Zoom Sicherheit

25.04.2024 15:50:23

FAQ-Artikel-Ausdruck

Kategorie:	Kommunikation & Kollaboration::Video- / Telefonkonferenzen	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	10:11:20 - 20.04.2023

Schlüsselwörter

Zoom Verschlüsselung

Lösung (öffentlich)

Ende-zu-Ende-Verschlüsselung (E2EE)

Sie können für Zoom-Meetings eine Verschlüsselung aktivieren, sodass nur die Teilnehmenden in der Lage sind, die übertragenen Inhalte zu entschlüsseln.
Die Verschlüsselung wird insbesondere empfohlen, wenn besonders sensible Kommunikation über Zoom-Meetings geführt wird.

Voraussetzungen für alle Teilnehmenden
(kostenloses) Zoom-Konto (per Telefonnummer verifiziert mit gültiger Abrechnungsoption) Nutzung des Zoom Desktop Client oder der Zoom Mobile App (in aktueller Version)

Nicht verfügbare Funktionen und Einschränkungen maximal 200 Teilnehmende Umfragen Livestreaming Beitritt vor Moderierenden Telefoneinwahl Breakouträume Live-Transkription

Aktivierung Als Erstes müssen Sie die Option über das [1]Webinterface von Zoom in Ihren Konto-Einstellungen aktivieren. Über den Link landen Sie in den Einstellungen, wo Sie bis zum Ende des Bereichs „Sicherheit“ scrollen. Dort aktivieren Sie die Option „End-to-End-Verschlüsselung nutzen“ und in der darunter erscheinenden Einstellung „Vorgegebene Verschlüsselungsart“ aktivieren Sie die Option „End-to-End-Verschlüsselung“.

Weitere Informationen finden Sie im [2]Zoom-Hilfsartikel

Tipps Damit Sie Ihre Videokonferenzen über Zoom ungestört abhalten können, beachten Sie die folgenden Hinweise.

Meeting erstellen

Stellen Sie sicher, dass mit der Option "Automatisch erzeugen" unter "Meeting-ID" eine zufällige Kennung erstellt wird, verwenden Sie keine Persönliche Meeting-ID (PMI) für nicht öffentliche oder fortlaufende Konferenzen.
Die PMI ist für Ihren persönlichen Konferenzraum gedacht, sie ändert sich nicht. Dieser Raum ist für Sofort-Meetings gedacht mit Personen, mit denen Sie sich regelmäßig treffen. Läuft Ihr persönliches Meeting, können alle Personen, die den Link bzw. die PMI Ihres persönlichen Raums kennen, jederzeit beitreten. Dies kann verhindert werden, indem Sie das Meeting sperren oder den Warteraum zur Einlasskontrolle aktivieren.

Zutritt regulieren
Sie können bei der Planung eines Meetings Teilnehmende auf Basis angegebener Regionen ein- oder ausschließen. Entweder nutzen Sie hier die Methode einer Allow- oder Blocklist.

Stellen Sie außerdem sicher, dass einmal entfernte Personen nicht wieder eintreten können. Dazu muss die Option "Entfernten Teilnehmern den erneuten Beitritt erlauben" in Ihren Zoom-Einstellungen unter "In Meeting (Grundlagen)" deaktiviert sein.

Meetingsicherheit in besonderen Situation

Sie haben die Möglichkeit, in den Zoom Einstellungen unter "Sicherheit" ([3]https://tu-dresden.zoom.us/profile/setting), den Zugang zum Meeting für spezielle Fälle einzuschränken. Wichtig: Alle diese Einstellungen erfordern einen Zoom-Account. Dieser wird für TU Dresden Angehörige bei Login via [4]https://tu-dresden.zoom.us automatisch erstellt, externe Nutzende über deren Institute oder unter https://zoom.us .

Für Prüfungssituationen wird die Einstellung "Nur Mitglieder der TU Dresden (Default)" genutzt. Jede der TU Dresden angehörige Person loggt sich mit ihrem ZIH-Login (Kürzel und Passwort) per Single Sign On (SSO bzw. Schlüsselsymbol) ein und ist somit automatisch authentifiziert.

Sollen Meetingteilnehmende z.B. nur von einer bestimmten Universtität aus beitreten, so kann die Auswahl "Universitätsdomäne(n) eintragen" (mit Komma getrennt, ohne Leerezeichen - universitaet1.de,universitaet2.de) genutzt werden.

Die hier getätigten Einstellungen können dann in der Meetingerstellung ausgewählt werden.

Einladungen

Sie sollten den Einladungslink und Kenncode Ihres Meetings nicht auf öffentlichen Plattformen verbreiten. Die Einladungsdaten können Sie den Teilnehmenden über sichere Kanäle wie E-Mail oder Textnachricht zukommen

lassen.

Passwort

Zoom erzeugt bei der Planung eines Meetings automatisch einen Kenncode. Dieser wird verschlüsselt in den Einladungslink eingefügt, sodass Teilnehmende dem Meeting direkt ohne Eingabe des Kenncodes beitreten können.

Es ist aber empfehlenswert, den Kenncode nur einem bestimmten Personenkreis zur Verfügung zu stellen und ihn nicht zu veröffentlichen. Damit Sie keinen Link mit integriertem Passwort erhalten, deaktivieren Sie die Option "Einbetten des Kenncodes in den Einladungslink für die Teilnahme mit einem Klick" in Ihren Zoom-Einstellungen im Abschnitt Meeting unter Sicherheit.

Warteraum

Für Meetings mit einem nicht definierten Personenkreis sollten Sie wenn möglich immer einen Warteraum einrichten. Eintretende gelangen dann nicht direkt in den Meeting-Raum, sondern zunächst in den Warteraum. Moderierende können dann jeden Teilnehmenden einzeln aus dem Warteraum in das Meeting aufnehmen oder entfernen.

Meeting sperren

Wenn die Teilnehmenden im Vorfeld bekannt sind, können Sie prüfen, ob alle Personen im Meeting anwesend sind. Das Meeting lässt sich dann für weitere Eintritte sperren. Gehen Sie dazu auf den Punkt "Sicherheit" unten links in der Menüleiste und wählen dort den Punkt "Meeting sperren" aus.

Klarnamen

Bitten Sie Teilnehmende im Vorfeld der Konferenz, ihren vollständigen Klarnamen anzugeben. Das erleichtert für Moderierende die Arbeit, ungewollte Gäste aus dem Meeting zu entfernen.

Aufzeichnung

Es steht die Lokale- sowie die Cloud-Aufzeichnung zur Verfügung.
[5]https://tu-dresden.zoom.us/profile/setting , Reiter 'Aufzeichnung'.
Nur Aufnahmen, die mit Schutzbedarf normal bzw. hoch eingestuft werden, sollten in der Cloud gespeichert werden.

Weitere Hinweise zu Einstellungen in Zoom finden Sie [6]hier (nur in Englisch verfügbar).

[1] https://tu-dresden.zoom.us/profile/setting
[2] https://support.zoom.us/hc/de/articles/360048660871-End-to-End-Verschl%C3%BCsselung-E2EE-f%C3%BCr-Meetings
[3] https://tu-dresden.zoom.us/profile/setting
[4] https://tu-dresden.zoom.us
[5] https://tu-dresden.zoom.us/profile/setting
[6] https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls