BlueJeans

TECHNISCHER LEITFADEN

BlueJeans Network Sicherheit und Datenschutz

Wir von BlueJeans wissen, dass moderne Unternehmen auf sichere digitale Kommunikation angewiesen sind. Deshalb verfügt die Plattform von BlueJeans über alle grundlegenden Sicherheitsmaßnahmen eines Videokonferenzservice der Enterprise-Klasse.

INHALTSVERZEICHNIS

Einhaltung der Datenschutz-Grundverordnung (DSGVO)

Sicherheit in unseren weltweit verteilten Rechenzentren

Die BlueJeans-Services basieren auf Software, die von Grund auf von den Experten von BlueJeans entwickelt wurde und auf den für Cloud-Computing ausgelegten Servern eines weltweit führenden Anbieters läuft. Dabei sind die für die Servicebereitstellung genutzten Servercluster auf verschiedene, nach ISO27001 zertifizierte Co-Location-Rechenzentren der Spitzenklasse verteilt. Dort werden unsere dedizierten Server-Cages und Racks rund um die Uhr überwacht und sind durch mehrstufige biometrische Zugangskontrollen geschützt. Der Zugang zu den Cages ist nur den für den Servicebetrieb zuständigen BlueJeans-Mitarbeitern gestattet.

Schutzmaßnahmen in Infrastruktur und Netzwerk

BlueJeans hat vielfältige Sicherheitsmaßnahmen implementiert, um Kunden sichere und zuverlässige Services bereitstellen zu können. Dazu zählen unter anderem Firewalls in der gesamten Netzwerkinfrastruktur, mit deren Hilfe Sicherheitszonen für verschiedene Anwendungen und Services geschaffen werden. Des Weiteren ist der Kernbereich der Bereitstellungsinfrastruktur vor externem Zugriff geschützt, da BlueJeans Proxyserver eingerichtet hat, über die der gesamte Datenaustausch mit Kunden und Drittanbietern erfolgt. Und schließlich wird der gesamte Datenverkehr in das und aus dem Internet über Load-Balancer geleitet, die Schutz vor verschiedenartigen Angriffen auf unsere Anwendungen bieten.

Neben den Firewalls, Proxyservern und Load-Balancern setzt BlueJeans auf regelmäßige Scans, um Sicherheitslücken auf der Netzwerk-, Port- und Anwendungsebene aufzudecken. Diese Schwachstellenscans werden zum einen durch einen führenden SaaS-Anbieter, zum anderen mithilfe unternehmensintern entwickelter Spezialtools durchgeführt. Darüber hinaus werden alle von Drittanbietern entwickelten Anwendungen und Betriebssysteme in regelmäßigen Abständen gepatcht und sämtliche Sicherheitshinweise der Hersteller gesichtet und überprüft.

Unsere Router, Firewalls, Load-Balancer und Proxy-Anwendungsserver sind sämtlich für die Abwehr zahlreicher Arten von DoS-Angriffen konfiguriert. Außerdem arbeitet BlueJeans mit externen Beratern zusammen, die Penetrationstests durchführen. Die Ergebnisse der Tests werden sorgfältig ausgewertet und gegebenenfalls in Maßnahmen zur Behebung der entdeckten Schwachstellen des Service umgesetzt.

Sicherheitsfeatures für Nutzer der Webanwendung

Dieser Abschnitt erläutert die Sicherheitsmaßnahmen, die auf Nutzerebene bereitgestellt werden.

Schutz von Nutzerkonten

- Alle Nutzerkonten werden mit den folgenden Technologien und Sicherheitsmaßnahmen geschützt:
- Der Zugriff auf ein BlueJeans-Konto ist nur nach Eingabe des Benutzernamens und Passworts möglich – oder vermittels einer SAML-2.0-Abfrage bei Ihrem Identity Provider.
- Die Übertragung von Authentifizierungsanfragen erfolgt stets über HTTPS.
- Passwörter werden in der Datenbank als SHA-256-Hashwerte gespeichert und können nie im Klartext eingesehen werden.
- Passwörter werden nie per E-Mail verschickt oder in anderer Weise elektronisch übertragen. (Die Funktion „Forgot Password“ – Passwort vergessen – ermöglicht lediglich das Zurücksetzen des Passworts des Nutzers.)

Sicherheitsfeatures für Konferenzteilnehmer

BlueJeans Meetings bietet optionale Sicherheitsfeatures, die von Nutzern standardmäßig verwendet oder bei Bedarf genutzt werden können.

Meeting-ID

Hierbei handelt es sich um eine zufällig generierte, neunstellige Nummer zur eindeutigen Identifizierung einer Konferenz.

Teilnehmer-PIN

Diese PINs stellen einen optionalen zweiten Authentifizierungsschritt dar, mit dem sich Konferenzen zusätzlich schützen lassen.

Meeting veröffentlichen

Die Deaktivierung dieser Option sorgt dafür, dass das entsprechende Meeting nicht im öffentlich zugänglichen Teil des Nutzerprofils angezeigt wird. Die Einwahl in eine derartige Konferenz ist nur per Klick auf den entsprechenden Link in der Einladungs-E-Mail oder über die Homepage bluejeans.com – durch Eingabe der Meeting-ID und/oder des Passworts – möglich.

Meeting verschlüsseln

Bei Auswahl dieser Option ist die Teilnahme an der BlueJeans-Konferenz nur über Endpunkte möglich, die über ausreichende Verschlüsselungsfunktionen verfügen. Weitere Informationen zum Thema Verschlüsselung finden Sie im Abschnitt „Verschlüsselung der digitalen Kommunikation“.

Teilnehmer ausschließen

Im Verlauf einer Konferenz kann der Organisator oder Moderator jeden beliebigen Teilnehmer per Klick auf den Button „Expel Participant“ aus dem Meeting entfernen.

Meeting sperren

Eine Konferenz kann zu jedem beliebigen Zeitpunkt für neue Teilnehmer gesperrt werden, sodass die bereits eingewählten Nutzer unter sich bleiben.

Sicherheit auf Administratorebene

Sicherheitsfeatures für Gruppenadministratoren

Als Gruppenadministrator können Sie in BlueJeans Sicherheitsmaßnahmen für sämtliche Nutzer aus Ihrem Unternehmen festlegen. Im Einzelnen stehen Ihnen Konfigurationsoptionen für folgende Sicherheitsfeatures zur Verfügung:

- Anmeldeverfahren für Nutzer (Passworteingabe oder SAML Single-Sign-On)
- Anforderungen an Nutzerpasswörter
- Verfahren für Passwortänderungen
- Benachrichtigungen über fehlgeschlagene Anmeldeversuche
- Zulässige Arten von Videoverbindungen (unterstützte Geräte und Standard-Endpunkte für Ihre Gruppe)

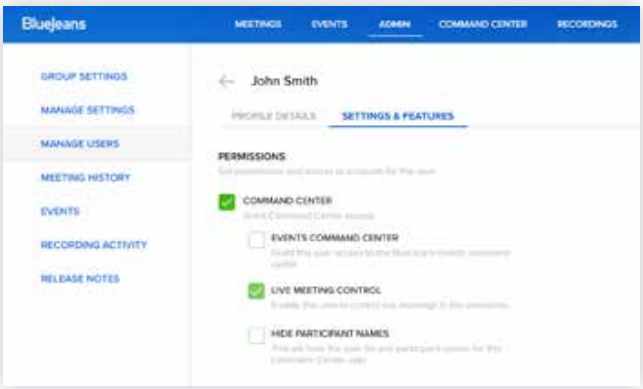
Darüber hinaus bietet BlueJeans die Möglichkeit, personenbezogene Daten (wie die Namen und IP-Adressen der Teilnehmer) in der Konsole des Command Centers zu maskieren. Auf diese Weise können IT-Mitarbeiter Konferenzen überwachen und bei auftretenden Problemen Unterstützung bereitstellen, ohne dass dadurch die Datenschutzrechte der Teilnehmer beeinträchtigt werden.

Moderation ohne Einwahl mit Live Meeting Control

Grundsätzlich verfügen Gruppenadministratoren über zwei verschiedene Möglichkeiten, Meetings zu moderieren und technischen Support bereitzustellen:

- Im Meeting: durch die Einwahl in die Konferenz
- Im Hintergrund: Meetings können in Echtzeit über die „Live Meeting Control“-Konsole des Command Center verwaltet werden. Dort stehen Funktionen für die Aktivierung bzw. Deaktivierung der Mikrofone der Teilnehmer, die Sperrung der Konferenz und die Festlegung eines verbindlichen Bildschirm-Layouts für alle Teilnehmer zur Verfügung.

Diese Art der Moderation eignet sich ideal für Konferenzen, bei denen die Vertraulichkeit sensibler Gespräche und Dokumente sichergestellt werden muss. Live Meeting Control wird zunächst für das Kundenunternehmen aktiviert und kann dann von den Verantwortlichen für bestimmte Administratoren freigegeben werden. Auf diese Weise lässt sich der Einsatz der leistungsstarken Konsole vollständig kontrollieren.



Datenschutz und Speicherung von Kundendaten

In der BlueJeans-Datenbank werden nur grundlegende Nutzerdaten aufbewahrt. Im Einzelnen speichert BlueJeans folgende nutzerbezogenen Daten:

Angaben aus dem Nutzerprofil

- Nutzername (ein Facebook-Login enthält den Facebook-Nutzernamen, ein LinkedIn-Login die Profil-URL des Nutzers)
- Passwort (als SHA-256-Hashwert)
- E-Mail-Adresse
- Vorname
- Zweiter Vorname
- Nachname
- Position
- Name des Unternehmens
- Profilbild

Rechnungsdaten

Die gesamte Abrechnung für die Nutzung des Service wird gegenwärtig von einem PCI-konformen Drittanbieter im Auftrag von BlueJeans erledigt. Das bedeutet, dass keinerlei Kreditkarten- oder Rechnungsdaten von Kunden in der BlueJeans-Datenbank gespeichert werden. Da unser Service von Tausenden Unternehmen aus aller Welt genutzt wird, achtet BlueJeans außerdem auf die Einhaltung des EU-U.S. Privacy Shield Frameworks.

Weitere Informationen zu diesem Thema finden Sie in der Datenschutzerklärung von BlueJeans unter: http://bluejeans.com/privacy-policy

Verschlüsselung der digitalen Kommunikation

Bei BlueJeans nehmen wir die Vertraulichkeit Ihrer Inhalte sehr ernst. Deshalb zeichnen wir keinerlei Videostreams oder freigegebene Bildschirminhalte auf, ohne dies vorab mit Ihnen zu besprechen und Ihr Einverständnis einzuholen. Zusätzlich empfehlen wir Kundenunternehmen, geeignete Maßnahmen für den Schutz der Endgeräte zu ergreifen, auf denen die softwarebasierten Videoclients installiert sind, damit Lauschangriffe auf Hardwareebene ausgeschlossen werden können. In diesem Zusammenhang ist zu betonen, dass BlueJeans den Verschlüsselungsstandard AES-128 unterstützt, der mittlerweile für die meisten Videoendpunkte verfügbar ist.

In BlueJeans-Konferenzen sind Videoverbindungen, die über BlueJeans-Clients oder Webbrowser hergestellt werden, standardmäßig verschlüsselt. Gleiches gilt für viele andere gängige Lösungen wie Cisco Jabber oder Microsoft Lync.

Wenn die Teilnahme an einer BlueJeans-Konferenz über ein Raumsysteme von Polycom, Lifesize, Cisco oder einem anderen Anbieter erfolgt, wird die Verbindung beim Aufbau verschlüsselt – unter der Voraussetzung, dass der Anbieter des Raumsystems dies unterstützt und die Teilnehmer die nötigen Sicherheitslizenzen von diesem Anbieter erworben haben.

Die meisten Raumsysteme verschlüsseln Videostreams standardmäßig, sofern dies von allen verbundenen Endpunkten unterstützt wird. Trotzdem ist es empfehlenswert, die Standardeinstellungen Ihres Systems so zu konfigurieren, dass alle Anrufe und Konferenzen immer verschlüsselt werden und Verbindungen nur unter dieser Voraussetzung hergestellt werden können. Wie bereits im Abschnitt „Sicherheitsfunktionen für Konferenzteilnehmer“ erwähnt, können Sie mithilfe der Option „Enforce Encryption“ (Verschlüsselung erzwingen) festlegen, dass die Einwahl in das von Ihnen anberaumte Meeting nur von einem Endgerät aus möglich ist, das die verschlüsselte Übertragung unterstützt. Auf diese Weise können Sie dafür sorgen, dass Ihre H.323- und SIP-Raumsysteme nur standardbasierte verschlüsselte Verbindungen mit BlueJeans herstellen.

Aufzeichnung, Speicherung und Freigabe von Videos

BlueJeans bietet die einzigartige Möglichkeit, während einer Konferenz Videos hochzuladen und für andere Teilnehmer freizugeben. Außerdem können Meetings aufgezeichnet und die Aufnahmen dann ebenfalls Dritten zugänglich gemacht werden. Da uns die Sicherheit dieser beiden Features ebenso stark am Herzen liegt wie unseren Kunden, beschreiben wir die entsprechenden Schutzmaßnahmen hier etwas ausführlicher.

Aufgezeichnete Konferenzen werden in verschlüsselter Form (AES, 256 Bit) in sicheren Containern in der Cloud gespeichert und sind nur für den Nutzer zugänglich, der die Aufzeichnung veranlasst hat. Der Auftraggeber kann die Aufzeichnung dann Dritten zugänglich machen, indem er deren E-Mail-Adressen in der Webschnittstelle von BlueJeans eingibt. Die Empfänger können die Aufzeichnungen über einen Webbrowser als AES-verschlüsselten Stream (128 Bit) abrufen oder auf einen lokalen Medienserver oder ein lokales Speichergerät herunterladen. Über die webbasierte Nutzeroberfläche können die Nutzer ihre mit BlueJeans erstellten Aufzeichnungen jederzeit löschen.

Videos, die für eine Konferenz hochgeladen und für andere Teilnehmer freigegeben werden, werden ebenfalls in sicheren Containern gespeichert und können ebenfalls als AES-verschlüsselter Stream (128 Bit) abgerufen werden. Außerdem können hochgeladene Videos – genau wie Konferenzaufzeichnungen – jederzeit über die Nutzeroberfläche gelöscht werden.

Service Organization Controls (SOC) 2

Neben den Sicherheitsmaßnahmen zum Schutz unserer Serviceinfrastruktur und den Sicherheitsfunktionen, die unseren Nutzern bei Meetings zur Verfügung stehen, haben wir auch wichtige Schritte unternommen, um für die Integrität unserer BlueJeans-internen Abläufe zu sorgen.

Dazu haben wir einen SOC 2-Bericht Typ 2 gemäß SSAE16 (Statement of Standards for Attestation Engagements) erstellt. Dies ist ein wichtiger Schritt, sowohl für BlueJeans Networks als Unternehmen als auch für unsere Kunden. Mit diesem Bericht bestätigt BlueJeans seinen Kunden, dass für die Bereitstellung unserer Services unternehmensweit die offiziell dokumentierten Prozeduren und Kontrollmaßnahmen implementiert wurden.

Der Bericht enthält Angaben über Maßnahmen zur Kontrolle von Richtlinien, Kommunikationsprozessen, Betriebsabläufen und Monitoring-Aktivitäten sowie Informationen zu Disaster-Recovery-Prozessen und zur Compliance mit dem EU-U.S. Privacy Shield Framework.

Einhaltung der Datenschutz-Grundverordnung (DSGVO)

Die DSGVO dient der Vereinheitlichung der Datenschutz- und Datensicherheitsvorgaben in der gesamten Europäischen Union und schreibt den Schutz personenbezogener Daten als Grundrecht von EU-Bürgern fest. Datensicherheit und der Schutz der Nutzerdaten genießen bei BlueJeans seit jeher höchste Priorität. Um unsere Kunden bei der DSGVO-konformen Nutzung der BlueJeans-Services zu unterstützen, haben wir unsere Software, Systeme und Abläufe so angepasst, dass Unternehmen datenbezogene Anfragen von EU-Bürgern schnellstmöglich und proaktiv bearbeiten können. Außerdem haben wir strukturierte Prozesse implementiert, um auf Anfragen von Nutzern reagieren zu können, die ihre personenbezogenen Daten berichtigen, einsehen oder löschen möchten. Wir werden unsere Systeme und Prozesse auch weiterhin unter Datenschutzgesichtspunkten überprüfen, um dem Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen Vorschub zu leisten.

Wenn Sie weitere Fragen oder Bedenken hinsichtlich der Sicherheit der Services von BlueJeans Network haben, können Sie eine E-Mail an **sales@bluejeans.com** senden. Unsere Mitarbeiter helfen Ihnen gern weiter.