Datenschutz und Datensicherheit

Cisco Webex Teams und Cisco Webex Meetings

Version 1.0, März 2020

Inhaltsverzeichnis

Umfang des Dienstes

Cisco Webex ist eine Software-as-a-Service-Lösung (SaaS), die über die Cisco Webex Cloud bereitgestellt wird, eine hochsichere Servicebereitstellungsplattform mit branchenführender Leistung, Integration, Flexibilität, Skalierbarkeit und Verfügbarkeit. Die Cisco Webex Cloud ist eine Kommunikationsinfrastruktur, die speziell für die Echtzeit-Webkommunikation entwickelt wurde.

Definition der Dienste

Cisco Webex Meetings

Cisco Webex Meetings ist ein cloud-basierter Web- und Video-Konferenzdienst welcher die Zusammenarbeit von global oder virtuelle Teams erlaubt. Teilnehmer können über einen Web Browser, mobile Endgeräte wie Smartphones oder Tablets, oder ein Video System teilnehmen. Die Lösung unterstützt u.a. Funktionen wie Bildschirmfreigabe für eine reibungslose Teamarbeit und die Aufzeichnung von Konferenzen.

Große Events mit bis zu 3000 Teilnehmern oder Liveübertragungen, inklusive Streaming in sozialen Netzen (z.B. Facebook Live) können mit Webex Meetings ebenso realisiert werden, wie virtuelle Fortbildungen oder Unterricht.

Cisco Webex Teams

Cisco Webex Teams ist eine cloud-basierte Kommunikations-Lösung die es globalen oder virtuellen Teams erlaubt jederzeit in Verbindung zu bleiben. Dabei lassen sich tagtägliche Arbeitsabläufe wie Informationsaustausch (Nachrichten- Übermittlung und Dateiaustausch), gemeinsames Arbeiten an Dokumenten oder interaktiven Whiteboards sowie Echtzeitkommunikation (Audio und Video) nahtlos miteinander verknüpfen. Bei Bedarf können über sichere vorgefertigte Schnittstellen zudem Systeme von Dritt-Anbietern angeschlossen werden.

Definition Datenschutz und Datensicherheit

Datenschutz ist am einfachsten mit dieser kurzen Definition zu verstehen: Unter Datenschutz versteht man den Schutz von personenbezogenen Daten. Hierunter fallen alle Daten, die sich auf eine natürliche Person beziehen. Ziel des Datenschutzes ist der Schutz des allgemeinen Persönlichkeitsrechts der betroffenen natürlichen Personen. Normen hierzu finden sich in der Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG). Der Datenschutz dient somit dem Zweck natürliche Personen und ihre Grundrechte und Grundfreiheiten zu schützen.

Datensicherheit beschäftigt sich hingegen generell mit der Sicherheit von Daten. Ziel der Datensicherheit ist der Schutz von Daten allgemein, nicht nur von personenbezogenen Daten. Hierunter fallen damit auch reine Unternehmensdaten, also Daten von juristischen Personen. Das oberste Ziel der Datensicherheit besteht in der Gewährleistung

- der Vertraulichkeit
- der Integrität und
- der Verfügbarkeit von Daten

Vereinfacht könnte man sagen, dass es sich hier um die praktischen Sicherheitsmaßnahmen oder Ansätze zum Schutz von Daten handelt (z.B. Maßnahmen zur Datensicherung, technischer Schutz vor Datenverlust usw.).

Abgrenzung zwischen Datenschutz und Datensicherheit an einem Beispiel:

Datenschutz – dürfen bestimmte (personenbezogene) Daten zu einem bestimmten Zweck verarbeitet werden?

Datensicherheit – welchen Maßnahmen schützen die erhobenen Daten?

Datenschutzproblematik: darf das Alter der Kunden erhoben bzw. verarbeitet werden?

Datensicherheitsproblematik: wie ist sichergestellt, dass nur autorisierte Mitarbeiter auf diese Daten Zugriff erhalten?

Zertifizierungen und Einhaltung gesetzlicher Vorschriften

Informationssicherheit erfordert ein solides Risikomanagement, ein umfassendes Sensibilisierungsprogramm und einen strukturierten Plan für Geschäftskontinuität. Daher ist die Sicherheit von Informationen für Cisco und seine Kunden von größter Bedeutung.

Das Unternehmen unternimmt große Anstrengungen, um vertrauliche Informa-tionen vor unbefugtem Zugriff zu schützen und gleichzeitig die Unter-nehmensstrategie zur Einhaltung der Sicherheitsbestimmungen voranzutreiben.

Das Cisco Information Security (InfoSec) Operations Audit Team verwaltet diesen Prozess, um aktiv Lückenanalysen durchzuführen, den Zertifizierungsstatus zu überwachen und beratend tätig zu werden, um das Erreichen und die fortlaufende Einhaltung dieser Zertifizierungsstandards zu unterstützen.

Im Rahmen fortlaufender Compliance-Standards führt das Auditteam von InfoSec Operations zusammen mit externen Organisationen regelmäßig Nachprüfungen oder Audits durch, um zu bestätigen, dass jede Cisco Organisationseinheit die Standards einhält, und arbeitet eng mit GRC und IT Risikomanagement zusammen.

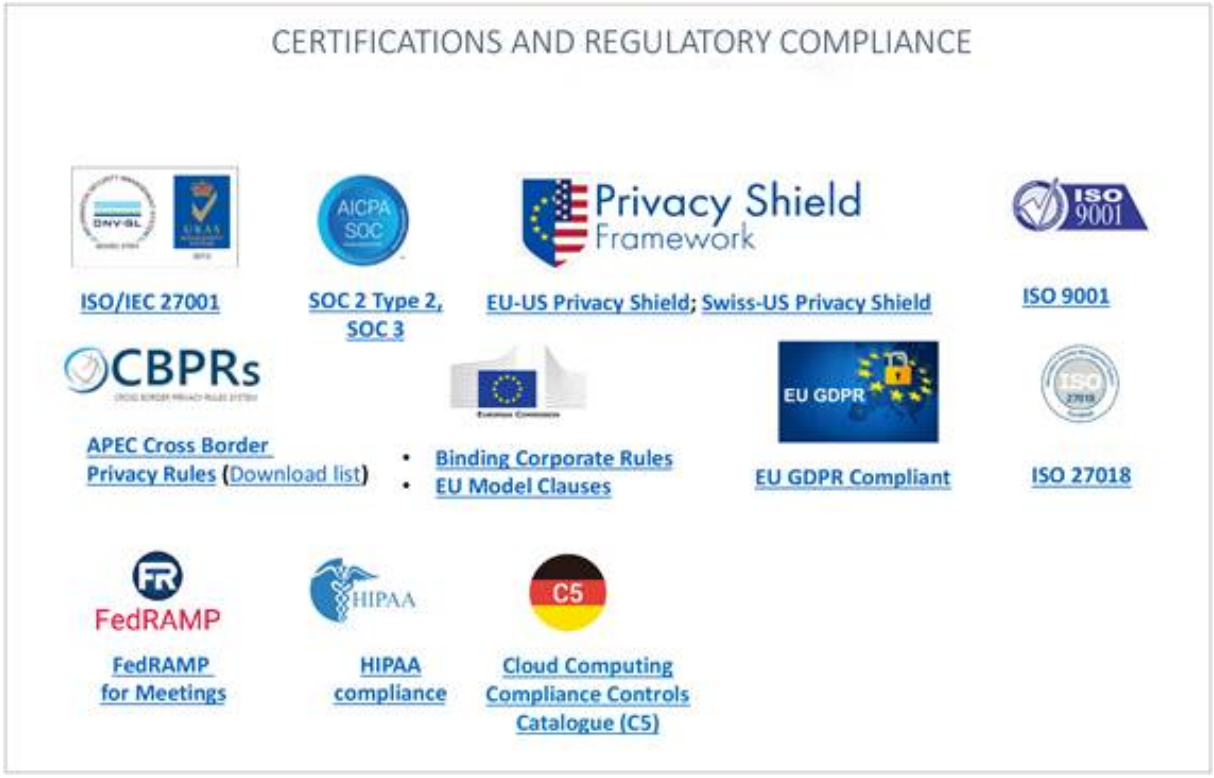
Darüber hinaus ist das Cisco Security & Trust Office in Deutschland der Ansprechpartner für alle Fragen rund um Cybersicherheit, Cisco Produkte und Dienstleistungen oder Cisco als Unternehmen. Cisco unterhält eine enge Zusammenarbeit mit Behörden und staatlichen Stellen, wie z.B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Cisco Security & Trust Office Deutschland

https://www.cisco.com/c/de_de/products/security/data-protection.html

Die folgenden Zertifikate und regulatorischen Anforderung werden durch Cisco Webex erfüllt:

- ISO / IEC 27001, 27017
- ISO 27018
- SOC 2 Typ 1 und Typ 2
- Cloud Computing-Katalog für Compliance-Kontrollen (C5) – Bundesamt für Sicherheit in der Informationstechnik
- EU-US-Datenschutzschild
- Grenzüberschreitende Datenschutzbestimmungen von APEC
- Verbindliche Unternehmensregeln
- EU-Standardvertragsklauseln
- EU-DSGVO



Verfügbare Zertifikate finden Sie unter: *https://trustportal.cisco.com/*

Datenschutz

Datenschutzvereinbarung innerhalb der EU

Die Datenverarbeitung von personenbezogenen Daten innerhalb der EU wird nach Art. 28 und 29 DSGVO (Erhebung, Verarbeitung oder Nutzung personen-bezogener Daten im Auftrag) geregelt.

Datenschutzvereinbarung außerhalb der EU

Um auch außerhalb der EU / des EWR Datenschutzanforderungen zwischen den Vertragspartnern zu gewährleisten, die den europäischen Anforderungen entsprechen wurden nachfolgende Maßnahmen umgesetzt:

- EU-US und Swiss-US Privacy Shields
- Datenschutzvereinbarung auf Basis der EU-Standardvertragsklauseln (EU-Model Clauses)
- EU-verbindliche Unternehmensregeln (Binding Corporate Rules – Controller)

EU-US and Swiss-US Privacy Shields

Cisco Systems Inc. und seine in den USA ansässigen Tochterunternehmen: Acano LLC, AppDynamics LLC, Broadsoft, Inc., Cisco OpenDNS LLC, Cisco Systems Capital Corporation, Cisco WebEx LLC, CliQr Technologies LLC, CloudLock LLC, Jasper International Services LLC, Jasper Technologies LLC , Meraki LLC und Scientific-Atlanta LLC (zusammen „Cisco-US“) beteiligen sich an den vom US-Handelsministerium in Bezug auf die Sammlung festgelegten Datenschutzschild-Frameworks und -Prinzipien der EU-USA und der Schweiz-USA und haben diese zertifiziert.

Verwendung und Speicherung personenbezogener Daten, die aus der Europäischen Union (EU), dem Vereinigten Königreich (UK) bzw. der Schweiz übertragen wurden. Cisco-US verpflichtet sich, alle personenbezogenen Daten, die aus Mitgliedsländern der Europäischen Union (EU), Großbritannien und der Schweiz unter Berufung auf die Privacy Shield Frameworks der EU-USA und der Schweiz-USA erhalten werden, den geltenden Grundsätzen der Frameworks zu unterwerfen. Wenn es einen Konflikt zwischen den Bestimmungen dieser Richtlinie und den Privacy Shield-Prinzipien gibt, gelten die Privacy Shield-Prinzipien. Weitere Informationen zu diesen Privacy Shield Frameworks finden Sie auf der Privacy Shield-Website des US-Handelsministeriums.

https://www.privacyshield.gov/Program-Overview

Cisco-US ist für die Verarbeitung personenbezogener Daten verantwortlich.

In Bezug auf diese Daten unterliegt Cisco-US den behördlichen Durchsetzungs-befugnissen der US Federal Trade Commission.

Datenschutzvereinbarung auf Basis der EU-Standardvertragsklauseln (EU-Model Clauses)

- Standardvertragsklauseln für den Austausch personenbezogener Daten mit Drittstaaten gemäß Direktive „95/46/EC of the European Parliament and of the Council“
- Zusatzvereinbarung zu den EU-Standardvertragsklauseln

EU-verbindliche Unternehmensregeln (Binding Corporate Rules – Controller)

Das globale Datenschutzprogramm und die Richtlinien von Cisco wurden von den niederländischen, polnischen, spanischen und anderen relevanten europäischen Datenschutzbehörden als angemessene Schutzmaßnahmen für den Schutz der Privatsphäre, der Grundrechte und der Freiheiten von Personen bei der Übertragung personenbezogener Daten, die nach europäischem Recht geschützt sind, genehmigt. Die verbindlichen Unternehmensregeln von Cisco (BCR-C) sehen vor, dass Übertragungen europäischer personenbezogener Daten durch Cisco weltweit angemessenen Schutzmaßnahmen unterliegen.

Weiter Informationen zur Globale Datenschutz- und Datenschutzrichtlinie

https://www.cisco.com/c/en/us/about/trust-center/customer-data-privacy-policy.html

Binding Corporate Rule

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

Datenschutzinformationen

Datenschutzbezogene Informationen finden Sie in den aktuellen "Datenschutzdatenblättern" der unten aufgeführten Produktgruppen.

Webex Teams - Privacy Data Sheet

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-teams-privacy-data-sheet1.pdf

Webex Meetings - Privacy Data Sheet

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf

Datenverarbeitung

Zugriffsrechte und Ort der Datenspeicherung sind in den jeweiligen Datenverarbeitungsübersichten (Privacy Data Map) festgelegt

Webex Meetings – Privacy Data Map

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatamap/collaboration/webex-meetings-privacy-data-map.pdf

Webex Teams – Privacy Data Map

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatamap/collaboration/webex-teams-privacy-data-map.pdf

Datenlokalität

Benutzerdaten werden in regionalen Rechenzentren gespeichert, die dem Standort des Unternehmens entsprechen, z.B. Kunde aus Deutschland, Nutzung der Rechenzentren in Europa (London, Amsterdam und Frankfurt).

Für Kunden in der europäischen Kontinentalregion (GEO) werden Benutzerdaten in Rechenzentren in London, Frankfurt und Amsterdam abgelegt.

Die bestehenden Rechenzentren in den Vereinigten Staaten von Amerika dienen weiterhin Nordamerika und dem "Rest der Welt" (RoW).

Weiter Informationen zur Lokalität der Daten in Webex Teams

https://help.webex.com/en-us/oybc4fb/Data-Residency-in-Cisco-Webex-Teams

Sicherheitsaspekte

Plattformsicherheit

Die Plattformsicherheit umfasst die Sicherheit des Netzwerks, der Systeme und der gesamten Rechenzentren die den Cisco Webex Service bereitstellen. Alle Systeme werden vor der Bereitstellung in der Produktion einer gründlichen Sicherheitsüberprüfung und Akzeptanzvalidierung unterzogen. Es erfolgt eine regelmäßige fortlaufende Sicherung, sowie eine kontinuierliche Überprüfung, Bewertung und sicherheitsrelevante Aktualisierungen der Komponenten.

Server werden gemäß den vom „National Institute of Standards and Technology“ (NIST) veröffentlichten „Security Technical Implementation Guidelines“ (STIGs) gehärtet.

Zugriffssteuerungslisten (Access Control Lists, ACLs) trennen die verschiedenen Sicherheitszonen. Angriffserkennungssoftware (Intrusion Detection Systems, IDS) sind vorhanden, und Aktivitäten werden kontinuierlich protokolliert und überwacht. Tägliche interne und externe Sicherheitsüberprüfungen werden für die Cisco Webex Cloud durchgeführt. Alle Systeme werden im Rahmen der regelmäßigen Wartung gehärtet und gepatcht. Darüber hinaus werden Schwachstellen-Scans und Bewertungen kontinuierlich durchgeführt.

Service Kontinuität und Notfallplanung

Die globalen Standortsicherungen und das Hochverfügbarkeitsdesign der Rechenzentren ermöglichen eine geografische Ausfallsicherheit der Cisco Webex-Dienste.

In Cisco Webex-Meetings werden Media Nodes verwendet, die sich in mehreren Rechenzentren auf der ganzen Welt befinden. Diese Rechenzentren befinden sich strategisch günstig in der Nähe wichtiger Internet-Zugangspunkte und verwenden dedizierte Glasfasern mit hoher Bandbreite, um den Verkehr rund um die Welt zu leiten. Cisco betreibt die gesamte Infrastruktur innerhalb der Cisco Webex Cloud mit branchenüblicher Unternehmenssicherheit.

Darüber hinaus betreibt Cisco PoP-Standorte (Point-of-Presence) im Netzwerk, die Backbone-Verbindungen, Internet-Peering, globale Standortsicherung und Caching-Technologien ermöglichen, um die Leistung und Verfügbarkeit für Endbenutzer zu verbessern.

Physische Sicherheit

Die physische Sicherheit im Rechenzentrum umfasst die Videoüberwachung von Einrichtungen und Gebäuden sowie die erzwungene Zwei-Faktor-Identifizierung für den Zugang. In den Rechenzentren wird der Zugriff über eine Kombination aus Ausweislesern und biometrischen Kontrollen gesteuert. Darüber hinaus tragen Umgebungskontrollen (z. B.

Temperatursensoren und Brandbekämpfungs-systeme) und die Infrastruktur für die Kontinuität des Dienstes (z. B. Notstrom-versorgung) dazu bei, dass die Systeme ohne Unterbrechung laufen. Innerhalb der Rechenzentren befinden sich auch „Vertrauenszonen“ oder segmentierter Zugriff auf Geräte, basierend auf der Sensibilität der Infrastruktur. Beispielsweise werden Datenbanken „eingesperrt“: Die Netzwerkinfrastruktur verfügt über dedizierte Räume und Racks sind gesperrt.

Nur sehr wenige Personen mit hohem Vertrauensniveau haben Zugriff auf das physische Netzwerk und die Komponenten.

Risikominimierung durch Webex

Viele Anbieter von Cloud-Kommunikations-Lösungen verweisen auf eine Vielzahl von Sicherheitsfunktionen, wenn es um die Sicherung der Cloud und den Schutz von Kundendaten geht. Anbieter bezeichnen Architekturmerkmale wie "Verschlüsselung von Daten während der Übertragung" und "Verschlüsselung von gespeicherten Daten" häufig als Grundlage für Sicherheitsmechanismen für ihren Dienst. Aber was bedeuten Begriffe wie diese wirklich, wenn es darum geht, Cloud Collaboration Services und die Geräte, die sie verwenden, zu sichern?

Webex Teams

Im „Cisco Webex Teams Security White Paper“ werden die nachfolgenden Ziele und Aspekte hinsichtlich der Sicherheit für die Cloud-Zusammenarbeit behandelt:

- Sicherheitsaspekte im Zusammenhang mit Cloud-Zusammenarbeit vom Unternehmensnetzwerk bis zur Cloud
- Sicherheit der Geräte und Anwendungen
- Sicherheitsrelevante Standards und Protokolle zu Kryptologie, Authentifizierung etc.
- Bewährte Methoden und Prozesse (Best Practices), die Cisco verwendet, um sicherzustellen, dass die Webex Cloud, die Webex Anwendungen und die Webex-Geräte sicher sind
- Sicherheitsmaßstäbe, an welchen Cloud-Collaboration-Produkte gemessen werden.

Dieses Whitepaper enthält eine ausführliche Beschreibung der Sicherung der Desktop-, Mobil- und Webanwendungen von Webex Teams durch Cisco.

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf

Vom ersten Tag an stand die Datensicherheit im Mittelpunkt des Designs von Cisco Webex. Der Eckpfeiler dieser Sicherheit ist die Ende-zu-Ende-Verschlüsselung, die innerhalb des Cisco Webex Teams Dienst genutzt wird und auf einem zentralen Key Management Service (KMS) basiert. Der KMS ist für die Erstellung und Verwaltung der kryptografischen Schlüssel verantwortlich, mit denen Endpunkte (Anwendungen, Endgeräte) Daten (z.B. Nachrichten, Dateien Whiteboards) dynamisch verschlüsseln und entschlüsseln.

Standardmäßig erhalten alle Cisco Webex-Kunden eine End-to-End-Verschlüsselung mit dynamischen Schlüsseln, die im Cloud-KMS, dem Sicherheitsbereich von Cisco, gespeichert sind.

Cisco Webex Hybrid Data Security (HDS) ermöglicht eine Verschiebung des KMS und andere sicherheitsrelevante Funktionen in das Unternehmens-Rechenzentrum des Kunden. Damit erhält der Kunde volle Hoheit über die kryptografischen Schlüssel.

Webex Meetings

Ende-zu-Ende-Verschlüsselung bei Cisco Webex-Meetings

Durch die optionale Ende zu Ende Verschlüsselung kann zwischen den Teilnehmer der „Webex-Meeting-App“ eine höheres Maß an Sicherheit zur Verfügung gestellt werden.

Eine detaillierte Ansicht aller Webex Meetings-Sicherheitslösungen finden Sie im Webex Meetings Security Whitepaper:

https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf

Datensicherheit

Die gesamte Kommunikation zwischen Cisco Webex-Anwendungen und Cisco Webex Cloud erfolgt über verschlüsselte Kanäle. Cisco Webex verwendet das TLS 1.2-Protokoll und hochsicher Chiffren (z. B. AES 256).

Nachdem eine Sitzung über TLS eingerichtet wurde, werden alle Medienströme (Audio-VoIP, Video, Bildschirmfreigabe und Dokumentfreigabe) verschlüsselt.

Das User Datagram Protocol (UDP) ist das bevorzugte Protokoll für die Übertragung von Medien. In UDP werden Medienpakete mit AES 128 verschlüsselt. Der anfängliche Schlüsselaustausch erfolgt auf einem TLS-gesicherten Kanal. Darüber hinaus verwendet jedes Datagramm die Hash-basierte Nachrichten-authentifizierung. Gespeicherten Daten werden auch verschlüsselt. Wenn Cisco Webex Meetings dies konfiguriert hat, speichert Cisco Webex Meetings Besprechungs- und Benutzerdaten, die für Ihr Unternehmen möglicherweise von entscheidender Bedeutung sind.

Aufzeichnungen von Webex Meetings werden sowohl auf Dateiebene als auch auf logischer Volume-Ebene verschlüsselt. Der Dateischlüssel ist ein 256-Bit-Block-AES-GCM-Schlüssel. Dieser Dateischlüssel wird dann mit einem Hauptschlüssel verschlüsselt, der auf AES (HMAC-SHA256) basiert und entsprechend der Richtlinie gedreht und in einer Datenbank gespeichert wird. Während des Wiedergabe- und Download-Ablaufs wird die verschlüsselte Aufnahmedatei dann vor oder während des Vorgangs entschlüsselt.

Deutschland:

Cisco Systems GmbH
Kurfürstendamm 22
D-10719 Berlin
Tel.: +49 30 97892700
Fax: +49 30 97892100

Cisco Systems GmbH
Neuer Wall 77
D-20354 Hamburg
Tel.: +49 40 37674600
Fax: +49 40 37674444

Cisco Systems GmbH
Hansaallee 249
D-40549 Düsseldorf
Tel.: +49 211 52029000
Fax: +49 211 52029010

Cisco Systems GmbH
Kaiserswerther Straße 115
D-40880 Ratingen
Tel.: +49 2102 1245000
Fax: +49 2102 1245499

Cisco Systems GmbH
Friedrich-Ebert-Allee 67–69
D-53113 Bonn
Tel.: 0800 1873652

Cisco Systems GmbH
Ludwig-Erhard-Straße 3
D-65760 Eschborn
Tel.: +49 6196 7739800
Fax: +49 6196 7739777

Cisco Systems GmbH
Business Service Center (BSC)
Janderstraße 8
D-68199 Mannheim
Tel.: 0800 1873652

Cisco Systems GmbH
City Plaza
Rotebühlplatz 21–25
D-70178 Stuttgart
Tel.: +49 711 23911332
Fax: +49 711 23911111

Cisco Systems GmbH
Leopoldstraße 240
D-80807 München
Tel.: +49 89 3581860
Fax: +49 89 35818619

Cisco Systems GmbH
Parkring 20
D-85748 Garching
Tel.: 0800 1873652
Fax: +49 811 5595443

Schweiz:

Cisco Systems GmbH
Richtistrasse 7
CH-8304 Wallisellen/Zürich
Tel.: +41 44 8789200
Fax: +41 44 8789292

Cisco Systems GmbH
Im Technopark
Morgenstrasse 129
CH-3018 Bern
Tel.: +41 31 9985050
Fax: +41 31 9984469

Cisco Systems GmbH
Avenue des Uttins 5
CH-1180 Rolle
Tel.: +41 21 8221600
Fax: +41 21 8221610

Österreich:

Cisco Systems Austria GmbH
Millennium Tower
Handelskai 94–96
A-1206 Wien
Tel.: 0800 297526
Fax: +43 12 40306300

Cisco Systems Austria GmbH
Bürocenter am Arenberg
Eberhard-Fugger-Straße 5
A-5020 Salzburg
Tel: 0800 297526
Fax: +43 12 40306300

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.