Ende-zu-Ende-Verschlüsselung für Webex Meetings

Sicherheit von Webex mit und ohne Ende-zu-Ende-Verschlüsselung

Für Videokonferenzlösungen wie Cisco Webex wird eine Client-Server-Architektur verwendet, bei der sich die Teilnehmer (Clients) mit ihren Endgeräten zum Meeting Server (unistuttgart.webex.com) verbinden. Auf diesem Server läuft das Meeting zentral ab und die Medienströme der einzelnen Teilnehmer werden empfangen und wieder an diese gesendet. Im Fall von Cisco Webex befindet sich dieser zentrale Server nicht im Rechenzentrum der Universität Stuttgart, sondern in einem Rechenzentrum von Cisco in Frankfurt/Main. Die Nutzung dieser "Software as a Service" (bzw. dieses Cloud-Dienstes) ist Gegenstand eines umfangreichen Vertragswerkes mit der US-amerikanischen Firma Cisco Systems Inc. bzw. ihrer europäischen Tochter.

Der Datentransfer zwischen dem Server und den einzelnen Clients findet grundsätzlich verschlüsselt statt.

Um bestimmte Funktionen zur Verfügung zu stellen, wie z. B. das Erstellen von cloudbasierten Aufzeichnungen, ist es jedoch erforderlich, dass auf dem Meeting Server der Medienstrom entschlüsselt wird. Rein theoretisch wäre es technisch möglich, dass Cisco in diesem Moment auf die Daten zugreifen kann. Cisco versichert den Kunden durch entsprechende Verträge und Zertifizierungen, dass keinerlei Zugriff stattfindet und dass dies durch technische und organisatorische Maßnahmen verhindert wird.

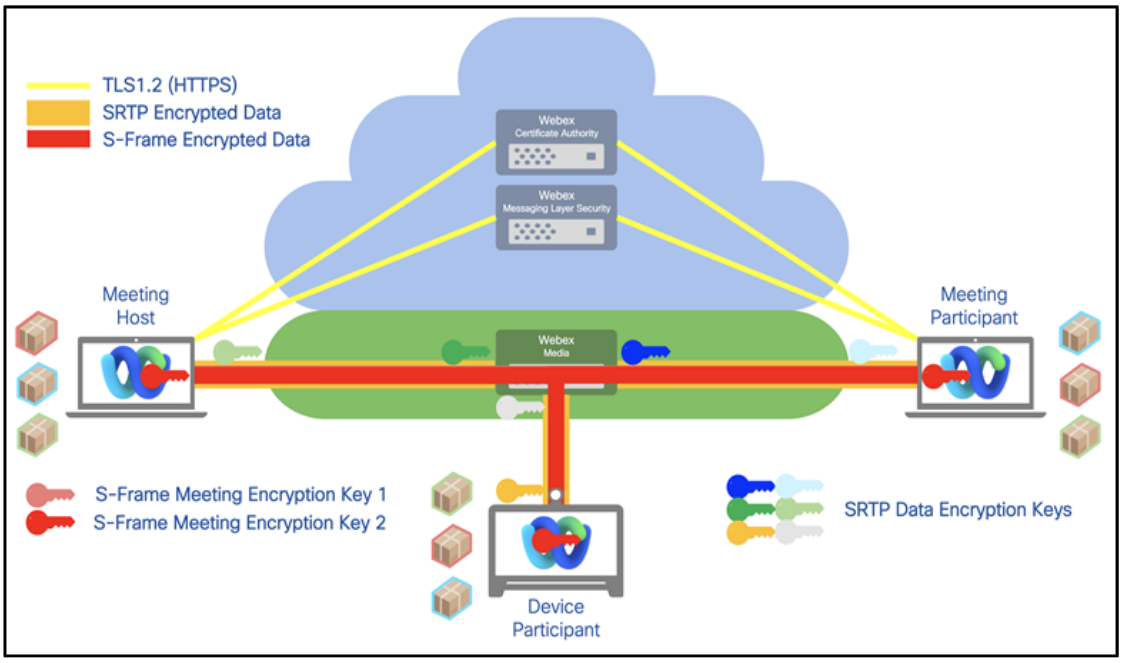
Cisco bietet Ende-zu-Ende-verschlüsselte Meetings an, bei denen der Medienstrom nicht auf dem Webex Server entschlüsselt wird. Hierbei ist der Funktionsumfang im Meeting eingeschränkt. Der Funktionsumfang und die Nutzung mit und ohne Ende-zu-Ende-Verschlüsselung werden in den folgenden Abschnitten detailliert erklärt.

Funktionsweise von Webex Meetings ohne Ende-zu-Ende-Verschlüsselung

Die Medienströme für Webex Meetings werden von einem Meeting Teilnehmer zum Webex Server gesendet und von dort zu den weiteren Teilnehmern eines Meetings. Grundsätzlich erfolgt die Übertragung der Medienströme vom Teilnehmer zum Webex Server und vom Webex Server zu den weiteren Teilnehmern eines Meetings verschlüsselt.

Medienströme von einem Client zu einem Webex Server werden erst entschlüsselt, nachdem sie die Webex Firewall innerhalb der Webex Cloud passiert haben. Dies ist z. B. erforderlich, um cloudbasierte Aufzeichnungen zu ermöglichen. Webex verschlüsselt den Medienstrom erneut, bevor dieser die Webex Cloud verlässt und an andere Clients gesendet wird.

Funktionsweise von Webex Meetings mit Ende-zu-Ende-Verschlüsselung



Für Webex Meetings, die eine höhere Sicherheitsstufe benötigen, bietet Webex zusätzlich eine Ende-zu-Ende-Verschlüsselung an. Mit dieser Option werden die Medienströme nicht in der Webex Cloud entschlüsselt, wie dies bei Standardmeetings der Fall wäre. Stattdessen wird ein TLS-Kanal für die Client-Server-Kommunikation erstellt. Zusätzlich generieren alle Webex Clients Schlüsselpaare und senden den öffentlichen Schlüssel an den Client des Meeting-Hosts.

Der Meeting-Host generiert einen zufälligen symmetrischen Schlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel, den der Client sendet, und sendet den verschlüsselten symmetrischen Schlüssel zurück an den Client. Der von Clients generierte Datenverkehr wird mit dem symmetrischen Schlüssel verschlüsselt. In diesem Modell kann der Datenverkehr nicht vom Webex Server entschlüsselt werden. Diese Option der Ende-zu-Ende-Verschlüsselung ist für Webex Meetings verfügbar.

Um ein Meeting mit Ende-zu-Ende-Verschlüsselung durchzuführen, muss beim Ansetzen des Meetings über die Weboberfläche der entsprechende Meetingtyp gewählt werden.

Dieser wird in der Auswahlliste der Meetingtypen angezeigt mit der Bezeichnung

Webex Meetings Pro-End to End Encryption_VOIPonly

Erstellen eines Ende-zu-Ende-verschlüsselten Meetings

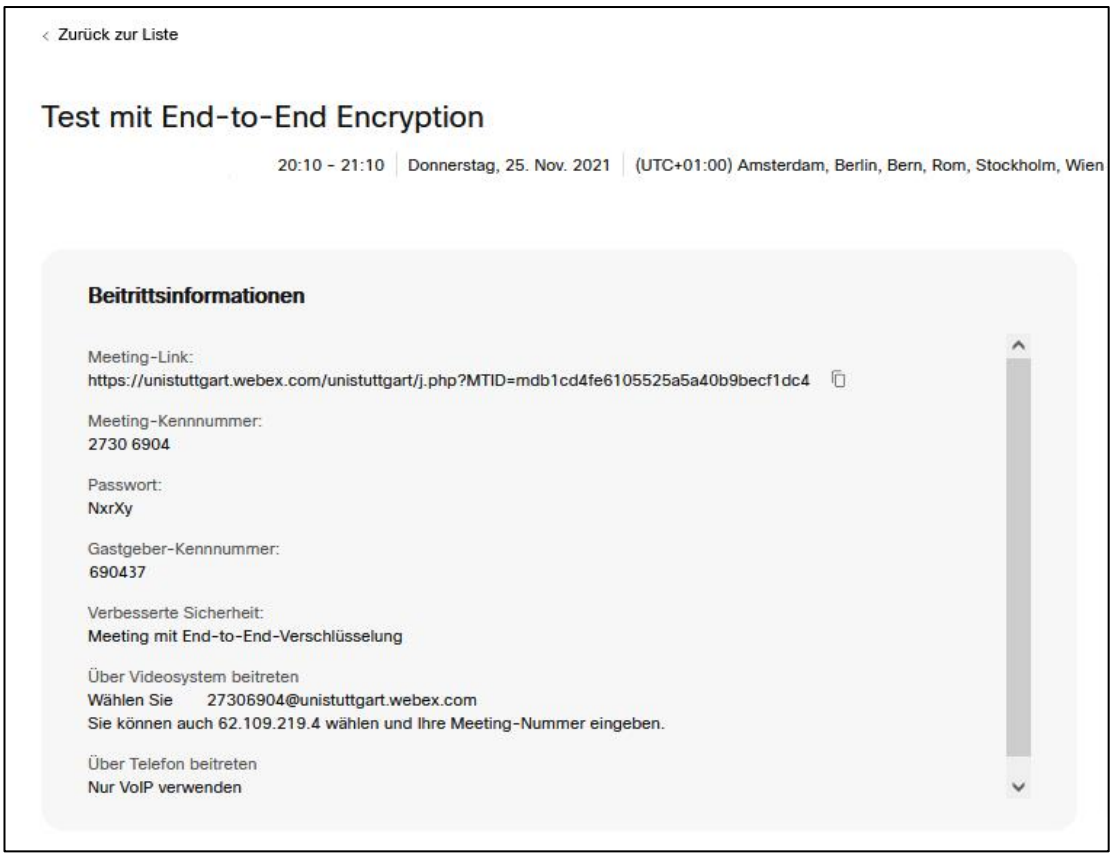
Melden sie sich auf der Webseite ***https://unistuttgart.webex.com*** an.

Klicken sie auf ***Meeting ansetzen***.

Wählen sie als Meeting-Typ die Option ***Webex Meetings Pro-End to End Encryption_VOIPonly***.

Speichern sie das konfigurierte Meeting.

Dass es sich um ein verschlüsseltes Meeting handelt, wird angezeigt, wenn sie das Meeting in der Meetingliste anklicken.



Verfügbare Meetingfunktionen und Einschränkungen bei Ende-zu-Ende-verschlüsselten Meetings

Verfügbare Funktionen

- Chat
- Umfragen
- Teilen des Desktops oder Teilen von Anwendungen und Remotesteuerung
- Dateitransfer
- lokale Aufzeichnungen
- Video
- Integriertes VOIP

Nicht verfügbare Funktionen

- Meetings in einem persönlichen Raum
- Beitreten vor dem Gastgeber
- Verschieben von Teilnehmern in die Lobby
- Videogerätfähige Meetings
- Breakouträume
- Teilnahme per Browser
- Linux-Clients
- cloudbasierte Aufzeichnungen
- Speichern von Sitzungsdaten, Abschriften und Meetingprotokollen
- Webex Assistant
- Hochladen geteilter Dateien im Meeting-Bereich am Ende von Webex Meetings
- Telefon (PSTN)-Einwahl/Rückruf: Bei aktivierter Telefoneinwahl werden Audio und Video von Teilnehmern, die sich per Telefon einwählen, nicht verschlüsselt.