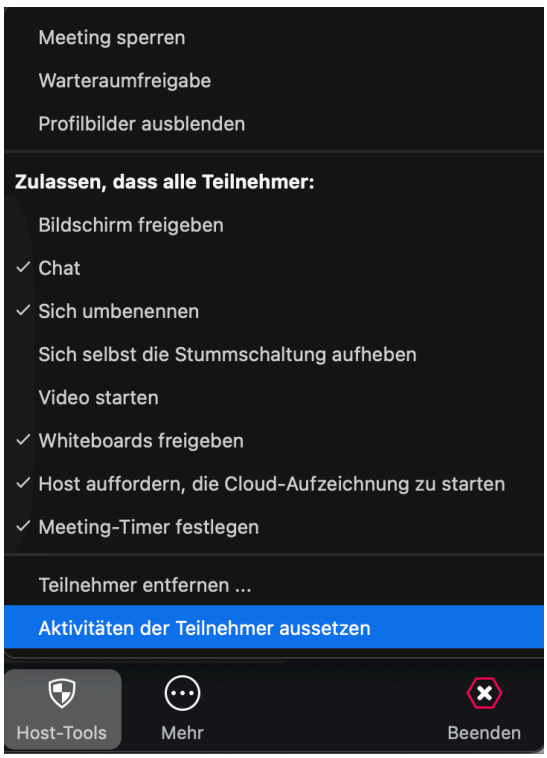


Sie können Personen auch über die **Teilnehmendenliste** und der Schaltfläche „**Mehr**“, neben den Namen entfernen.

Wenn alle Stricke reißen; der Panik-Knopf

Sollten aus unerfindlichen Gründen die oben beschriebenen Maßnahmen nicht greifen oder für den Fall dass Sie alles sehr schnell unterbinden möchten, gibt es als letzte Lösung noch einen sogenannten „*Panic Button*“. Auch dieser Findet sich wieder unter der Schaltfläche „Sicherheit“ und ist in roter Schrift unterlegt. Verwenden Sie diesen Knopf, wird in der Sitzung sofort **alles** gesperrt. Mit dieser Optionen verhindern Sie mit einem Schlag Schlimmeres.

Wählen Sie „**Aktivitäten der Teilnehmer aussetzen**“.



Autoren: Ingo Riehl
v4 Stand: 16.04.2024
CMS Humboldt-Universität zu Berlin

Bei Fragen rund um die digitale Lehre: digitale-lehre@hu-berlin.de
E-Mails an diese Adresse werden mit einem elektronischen Ticketsystems bearbeitet.