Rotary Distrikt 1870 | Kommunikations-ausschuss

Kurzanleitung für Zoom

Stand: 24.06.2020
erstellt von: Dr. Hauke Holdefleiss, (Internetbeauftragter RC Gelsenkirchen – Schloss Horst)

Für alle Erstnutzer:

Vorbereitung: Ihr benötigt ein Gerät mit funktionierender Kamera, Mikrofon und Lautsprecher. Zoom funktioniert sowohl am Computer, MAC, Laptop, tablet, smartphone. Für alle ohne Computer oder Mikro: es geht auch per Telefoneinwahl, dann natürlich nur ohne Bild. Diese Variante geht auch parallel zur Computernutzung für den Audiobereich (statt Mikrofon/Lautsprecher).

1.) Am einfachsten ist der Einstieg per Laptop oder Computer, da dort der Bildschirm größer ist als am smartphone. Möglichst die Software installieren, da die direkte Nutzung im Browser (Chrome, Firefox o.ä.) nicht nur schnell frustriert, sondern (noch) weniger sicher ist.
Dazu vor dem Meeting auf der Seite zoom.us unter Ressourcen (ganz oben rechts) die Funktion „Zoom client runterladen“ wählen, dann den „Zoom-Client für Meetings“ laden und installieren. Nach Fertigstellung (Nutzungsbedingungen und ggfs. Nutzungserlaubnissen Kamera/Mikrofon zustimmen) könnt ihr direkt auf Meeting beitreten klicken (Registrierung kann gemacht werden, ist aber nicht nötig). Es gibt etliche Anleitungen dazu auf youtube.

2.) iphone/ipad/smartphone: ladet vorher aus dem store die App „Zoom Cloud Meeting“, installiert diese und geht dann auf Meeting beitreten. Zugangsdaten siehe oben

Bei Zoom kann man sich registrieren und angemeldet arbeiten; für die Teilnahme an einem Meeting ist das jedoch nicht nötig. Die Registrierung (auch in der kostenlosen Version) hat den Vorteil, dass ein paar Grundeinstellungen, wie zB angezeigter Name oder weitere virtuelle Hintergründe, gespeichert werden. Die Meetingdauer hängt von der Zoom Version des Hostes (Gastgebers) ab.

Rotary Distrikt 1870 | Kommunikations-ausschuss

Sicherheitsanmerkungen

Und hier kurz ein paar Anmerkungen zur Zoom Sicherheit (darf gerne weiter gegeben werden, ohne Anspruch auf Vollständigkeit):

Bzgl. Zoom Sicherheit hat das Unternehmen auf Kritik bereits mit deutlichen Verbesserungen reagiert.

Bekannte Schwachstellen sind:

1. Bombering (Fremde blenden sich mit seltsamen/illegalem/pornographischen Inhalten ein)
2. Unerwünschten Kamerafreigaben bei der Nutzung im Browser bzw bei Installation (apple)
3. Unkontrollierte Datenweitergabe an facebook etc. (angeblich mittlerweile eingestellt)
4. Un- bzw schlecht verschlüsselte Kommunikation (behoben ab Version 5.0)

Bei der Nutzung von allen us-amerikanischen Diensten (facebook, google, whatsapp, dropbox etc.) muss man immer bedenken, dass in den USA andere Datenschutzbestimmungen gelten als in der EU. Im Gegensatz zu einigen anderen hat Zoom jedoch eine Konformitätserklärung zur DSGVO abgegeben. Die Datenserver stehen immer in den USA mit gesetzlich festgeschriebenem NSA u.a. Zugriff.

Im Gegensatz zu whatsapp oder dem facebook-messenger hat Zoom jedoch keinen Zugriff auf die Adressbücher (das sollten whatsapp Nutzer beachten….). Daher möglichst keine Freigaben für „Kalenderverknüpfungen“ o.a. installieren.

Der Vorteil all dieser Anwendungen liegt in der sehr guten Funktionalität, der einfachen Bedienung und einer hohen benutzerfreundlichen Gestaltung.

Für Teilnehmer:

- Wer ganz sicher gehen will (oder sicherheitsrelevante Daten hat) sollte für Zoom wie für alle Internetfunktionen einen extra Laptop/Computer nutzen (physische Trennung von Intranet/sensiblen Daten).
- Keine Anmeldung/Zutritt per google oder facebook-Konten
- Zoom App nicht automatisch starten (autostart / Häkchen „angemeldet bleiben“ weg)
- Nach Beendigung eines Meeting: alle Zoom Apps schließen.
- Immer aktuelle Version nutzen. Ab Version 5.0 nutzt Zoom obligatorisch Datenverschlüsselung (AES 256 Bit GCM).

Für Moderatoren:

Sinnvolle Sicherheitseinstellungen im Profil unter Einstellungen oder bei der Anlage der Meetings:

1. Immer die Passwortfunktion für das Meeting aktivieren; ab und an das Passwort wechseln. Gelegentlich die Meeting ID wechseln.
2. Deaktivieren der Funktion „Beitritt vor Moderator aktivieren“ (ausser bei Moderatorenschlüssel, s.u.)
3. Meeting ID und besonders das Passwort nicht veröffentlichen (zB auf der Homepage)
4. Falls Bombering-Gefahr erhöht (zB weil wegen interessantem Vortrag die Meeting ID plus Passwort ausserhalb des Clubs verteilt wurde): Wartezimmerfunktion einschalten

5. Im Meeting: unter der Funktion „Bildschirm teilen“ die Version „Nur Host, nicht Teilnehmer“ aktivieren. Damit lässt sich steuern, wer Inhalte teilen darf. Für den Vortragenden lässt sich das wieder deaktivieren
6. Telefoneinwahl (wenn überhaupt gewünscht) nur aus Deutschland zulassen (in Meeting-einstellung). Telefoneinwahl verhindert Verschlüsselung!
7. Generell keine Anmeldung in der App per facebook oder google erlauben (kann in „Einstellungen“ deaktiviert werden), sondern wenn Anmeldung dann immer manuell eingeben (wäre zwar einfacher, aber stellt direkt eine Verknüpfung her und gibt evtl. Zugriffsrechte an FB weiter)
8. Falls Bombering oder unerwünschte Teilnehmer: deaktivieren der Funktion „entfernten Teilnehmern den erneuten Beitritt erlauben“
9. Kamerafernsteuerung deaktivieren (Profil-Einstellungen-sonstiges)
10. Erweiterungen des Programmes aus dem App-Markt (Kalenderverknüpfungen etc.) vermeiden
11. Unter Einstellung lassen sich die Rechenzentren nach Regionen beschränken. Für Inner-europäische Konferenzen sollte nur Europa (+ USA als Muss-Option) ausgewählt werden.
12. DSGVO: ein Auftragsverarbeitungsvertrag mit Zoom wird mittlerweile automatisch mit Akzeptanz der AGB geschlossen

Bei größeren Meetings empfiehlt es sich, wenn eine Dritte Person sich nur um die Meetingtechnik kümmert (zB als Host oder Co-Host), unabhängig vom Vortrag, Präsident etc..

Ich habe dann meist noch einen separaten Laptop zusätzlich mit der Einwahl als „Testaccount“ laufen. Dort kann ich aus der Sicht eines Teilnehmers das Meeting verfolgen.

Nützliche Zusatzfunktionen:

1.) Bei vielen Teilnehmern oder um Gespräche in kleinen Gruppen zu ermöglichen gibt es bei Zoom die Möglichkeit, mehrere Unter-Räume zu öffnen („breakoutrooms“). Diese Funktion muss im Profil aktiviert werden; dann lassen sich die Räume sowohl während als auch bereits vor dem Meeting erstellen. Die Teilnehmer können automatisch oder manuell zugeteilt werden. Falls gewünscht können die Räume zeitlich befristet werden.
2.) Der Moderator kann (zB bei Verhinderung) einen Stellvertreter das Meeting steuern lassen. Dafür gibt es im Profil die Möglichkeit einen Moderatorenschlüssel anzulegen. Im Meeting gibt es die Funktion „Host anfordern“. Nach Eingabe des Schlüssels erhält man Hostfunktion. Das funktioniert allerdings derzeit nur, wenn ein Zutritt zum Meeting auch vor dem Host möglich ist.
3.) Während des Meetings kann anderen Teilnehmern die Co-Host Funktion zugewiesen werden. Dies ist insbesondere dann sinnvoll wenn der Moderator nur über eine instabile Internetverbindung verfügt (oder wenn es Probleme bei der Bildschirmfreigabe des Vortragenden gibt = diesen als Co-Host aktivieren).
4.) Musikübertragung: Zoom ist standardmässig für Sprachübertragung optimiert (dh hohe und tiefe Frequenzen werden geglättet). Für Musikübertragungen lässt sich in Einstellungen die Funktion „Originalton“ aktivieren; es wird dann die gesamte Bandbreite übertragen, erfordert allerdings etwas mehr Internetleistung.