Whitepaper

Sicherheit mit Webex Meetings

webex by CISCO

Inhalt

Einführung

Webex Meetings ermöglicht MitarbeiterInnen weltweit und virtuellen Teams die standortunabhängige Zusammenarbeit in Echtzeit, so als befänden sie sich im selben Raum. Unternehmen, Institutionen und Behörden auf der ganzen Welt setzen auf Webex Meetings-Lösungen. Diese Lösungen vereinfachen Geschäftsprozesse, steigern den Umsatz, optimieren Marketing- und Schulungsaktivitäten sowie das Projektmanagement und unterstützen Teams.

Sicherheit ist in Unternehmen und Behörden weltweit einer der wichtigsten Aspekte. Sie muss bei Online-Collaboration auf mehreren Ebenen gewährleistet sein – von der Terminplanung für Meetings über die Authentifizierung der TeilnehmerInnen bis hin zur Freigabe von Dokumenten.

Cisco legt bei Design, Entwicklung, Bereitstellung und Wartung seiner Netzwerke, Plattformen und Anwendungen größten Wert auf Sicherheit. Sie können Webex Meetings-Lösungen problemlos in Ihre Geschäftsprozesse einbinden, selbst bei strengsten Sicherheitsauflagen.

Die Informationen in diesem Whitepaper zu den Sicherheitsmaßnahmen von Webex Meetings und der zugrunde liegenden Infrastruktur sind eine wertvolle Hilfe bei Ihren wichtigen Investitionsentscheidungen.

Inhalte

In diesem Whitepaper werden die Sicherheitsfunktionen von Webex Meetings Suite beschrieben. Es werden die Tools und Prozesse sowie das Engineering erläutert, die Kunden die sichere Zusammenarbeit in Webex ermöglichen.

Webex Meetings umfasst Folgendes:

- Webex Meetings
- Webex Webinare[1]
- Webex Training
- Webex Support
- Webex Edge
- Webex Cloud Connected Audio
- Webex Assistant
- Slido (Umfragen)[2]

Webex Sicherheitsmodell

Cisco wird auch in Zukunft alles tun, um seiner Führungsposition im Bereich Cloud-Security gerecht zu werden. Die Security and Trust Organization von Cisco arbeitet mit Teams in unserem gesamten Unternehmen zusammen, um einen Rahmen aus Sicherheit, Vertrauen und Transparenz zu schaffen, der Design, Entwicklung und Betrieb von Kerninfrastrukturen unterstützt und die größtmögliche Sicherheit für alle unsere Aktivitäten gewährleistet.

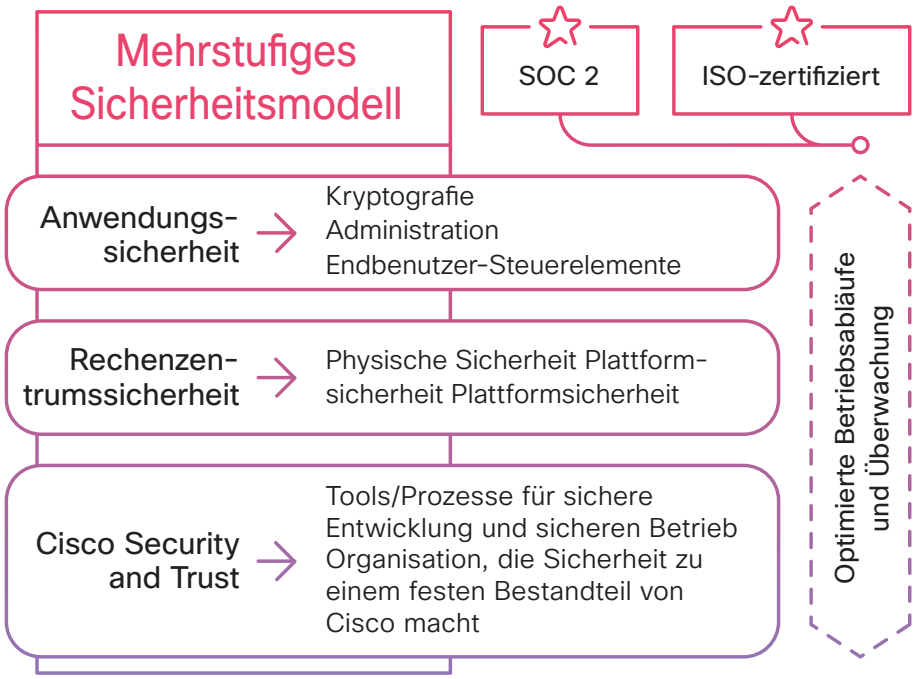
Diese Organisation stellt auch unseren Kunden die Informationen zur Verfügung, die sie zur Minimierung und Bewältigung von Cyberrisiken benötigen.

Das Webex Sicherheitsmodell (Abbildung 1) basiert auf derselben Sicherheitsgrundlage, die fest in die Prozesse von Cisco integriert ist.

Die Webex Organisation folgt konsequent den grundlegenden Prinzipien für sichere Entwicklung, Ausführung und Überwachung von Webex Services. Einige dieser Prinzipien werden in diesem Dokument näher erläutert.

[1] Ehemals Webex Events

[2] Informationen zur Sicherheit von Slido finden Sie im Security-Whitepaper zu Slido in Webex (Umfragen) unter cisco.com/content/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Slido-in-Webex-Security-Paper_1-0.pdf



„Sicherheit und Vertrauen machen Cisco zur Nummer eins der IT-Unternehmen.“

Abbildung 1: Webex Sicherheitsmodell

Cisco Security and Trust

Sicherheitstools und -prozesse von Cisco

Cisco Secure Development Lifecycle

Bei Cisco wird die Sicherheit nicht nachträglich aufgesetzt. Sie ist vielmehr von Anfang an als disziplinierter Ansatz für die Entwicklung und Bereitstellung erstklassiger Produkte und Services integriert. Alle Produktentwicklungsteams von Cisco® müssen dem Cisco Secure Development Lifecycle folgen. Dabei handelt es sich um einen wiederholbaren und messbaren Prozess, der entwickelt wurde, um die Widerstandsfähigkeit und Zuverlässigkeit von Cisco Produkten zu verbessern. Die Kombination aus Tools, Prozessen und Sensibilisierungsschulungen in allen Phasen des Entwicklungs-Lifecycles schafft fest verankerte Verteidigungsmaßnahmen. Darüber hinaus bietet sie einen ganzheitlichen Ansatz für die Widerstandsfähigkeit. Das Webex Produktentwicklungsteam folgt diesem Lifecycle gewissenhaft in sämtlichen Aspekten der Produktentwicklung.

Weitere Informationen zu Secure Development Lifecyle.

Grundlegende Sicherheitstools von Cisco

Die Cisco Security and Trust Organization gibt allen EntwicklerInnen den Prozess und die erforderlichen Tools für ein konsistentes Vorgehen bei Sicherheitsentscheidungen an die Hand.

Dedizierte Teams, die diese Tools entwickeln und bereitstellen, nehmen die Unsicherheit aus der Produktentwicklung.

Einige Beispiele für diese Tools:

- Product Security Baseline (PSB)-Anforderungen, welche die Produkte erfüllen müssen
- Threat-Builder-Tools, die bei der Bedrohungsmodellierung verwendet werden
- Codierungsrichtlinien
- Validierte oder zertifizierte Bibliotheken, die EntwicklerInnen verwenden können, anstatt eigene Sicherheitscodes schreiben zu müssen
- Tools zur Ermittlung von Schwachstellen (für statische und dynamische Analyse), mit denen nach der Entwicklung Sicherheitsmängel festgestellt werden können
- Software-Tracking zur Überwachung der Bibliotheken von Cisco und Drittanbietern mit Benachrichtigung der Produktteams, wenn eine Schwachstelle gefunden wurde

Organisation, welche die Sicherheit in den Prozessen von Cisco gewährleistet

Cisco verfügt über dedizierte Abteilungen, die Sicherheitsprozesse im gesamten Unternehmen integrieren und verwalten. Sicherheitsbedrohungen und -herausforderungen trägt Cisco Rechnung dank:

- Cisco Information Security (InfoSec) Cloud Team
- Cisco Product Security Incident Response Team (PSIRT)
- gemeinsamer Sicherheitsverantwortung

Cisco InfoSec Cloud

Unter Führung des Chief Security Officers für die Cloud ist dieses Team für die Bereitstellung einer sicheren Webex Umgebung für unsere Kunden verantwortlich. Zu diesem Zweck legt InfoSec Sicherheitsprozesse und -tools für alle Funktionen fest, die an der Bereitstellung von Webex für unsere Kunden beteiligt sind, und setzt diese durch.

Darüber hinaus arbeitet Cisco InfoSec Cloud mit anderen Teams bei Cisco zusammen, um auf alle gegen Webex gerichteten Sicherheitsbedrohungen angemessen zu reagieren.

Cisco InfoSec ist außerdem für die kontinuierliche Verbesserung des Sicherheitsstatus von Cisco Webex verantwortlich.

Cisco Product Security Incident Response Team (PSIRT)

Das Cisco PSIRT ist ein dediziertes globales Team, das sich mit dem Auftreten, der Untersuchung und der Berichterstattung von Sicherheitsproblemen für Cisco Produkte und Services befasst. Das PSIRT bedient sich zur Veröffentlichung verschiedener Medien, je nach Schweregrad des Sicherheitsproblems. Die Berichterstellung richtet sich nach den folgenden Umständen:

- Es existieren Software-Patches oder Workarounds, um die Schwachstelle zu beseitigen, oder es ist eine anschließende Veröffentlichung von Code-Fixes für schwerwiegende Schwachstellen geplant.
- Das PSIRT hat die aktive Ausnutzung einer Schwachstelle festgestellt, die zu einem erhöhten Risiko für Cisco Kunden führen könnte. Das PSIRT kann die Veröffentlichung einer Sicherheitsankündigung beschleunigen, welche die Schwachstelle in diesem Fall beschreibt, ohne dass Patches in vollem Umfang verfügbar sind.
- Die öffentliche Kenntnis einer Schwachstelle, die Produkte von Cisco betrifft, kann zu einem erhöhten Risiko für Cisco Kunden führen. Das PSIRT kann Kunden auch in diesem Fall warnen, ohne dass Patches in vollem Umfang verfügbar sind.

In jedem Fall teilt das PSIRT die Informationen mit, die BenutzerInnen mindestens benötigen, um die Auswirkungen einer Schwachstelle bewerten und die erforderlichen Schritte zum Schutz ihrer Umgebung unternehmen zu können. Das PSIRT bewertet den Schweregrad eines festgestellten Sicherheitsproblems anhand der CVSS-Skala (Common Vulnerability Scoring System). Es stellt keine Details zu Schwachstellen bereit, welche die Entwicklung eines Exploits ermöglichen könnten.

Weitere Informationen zu PSIRT finden Sie online hier.

Sicherheitsverantwortung

In der Webex Gruppe ist jeder für die Sicherheit verantwortlich, insbesondere:

- Chief Security Officer, Cloud
- Vice President and General Manager, Cisco Cloud Collaboration Applications
- Vice President, Engineering, Cisco Cloud Collaboration Applications
- Vice President, Product Management, Cisco Cloud Collaboration Applications

Interne und externe Penetrationstests

Die Webex Gruppe führt regelmäßig strenge Penetrationstests mit internen PrüferInnen durch. Zusätzlich zu seinen eigenen strikten internen Verfahren beauftragt Cisco InfoSec mehrere unabhängige Dritte mit der Durchführung strenger Audits auf der Basis der internen Richtlinien, Verfahren und Anwendungen von Cisco. Diese Audits sollen die missionskritischen Sicherheitsanforderungen sowohl für gewerbliche als auch behördliche Anwendungen überprüfen. Cisco führt mithilfe von Drittanbietern auch fortlaufende und gründliche Code-gestützte Sicherheitsprüfungen und Serviceanalysen durch. Im Rahmen dieser Prüfungen führt der Drittanbieter folgende Sicherheitsbewertungen durch:

- Ermittlung kritischer Anwendungs- und Servicelücken sowie Unterbreitung entsprechender Lösungen
- Aufzeigen allgemeiner Bereiche zur Verbesserung der Architektur
- Ermittlung von Kodierungsfehlern und Leitlinien zur Verbesserung

Die externen Prüfer arbeiten direkt mit den Webex Engineering-MitarbeiterInnen zusammen, um die Ergebnisse zu erläutern und die Problembehebung zu validieren. Bei Bedarf kann Cisco InfoSec eine Bescheinigung von diesen Anbietern zur Verfügung stellen.

Webex Rechenzentrumssicherheit

Webex ist eine Software-as-a-Service (SaaS)-Lösung, deren Bereitstellung über die Webex Cloud erfolgt, eine hochsichere Plattform mit branchenführender Leistung, Integration, Flexibilität, Skalierbarkeit und Verfügbarkeit. Die Webex Cloud ist eine Kommunikationsinfrastruktur, die speziell für die Echtzeitkommunikation über das Internet entwickelt wurde.

Die Switching-Geräte, die bei Webex Meetings zum Einsatz kommen, befinden sich in verschiedenen Rechenzentren auf der ganzen Welt. Für die meisten Webex Cloud-Services werden Cisco Rechenzentren genutzt. SOC2- und ISO-konforme Amazon Web Services (AWS)- und Microsoft Azure-Rechenzentren werden ebenfalls genutzt, um zusätzliche Services in Private-Cloud-Instanzen bereitzustellen. Diese Rechenzentren wurden strategisch in der Nähe wichtiger Internet-Zugriffspunkte platziert und nutzen spezielle Glasfaserleitungen für hohe Bandbreite, um den Traffic um die Welt zu leiten.

Zusätzlich betreibt Cisco vier Netzwerk-PoPs (Points-of-Presence). Sie vereinfachen Backbone-Verbindungen, Internet-Peering, globale Standort-Backups sowie den Einsatz von Caching-Technologien, um die Leistung und Verfügbarkeit für die EndnutzerInnen zu optimieren.

Physische Sicherheit

Die physische Sicherheit des Rechenzentrums wird durch die Videoüberwachung von Einrichtungen und Gebäuden sowie eine Zwei-Faktor-Identifizierung für den Einlass gewährleistet. Innerhalb der Cisco Rechenzentren wird der Zutritt durch eine Kombination aus Badge-Readern und biometrischen Kontrollen gesteuert. Darüber hinaus stellen Umgebungskontrollen (z. B. Temperatursensoren und Brandschutzsysteme) sowie eine Infrastruktur für Service Continuity (z. B. PowerBackup) den unterbrechungsfreien Betrieb der Systeme sicher.

Die Server im Rechenzentrum sind je nach Empfindlichkeit der Infrastruktur in „Vertrauenszonen“ unterteilt. So sind beispielsweise Datenbanken „eingesperrt“: Die Netzwerkinfrastruktur befindet sich in speziellen Räumen und alle Geräte-Racks sind verschlossen. Nur Cisco Sicherheitspersonal und autorisierte BesucherInnen, die von Cisco MitarbeiterInnen begleitet werden, können die Rechenzentren betreten.

Das Produktionsnetzwerk von Cisco ist hochgradig vertrauenswürdig: Nur sehr wenige Personen mit hoher Vertrauensstufe haben Zugriff auf das Netzwerk.

Infrastruktur- und Plattformsicherheit

Die Plattformsicherheit umfasst die Sicherheit des Netzwerks, der Systeme und des gesamten Webex Rechenzentrums. Alle Systeme werden vor der Bereitstellung in der Produktionsumgebung einer gründliche Sicherheitsprüfung und Abnahmevalidierung unterzogen. Außerdem werden fortlaufend Absicherungsmaßnahmen und Sicherheitspatchings sowie Scans nach Schwachstellen mit Bewertung durchgeführt.

Die Server werden mithilfe der Security Technical Implementation Guidelines (STIGs) abgesichert, die vom National Institute of Standards and Technology (NIST) veröffentlicht werden. Firewalls schützen den Netzwerkperimeter. Zugriffskontrolllisten (Access Control Lists, ACLs) trennen die verschiedenen Sicherheitszonen. Es sind Intrusion Detection Systems (IDSs) eingerichtet und die Aktivitäten werden kontinuierlich protokolliert und überwacht. Täglich werden interne und externe Sicherheitsscans für Webex durchgeführt. Alle Systeme werden im Rahmen der regelmäßigen Wartung abgesichert und gepatcht. Darüber hinaus finden ständig Schwachstellenscans und -bewertungen statt.

Service Continuity und Disaster Recovery sind wichtige Komponenten der Sicherheitsplanung. Die globalen Standort-Backups und das Hochverfügbarkeitsdesign der Cisco Rechenzentren ermöglichen das geografische Failover von Webex Services. Es gibt keinen Single-Point-of-Failure.

Webex Sicherheit

Kryptografie

Verschlüsselung von Daten während der Übertragung

Die gesamte Kommunikation zwischen in der Cloud registrierten Webex Apps, Webex Geräten und den Webex Services erfolgt über verschlüsselte Kanäle. Webex verwendet das TLS-Protokoll in der Version 1.2 oder höher mit hochsicheren Verschlüsselungssuiten für die Signalisierung.

Nachdem eine Sitzung über TLS eingerichtet wurde, werden alle Medienstreams (Audio-VoIP, Video, Bildschirmfreigabe und Dokumentenfreigabe) verschlüsselt[3].

Verschlüsselte Medien können über UDP, TCP oder TLS transportiert werden. Als Transportprotokoll für Webex Sprach- oder Video-Medienstreams bevorzugt und empfiehlt Cisco dringend UDP. Der Grund dafür ist, dass TCP und TLS verbindungsorientierte Transportprotokolle sind, die darauf ausgelegt sind, korrekt geordnete Daten zuverlässig an Protokolle der oberen Schicht zu übermitteln. Bei der Verwendung von TCP oder TLS sendet der Sender verlorene Pakete erneut, bis sie bestätigt werden, und der Empfänger puffert den Paketstrom, bis die verlorenen Pakete wiederhergestellt sind. Bei Medienstreams über TCP oder TLS macht sich dieses Verhalten durch erhöhte Latenz/Jitter bemerkbar, was sich wiederum auf die Medienqualität der AnrufteilnehmerInnen auswirkt.

Die Medienpakete werden entweder mit AES 256 oder AES 128 verschlüsselt. Die Webex App und die Webex Room Geräte verwenden AES-256-GCM zur Verschlüsselung von Medien. Diese Medienverschlüsselungsschlüssel werden über TLS-gesicherte Signalisierungskanäle ausgetauscht. SIP- und H323-Geräte, die Medienverschlüsselung mit SRTP unterstützen, können AES-256-GCM, AES-128-GCM oder AES-CM-128-HMAC-SHA1 verwenden (AES-256-GCM ist der von Webex bevorzugte Medienverschlüsselungscode).

Auf Zero-Trust-Security basierte End-to-End-Verschlüsselung für Webex Meetings

Bei Standard-Meetings, bei denen Geräte und Services SRTP zur Verschlüsselung der Medien auf Hop-by-Hop-Basis verwenden, benötigen Webex Medienserver Zugriff auf die Medienverschlüsselungsschlüssel, um die Medien für jeden SRTP-Anrufabschnitt zu entschlüsseln. Dies gilt für jeden Konferenzanbieter, der SIP, H323, PSTN, Aufzeichnung und andere Services mit SRTP unterstützt.

[3] Für SIP- und H323-basierte Endpunkte, die eine Verbindung zu einem Webex Meeting herstellen, empfiehlt Cisco dringend, alle Medien- und Signalisierungsströme vom Endpunkt, Expressway/SBC am Rand des Unternehmensnetzwerks zu verschlüsseln, sodass kein unverschlüsselter Traffic das Internet passiert.

Für Unternehmen, die ein höheres Sicherheitsniveau benötigen, bietet Cisco Webex jedoch auch End-to-End-Verschlüsselung für Meetings. Bei dieser Option hat die Webex Cloud keinen Zugriff auf die von den Meeting-TeilnehmerInnen verwendeten Verschlüsselungsschlüssel und kann deren Medienstreams nicht entschlüsseln. Auf Zero-Trust-Security basierte End-to-End-Verschlüsselung für Webex verwendet standardkonforme Protokolle, um einen gemeinsamen Meeting-Verschlüsselungsschlüssel (Messaging Layer Security [MLS]) zu generieren, der zur Verschlüsselung von Meeting-Inhalten (Secure Frame [S-Frame]) verwendet wird. Bei MLS wird der Verschlüsselungsschlüssel für das Meeting von der Webex App/dem Webex Gerät aller TeilnehmerInnen generiert. Dabei wird eine Kombination aus dem gemeinsamen öffentlichen Schlüssel aller TeilnehmerInnen und dem privaten Schlüssel der TeilnehmerInnen (der niemals gemeinsam genutzt wird) verwendet. Der Verschlüsselungsschlüssel für Meetings wird nie in der Cloud übertragen und wird bei Eintritt und Verlassen des Meetings ausgetauscht. Weitere Informationen zu auf Zero-Trust-Security basierte End-to-End-Verschlüsselung finden Sie im Whitepaper zu Zero-Trust-Security für Webex.

Bei End-to-End-Verschlüsselung werden alle von der Webex App und den Webex Geräten erzeugten Meeting-Daten (Sprache, Video, Chat usw.) mit dem lokal abgeleiteten Meeting-Verschlüsselungsschlüssel verschlüsselt, und diese Daten können vom Webex Service nicht entschlüsselt werden.

Für Webex Meetings sind verschlüsselte End-to-End-Meetings verfügbar. Wenn End-to-End-Verschlüsselung aktiviert ist, werden Webex Services und Endpunkte, die zum Entschlüsseln von Inhalten Zugriff auf Sitzungsschlüssel benötigen (z. B. Geräte, die SRTP verwenden, bei denen die Verschlüsselung Hop-by-Hop erfolgt), nicht unterstützt. Dadurch können nur Personen an einem Meeting teilnehmen, welche die Webex App oder in der Cloud registrierte Webex Geräte verwenden. Ebenso sind Services wie netzwerkbasierte Aufzeichnung, Spracherkennung usw. ausgeschlossen.

Nähere Informationen zu unterstützten und nicht unterstützten Features finden Sie unter End-to-End-Verschlüsselung mit Identitätsprüfung für Webex Meetings.

Private Webex Meetings

Wenn Ihr Unternehmen über Video Mesh in seinem Netzwerk verfügt, können AdministratorInnen mit Unterstützung der Kundenbetreuung private Meetings aktivieren. Mit dieser Funktion wird die Verbindung zu den Medien in Ihren Räumlichkeiten getrennt, was die Sicherheit Ihres Meetings erhöht. Wenn Sie ein privates Meeting planen, werden die Medien immer auf den Videonetzknoten innerhalb Ihres Unternehmensnetzwerks beendet, ohne dass eine Cloud-Kaskade entsteht.

Weitere Informationen zu privaten Webex Meetings und Hinweise zum Entwurf für Webex Edge Video Mesh finden Sie hier.

Verschlüsselte Webex Signalisierung

Webex Services unterstützen TLS Version 1.2 und höher. Die TLS Version 1.2-Verschlüsselungssuiten sind unten in der Reihenfolge aufgeführt, in der sie für die sichere Kommunikation verwendet werden sollten. Webex Services wählen das stärkste Verschlüsselungsverfahren aus, das für die Umgebung des Kunden geeignet ist.

In Tabelle 1 sind die typischen Verschlüsselungssuiten und die Bit-Länge der Verschlüsselungssuite aufgeführt.

Tabelle 1: Verschlüsselungssuiten und Bit-Länge

VERSCHLÜSSELUNGSSUITEN	BIT-LÄNGE
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128

Schutz von Meeting-Inhalten, die in der Webex Cloud gespeichert sind

Der Webex Service ermöglicht Ihnen die sichere Speicherung von Meeting-Aufzeichnungen und -Protokollen in der Webex Cloud. Diese Dateien werden einzeln verschlüsselt und in Ihrer Region gespeichert.

Meeting-Aufzeichnungen und -Protokolle werden mit dem Verschlüsselungsverfahren AES-256-GCM verschlüsselt. Diese Dateien werden auf ähnliche Weise geschützt wie die in Webex Spaces freigegebenen Dateien und Nachrichten.

- Für jedes Webex Meeting wird ein Meeting-Container (ähnlich wie ein Webex Space) mit einem eindeutigen AES-256-GCM-Verschlüsselungsschlüssel erstellt.
- Wenn eine Meeting-Aufzeichnung verschlüsselt und in der Webex Cloud gespeichert wird, wird dem Meeting-Container eine Nachricht mit dem zur Verschlüsselung der Datei verwendeten Schlüssel und einer URL für den Speicherort der verschlüsselten Datei hinzugefügt. Diese Nachricht wird mit dem Verschlüsselungscode des Meeting-Containers verschlüsselt.

- BenutzerInnen mit Zugriffsberechtigung auf den Meeting-Container können Aufzeichnungen und Protokolle abrufen, indem sie die verschlüsselte Nachricht mit dem Speicherort der Datei und dem Dateiverschlüsselungsschlüssel abrufen und diese Nachricht dann mit dem Verschlüsselungsschlüssel des Meeting-Containers entschlüsseln.

Meeting-Container verwenden dasselbe Schlüsselmanagementsystem (KMS) wie Webex Messaging, sodass Unternehmen, die den Webex Meetings Service nutzen, Services für hybride Datensicherheit (On-Premises-KMS) und Bring Your Own Key (BYOK) einsetzen können, um die sichere Speicherung und den Schutz von Verschlüsselungsschlüsseln zu verbessern.

Speicherung, Bereitstellung und Löschung von Meeting-Aufzeichnungen und -Protokollen

AdministratorInnen können im Control Hub eine Aufbewahrungsfrist für gespeicherte Meeting-Inhalte festlegen. Sobald die Aufbewahrungsfrist erreicht ist, werden die gespeicherten Inhalte aus der Webex Cloud gelöscht. Aufzeichnungen können auch über die Webex Recordings API aufgelistet, exportiert und gelöscht werden. Weitere Informationen.

In der Webex Cloud gespeicherte Aufzeichnungen und Protokolle können:

- kennwortgeschützt werden (Kennwörter werden mit SHA-2 [One-Way-Hashing-Algorithmus] und Salts gespeichert)
- auf angemeldete BenutzerInnen beschränkt werden
- vor dem Herunterladen geschützt werden
- von InhaltseigentümerInnen über die Webex Seite/Webex App verwaltet werden

Die AdministratorInnen können BenutzerInnen auch erlauben, Besprechungen auf ihren Computern aufzuzeichnen.

Webex Meetings – Lobby-Kontrollen und Identitätsprüfung

Über die Webex Meeting-Lobby können GastgeberInnen (und Co-GastgeberInnen) von Meetings BenutzerInnen überprüfen und verwalten, bevor sie als TeilnehmerInnen zu einem Meeting zugelassen werden. BenutzerInnen in der Meeting-Lobby werden in drei Kategorien gruppiert und verwaltet (Abbildung 2):

1. Angemeldete (authentifizierte) BenutzerInnen in Ihrem Unternehmen
2. Angemeldete (authentifizierte) BenutzerInnen außerhalb Ihres Unternehmens
3. Nicht geprüfte BenutzerInnen: nicht authentifizierte GastbenutzerInnen, deren Identität nicht überprüft wurde

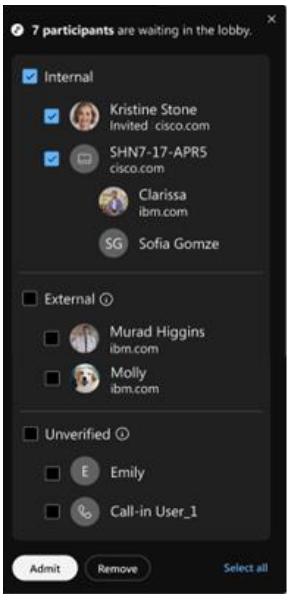


Abbildung 2: Webex Meeting-Lobby

Während eines Meetings werden den Meeting-GastgeberInnen (und Co-GastgeberInnen), die Webex Apps oder Webex Geräte verwenden, Nachrichten angezeigt, die sie über neue BenutzerInnen in der Lobby informieren, sowie Steuerelemente, mit denen sie diese BenutzerInnen zum Meeting zulassen oder aus dem Meeting/der Lobby entfernen können (Abbildung 3).

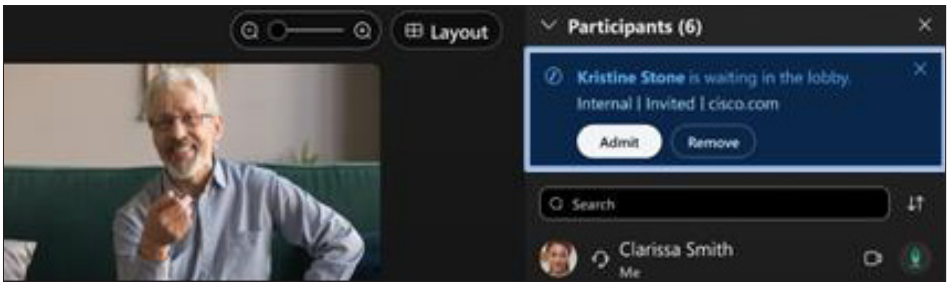


Abbildung 3: Lobby-Benachrichtigung

Rollenbasierter Webex Zugriff

Das Verhalten von Webex Anwendungen ist auf fünf Rollen ausgelegt, von denen jede unterschiedliche Privilegien erhält. Diese Rollen werden nachstehend näher beschrieben.

GastgeberIn

GastgeberInnen setzen Webex Meetings an und starten sie. Sie kontrollieren das Meeting-Erlebnis für alle TeilnehmerInnen und treffen relevante Entscheidungen bei der Planung sowie während des Meetings.

Site-AdministratorInnen (diese Rolle wird später näher beschrieben) können viele dieser Kontrollen vorgeben. Wenn sie nicht vorgegeben sind, können GastgeberInnen über den Schutz von Meetings entscheiden.

Co-GastgeberInnen (nur in Webex Meetings und Webex Webinars)

Bei der Planung oder während eines Meetings können GastgeberInnen Co-GastgeberInnen zuweisen, die mit ähnlichen Rechten wie die GastgeberInnen ausgestattet sind. Co-GastgeberInnen können dazu beitragen, die Produktivität von Meetings zu verbessern. Wenn sich GastgeberInnen verspäten oder nicht teilnehmen können, können Co-GastgeberInnen das Meeting beginnen und leiten. Co-GastgeberInnen können GastgeberInnen auch bei der Leitung des Meetings unterstützen, was bei größeren Meetings nützlich ist.

ModeratorIn

ModeratorInnen können Präsentationen, bestimmte Anwendungen oder den gesamten Desktop freigeben. Sie steuern die Kommentar-Tools. Was die Sicherheit betrifft, können ModeratorInnen anderen TeilnehmerInnen die Remote-Kontrolle freigegebener Anwendungen und Desktops ermöglichen bzw. ihnen diese Berechtigung entziehen.

DiskussionsteilnehmerInnen (nur in Webex Training und Webex Webinars)

DiskussionsteilnehmerInnen sollen in erster Linie GastgeberInnen und ModeratorInnen bei der reibungslosen Durchführung der Veranstaltung unterstützen. DiskussionsteilnehmerInnen können bei der Planung zugewiesen oder von GastgeberInnen aus der Teilnehmerliste während des Events ausgewählt werden. GastgeberInnen können die DiskussionsteilnehmerInnen bitten, als FachexpertInnen zu fungieren und Teilnehmerfragen in einer Frage- und Antwortrunde anzuzeigen und zu beantworten. Sie können auf öffentliche und private Chat-Nachrichten antworten, freigegebene Inhalte kommentieren oder als UmfragekoordinatorInnen die in Webex integrierten Umfragen verwalten.

TeilnehmerIn

TeilnehmerInnen haben keine Sicherheitsaufgaben oder Privilegien, es sei denn, sie werden ModeratorInnen oder GastgeberInnen.

Site-AdministratorInnen und GastgeberInnen können TeilnehmerInnen erlauben, jederzeit im Verlauf des Meetings über das Webex Ballsymbol die Moderationsrolle zu übernehmen. Diese Einstellung ist standardmäßig deaktiviert.

DolmetscherIn (nur in Webex Meetings und Webex Webinars)

DolmetscherInnen haben die Aufgabe, die Aussagen der SprecherInnen in eine andere Sprache zu übersetzen, die von GastgeberInnen in einem separaten Audiokanal für die Simultandolmetschfunktionen zugewiesen wird. GastgeberInnen können DolmetscherInnen bei der Planung oder innerhalb von Meetings zuweisen.

Site-AdministratorIn

Diese Rolle ist für die Verwaltung von Konten sowie für die Verwaltung und Durchsetzung von Richtlinien auf Seiten- oder Benutzerbasis autorisiert. AdministratorInnen können die Webex Funktionen auswählen, die allen anderen Rollen und BenutzerInnen zur Verfügung stehen.

Einmalige Anmeldung (Single Sign-On)

Webex unterstützt die Benutzerauthentifizierung über einen Identitätsanbieter (IdP) mit Single Sign-On (SSO) auf der Grundlage des SAML 2.0-Protokolls (Security Assertion Markup Language). Mit SSO können BenutzerInnen einen einzigen, gemeinsamen Satz von Anmeldeinformationen für die Webex App und andere Anwendungen in Ihrem Unternehmen verwenden. Die Webex App verwendet den Webex Service zur Kommunikation mit dem Webex Identity Service. Der Webex Identity Service erstellt eine Vereinbarung mit dem IdP, sodass sich die Webex App beim IdP authentifizieren kann. Beispiele für IdPs sind Microsoft Active Directory Federation Services, PingFederate, CA SiteMinder Single Sign-On, OpenAM und Oracle Access Manager.

Zur Aktivierung von SSO muss ein Zertifikat für Ihre Organisation generiert werden. Dabei kann es sich um ein selbst signiertes Zertifikat handeln, das von Webex signiert wurde, oder um ein von einer öffentlichen Zertifizierungsstelle (CA) signiertes Zertifikat. Dann müssen Metadaten zwischen dem IdP und Webex ausgetauscht werden.

Wenn sich BenutzerInnen über die Webex App authentifizieren, wird eine Anfrage vom Webex Identity Service über die Webex App an den IdP gesendet und eine SAML-Assertion wird vom IdP über die Webex App an den Webex Identity Service zurückgegeben.

Durch die Implementierung von Single Sign-On für Webex erhalten Sie die volle Kontrolle über die Benutzer- und Zugangsverwaltung, um Ihre Unternehmensrichtlinien einzuhalten. Zu den Vorteilen der Verwendung von SSO mit Ihrem IdP zählen folgende:

- Der IdP validiert die Benutzeranmeldeinformationen (Zertifikat, Fingerabdruck oder eine andere Identifizierungsart).
- Webex speichert keine Benutzeranmeldeinformationen.
- Kunden steuern, wer auf den Webex Service zugreift

Weitere Informationen dazu finden Sie in diesem Webex Hilfeartikel zur Integration von Single Sign-On in Control Hub.

BenutzerInnen, die sich im Verzeichnis befinden, kann Webex mithilfe von Directory Connector mit Active Directory oder der System for Cross-Domain Identity Management (SCIM) API mit Azure AD oder Okta aus einem unterstützten Verzeichnis mit Webex Identity synchronisieren. Dadurch wird sichergestellt, dass BenutzerInnen immer zwischen dem Verzeichnis und der Webex Organisation synchronisiert sind. Immer wenn BenutzerInnen im Verzeichnis erstellt, aktualisiert oder entfernt werden, werden die Änderungen synchronisiert und im Control Hub angezeigt.

Ausführliche Informationen zur Benutzersynchronisierung zwischen Active Directory und Webex mit Cisco Directory Connector finden Sie im Bereitstellungsleitfaden für Cisco Directory Connector.

Ausführliche Informationen zur Benutzersynchronisierung zwischen Azure AD und Webex unter Verwendung der SCIM-API finden Sie im Hilfeartikel Synchronisieren von Azure Active Directory-Benutzern in Control Hub.

Ausführliche Informationen zur Benutzersynchronisierung zwischen Okta und Webex unter Verwendung der SCIM-API finden Sie im Hilfeartikel Okta-Benutzer in Cisco Webex Control Hub synchronisieren.

Meeting-Einstellungen

Dank granularer Einstellungen für Webex Meetings kann das Verhalten von BenutzerInnen und Systemen vor, während und nach Meetings gesteuert werden. Üblicherweise können diese Einstellungen auf Standortebene vorgenommen werden, damit sich Meetings unterschiedlich verhalten und auf die erforderlichen Anwendungsfälle für alle BenutzerInnen abgestimmt werden können. Webex AdministratorInnen sollten sicherstellen, dass alle Meetings sicher und nur für die vorgesehenen BenutzerInnen und Geräte zugänglich sind. Außerdem sollten die AdministratorInnen Sicherheitsrichtlinien durchsetzen und nur autorisierten BenutzerInnen den Zugriff auf Meeting-Inhalte erlauben. Best Practices für AdministratorInnen rund um Meeting-Sicherheit finden Sie in den Hilfeartikeln Bewährte Webex-Methoden für sichere Meetings: Site-Administration und Bewährte Webex-Methoden für sichere Meetings: Control Hub.

GastgeberInnen eines Meetings haben die vollständige Kontrolle über die Einrichtung des Meetings und sollten sicherstellen, dass nur die vorgesehenen TeilnehmerInnen teilnehmen können. Außerdem sollten GastgeberInnen die Sicherheitsrichtlinien des Unternehmens für die Planung der Meetings beachten. Wie Sie die Sicherheit von Webex Meetings als GastgeberIn gewährleisten können, erfahren Sie im Hilfeartikel Bewährte Webex-Methoden für sichere Meetings: Gastgeber.

Je nach ihren Sicherheitsrichtlinien können einige Unternehmen ihren BenutzerInnen die Teilnahme an externen Meetings ganz untersagen oder nur die Teilnahme an Meetings auf einer Liste genehmigter externer Websites erlauben. Darüber hinaus kann ein Unternehmen die Nutzung bestimmter Meeting-Funktionen wie Chats, Dateiübertragungen, Anmerkungen, Fragen und Antworten sowie Umfragen einschränken, wenn sie an einem externen Meeting teilnehmen. Diese Funktionen können mit den Zusammenarbeitsbeschränkungen von Webex bereitgestellt werden. Weitere Informationen finden Sie im Hilfeartikel Zusammenarbeitsbeschränkungen für Webex Meetings in Control Hub.

Zusätzliche Webex Funktionen und Sicherheitsmaßnahmen

Die BenutzerInnen können flexibel verschiedene Clients und Geräte verwenden, um einem Webex Meeting beizutreten oder es zu starten. Bei Verwendung eines Videogeräts zur Teilnahme an einem Meeting oder zum Starten eines Meetings können Meeting-TeilnehmerInnen ein Webex Gerät (Cisco Unified CM-registrierte [SIP] oder Webex Cloud-registrierte Geräte [HTTP]) oder ein standardbasiertes (SIP oder H.323) Videogerät oder eine Anwendung eines Drittanbieters verwenden. Dazu wählen Sie die Videoadresse des Meetings. Bei Verwendung eines bei Unified CM registrierten Geräts, das über Expressway eine Verbindung zu Webex herstellt, kann die SIP-Signalisierung zwischen Expressway-E und Webex unverschlüsselt (TCP) oder verschlüsselt (TLS oder MTLS) erfolgen. Die verschlüsselte SIP-Signalisierung mit MTLS wird bevorzugt, da die zwischen der Webex Cloud und Expressway-E ausgetauschten Zertifikate vor dem Verbindungsaufbau validiert werden können. Bei SIP/TLS wird der Webex Cloud-Medienstream mit SRTP verschlüsselt.

Mit Webex Geräten können BenutzerInnen der Webex App auch unsere Proximity-Funktion nutzen, um sich mit einem Webex Raumgerät zu verbinden und einem Meeting beizutreten. Weitere Informationen finden Sie hier.

Darüber hinaus kann eine Seite so konfiguriert werden, dass für die Teilnahme an Meetings mit einem Videogerät ein numerischer Passcode (Audio-PIN) erforderlich ist.

BenutzerInnen können auch von einem Webex Gerät aus an einem Microsoft Teams-Meeting teilnehmen. VIMT (Webex Video Integration with Microsoft Teams) ermöglicht die Teilnahme an Microsoft Teams-Meetings von Cisco und SIP-fähigen Videogeräten aus, die entweder in der Cloud oder On-Premises registriert sind. Diese Integration ermöglicht ein funktionsreiches, nahtloses Meeting-Erlebnis, ohne dass die Zusammenarbeit mit Drittanbietern erforderlich ist. Der Medienpfad für Videointegrationsanrufe wird von speziellen Medienclustern in der Webex Cloud abgewickelt. Weitere Informationen zu VIMT (Webex Video Integration with Microsoft Teams) finden Sie in diesem Artikel.

Die andere Videoendpunkt-Integration erfolgt mit Webex Web-Engine-fähigen Geräten, die an B2B-Meetings von Microsoft teilnehmen können. Diese Integration kann z. B. verwendet werden, wenn ein externes Unternehmen kein VIMT hat. Bei dieser Integration werden die Signalisierung und die Medien über WebRTC-Streams gesendet.

Ebenso können BenutzerInnen auch von einem Webex Gerät aus an einem Google Meet-Meeting teilnehmen. Die Webex Integration mit Google Meet ermöglicht es, an Google Meet-Anrufen von Webex Geräten aus teilzunehmen, wobei Medien und Signalisierung direkt von der Google-Cloud zum Webex Gerät gesendet werden und die WebRTC-Technologie genutzt wird. Umgekehrt können Google Meet-Geräte unter Verwendung der vertrauten Google Meet-Benutzeroberfläche, der Anruffunktionen und der Webex Meeting-Erfahrung an Webex Meetings teilnehmen.

Audiotarife für Webex Meetings

Bei Webex gibt es integrierte Calling-Tarife von standortbasierten Systemen aus, welche die bestehenden Calling-Lösungen der Kunden nutzen, bis hin zu zugelassenen Cloud Connected Calling Providern (CCPP) sowie Cloud Connected Audio Service Provider (CCA-SP), BYoPSTN und Cisco PSTN.

Cisco PSTN bietet TeilnehmerInnen in Webex Meetings, Webex Webinars und Webex Trainings die weltweit umfangreichsten Einwahl- und Anrufservices über PSTN (Public Switched Telephone Network). Die mit Webex Produkten verfügbaren Audio-Optionen ermöglichen eine umfassende Integration und fördern so effiziente Gespräche unter den TeilnehmerInnen. Als Cloud-basierte PSTN-Audio-Option bietet Webex Meetings Audio eine breite Abdeckung mit gebührenpflichtiger Einwahl, gebührenfreier Einwahl und Anruffunktionen für lokale und globale Verbindungen. Sie lässt sich auf einer Vielzahl von Geräten einsetzen, darunter Mobiltelefone, IP-Telefone und Softphones, und ermöglicht die Zusammenarbeit von TelefonteilnehmerInnen sowie von TeilnehmerInnen und Geräten, die VoIP (Voice over IP) verwenden, in derselben Sitzung. Cisco PSTN ist überall dort verfügbar, wo es Webex gibt.

Webex CCP (Cloud Connected PSTN) ist ein Cloud-Service, der über Webex bereitgestellte Anruffunktionen in Unternehmensqualität bietet. Diese Plattform ist Teil der umfassenden Webex Suite, die für Anrufe, Messaging, Meetings und Contact Center-Workloads eingesetzt wird, die das Marktsegment mit über 100 BenutzerInnen benötigt. Webex unterstützt das „Bring Your Own Carrier“-Modell, bei dem Kunden durch Einsatz eines lokalen Gateways einen Anbieter ihrer Wahl für PSTN-Services nutzen können. Mit CCP können Kunden einen autorisierten CCP-Anbieter für ihren PSTN-Zugang nutzen. Cisco arbeitet mit autorisierten PSTN-Anbietern zusammen, um Webex Kunden ein kostengünstiges und zuverlässiges PSTN in der Cloud zu ermöglichen, ohne dass ein Gateway vor Ort benötigt wird. Cloud Connected PSTN-Anbieter haben eine Reihe von All-inclusive-Servicepaketen erstellt, um Ihre Webex BenutzerInnen mit höchster Qualität und Sicherheit mit der Welt zu verbinden. Cloud Connected PSTN bietet Sicherheit über SIP-Digest-Authentifizierung und TLS/SRTP für den Einstiegspunkt des lokalen Gateways (beim Kunden) zwischen dem Kunden-SBC und dem Webex Edge, wenn ein lokales Kunden-Gateway eingesetzt wird. Für Kunden, die nur die Cloud Calling-Komponenten von Webex Cloud Connected PSTN verwenden, ist die Sicherheit zwischen der Webex App und Geräten direkt mit der Webex Cloud gewährleistet, wie im Abschnitt „Webex Sicherheit“ beschrieben.

Webex for Broadworks-Kunden haben eine zusätzliche Option, die als BYoPSTN bezeichnet wird. Die Bring Your Own PSTN (BYoPSTN)-Lösung ermöglicht es Webex for BroadWorks-Service-Providern, eigene Telefonnummern zur Verfügung zu stellen, welche die BenutzerInnen für die Teilnahme an Webex Meetings verwenden können. Die Lösung ermöglicht es Partnern, ihre eigenen PSTN-Netzwerke zu nutzen und auf bestehende Beziehungen zu PSTN-Anbietern zurückzugreifen, anstatt die von Cisco bereitgestellten Nummern zu verwenden.

Die Referenzarchitektur bietet einen End-to-End-Entwurf für die BYoPSTN-Option. Diese Architektur wurde von Cisco überprüft und verwendet Cisco Unified Border Element (CUBE) als Session Border Controller (SBC) für den Anruf-Traffic zwischen BroadWorks und Webex Meetings. Weitere Informationen finden Sie im Leitfaden zur BYoPSTN-Lösung.

Anrufe, die innerhalb der Partnerinfrastruktur von BroadWorks zu CUBE weitergeleitet werden, verwenden SIP TCP für die Anrufsignalisierung und RTP für Medien. Von CUBE zu Webex verwenden die Anrufe SIP MTLS für die Signalisierung und SRTP für Medien. Die Anrufweiterleitung von CUEB zu Webex erfolgt über das Internet und es wird kein SIP Trunk verwendet. BYoPSTN nutzt die Webex Edge Audio-Architektur, die eine Authentifizierung für SBC und die Verschlüsselung aller Audiomedien beinhaltet, die über SRTP übertragen werden.

Cloud Connected Audio (CCA)-Konnektivität wird über private Punkt-zu-Punkt-Verbindungen zu Webex hergestellt. CCA-Verbindungen werden zu bestimmten Kunden-Ports geleitet. Zugriffskontrolllisten auf Edge-Routern und Firewalls in den Rechenzentren von Kunden und Cisco schützen die Verbindungen. Der CCA-Service hat IP-Subnetze segmentiert. Nur das Cisco Unified Border Element (CUBE)-IP-Segment wird den Kunden präsentiert. Kein Kunde hat Einblick in das IP-Segment oder das CUBE eines anderen Kunden.

Webex CCA bietet ein hohes Maß an Sicherheit, ohne unnötigen Overhead für den Traffic zu verursachen oder das Design zu belasten. Weitere Informationen finden Sie auf Webex CCA.

Datenschutz bei Webex

Webex nimmt den Schutz der Kundendaten ernst. Wir erfassen, verwenden und verarbeiten Kundendaten nur in Übereinstimmung mit der Cisco Datenschutzerklärung und dem Cisco Datenblatt zum Datenschutz für Webex Meetings.

Bei der Erstellung des Services stand Datenschutz von vornherein im Mittelpunkt, und er ist so konzipiert, dass er in Übereinstimmung mit den globalen Datenschutzanforderungen verwendet werden kann. Dazu zählen die Datenschutz-Grundverordnung der Europäischen Union (DSGVO), der California Consumer Privacy Act (CCPA), der Personal Information Protection and Electronic Documents Act (PIPEDA) von Kanada, der Personal Health Information Protection Act (PHIPA), der Health Insurance Portability and Accountability Act (HIPAA) und der Family Educational Rights and Privacy Act (FERPA).

Administrative Daten

Informationen über MitarbeiterInnen oder VertreterInnen von Kunden oder anderer Dritter, die von Cisco erfasst und verwendet werden, um die Bereitstellung von Produkten oder Services durch Cisco sowie die Konten von Kunden oder Dritten für die Geschäftszwecke von Cisco zu verwalten.

Administrative Daten können Name, Adresse, Telefonnummer und E-Mail-Adresse sowie Informationen zu den Vertragsbeziehungen zwischen Cisco und einem Drittanbieter umfassen. Dabei ist es unerheblich, ob sie zum Zeitpunkt der ursprünglichen Registrierung oder später in Verbindung mit der Verwaltung von Produkten oder Services von Cisco erfasst werden.

Zu administrativen Daten zählen auch Meeting-Titel, Uhrzeit und andere Attribute der Meetings, die auf Webex von MitarbeiterInnen oder VertreterInnen eines Kunden durchgeführt werden. Weitere Beispiele für administrative Daten sind Meeting-Titel, Meeting-Uhrzeit und andere Attribute der Meetings, die auf Webex gehostet werden.

Kundendaten

Dazu zählen alle Daten (einschließlich Text-, Audio-, Video- und Bilddateien sowie Aufzeichnungen), die Cisco von einem Kunden im Zusammenhang mit seiner Nutzung von Produkten oder Services von Cisco bereitgestellt werden, sowie Daten, die auf besonderen Wunsch eines Kunden im Rahmen einer Leistungsbeschreibung oder eines Vertrags von Cisco entwickelt werden.

Zu Kundendaten zählen auch Protokoll-, Konfigurations- oder Firmware-Dateien sowie Core-Dumps.

Es handelt sich dabei um Daten von einem Produkt oder Service, die Cisco zur Behebung eines Problems in Verbindung mit einer Support-Anfrage zur Verfügung gestellt werden. Administrative Daten, Supportdaten oder Telemetriedaten sind keine Kundendaten.

Supportdaten

Informationen, die Cisco erfasst, wenn ein Kunde eine Anfrage für Supportleistungen oder andere Fehlerbehebungsmaßnahmen sendet, einschließlich Informationen zu Hardware oder Software. Dazu gehören auch Details zum jeweiligen Support-Fall, beispielsweise Authentifizierungsinformationen, Informationen zum Zustand des Produkts, System- und Registrierungsdaten zu Softwareinstallationen und Hardwarekonfigurationen sowie Fehlernachverfolgungsdateien. Zu Supportdaten zählen nicht Protokoll-, Konfigurations- oder Firmware-Dateien oder Core-Dumps von einem Produkt, die uns zur Behebung eines Problems in Verbindung mit einer Support-Anfrage zur Verfügung gestellt werden. Dies sind Beispiele für Kundendaten.

Telemetriedaten

Informationen, die durch Instrumentierungs- und Protokollierungssysteme erzeugt und durch die Nutzung und den Betrieb des Produkts oder Services erstellt werden.

Alle in der Webex Cloud erfassten Daten werden auf mehreren Ebenen durch robuste Sicherheitstechnologien und -prozesse geschützt. Nachfolgend finden Sie einige Beispiele für Kontrollen, die in verschiedenen Schichten von Webex zum Schutz von Kundendaten eingesetzt werden:

- **Physische Zugriffskontrolle:** Der physische Zugriff wird durch Biometrie, Badges und Videoüberwachung gesteuert. Der Zugriff auf das Rechenzentrum erfordert Genehmigungen und wird über ein elektronisches Ticket-System verwaltet.
- **Netzwerkzugriffskontrolle:** Der Webex Netzwerkperimeter ist durch Firewalls geschützt. Jeder Netzwerk-Traffic in das und aus dem Webex Rechenzentrum wird kontinuierlich durch ein Intrusion Detection System (IDS) überwacht. Das Webex Netzwerk ist außerdem in separate Sicherheitszonen aufgeteilt. Der Traffic zwischen den Zonen wird durch Firewalls und Zugriffskontrolllisten (Access Control Lists, ACLs) gesteuert.
- **Infrastrukturüberwachung und Managementkontrollen:** Sämtliche Komponenten der Infrastruktur, einschließlich Netzwerkgeräten, Anwendungsservern und Datenbanken, werden nach strengen Richtlinien abgesichert. Sie werden außerdem regelmäßigen Scans unterzogen, um Sicherheitsprobleme zu identifizieren und zu beheben.
- **Kryptografische Kontrollen**: Wie bereits erwähnt, werden alle Daten zum und vom Webex Rechenzentrum an Cloud-registrierte Webex Apps und Webex Geräte verschlüsselt. Die einzige Ausnahme bilden PSTN-Traffic und unverschlüsselte SIP/H323-Videogeräte in einem Cloud-fähigen Meeting. Darüber hinaus werden wichtige Daten, die in Webex gespeichert sind, z. B. Kennwörter, verschlüsselt.

Cisco MitarbeiterInnen greifen nur auf Kundendaten zu, wenn der Kunde aus Support-Gründen den Zugriff anfordert. In diesem Fall wird der Zugriff auf Systeme von ManagerInnen ausschließlich nach dem Prinzip der „Aufgabentrennung“ erlaubt. Zugriff wird nur bei Notwendigkeit der Kenntnis und nur in dem für die Aufgabe erforderlichen Umfang gewährt. Der Zugriff von MitarbeiterInnen auf diese Systeme wird außerdem regelmäßig im Hinblick auf die Compliance überprüft. MitarbeiterInnen mit Zugriffsberechtigung müssen an der jährlichen Schulung für Information Security Awareness nach ISO 27001 (International Organization for Standardization) teilnehmen.

Zusätzlich zu diesen speziellen Kontrollen wird für alle MitarbeiterInnen von Cisco ein Background-Check durchgeführt. Darüber hinaus müssen alle Cisco MitarbeiterInnen eine Geheimhaltungsvereinbarung (Nondisclosure Agreement, NDA) unterschreiben und an der Schulung zum Verhaltenskodex (Code of Business Conduct, COBC) teilnehmen.

Health Insurance Portability and Accountability Act (HIPAA)

Cisco kann Informationen zu Funktionen, Technologie und Sicherheit von Webex bereitstellen. Unternehmen, für die das Datenschutzgesetz HIPAA gilt, müssen zusammen mit ihrem Rechtsbeistand klären, ob die Funktionen von Webex für ihre Geschäftsprozesse geeignet und DSGVO-konform sind.

- Einhaltung der DSGVO
- Datenschutz in Webex Meetings

Branchenstandards und Zertifizierungen

Neben der Einhaltung eigener strenger interner Standards führt Cisco Webex kontinuierlich Validierungen durch Dritte durch, um somit sein Engagement für die Informationssicherheit zu demonstrieren. Webex verfügt über Folgendes:

- ISO 27001-, 27017-, 27018- und 27701-Zertifizierungen
- Prüfung nach Service Organization Controls (SOC) 2 Typ II
- SOC-3-Zertifizierung
- Cloud Code of Conduct
- CSTAR
- Cloud Computing Compliance Controls Catalogue (C5)-Nachweis
- FedRAMP-Zertifizierung (weitere Informationen, u. a. über Umfang und Verfügbarkeit, finden Sie unter cisco.com/go/fedramp)

Hinweis: Der FedRAMP-zertifizierte Webex Service steht nur US-Behörden und US-Kunden aus dem Bildungswesen zur Verfügung.

Fazit

Mit den bewährten und branchenführenden Webex Lösungen für Web- und Videokonferenzen können Sie die Zusammenarbeit noch produktiver und effektiver gestalten. Webex bietet eine skalierbare Architektur, konsistente Verfügbarkeit und validierte mehrstufige Sicherheit, die kontinuierlich überwacht wird, um strenge interne und externe Branchenstandards zu erfüllen. Wir gestalten eine vernetzte digitale Zukunft, in der das Unmögliche möglich wird. Mit Sicherheit.

Informationen zum Kauf

Um Kaufoptionen anzuzeigen und mit dem Cisco Sales Team zu sprechen, besuchen Sie cisco.com/c/de_de/buy.html.

Weitere Informationen
Webex Meetings | Webex Events | Webex Training
Webex Support | Cloud Connected Audio

Februar 2022