

Einführung

Unternehmen, die sich einen Wettbewerbsvorteil sichern möchten, suchen mehr und mehr nach Möglichkeiten der Zusammenarbeit in Echtzeit, mit dem Ziel, Mitarbeiter und virtuelle Teams auf der ganzen Welt miteinander zu verbinden. Überall auf der Welt verlässt sich eine große und stetig zunehmende Zahl von Unternehmen und Behörden auf Cisco WebEx™-Software-as-a-Service (SaaS)-Lösungen zur Rationalisierung ihrer Geschäftsabläufe für Vertrieb, Marketing, Schulungen, Projektmanagement und Support. Cisco® legt bei der Auslegung, Einrichtung und Wartung von WebEx®-Netzwerk, Plattform und Applikationen allerhöchsten Wert auf Sicherheit. Daher können Sie WebEx®-Lösungen in Ihre laufenden Geschäftsvorgänge integrieren – sofort und mit vollem Vertrauen – auch in Umgebungen mit den striktesten Sicherheitsanforderungen.

Das Verständnis der Sicherheitsmerkmale der Cisco WebEx-Online-Applikationen und der ihnen zu Grunde liegenden Kommunikationsinfrastruktur – die Cisco Collaboration Cloud – bildet einen wichtigen Bestandteil Ihrer Kaufentscheidung.

Hier finden Sie detaillierte Sicherheitsinformationen zu folgenden Themen:

- Infrastruktur der Cisco Collaboration Cloud
- Sichere WebEx-Meetings
 - Konfigurierung der Meeting-Site
 - Sicherheitsoptionen beim Ansetzen von Meetings
 - Start und Beitritt zu einem WebEx-Meeting
 - Verschlüsselungstechniken
 - Sicherheit der Transportschicht
 - Firewall-Kompatibilität
 - Datenspeicherung nach Meeting-Abschluss
 - Einzelanmeldung
- Akkreditierungen durch Dritte: Unabhängige Prüfungen bestätigen die Sicherheit von Cisco WebEx

Die Begriffe „WebEx-Meeting(s)“ und „Cisco WebEx-Meeting-Sitzung“ beziehen sich auf die in allen Cisco WebEx-Online-Produkten verwendeten integrierten Audio-Konferenzen und Single- und Multi-Point-Videokonferenzen, wie:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- 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-Applikationen und Services.

WebEx Meeting-Rollen

Die vier Hauptrollen in einem WebEx-Meeting sind die Rollen Gastgeber, anderer Gastgeber, Moderator und Teilnehmer.

Gastgeber

Der Gastgeber setzt WebEx-Meetings an und startet sie. Der Gastgeber kontrolliert die Meetinggestaltung und kann – als der anfängliche Moderator – Teilnehmern Moderatorprivilegien verleihen. Der Gastgeber kann den Audio-Konferenzteil einer Sitzung starten, ein Meeting sperren und Teilnehmer ausschließen.

Alternativer Gastgeber

Der Gastgeber ernennt einen anderen Gastgeber. Der andere Gastgeber kann anstelle des Gastgebers ein angesetztes WebEx-Meeting starten. Der andere Gastgeber verfügt über dieselben Privilegien wie der Gastgeber und kann das Meeting kontrollieren, wenn der Gastgeber nicht zur Verfügung steht.

Moderator

Ein Moderator teilt Präsentationen, bestimmte Anwendungen oder den gesamten Desktop. Der Moderator steuert die Kommentar-Tools und kann einzelnen Teilnehmern die Fernsteuerung geteilter Anwendungen und des Desktops ermöglichen, ihnen diese Rechte allerdings auch wieder entziehen.

Teilnehmer

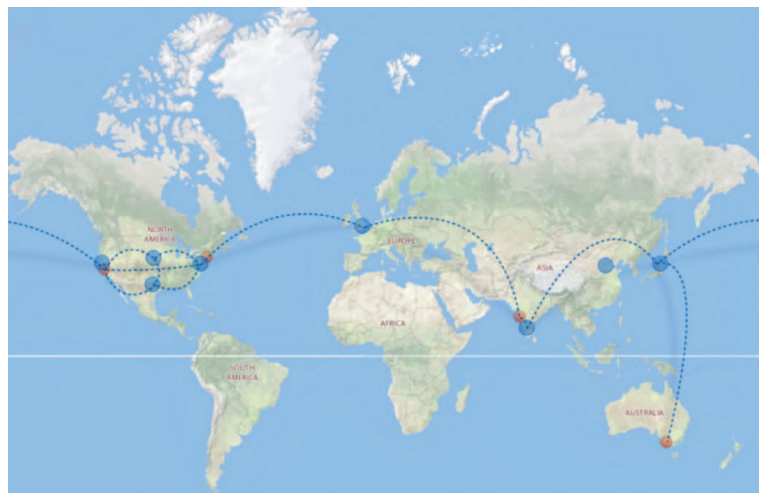
Die Verantwortung von Teilnehmern ist minimal und beschränkt sich normalerweise auf das Verfolgen der Sitzungsinhalte.

Infrastruktur der Cisco Collaboration Cloud

Die Cisco Collaboration Cloud ist eine Kommunikationsinfrastruktur, die speziell zur Echtzeitkommunikation über das Internet ausgelegt wurde. Strategisch in der Nähe wichtiger Internet-Zugangspunkte angesiedelte Datenzentren verwenden dedizierte Glasfaserleitungen mit hoher Bandbreite, um den Datenverkehr um die ganze Welt zu leiten.

Switch-Architektur

Cisco verwendet ein einzigartiges, global verteiltes und dediziertes Netzwerk aus Hochgeschwindigkeits-Meeting-Switches. Daten einer Meeting-Sitzung, die von dem Computer des Moderators versandt werden und auf den Computern der Teilnehmer eintreffen, werden von der Cisco Collaboration Cloud weitervermittelt – aber niemals dauerhaft gespeichert. Die Cisco Collaboration Cloud ermöglicht eine sichere, extrem skalierbare und hochverfügbare Meeting-Infrastruktur.



Rechenzentren

WebEx-Meeting-Sitzungen verwenden eine Switch-Ausrüstung, die auf eine Vielzahl von Datenzentren auf der ganzen Welt verteilt ist. Cisco ist der Eigentümer und Betreiber der gesamten im Rahmen der Cisco Collaboration Cloud genutzten Infrastruktur. Dieses Netzwerk besteht zurzeit aus Rechenzentren in Mountain View, Kalifornien;Thornton, Colorado;Richardson, Texas;Ashburn, Virginia;London, Großbritannien;Bangalore, Indien;Peking, China;und Tokio, Japan. Zusätzlich betreibt Cisco vier iPoPs (Knotenpunkte im Datennetzwerk), die Backbone-Verbindungen, Internet Peering und Caching-Technologien erleichtern, die für verbesserte Leistung und Verfügbarkeit beim Endnutzer eingesetzt werden. Die iPoPs befinden sich in San Jose, Kalifornien;New York City, NY;Mumbai, Indien;und Melbourne, Australien. Mitarbeiter von Cisco sind rund um die Uhr verfügbar, um die erforderliche logistische Sicherheit zu gewährleisten und Betrieb und Change Management zu unterstützen.

Sichere WebEx-Meetings

Konfiguration der WebEx-Meeting-Site

Das Modul WebEx Site Administration verwaltet und implementiert die Sicherheitsrichtlinien für Ihre angepasste WebEx-Site. Die auf dieser Ebene kontrollierten Einstellungen legen die Gastgeber- und Moderatorprivilegien zum Ansetzen von Meetings fest. So können Sie beispielsweise einem Moderator die Fähigkeit nehmen, Applikationen zu teilen, oder Sie können die Übertragung von Dateien auf eine bestimmte Anzahl pro Site oder pro Nutzer beschränken, indem Sie die Sitzungskonfiguration so anpassen, dass sie Ihren Geschäftszielen und Sicherheitsanforderungen entspricht. Das Modul WebEx Site Administration verwaltet folgende sicherheitsbezogene Funktionen:

Account-Management

- Einen Account nach einer konfigurierbaren Anzahl fehlgeschlagener Login-Versuche sperren.
- Einen gesperrten Account nach Ablauf einer bestimmten Zeit automatisch wieder entsperren.
- Accounts nach einer bestimmten Zeit der Inaktivität deaktivieren.

Account-Management-Aktionen für einzelne Nutzer-Accounts

- Einen Nutzer auffordern, beim nächsten Login das Passwort zu ändern.
- Einen Nutzer-Account sperren oder entsperren.
- Einen Nutzer-Account aktivieren oder deaktivieren.

Account-Erstellung

- Eine E-Mail-Bestätigung für neue Accounts verlangen.
- Einen Sicherheitstext für neue Account-Anfragen verlangen.
- Eine Selbstregistrierung (Sign-Up) für neue Accounts zulassen.
- Regeln zur Selbstregistrierung für neue Accounts konfigurieren.

Account-Passwörter

- Strenge Account-Passwortkriterien erzwingen.
- Die Anzahl von Tagen bis zum Ablauf eines vorläufigen Passworts konfigurieren.
- Gastgeber auffordern, die Account-Passwörter in konfigurierbaren Abständen zu ändern.
- Gastgeber auffordern, das Account-Passwort beim nächsten Login zu ändern.

Sichere Account-Passwortkriterien

- Mindestlänge.
- Groß- und Kleinschreibung
- Mindestanzahl an Ziffern.
- Mindestanzahl an Buchstaben.
- Mindestanzahl an Sonderzeichen.
- Nicht zulassen, dass ein Zeichen mehr als dreimal hintereinander verwendet wird.
- Die Wiederverwendung einer bestimmten Zahl früherer Passwörter nicht zulassen.
- Dynamischen Text nicht zulassen (Sitename, Gastgebername, Nutzername).
- Passwörter aus einer konfigurierbaren Liste nicht zulassen (z. B. „Passwort“).
- Mindestintervall für Passwortänderung.

Sichere Meeting-Passwortkriterien

- Für alle Meetings Passwörter vorschreiben.
- Mindestlänge.
- Groß- und Kleinschreibung
- Mindestanzahl an Ziffern.
- Mindestanzahl an Buchstaben.
- Mindestanzahl an Sonderzeichen.
- Nicht zulassen, dass ein Zeichen mehr als dreimal hintereinander verwendet wird.
- Dynamischen Text nicht zulassen (Sitename, Gastgebername, Nutzername, Meeting-Thema).
- Passwörter aus einer konfigurierbaren Liste nicht zulassen (z. B. „Passwort“).

Persönliche Meeting-Fenster – zugänglich über eine personalisierte URL und ein Passwort – helfen dem Gastgeber, angesetzte und laufende Meetings aufzulisten, Meetings zu starten, ihnen beizutreten und Dateien mit Meeting-Teilnehmern zu teilen. Sie können die Site Administration auch dazu verwenden, sicherheitsbezogene Funktionen für persönliche Meeting-Fenster festzulegen.

- Die URL des persönlichen Meeting-Fensters ändern.
- Die Optionen zum Teilen von Dateien im persönlichen Meeting-Fenster konfigurieren.
- Die Passwortanforderungen für Dateien im persönlichen Meeting-Fenster konfigurieren.

Weitere sicherheitsbezogene Funktionen werden über die WebEx Site Administration aktiviert.

- Einem Gastgeber oder Teilnehmer erlauben, Namen und E-Mail-Adresse zu speichern, oder das Beitreten von aufeinanderfolgenden Meetings erleichtern.
- Einem Gastgeber die Neuzuweisung von Aufzeichnungen an andere Gastgeber erlauben.
- Eingeschränkter Site-Zugang – der Site-Administrator kann für jeden Gastgeber- und Teilnehmerzugriff eine Authentifizierung verlangen. Sogar zum Zugreifen auf Site-Informationen – z.B. aufgelistete Meetings – ist eine Authentifizierung erforderlich, ebenso wie für den Zugang zu Meetings auf der Site.
- Strenge Meeting-Passwörter für Cisco WebEx Remote Access-Sitzungen verlangen.
- Die Entfernung aller Meetings aus der Liste verlangen.

Sie können außerdem weitere Konfigurierungen bei Ihrem WebEx Customer Success-Händler anfordern.

- Genehmigung für " Passwort vergessen? " einfordern.
- Den Site-Administrator auffordern, Account-Passwörter zurückzusetzen, anstatt sie für den Nutzer neu einzugeben.
- Passwörter mit dem One-Way-Hash-Verfahren speichern

Sicherheitsoptionen beim Ansetzen von Meetings

Erteilen Sie einzelnen Gastgebern die Möglichkeit, die Sicherheit für den Meeting-Zugang festzulegen, und zwar innerhalb der auf Site-Administrator-Ebene festgelegten Parameter, die nicht außer Kraft gesetzt werden können.

- Ein Meeting als ungelistet ansetzen, so dass es nicht auf dem sichtbaren Kalender angezeigt wird.
- Teilnehmern erlauben, dem Meeting vor dem Gastgeber beizutreten.
- Teilnehmern erlauben, dem Audioteil vor dem Gastgeber beizutreten.
- Während des Meetings Telefonkonferenz-Informationen anzeigen.
- Meetings nach einer konfigurierbaren Zeit automatisch beenden, wenn nur noch ein Teilnehmer anwesend ist.
- Den Gastgeber-Schlüssel in die Meeting-E-Mails einfügen.
- Teilnehmer auffordern, beim Beitreten zum einem Meeting ihre E-Mail-Adresse einzugeben.

Gelistete oder nicht gelistete Meetings

Gastgeber können entscheiden, ein Meeting auf dem öffentlichen Meeting-Kalender auf Ihrer angepassten WebEx-Site aufzuführen. Sie können das Meeting aber auch ohne Auflistung ansetzen, so dass es niemals auf dem Meeting-Kalender erscheint. Bei nicht gelisteten Meetings muss der Gastgeber die Teilnehmer ausdrücklich von der Existenz des Meetings unterrichten – entweder über einen Link, der den Teilnehmern im Verlauf des E-Mail-Einladungsprozesses zugesandt wird, oder indem die Teilnehmer aufgefordert werden, auf der Seite „Meeting beitreten“ die angegebene Meeting-Nummer einzugeben.

Interne oder externe Meetings

Gastgeber können die Teilnehmer eines Meetings auf Personen mit einem Account auf Ihrer angepassten WebEx-Site beschränken, die sich dadurch ausweisen, dass sie dazu in der Lage sind, sich bei der Site anzumelden, um dem Meeting beizutreten.

Meeting-Passwörter

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

Einschreibung

- Meeting-Zugang mit der Anmeldungsfunktion einschränken. Der Gastgeber erzeugt eine „Zugangskontrollliste“, die das Beitreten nur Eingeladenen erlaubt, die sich angemeldet und vom Gastgeber ausdrücklich genehmigt wurden.
- Mehr Kontrolle über die Verbreitung von Informationen zum Meeting-Zugang durch die Option, keine E-Mail-Einladungen für ein Meeting zu verschicken.
- Meetings durch Blockieren der Wiederverwendung von Registrierungs-IDs sichern – in den WBS27-Versionen von WebEx Training Center und WebEx Event Center. Ein Teilnehmer, der versucht, eine bereits verwendete Registrierungs-ID wiederzuverwenden, wird daran gehindert, dem Meeting beizutreten.

Außerdem kann der Gastgeber die Meeting-Sicherheit durch eingeschränkten Zugriff und das Ausschließen von Teilnehmern gewährleisten.

Durch beliebiges Kombinieren dieser Ansetzoptionen können Sie eine Feinabstimmung Ihrer WebEx-Meetings erreichen und so Ihre Sicherheitsrichtlinien erfüllen.

Start und Beitritt zu einem WebEx-Meeting

Ein WebEx-Meeting startet, wenn die Nutzer-ID und das Passwort eines Gastgebers von Ihrer angepassten WebEx-Site authentifiziert wurden. Die Kontrolle über das Meeting liegt zunächst beim Gastgeber, der gleichzeitig auch erster Moderator ist. Der Gastgeber kann jedem beliebigen Teilnehmer Gastgeber- oder Moderatorenrechte erteilen oder entziehen, ausgewählte Teilnehmer ausschließen oder die Sitzung jederzeit beenden.

Der Gastgeber kann einen anderen Gastgeber ernennen, der das Meeting startet und kontrolliert, falls der Gastgeber selbst nicht teilnehmen kann oder seine Verbindung zum Meeting unterbrochen wird. Die Gastgeberrolle wird einem nicht erwarteten oder nicht autorisierten Teilnehmer zugewiesen.

Sie können Ihre WebEx-Site so konfigurieren, dass Teilnehmer dem Meeting – einschließlich dem Audioteil – vor dem Gastgeber beitreten können, wobei sich die verfügbaren Funktionen für Frühteilnehmer auf Chat und Audio beschränken lassen.

Wenn ein Teilnehmer zum ersten Mal einem WebEx-Meeting beitrifft, lädt die WebEx-Applikation automatisch einen vollständigen Dateisatz auf den Computer des Teilnehmers herunter. VeriSign stellt Sicherheitszertifikate mit digitaler Signatur für diese Downloads aus, damit der Teilnehmer weiß, dass sie von WebEx kommen. In anschließenden Meetings lädt die WebEx-Applikation nur Dateien herunter, die Änderungen oder Updates enthalten. Teilnehmer können die Deinstallationsfunktion ihres Computer-Betriebssystems nutzen, um alle WebEx-Dateien problemlos zu entfernen.

Die Cisco Collaboration Cloud schützt jede einzelne Meeting-Sitzung und die darin geteilten dynamischen Daten.

Verschlüsselungstechniken

WebEx-Meetings sind dazu ausgelegt, eine Vielzahl von Medieninhalten in Echtzeit sicher für die einzelnen Teilnehmer einer WebEx-Meeting-Sitzung bereitzustellen. Wenn ein Moderator ein Dokument oder eine Präsentation teilt, werden die zu teilenden Daten im Universal Communications Format (UCF), einer Cisco-eigenen Technik, codiert und optimiert. Die WebEx Meeting-Applikation auf mobilen Geräten (wie iPad, iPhone und BlackBerry) verwendet ähnliche Verschlüsselungsmechanismen wie der PC-Client.

WebEx-Meetings bietet folgende Verschlüsselungsmechanismen:

1. Die Daten für WebEx-Meetings auf PCs oder mobilen Geräten werden vom Client zur Cisco Collaboration Cloud mittels der Secure Socket Layer-Version 3 (SSLv3) mit 128 Bit übermittelt.
2. Dokumente und Präsentationen werden vor der Übermittlung vom Anfang bis zum Ende mit 256-Bit-AES (Advanced Encryption Standard) verschlüsselt.
3. Die E2E-Verschlüsselung von Ende bis Ende (End-to-End, E2E) ist eine Option, die ab Cisco WebEx Meeting Center Version WBS26 zur Verfügung steht. Dieses Verfahren verschlüsselt den gesamten Meeting-Inhalt von Ende bis Ende (E2E) zwischen den Teilnehmern mit Hilfe des Verschlüsselungsstandards AES mit einem 256-Bit-Schlüssel, der zufällig auf dem Computer des Gastgebers erzeugt und über einen Public-Key-basierten Mechanismus an die Teilnehmer übermittelt wird.
4. Die End-to-End-Verschlüsselung auf PKI- (Public Key Infrastructure)-Basis ist eine Option, die den Verschlüsselungsstandard 256-Bit-AES verwendet und ab WebEx Meeting Center Version WBS27 zur Verfügung steht. Bei diesem Mechanismus müssen die Teilnehmer über ein X.509-Zertifikat verfügen, um ein Meeting zu starten oder ihm beizutreten.
5. Das Anmelde-Passwort des Nutzers für WebEx-Meetings auf mobilen Geräten wird mit dem Data Encryption Standard (DES) mit einem 128-Bit-Schlüssel verschlüsselt.

Die Site-Administratoren und Gastgeber können unter der Option „Meeting-Typ“ zwischen E2E und PKI auswählen. E2E- und PKI-Lösungen bieten einen größeren Schutz als AES allein (obwohl E2E und PKI zur Verschlüsselung der Datenmasse ebenfalls AES benutzen), da der Schlüssel nur dem Meeting-Gastgeber und den Teilnehmern bekannt ist.

Jede WebEx-Meeting-Verbindung muss richtig authentifiziert sein, bevor zum Beitritt zu einem Meeting eine Verbindung mit der Cisco Collaboration Cloud hergestellt wird. Der Client-Authentifizierungsprozess verwendet ein eindeutiges, client- und sitzungsspezifisches Cookie, um die Identität der einzelnen Teilnehmer zu bestätigen, die einer WebEx-Sitzung beizutreten versuchen. Jedes Meeting enthält einen besonderen Satz aus Sitzungsparametern, die von der Cisco Collaboration Cloud erzeugt werden. Alle authentifizierten Teilnehmer müssen sowohl auf diese Sitzungsparameter als auch auf das spezielle Sitzungscookie zugreifen können, um dem Meeting erfolgreich beizutreten.

Sicherheit der Transportschicht

Zusätzlich zu den Sicherheitsmechanismen für die Anwendungsschicht werden alle Meeting-Daten mittels 128-Bit-SSLv3 übertragen. Anstatt die Firewall über den Firewall-Port 80 (Standard-HTTP-Internetverkehr) zu durchtreten, verwendet SSL den Firewall-Port 443 (HTTPS-Verkehr) und schränkt den Zugang über Port 80 ein, ohne den WebEx-Verkehr dadurch zu behindern.

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

Firewall-Kompatibilität

Die WebEx Meeting-Applikation kommuniziert mit der Cisco Collaboration Cloud, um über HTTPS (Port 443) eine zuverlässige und sichere Verbindung herzustellen, damit Ihre Firewalls nicht speziell für die Durchführung von WebEx-Meetings konfiguriert zu werden müssen.

Datenspeicherung nach Meeting-Abschluss

In der Cisco Collaboration Cloud oder auf Computern der Teilnehmer bleiben nach Abschluss des WebEx-Meetings keinerlei Sitzungsdaten zurück. Cisco speichert nur zwei Arten von Informationen über das Meeting.

- **Ereignisdetaillaufzeichnungen (Event Detail Records, EDRs):** Cisco verwendet die EDRs zu Abrechnungs- und Berichtszwecken. Sie können die Ereignisdetaillaufzeichnungen auf Ihrer angepassten WebEx-Site unter Verwendung Ihrer Gastgeber-ID einsehen. Nach erfolgreicher Authentifizierung können Sie diese Daten auch von Ihrer WebEx-Site herunterladen oder über die WebEx APIs auf sie zugreifen.
- **Netzwerkbasierter Aufzeichnungsdateien (NBR):** Wenn ein Gastgeber eine WebEx-Meeting-Sitzung aufzeichnen möchte, wird die Aufzeichnung in der Cisco Collaboration Cloud gespeichert und kann über den Bereich „My Recordings“ Ihrer angepassten WebEx-Site abgerufen werden

Einzelanmeldung

Cisco unterstützt die föderierte Authentifizierung für den Single Sign On (SSO) durch den Nutzer unter Verwendung der Protokolle SAML 1.1, 2.0 und WS-Fed 1.0. Zur Nutzung der föderierten Authentifizierung müssen Sie ein Public-Key-X.509-Zertifikat auf Ihre angepasste WebEx-Site laden. Sie können dann SAML-Aussagen mit Nutzerattributen erzeugen und die Aussagen mit dem passenden Private Key mit einer digitalen Signatur versehen. WebEx gleicht die SAML-Aussagensignatur mit dem vorgeladenen Public-Key-Zertifikat ab, bevor der Nutzer authentifiziert wird.

Prüfberichte von Dritten

Über seine eigenen strikten internen Prozesse hinaus beauftragt das WebEx Office of Security zahlreiche unabhängige Dritte mit der Durchführung rigoroser Prüfungen auf der Basis interner Richtlinien, Vorgänge und Applikationen. Diese Prüfungen sollen die missionskritischen Sicherheitsanforderungen sowohl für gewerbliche als auch behördliche Anwendungen überprüfen.

Zu diesen Prüfinstituten gehören Information Security Partners und LLC (iSec Partners). Sie prüfen das Netzwerk-Routing und die Applikation eingehend. PriceWaterhouseCoopers prüft zudem gemäß SAS-70 Typ II.

iSEC Netzwerk-Routing

iSEC Partners führte eine Reihe von Tests durch, um das Routing zu und von den WebEx-Meeting-Teilnehmern und der Cisco Collaboration Cloud zu überprüfen. Bei den Tests wurden sowohl Spuren von WebEx-Produktionsservern als auch Spuren bei der Weiterleitung für verschiedene Netzwerkgerätekonfigurationen wie Router, Firewalls und Lastverteiler untersucht. Die Ergebnisse dieser Tests zeigen, dass die Kommunikation bei in den USA gehosteten WebEx-Sites nicht außerhalb der USA geroutet wird. Zur weiteren Information können Sie beim WebEx Office of Security eine Ausfertigung dieses Berichts anfordern.

iSEC Quellcodeprüfung

iSEC Partners führt laufend, gründliche Code-gestützte Sicherheitsüberprüfungen aus der Perspektive eines Angreifers sowie Serviceanalysen durch. Dabei erhält iSEC Partners sowohl Zugang zu WebEx-Servern als auch zum Quellcode und steht mit unseren Technikern in Kontakt. Anders als bei Black-Box-Tests ermöglicht diese hohe Zugänglichkeit iSEC Partners Folgendes:

- Ermitteln bedenklicher Anwendungen und/oder Serviceschwachstellen und Unterbreitung entsprechender Lösungen.
- Aufzeigen allgemeiner Bereiche zur Verbesserung in der Architektur.
- Identifizieren von Codierungsfehlern und Anleitung zu einer besseren Codierungspraxis.
- Direkte Zusammenarbeit mit WebEx-Technikern, um Ergebnisse zu erläutern, und Unterbreitung von Richtlinien zur Korrektur der Defizite.

Zur weiteren Information können Sie beim WebEx Office of Security eine Ausfertigung dieses Berichts anfordern.

SAS-70 Type II

PriceWaterhouseCoopers LLP führt eine jährliche SAS-70 Typ II-Prüfung durch, die den von der AICPA aufgestellten Normen entspricht. Weitere Informationen zur SAS-70-Norm finden Sie hier: www.sas70.com/index2.htm. Zur weiteren Information können Sie über Ihren Cisco-Kundenbeauftragten eine Ausfertigung des SAS-70-Berichts von PriceWaterhouseCoopers beim WebEx Office of Security anfordern.

ISO-27001/2

Die SAS70-Prüfungen wurden von Cisco erstellt, um den Datensicherheitsprüfungen gemäß ISO-27002, die im Anhang zu ISO-27001 aufgeführt sind, Genüge zu tun. ISO-27001 ist ein internationaler Datensicherheitsstandard der International Organization of Standardization (ISO), der Empfehlungen und bewährte Verfahren für ein Informationssicherheits-Managementsystem (ISMS) beinhaltet. Ein ISMS ist ein Gerüst aus Richtlinien und Verfahren, die sämtliche gesetzlichen, physischen und technischen Kontrollen enthalten, die in die Managementprozesse bezüglich Informationsrisiken in einem Unternehmen einfließen. Laut 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-27001/2 finden Sie unter: <http://www.27000.org/>

Schlussbemerkung

Bei der Kollaboration und der Rationalisierung der Geschäftsabläufe kann Ihre Organisation auf Cisco WebEx-Online-Applikationen vertrauen – auch in Umgebungen mit strengsten Sicherheitsanforderungen. Entscheiden Sie sich für die einfach zu bedienenden, zuverlässigen, bewährten und sicheren Software-as-a-Service-Kollaborationslösungen von Cisco WebEx.

