

# Webkonferenzen – nutzen Sie das volle Potenzial einer sicheren Zusammenarbeit in Echtzeit

Dieses Whitepaper enthält Sicherheitsinformationen zum Cisco WebEx Meeting Center, zum Cisco WebEx Training Center, zum Cisco WebEx Support Center und zum Cisco WebEx Event Center.

## Einführung

Die Cisco WebEx<sup>®</sup> Online-Lösungen ermöglichen Mitarbeitern und virtuellen Teams eine standortunabhängige Kommunikation und Zusammenarbeit in Echtzeit, so als befänden sie sich im selben Raum. Tatsächlich ist die Online-Zusammenarbeit der herkömmlichen persönlichen Zusammenarbeit in vielen Punkten überlegen, da sie Dienstreisen und physische Konferenzräume praktisch überflüssig macht und damit Zeit und Kosten einspart. Unternehmen, Institutionen und Behörden rund um den Globus vertrauen auf die Cisco WebEx<sup>®</sup> Lösungen. Sie vereinfachen damit geschäftliche Prozesse, steigern ihre Umsätze, optimieren Marketing- und Schulungsaktivitäten sowie das Projektmanagement und unterstützen ihre Teams.

Sicherheit ist in Unternehmen und Behörden weltweit einer der wichtigsten Aspekte. Bei der Online-Zusammenarbeit muss die Sicherheit auf unterschiedlichen Ebenen gewährleistet werden: von der Planung von Meetings, der Authentifizierung der Teilnehmer bis hin zur Freigabe von Dokumenten.

Cisco legt beim Design, bei der Bereitstellung und bei der Wartung seiner Netzwerke, Plattformen und Anwendungen allerhöchsten Wert auf Sicherheit. Sie können die WebEx<sup>®</sup> Lösungen problemlos in Ihre Geschäftsprozesse einbinden, selbst bei strengsten Sicherheitsauflagen.

Um eine fundierte Investitionsentscheidung treffen zu können, sollten Sie die Funktionen der Cisco WebEx Online-Anwendungen sowie die zugrunde liegende Kommunikationsstruktur, die Cisco WebEx Cloud, kennen und verstehen.

## Die Cisco WebEx Cloud-Infrastruktur

Cisco WebEx Meetings 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 Implementierung und Anwendungsbereitstellung der Cisco WebEx Cloud ist denkbar einfach. Sie senkt die Gesamtbetriebskosten und sorgt gleichzeitig für ein Höchstmaß an Sicherheit im Unternehmen.

## Switch-Architektur

Cisco verfügt über ein weltweit verteiltes, dediziertes Netzwerk von Hochgeschwindigkeits-Meeting-Switches. Daten einer Meeting-Sitzung, die vom Computer des Moderators an die Computer der Teilnehmer gesendet werden, werden von der Cisco WebEx Cloud weitergeleitet, jedoch nie dauerhaft gespeichert.<sup>1</sup>

---

<sup>1</sup> Erst wenn ein Benutzer die netzwerkbasierte Aufzeichnungsfunktion (Network-based Recording, NBR) aktiviert, wird das Meeting aufgezeichnet und gespeichert. Darüber hinaus speichert WebEx auch Benutzerprofildaten und Benutzerdateien.

---

## Rechenzentren

Die Cisco WebEx Cloud ist eine Kommunikationsinfrastruktur, die speziell für die Echtzeitkommunikation über das Internet entwickelt wurde. Die Switching-Geräte, die bei WebEx Meetings zum Einsatz kommt, befinden sich in verschiedenen Rechenzentren auf der ganzen Welt. Diese Rechenzentren wurden strategisch in der Nähe wichtiger Internet-Zugriffspunkte platziert und nutzen spezielle Glasfaserleitungen für hohe Bandbreite, um den Datenverkehr um die Welt zu leiten. Cisco betreibt die gesamte Infrastruktur in der Cisco WebEx Cloud. Daten in den Vereinigten Staaten bleiben in den USA, während Daten in Europa im europäischen Raum bleiben.

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 Endbenutzer zu optimieren. Die Experten von Cisco stehen Ihnen rund um die Uhr für Fragen und Support zur logistischen Sicherheit sowie zum Betriebs- und Änderungsmanagement zur Verfügung.

## Das umfassend abgesicherte WebEx Meeting-Erlebnis im Überblick

Das WebEx Meeting-Erlebnis umfasst folgende Aspekte:

- Konfiguration der Meeting-Website
- Sicherheitsoptionen für die Meeting-Planung
- Optionen zum Start und zur Teilnahme an WebEx Meetings
- Verschlüsselungstechnologien
- Transport Layer Security
- Firewall-Kompatibilität
- Schutz von Meeting-Daten
- Sicherheit während des Meetings
- Single Sign-On
- Überprüfungen durch Dritte (unabhängige Audits bestätigen die Sicherheit von Cisco WebEx)

Die Begriffe „WebEx Meeting(s)“ und „Cisco WebEx Meeting-Sitzungen“ beziehen sich auf die in alle Cisco WebEx Online-Produkte integrierten Audio-Konferenzen sowie Single- und Multi-Point-Videokonferenzen. Zu diesen Produkten gehören:

- das Cisco WebEx Meeting Center
- das Cisco WebEx Training Center
- das Cisco WebEx Event Center
- das Cisco WebEx Support Center (einschließlich Cisco WebEx Remote Support und Cisco WebEx Remote Access)

Soweit nicht anders angegeben, gelten die in diesem Dokument beschriebenen Sicherheitsmerkmale in gleichem Umfang für alle oben genannten WebEx Anwendungen.

## WebEx Meeting-Rollen

Die vier Rollen in einem WebEx Meeting sind Gastgeber, alternativer Gastgeber, Moderator und Teilnehmer. In den folgenden Abschnitten werden die Sicherheitsberechtigungen der einzelnen Rollen beschrieben.

---

## Host

Der Gastgeber setzt WebEx Meetings an und startet sie. Er kontrolliert das Teilnehmererlebnis während des Meetings. Was die Sicherheit betrifft, so kann der Gastgeber den Teilnehmern Moderatorberechtigungen erteilen. Außerdem kann er das Meeting sperren und Teilnehmer ausschließen.

## Alternativer Gastgeber

Der Gastgeber bestimmt einen alternativen Gastgeber, der anstelle des Gastgebers ein geplantes WebEx Meeting starten kann. Im Hinblick auf die Sicherheit verfügt der alternative Gastgeber über dieselben Berechtigungen wie der Gastgeber.

## Moderator

Ein Moderator gibt Präsentationen, bestimmte Anwendungen oder den gesamten Desktop frei. Er kontrolliert die Kommentar-Tools. Was die Sicherheit betrifft, kann der Moderator anderen Teilnehmern die Fernkontrolle freigegebener Anwendungen und Desktops ermöglichen bzw. ihnen diese Berechtigung entziehen.

## Teilnehmer

Ein Teilnehmer verfügt über keinerlei Sicherheitsverantwortung oder Berechtigungen.

## WebEx Site Administration-Modul

Das WebEx Site Administration-Modul ermöglicht autorisierten Administratoren die Verwaltung und Durchsetzung von Sicherheitsrichtlinien auf Meeting-Basis hinsichtlich der Gastgeber- und Moderatorberechtigungen. Sie können beispielsweise durch die Anpassung der Sitzungskonfigurationen Moderatoren die Freigabe von Anwendungen oder die Übertragung von Dateien verweigern, entweder auf Website- oder auf Benutzerbasis.

Mit dem WebEx Site Administration-Modul können Sie die folgenden Sicherheitsfunktionen verwalten:

### Account-Management

- Sperrung von Konten nach einer konfigurierbaren Anzahl fehlgeschlagener Anmeldeversuche
- Automatische Entsperrung eines gesperrten Kontos nach einem festgelegten Zeitintervall
- Deaktivierung von Konten nach einer bestimmten Zeit der Inaktivität

### Bestimmte Aktionen für einzelne Benutzerkonten

- Aufforderung eines Benutzers zur Passwortänderung bei der nächsten Anmeldung
- Sperrung oder Entsperrung eines Benutzerkontos
- Aktivierung oder Deaktivierung eines Benutzerkontos

### Konto-Erstellung

- Aufforderung zum Erstellen von Sicherheitstext bei der Beantragung eines neuen Kontos
- Anforderung einer E-Mail-Bestätigung für neue Konten
- Möglichkeit zur Selbstregistrierung für neue Konten
- Konfiguration von Regeln zur Selbstregistrierung für neue Konten

### Konto-Passwörter

Durchsetzung von Kriterien für sichere Passwörter, darunter:

- Groß- und Kleinschreibung

- 
- Mindestlänge
  - Mindestanzahl an Zahlen
  - Mindestanzahl an Buchstaben
  - Mindestanzahl an Sonderzeichen
  - Maximal zweifache Wiederholung eines Zeichens
  - Keine Wiederverwendung einer bestimmten Anzahl früherer Passwörter
  - Kein dynamischer Text (Website-Name, Gastgebername, Benutzername)
  - Keine Passwörter aus konfigurierbaren Listen (Beispiel: „Passwort“)
  - Zeitliches Mindestintervall vor einer Passwortänderung
  - Änderung des Passworts für ein Konto durch den Gastgeber nach konfigurierbaren Zeitintervallen
  - Änderung des Konto-Passworts durch Benutzer bei der nächsten Anmeldung

### **Persönliche Meeting-Räume**

Der Zugriff auf persönliche Meeting-Räume erfolgt über eine individuelle URL und das persönliche Passwort. In diesen Meeting-Räumen kann der Gastgeber angesetzte und laufende Meetings auflisten, Meetings starten, ihnen beitreten und Dateien für Meeting-Teilnehmer freigeben. Administratoren können sicherheitsrelevante Funktionen für persönliche Meeting-Räume erstellen, darunter:

- Optionen zum Freigeben von Dateien im persönlichen Meeting-Raum
- Passwortanforderungen für Dateien im persönlichen Meeting-Raum

### **Weitere, von WebEx Site Administration bereitgestellte sicherheitsrelevante Funktionen**

- Speicherung der Namen und E-Mail-Adressen von Gastgebern oder Teilnehmern für eine vereinfachte Meeting-Planung oder den einfachen Beitritt zu Meetings
- Neuuzuweisung von Aufzeichnungen an andere Gastgeber durch den Gastgeber
- Einschränkung des Website-Zugriffs per Authentifizierungsanforderung für Gastgeber und Teilnehmer  
Authentifizierungsanforderung für den Zugriff auf bestimmte Website-Informationen, z. B. aufgeführte Meetings sowie den Zugriff auf Meetings über die Website
- Einrichtung von Regeln für sichere Passwörter für WebEx Access Anywhere
- Löschen aller Meetings aus der Liste
- Genehmigungsanforderung für eine „Passwort vergessen“-Option
- Anforderung zum Zurücksetzen von Konto-Passwörtern anstatt der erneuten Eingabe für einen Benutzer

### **Sicherheitsoptionen zum Ansetzen von WebEx Meetings**

- Möglichkeit zur Festlegung von Sicherheitsanforderungen für den Meeting-Zugriff für individuelle Gastgeber (im Rahmen von Parametern, die auf Website-Administratorebene konfiguriert werden und nicht außer Kraft gesetzt werden können)
- Löschen von Meetings aus der Liste, sodass diese nicht mehr im sichtbaren Kalender angezeigt werden
- Möglichkeit zum Meeting-Beitritt der Teilnehmer vor dem Gastgeber
- Möglichkeit zur Audioeinwahl der Teilnehmer vor dem Gastgeber
- Berechtigung zum Meeting-Beitritt nur für Teilnehmer mit einem WebEx Konto

- 
- Anzeige der Telefonkonferenzinformationen im Meeting
  - Automatische Beendigung von Meetings nach einer konfigurierbaren Zeit, wenn nur noch ein Teilnehmer anwesend ist
  - Aufforderung der Teilnehmer zur Eingabe der E-Mail-Adresse beim Beitritt zu Meetings

### **Aufgeführte oder nicht aufgeführte Meetings**

Der Gastgeber kann Meetings in einem öffentlichen Meeting-Kalender auf einer benutzerdefinierten WebEx Website aufführen. Wahlweise können die Meetings aber auch ohne Auflistung angesetzt werden, sodass das Meeting nicht im öffentlichen Meeting-Kalender erscheint. Bei nicht aufgeführten Meetings muss der Gastgeber die Teilnehmer ausdrücklich auf das angesetzte Meeting hinweisen – entweder über einen Link, der den Teilnehmern im Verlauf des E-Mail-Einladungsprozesses zugesandt wird, oder indem die Teilnehmer aufgefordert werden, auf der Seite „Einem Meeting beitreten“ die angegebene Meeting-Kennnummer einzugeben.

### **Interne oder externe Meetings**

Gastgeber können die Teilnehmer eines Meetings auf Personen mit einem Konto für eine benutzerdefinierte WebEx Website beschränken. In diesem Fall müssen sich die Teilnehmer bei der Website anmelden, um dem Meeting beizutreten.

### **Meeting-Passwort**

Ein Gastgeber kann ein Meeting-Passwort festlegen und es dann wahlweise in die Einladungs-E-Mail für das Meeting einfügen.

### **Registrierung**

- Über die Registrierungsfunktion kann der Gastgeber den Zugriff auf ein Meeting einschränken. Der Gastgeber generiert eine „Zugriffskontrollliste“, die nur eingeladenen Personen, die registriert sind und vom Gastgeber ausdrücklich genehmigt wurden, den Meeting-Beitritt gestattet.
- Meetings können zusätzlich abgesichert werden, indem die Wiederverwendung von Registrierungs-IDs im WebEx Training Center und im WebEx Event Center gesperrt wird. Ein Teilnehmer, der versucht, eine bereits verwendete Registrierungs-ID wiederzuverwenden, kann dem Meeting nicht beitreten. Damit wird verhindert, dass mehrere Teilnehmer dieselbe ID benutzen.
- Darüber hinaus kann der Gastgeber die Meeting-Sicherheit durch die Einschränkung des Zugriffs und das Ausschließen von Teilnehmern gewährleisten.

Zur Unterstützung Ihrer Sicherheitsrichtlinien können beliebige Kombinationen dieser Planungsoptionen weiter angepasst werden.

### **Start von und Beitritt zu WebEx Meetings**

Ein WebEx Meeting startet, wenn die Benutzer-ID und das Passwort eines Gastgebers von der individuellen WebEx Website authentifiziert wurden. Der Gastgeber hat zunächst die Kontrolle über das Meeting und ist gleichzeitig auch der anfängliche Moderator. Er kann jedem Teilnehmer Gastgeber- oder Moderatorberechtigungen erteilen oder diese widerrufen, ausgewählte Teilnehmer ausschließen oder die Sitzung jederzeit beenden.

Der Gastgeber kann einen alternativen Gastgeber benennen, der das Meeting startet und kontrolliert, falls der Gastgeber selbst nicht teilnehmen kann oder seine Verbindung zum Meeting unterbrochen wird. So bleiben Meetings sicher, da die Gastgeberrolle nicht einem unerwarteten oder nicht autorisierten Teilnehmer zugewiesen werden kann.

---

Sie können Ihre individuelle WebEx Website so konfigurieren, dass Teilnehmer dem Meeting (einschließlich Audioverbindung) bereits vor dem Gastgeber beitreten können. Die verfügbaren Funktionen bei einem frühzeitigen Beitritt können auf Chat und Audio beschränkt werden.

Wenn ein Teilnehmer zum ersten Mal einem WebEx Meeting beitrifft, wird die WebEx Client-Software automatisch heruntergeladen und auf dem Computer des Teilnehmers installiert. Die WebEx Client-Software verfügt über eine digitale Signatur durch ein von VeriSign ausgegebenes Zertifikat. Bei nachfolgenden Meetings lädt die WebEx Anwendung nur Dateien mit Änderungen oder Updates herunter und installiert diese. Die WebEx Dateien lassen sich mithilfe der Deinstallationsfunktion des Computer-Betriebssystems der Teilnehmer problemlos entfernen.

### **Verschlüsselungstechnologien**

WebEx Meetings ermöglichen die sichere Bereitstellung von Rich-Media-Inhalten in Echtzeit für alle Teilnehmer einer WebEx Meeting-Sitzung. Gibt ein Moderator ein Dokument oder eine Präsentation frei, wird diese/s mithilfe von UCF (Universal Communications Format), einer proprietären Cisco<sup>®</sup> Technologie, kodiert. Dadurch werden die Daten für die Freigabe optimiert. Die WebEx Meeting-Anwendung für Mobilgeräte wie iPad, iPhone und BlackBerry verwendet ähnliche Verschlüsselungsmechanismen wie der PC-Client.

WebEx Meetings bieten folgende Verschlüsselungsmechanismen:

- Die Daten für WebEx Meetings auf PCs oder Mobilgeräten werden mittels Secure Socket Layer (SSL) mit 128 Bit vom Client zur Cisco WebEx Cloud übermittelt.
- Die End-to-End (E2E)-Verschlüsselung wird als Option über das Cisco WebEx Meeting Center bereitgestellt. Dieses Verfahren verschlüsselt den gesamten Meeting-Inhalt zwischen den Teilnehmern mithilfe des Advanced Encryption Standard (AES)-Verschlüsselungsstandards mit einem 256-Bit-Schlüssel, der per Zufallsmechanismus auf dem Computer des Gastgebers erzeugt und über einen Public-Key-basierten Mechanismus an die Teilnehmer übermittelt wird. Anders als die SSL-Verschlüsselung, die nur bis zur Cisco WebEx Cloud reicht, werden bei der E2E-Verschlüsselung alle Meeting-Inhalte in der gesamten Cisco WebEx Cloud-Infrastruktur verschlüsselt. Die Meeting-Inhalte werden in Form von Klartext nur im Computerspeicher der Meeting-Teilnehmer dargestellt.<sup>2</sup>
- Wenn ein Benutzer die verwandte Option „Anmeldedaten speichern“ auswählt, werden die Anmelde-ID und das Passwort des Benutzers für WebEx Meetings, die auf PCs und Mobilgeräten gespeichert sind, mit dem 128-Bit-AES-Standard verschlüsselt.

Die Website-Administratoren und Gastgeber können unter der Option „Meeting-Typ“ zwischen E2E und PKI wählen. Die E2E-Lösung gewährleistet mehr Sicherheit als nur AES (obwohl die E2E-Verschlüsselung ebenfalls AES für die Payload-Verschlüsselung verwendet), da nur der Meeting-Gastgeber und die Teilnehmer den Schlüssel kennen.

Jede Verbindung zwischen dem WebEx Meeting-Client und der WebEx Cloud wird mittels eines kryptografischen Tokens authentifiziert, sodass nur autorisierte Benutzer an einem bestimmten Meeting teilnehmen können.

### **Transport Layer Security**

Zusätzlich zu den Sicherheitsmechanismen für die Anwendungsebene werden alle Meeting-Daten mittels 128-Bit-SSL übertragen. Statt des Firewall-Ports 80 (für Standard-HTTP-Internetdatenverkehr) verwendet SSL Firewall-Port 443 (für HTTPS-Datenverkehr) zum Weiterleiten der Daten durch die Firewall.

---

<sup>2</sup> Beachten Sie, dass NBR nicht verfügbar ist, wenn die E2E-Verschlüsselung aktiviert ist. Diese Option steht nur für das WebEx Meeting Center bereit.

---

Die Teilnehmer eines WebEx Meetings verbinden sich über eine logische Verbindung auf der Anwendungs-/Präsentations-/Sitzungsebene mit der Cisco WebEx Cloud. Zwischen den Computern der Teilnehmer besteht keine Peer-to-Peer-Verbindung.

### **Firewall-Kompatibilität**

Die WebEx Meeting-Anwendung kommuniziert mit der Cisco WebEx Cloud, um eine zuverlässige und sichere Verbindung über HTTPS (Port 443) herzustellen. Daher müssen Sie Ihre Firewalls nicht speziell für WebEx Meetings konfigurieren.

### **Schutz von Meeting-Daten**

Alle WebEx Meeting-Inhalte (Chat, Audio, Video, freigegebene Desktops oder Dokumente) sind nicht permanent (d. h. sie existieren nur während des Meetings). Standardmäßig werden Meeting-Inhalte weder in der Cisco Cloud noch auf dem Computer eines Teilnehmers gespeichert. Cisco speichert nur zwei Arten von Informationen über das Meeting. Diese umfassen:

- **Ereignisdetaillaufzeichnungen (Event Detail Records, EDRs):** Diese EDR-Daten verwendet Cisco für die Rechnungsstellung und das Berichtswesen. Sie können die Ereignisdetaillaufzeichnungen auf Ihrer individuellen WebEx Website einsehen, wenn Sie sich mit Ihrer Gastgeber-ID anmelden. Nach der Authentifizierung können Sie diese Daten auch von Ihrer WebEx Website herunterladen oder über die WebEx APIs auf sie zugreifen. EDRs enthalten die grundlegenden Informationen zur Meeting-Teilnahme, darunter wer (Benutzername und E-Mail-Adresse) an welchem Meeting (Meeting-ID) wann (Zeitpunkt des Beitritts und Verlassens des Meetings) teilgenommen hat.
- **NBR-Dateien (Network-Based Recording):** Wenn ein Gastgeber eine WebEx Meeting-Sitzung aufzeichnet, wird die Aufzeichnung in der Cisco WebEx Cloud gespeichert und kann auf Ihrer individuellen WebEx Website im Bereich „Meine Aufzeichnungen“ abgerufen werden. Diese Datei wird nur erstellt, wenn ein Gastgeber während des Meetings NBR aktiviert bzw. eine übergreifende Option zur Aufzeichnung aller Meetings ausgewählt hat. Der Zugriff auf NBRs erfolgt über URL-Links. Jeder Link enthält ein nicht vorhersehbares Token. Der Gastgeber hat die volle Kontrolle über den Zugriff auf eine NBR-Datei, einschließlich der Möglichkeit, diese zu löschen, sie freizugeben oder einen Passwortschutz hinzuzufügen. Die NBR-Funktion ist optional und kann vom Administrator deaktiviert werden.

### **Single Sign-On**

Cisco unterstützt die föderierte Authentifizierung für Single Sign-On (SSO) mit SAML 1.1 und 2.0 (Security Assertion Markup Language) und den WS-Federation 1.0-Protokollen. Die Unterstützung für SAML 1.1 läuft aus. Zur Nutzung der föderierten Authentifizierung müssen Sie ein Public-Key-X.509-Zertifikat auf Ihre individuelle WebEx Website hochladen. Sie können dann SAML-Assertions mit Benutzerattributen generieren und die Assertions mit dem passenden Private Key mit einer digitalen Signatur versehen. WebEx validiert die Signatur der SAML-Assertion anhand des vorab geladenen Public-Key-Zertifikats, bevor der Benutzer authentifiziert wird.

### **Prüfberichte von Dritten**

Neben seinen eigenen strikten internen Prozessen beauftragt das WebEx Office of Security zahlreiche 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.

---

## Sicherheitsbewertung durch Dritte

Cisco führt mithilfe von Drittanbietern fortlaufende und gründliche Code-gestützte Sicherheitsprüfungen und Serviceanalysen durch. Im Rahmen dieser Prüfungen führt der Drittanbieter folgende Sicherheitsbewertungen durch:

- Ermittlung kritischer Anwendungs- und/oder Servicelücken sowie Unterbreitung entsprechender Lösungen
- Aufzeigen allgemeiner Bereiche zur Verbesserung der Architektur
- Ermittlung von Kodierungsfehlern und Leitlinien zur Verbesserung
- Direkte Zusammenarbeit mit WebEx Technikern zur Erläuterung der Ergebnisse und Vorschläge zur Problembhebung

## Safe Harbor-Zertifizierung

Im März 2012 erhielt Cisco die Safe Harbor-Zertifizierung für Kunden- und Partnerdaten (die Safe Harbor-Zertifizierung für Mitarbeiterdaten erhielt Cisco bereits 2011). Diese Zertifizierung ist ein weiterer Nachweis für das umfassende Datenschutzprogramm von Cisco. Sie wird zwar von keiner Behörde oder Standardisierungsinstitution angefordert, Cisco ist sich jedoch bewusst, dass viele Kunden Wert auf diese Zertifizierung legen.

Die europäische Datenschutzrichtlinie untersagt den Transfer von personenbezogenen Daten europäischer Bürger an Nicht-EU-Länder, die den seitens der EU geforderten „Angemessenheitsstandard“ nicht erfüllen. Das US-Handelsministerium hat, in Absprache mit der Europäischen Kommission, das Safe Harbor-Abkommen entwickelt, das US-Unternehmen die Erfüllung der Richtlinie ermöglicht, wenn sie die Safe-Harbor-Grundsätze zum Datenschutz einhalten. Die Unternehmen attestieren ihre Einhaltung dieser Grundsätze auf der Website des US-Handelsministeriums. Das Abkommen wurde im Jahr 2000 von der EU genehmigt und garantiert Unternehmen, die die Grundsätze einhalten, die Gewissheit, dass die EU ihre Verfahrensweise als „angemessenen“ Datenschutz für EU-Bürger betrachtet.

## SSAE16

PricewaterhouseCoopers führt einen jährlichen Statement of Standards for Attestation Engagements No. 16 (SSAE16)-Audit entsprechend der vom American Institute of Certified Public Accountants festgelegten Standards durch. Weitere Informationen zu SSAE16 finden Sie unter: <http://www.ssaе16.com>.

## ISO 27001 und 27002

Im Oktober 2012 erhielt Cisco die ISO 27001-Zertifizierung für seine WebEx Services. Die Zertifizierung wird alle drei Jahre nach einem jährlichen externen Zwischenaudit verlängert. ISO 27001 ist ein internationaler Datensicherheitsstandard der International Organization of Standardization (ISO), der Empfehlungen und Best Practices für ein Information Security Management System (ISMS) beinhaltet. Ein ISMS ist ein Rahmenwerk von Richtlinien und Verfahren, das sämtliche gesetzlichen, administrativen, physischen und technischen Kontrollen enthält, die in die Informationsrisiko-Managementprozesse eines Unternehmens einfließen. Laut der Dokumentation wurde ISO 27001 konzipiert, um „ein Modell für das Einrichten, Implementieren, Ausführen, Überwachen, Prüfen, Pflegen und Verbessern eines Managementsystems zur Informationssicherheit bereitzustellen“. Weitere Informationen zu ISO 27001 und 27002 finden Sie unter: <http://www.27000.org/>.



---

## Weitere Informationen

Weitere Informationen zu den Cisco WebEx Lösungen erhalten Sie unter [www.cisco.com/web/DE/products/webex/index.html](http://www.cisco.com/web/DE/products/webex/index.html) oder von Ihrem Cisco Vertriebsmitarbeiter.




---

**Hauptgeschäftsstelle Nord- und Südamerika**  
Cisco Systems, Inc.  
San Jose, CA

**Hauptgeschäftsstelle Asien-Pazifik-Raum**  
Cisco Systems (USA) Pte. Ltd.  
Singapur

**Hauptgeschäftsstelle Europa**  
Cisco Systems International BV Amsterdam,  
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)