WHITEPAPER

DIE ARCHITEKTUR VON JOIN.ME

Die sichere und zuverlässige Architektur
von **join.me** aus technischer Sicht.

join.me

1 **EINLEITUNG**
Designgrundlagen
Definitionen

4 **ÜBERBLICK ÜBER DIE ARCHITEKTUR**
Hohe Verfügbarkeit
Redundanz

7 **FUNKTIONSWEISE**
Bildschirmfreigabe, Dateiübertragung, Chat
Telefonkonferenzen
Videokonferenzen
Aufzeichnung von Besprechungen

14 **DATENSICHERHEIT**
Sitzungs- und Website-Sicherheit

17 **ÜBERBLICK ÜBER DIE HOSTING-EINRICHTUNGEN**

18 **SCHLUSSBEMERKUNG**

Einleitung

join.me ist ein einfaches, aber gleichzeitig äußerst leistungsstarkes Tool für die Bildschirmfreigabe, welches über folgende beliebte Funktionen verfügt:

- private Besprechungen
- Bildschirmfreigabe
- Telefon-/Videokonferenzen
- Aufzeichnung von Besprechungen
- Chat (schriftliche Nachrichten)
- Senden von Dateien
- Übergeben der Moderatorenrolle an andere Teilnehmer
- Anmerkungen
- gemeinsame Maussteuerung (Fernsteuerung)
- Planen von Besprechungen
- mobiles Whiteboard

Die Komponenten von **join.me** sind mit den meisten führenden Betriebssystemen kompatibel:

- Windows
- Mac OS X
- iOS (iPhone, iPad)
- Apple Watch™
- Android

Dieses Dokument enthält technische Informationen dazu, wie **join.me** diese Dienste auf stabile und sichere Weise erbringt.

Designgrundlagen

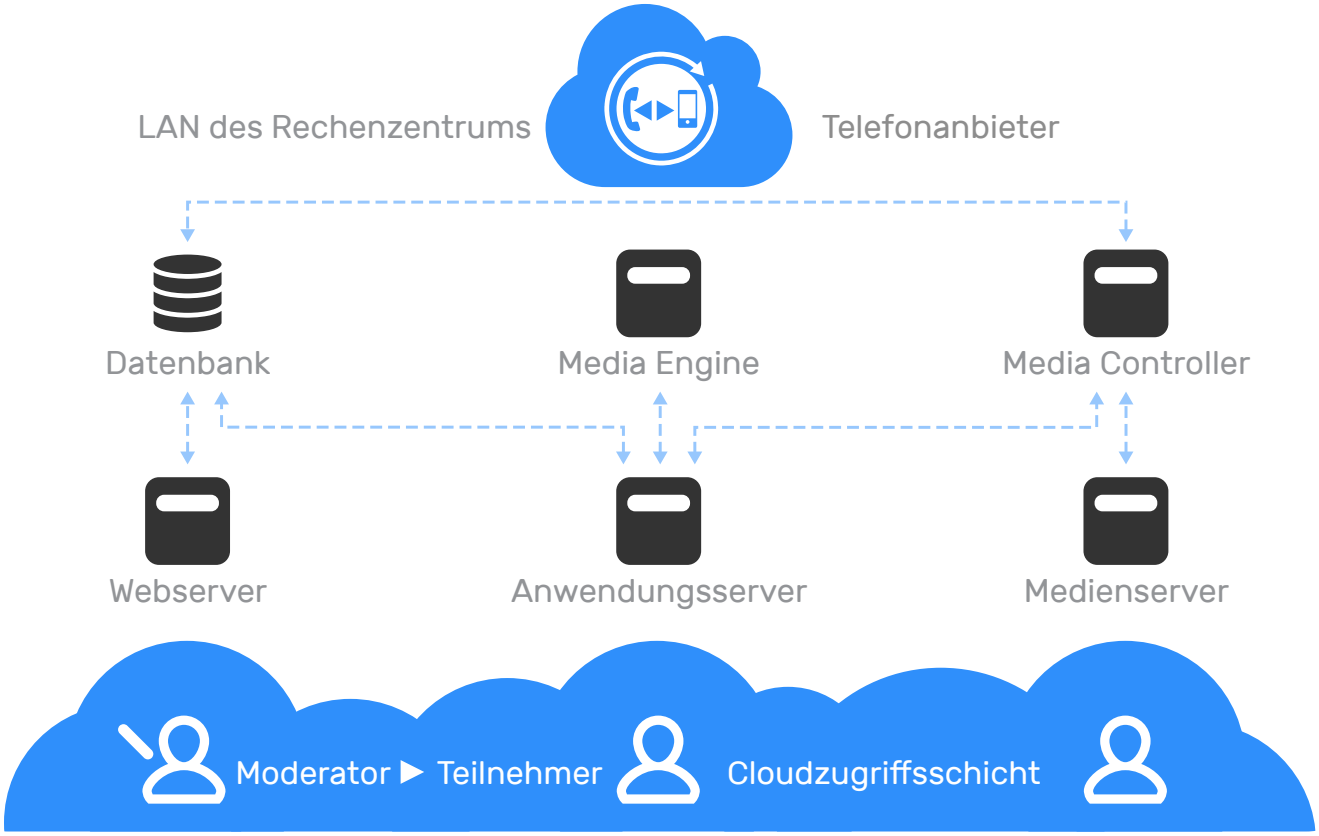
Ein einfaches und schnelles Bildschirmfreigabetool
Über die **join.me**-Website in Sekundenschnelle einsatzbereit.
Hohe Verfügbarkeit
Die Verfügbarkeit liegt bei 99,99 % oder darüber.
Hohe Sicherheit
Auf allen Ebenen kommen unter Verwendung der neuesten Sicherheitsstandards Sicherheitsmaßnahmen zum Einsatz.
Hohe Leistung und Skalierbarkeit
Die Architektur ist unbegrenzt skalierbar.
Redundanz
Es gibt keinen Single Point of Failure und die Lösung ist geografisch redundant ausgelegt.
Zukünftige Trends
Die Software baut auf den neuesten Entwicklungsmethoden und Technologien auf.

Definitionen

Moderator
Der Organisator einer Besprechung.
Präsentationssoftware
Die auf dem Gerät des Moderators ausgeführte Instanz der **join.me**-Software.
Teilnehmer (einer oder mehrere)
Teilnehmer einer Besprechung.
Anzeigesoftware
Die auf dem Gerät des Teilnehmers ausgeführte Instanz der **join.me**-Software.
Sitzungscode
Die neunstellige eindeutige Kennung der Besprechung.

Überblick über die Architektur

Eine typische **join.me**-Besprechung besteht mindestens aus folgenden Komponenten:



Webserver – Benutzerregistrierung, Konto- und Besprechungseinstellungen, Besprechungsstart

Anwendungsserver – hostet die Besprechungen, verteilt die Daten an die betreffenden Teilnehmer

Medienserver – verteilt die Medienstreams an die betreffenden Teilnehmer

Datenbank – speichert Benutzerprofile und Besprechungseinstellungen

Media Controller – steuert Mediensitzungen und Festnetzverbindungen

Media Engine – Nachbearbeitung der Medienelemente, um eine Videoaufzeichnung der Besprechung zu erstellen

Überblick über die Architektur (Fortsetzung)

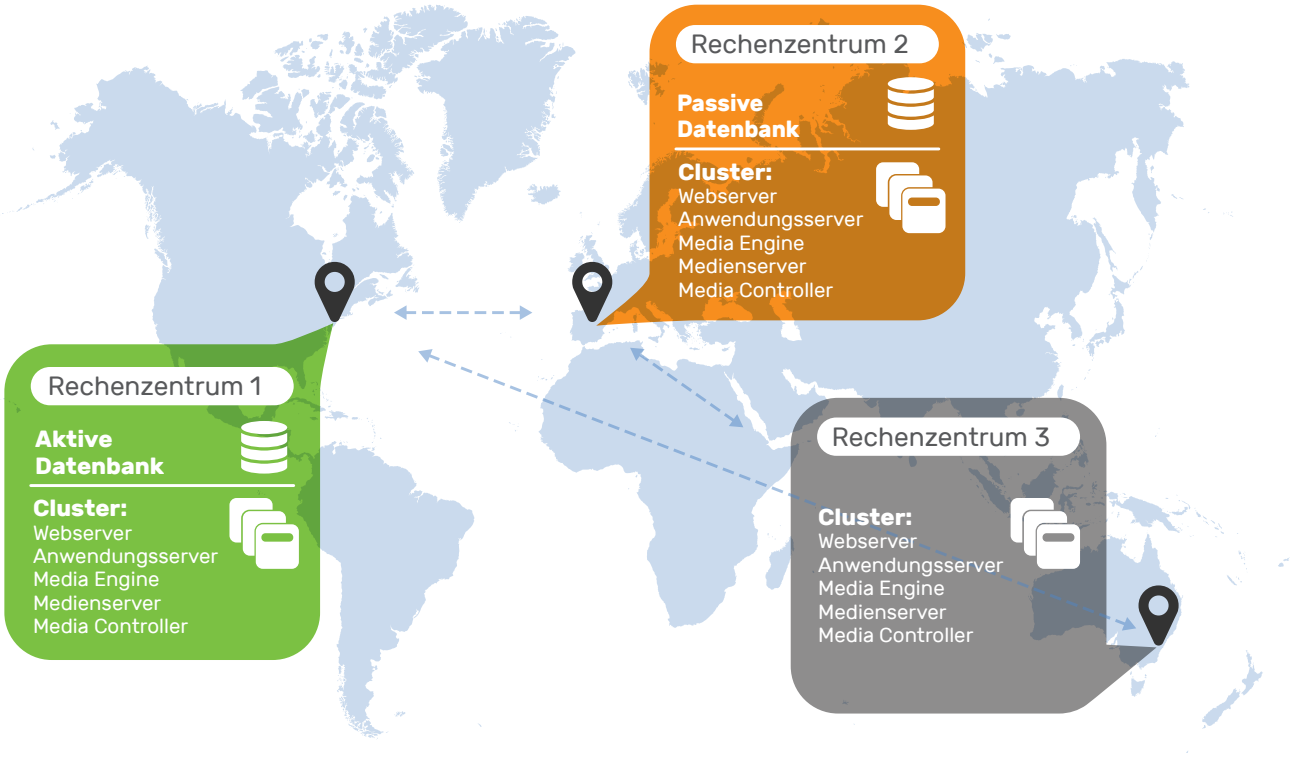
Hohe Verfügbarkeit

Zum Veröffentlichungszeitpunkt dieser Publikation waren die **join.me**-Server in **acht geografisch verteilten Rechenzentren** untergebracht.

Überblick über die Architektur (Fortsetzung)

Redundanz

Ein Blick auf die serverseitige Architektur verdeutlicht die Redundanzschichten der höchsten Ebene (siehe unten). Im Wesentlichen kann man sagen, dass die Präsentationssoftware nach dem Sitzungsaufbau über einen bestimmten Anwendungsserver mit einem oder mehreren Teilnehmern kommuniziert. Das System ist mehrschichtig redundant aufgebaut.



Die Rechenzentren sind über ein vermaschtes VPN miteinander verbunden, d. h. wenn die direkte Verbindung zwischen Rechenzentrum 1 und Rechenzentrum 2 unterbrochen würde, würde die Kommunikation stattdessen über Rechenzentrum 3 erfolgen. Die Datenübertragung zwischen den Rechenzentren ist von großer Bedeutung, da nur ein Rechenzentrum eine aktive **join.me**-Datenbank hostet. In der obigen Abbildung ist dies Rechenzentrum 1.

In einem Rechenzentrum (hier Rechenzentrum 2) befindet sich die so genannte passive Datenbank, die laufend von ihrem aktiven Gegenüber Datenbank-Transaktionsprotokolle zugeschickt bekommt. Falls es in Rechenzentrum 1 zu einem längeren Ausfall kommt, kann die passive Datenbank in Rechenzentrum 2 schnell in den aktiven Zustand versetzt werden, um den Betrieb fortzusetzen.

Server in derselben Einrichtung kommunizieren über das LAN; zwischen den Einrichtungen über das vermaschte VPN.

Die Moderatoren stellen unter Verwendung des geografischen Lastenausgleichs eine Verbindung zu einem Anwendungsserver her. Zunächst wird abhängig von der Verfügbarkeit, geografischen Nähe und

Auslastung ein Rechenzentrum ausgewählt und dann wird dem Moderator je nach Verfügbarkeit und Auslastung ein bestimmter Anwendungsserver innerhalb dieses Rechenzentrums zugewiesen.

Eine auf Anwendungsebene eingesetzte Logik stellt sicher, dass die Teilnehmer immer eine Verbindung zum selben Anwendungsserver herstellen wie der Moderator. Dies ist insofern wichtig, als dass der Anwendungsserver den Sitzungsstatus speichert (z. B. den aktuellen Bildschirminhalt des Moderators).

Sollte ein Anwendungsserver oder Rechenzentrum ausfallen oder für den Moderator nicht mehr zugänglich sein, so wird die Sitzung innerhalb von Sekunden an einen anderen Anwendungsserver übertragen. Die Nutzer nehmen nur eine kurze Unterbrechung wahr. Die Webserver innerhalb eines Rechenzentrums sind ebenfalls auswechselbar, da sie den Sitzungsstatus über einen großen Arbeitsspeicher-Cache-Cluster untereinander austauschen.

Von sämtlichen Komponenten gibt es innerhalb eines Rechenzentrums mehrere Instanzen mit einer automatisierten Ersatzschaltung (Failover), welche für die Benutzer so gut wie gar nicht wahrnehmbar ist. Bei schwerwiegenderen Problemen erfolgt ein Failover zwischen zwei Rechenzentren.

Funktionsweise

Bildschirmfreigabe, Dateiübertragung, Chat

Sitzungsablauf

Der Sitzungsablauf sieht in der Regel so aus:

Alle zwischen den Komponenten übertragenen Informationen werden über einen sicheren, verschlüsselten Kanal übermittelt. Während der Dateiübertragung und des Chats werden die Daten vom Anwendungsserver zwischen den Teilnehmern ausgetauscht; **join.me** speichert dabei keine Daten. Nähere Informationen hierzu erfahren Sie unter „Datensicherheit".

Überlegungen zur Bandbreite

Die Bildschirmfreigabe von join.me macht sich die gesamte verfügbare Bandbreite zunutze, um Latenzzeiten so weit wie möglich zu minimieren. Der **join.me**-Codec geht mit Bandbreitendifferenzen zwischen den Besprechungsteilnehmern besonders effizient um.

Während der Bildschirmfreigabe überwacht **join.me** den Bildschirminhalt. Bei jeder Aktualisierung des Bildschirms ermittelt es den kleinstmöglichen Ausschnitt mit aktualisierten Inhalten. Diese Ausschnitte werden dann an den Codec übertragen, welcher die erfasste Bitmap komprimiert und die resultierenden Daten für den Upload vorbereitet. Wenn der Bildschirm öfter aktualisiert wird als vom Netzwerk unterstützt, dann überspringt der Codec Ausschnitte, die mit späteren Aktualisierungen überlappen. Die Gründe für dieses Überspringen können eine vorübergehende Netzwerküberlastung, ein Uplink mit permanent niedriger Bandbreite oder auch zu häufige Animationen/Änderungen des Bildschirminhalts sein, mit denen selbst adäquate Netzwerkverbindungen nicht zurechtkommen. Die Bildschirmausschnitte werden an unser firmeneigenes Meetingrelay hochgeladen, welches diese dann mit Hilfe eines ähnlichen Schedulers an die Besprechungsteilnehmer verteilt.

Die Bildschirmfreigabe von **join.me** funktioniert im gesamten möglichen Spektrum der Netzwerkbedingungen ohne Aussetzer oder drastische Änderungen der Qualität. Bei extrem niedriger Bandbreite werden die Bildschirmausschnitte gegenüber dem Originalbildschirm verzögert übermittelt (bzw. empfangen, falls der Schwachpunkt auf Teilnehmerseite ist). Aufgrund der weniger häufigen Aktualisierungen verschlechtert sich die Bildschirmqualität zusehends. In diesem Fall kann es vorkommen, dass der Teilnehmer nicht kongruente Bildschirminhalte sieht, da die einzelnen Ausschnitte des Moderatorbildschirms unter Umständen zu verschiedenen Zeitpunkten erfasst wurden. Da all unsere Relays denselben Algorithmus zur Verteilung der Bildschirmausschnitte an die Teilnehmer verwenden, kann das Nutzungserlebnis bei der Bildschirmfreigabe für jeden einzelnen Teilnehmer optimiert werden.

> **Tipp:** Die tatsächlichen Bandbreitenanforderungen für eine qualitativ hochwertige Bildschirmfreigabe hängen von der Bildschirmauflösung und den freigegebenen Inhalten ab. Im Allgemeinen empfehlen wir eine Mindestbandbreite von 1 Mbit/s sowohl auf Moderator- als auch auf Teilnehmerseite, um eine ununterbrochene Vollbildanimation und gemeinsame Steuerung (wenn ein Teilnehmer den Bildschirm des Moderators fernsteuert) zu ermöglichen. Inhalte, die sich nicht häufig ändern (z. B. PowerPoint-Präsentationen), können selbst bei schwachen Verbindungen wie GPRS-Verbindungen auf zweckmäßige Weise freigegeben werden.

Für unsere Telefonkonferenzlösung verwenden wir einen Standard-VoIP-Stack mit einem hochentwickelten Codec, der eine hohe Qualität gewährleistet und nur wenig Bandbreite beansprucht. Um Qualitätsprobleme zu vermeiden, wird für die Internettelefonie (VoIP) eine kontinuierliche Bandbreite von mindestens 100 Kbit/s benötigt; vorzugsweise in Form einer stabilen Verbindung mit geringer Latenz. Bei Netzwerküberlastung kann es zu immer längeren Ausfällen der Tonübertragung kommen, bis die Verbindung wiederhergestellt wurde.

Die folgende Tabelle gibt Ihnen einen Überblick über den geschätzten Bandbreitenverbrauch in verschiedenen Szenarien.

Freigegebener Inhalt	Beispiel	Details	Bandbreite
Kleines Video	YouTube	360p-Videoclip, nur sehr geringe Fragmentierung der Bildschirmblöcke	~800 Kbit/s
Vollbildvideo		1080p-Videoclip, geringe Fragmentierung der Bildschirmblöcke	~2500 Kbit/s
Website mit verschiedenen Inhalten	Facebook	Intensives Scrollen	~800 Kbit/s
Website mit hauptsächlich Text	News-Website	Wenig Scrollen	~400 Kbit/s
Präsentation	PowerPoint	Viele Bilder, Farben, Animationen	~800 Kbit/s
Präsentation	PowerPoint	Hauptsächlich Aufzählungspunkte und einfarbiger Hintergrund	~400 Kbit/s

Tipp: Siehe auch Überlegungen zur Bandbreite bei der Videoübertragung.

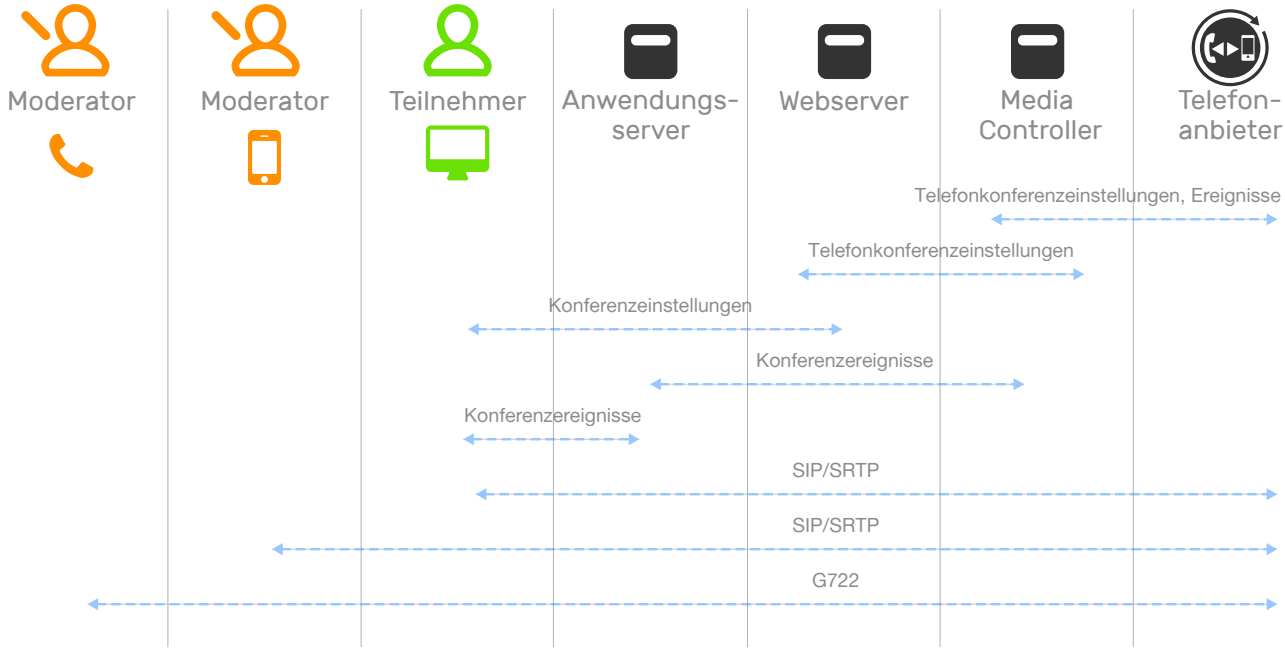
Telefonkonferenzen

join.me bietet den Benutzern mehrere Möglichkeiten zur Einwahl in eine Telefonkonferenz:

- über ein herkömmliches Festnetz- oder Mobiltelefon via Einwahlnummern in mehr als 50 Ländern
- über ein SIP-fähiges Gerät
- über die nativen **join.me**-Apps, die für die Plattformen Windows, Mac OS X, iOS und Android zum Download zur Verfügung stehen
- über die HTML5-App von **join.me**, die im Google-Chrome-Browser ausgeführt wird (kein Download erforderlich)

Funktionsweise / Telefonkonferenzen (Fortsetzung)

Zur Bereitstellung dieser Dienste arbeitet **join.me** mit einem externen Telekommunikationsanbieter zusammen. Dieses Unternehmen stellt die Software- und Hardware-basierte Telefonkonferenzinfrastruktur zur Verfügung, über die die Gesprächsteilnehmer unabhängig von der Einwahlmethode eine Verbindung zueinander herstellen können. Da verschiedene Endpunkte, Geräte und Technologien zum Einsatz kommen, muss **join.me** mit verschiedenen Ereignissen und Protokollen arbeiten können. All diese Protokolle sind absolut sicher. Hier eine schematische Darstellung einer typischen Telefonkonferenz:



Die Tonübertragung bei **join.me** erfolgt mittels Voice over IP (VoIP) und nutzt den sicheren SIPS-Standard, um eine Kommunikation zwischen dem Computer des Teilnehmers und der Audioinfrastruktur zu ermöglichen. In manchen Netzwerkumgebungen müssen dazu unter Umständen die folgenden Ports und IP-Bereiche in der Firewall geöffnet werden:

Zu öffnende Portbereiche:

- 5060–5100, ausgehender TCP-Datenverkehr (SIP-Signalisierungsports)
- 7800–32000, ausgehender UDP-Datenverkehr (Ports für Gesprächsdaten)

Die oben genannten Ports sind für die folgenden IP-Adressbereiche zu öffnen:

- 64.95.96.144/28
- 66.151.98.0/26
- 189.8.82.112/28
- 199.195.235.64/28
- 209.197.28.0/25
- 216.133.231.0/26
- 117.120.4.96/28
- 115.187.137.232/29

Diese Informationen können jederzeit geändert werden. Auf **help.join.me** finden Sie eine aktuelle Liste der Bereiche.

Abhängig von der verwendeten Version von join.me können bis zu 250 Teilnehmer gleichzeitig an dem zu einer Besprechung gehörenden Konferenzgespräch teilnehmen. Verschiedene Modi sind miteinander kompatibel, sodass den Teilnehmern entsprechend ihrer Verbindung zur Audioinfrastruktur immer die höchstmögliche Qualität geboten wird. Die Telefonkonferenzfunktionen lassen sich von jedem beliebigen Teilnehmer steuern, sofern dieser im Konferenzgespräch die Rolle des Organisators innehat. In der nativen und der HTML5-App von **join.me** werden diese Audiofunktionen über die **join.me**-Benutzeroberfläche ausgeführt; Anrufer aus dem Festnetz, von Mobiltelefonen und von SIP-Geräten verwenden die Wähltastatur (in der Online-Wissensdatenbank von **join.me** ist eine vollständige Liste der Befehle zu finden).

Videokonferenzen

join.me nutzt die WebRTC-Technologie, um Videokonferenzen auf den folgenden Plattformen zu ermöglichen:

- Windows mit der **join.me**-Computer-App
- Mac OS X mit der **join.me**-Computer-App
- HTML5-Client in Google Chrome
- auf iOS und Android in Kürze

Abhängig von der verwendeten Version von join.me können sich bis zu zehn Besprechungsteilnehmer mit einem Videofeed einwählen, der dann von bis zu 250 Personen gesehen werden kann. Während der Videokonferenz werden alle Videostreams von einem zentralen Dienst (dem Medienserver) weitergeleitet. Die Videostreams sind mittels DTLS-SRTP verschlüsselt. Sie werden von der LogMeIn-Infrastruktur nur weitergeleitet; auf unseren Servern werden keine Daten gespeichert.

Zur Nutzung der Videokonferenzfunktion sind folgende Portbereiche zu öffnen:

- UDP 1853
- TCP 443 (Ausweichport, falls UDP gefiltert wird)

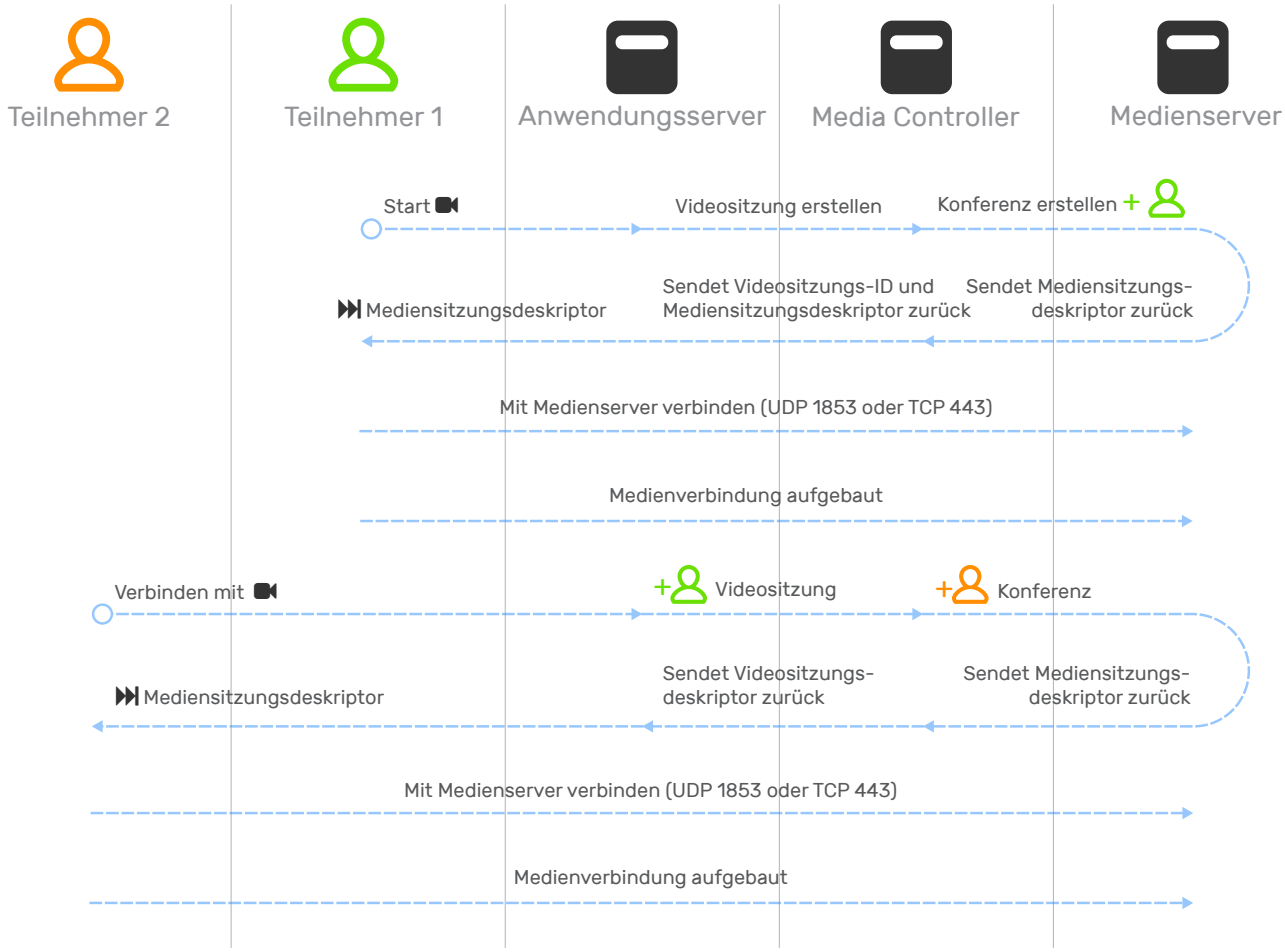
join.me video verwendet die folgenden IP-Bereiche:

- 64.94.18.0/24
- 64.74.103.0/24
- 64.74.17.0/24
- 63.251.34.0/24
- 216.52.233.0/24
- 111.221.57.0/24
- 117.20.45.0/24
- 190.210.65.0/24
- 177.154.130.0/24
- 95.172.70.0/24

Diese Informationen können jederzeit geändert werden. Auf **help.join.me** finden Sie eine aktuelle Liste der Bereiche.

Funktionsweise / Videokonferenzen (Fortsetzung)

Hier eine schematische Darstellung einer Besprechung inklusive Videokonferenz:



Überlegungen zur Bandbreite bei der Videoübertragung

WebRTC arbeitet mit dem VP8-Codec, welcher eine Mindestbandbreite von 100 Kbit/s erfordert. Die folgende Tabelle gibt Ihnen einen Überblick über den geschätzten Bandbreitenverbrauch in verschiedenen Szenarien.

	Auflösung	Bandbreite (bei 30 fps)
Bildschirm freigegeben	320 x 240	100–500 Kbit/s
Bildschirmfreigabe angehalten (zwei Teilnehmer)	1280 x 720	1,0–2,0 Mbit/s
Bildschirmfreigabe angehalten (mehr als zwei Teilnehmer)	640 x 480	0,5–1,0 Mbit/s

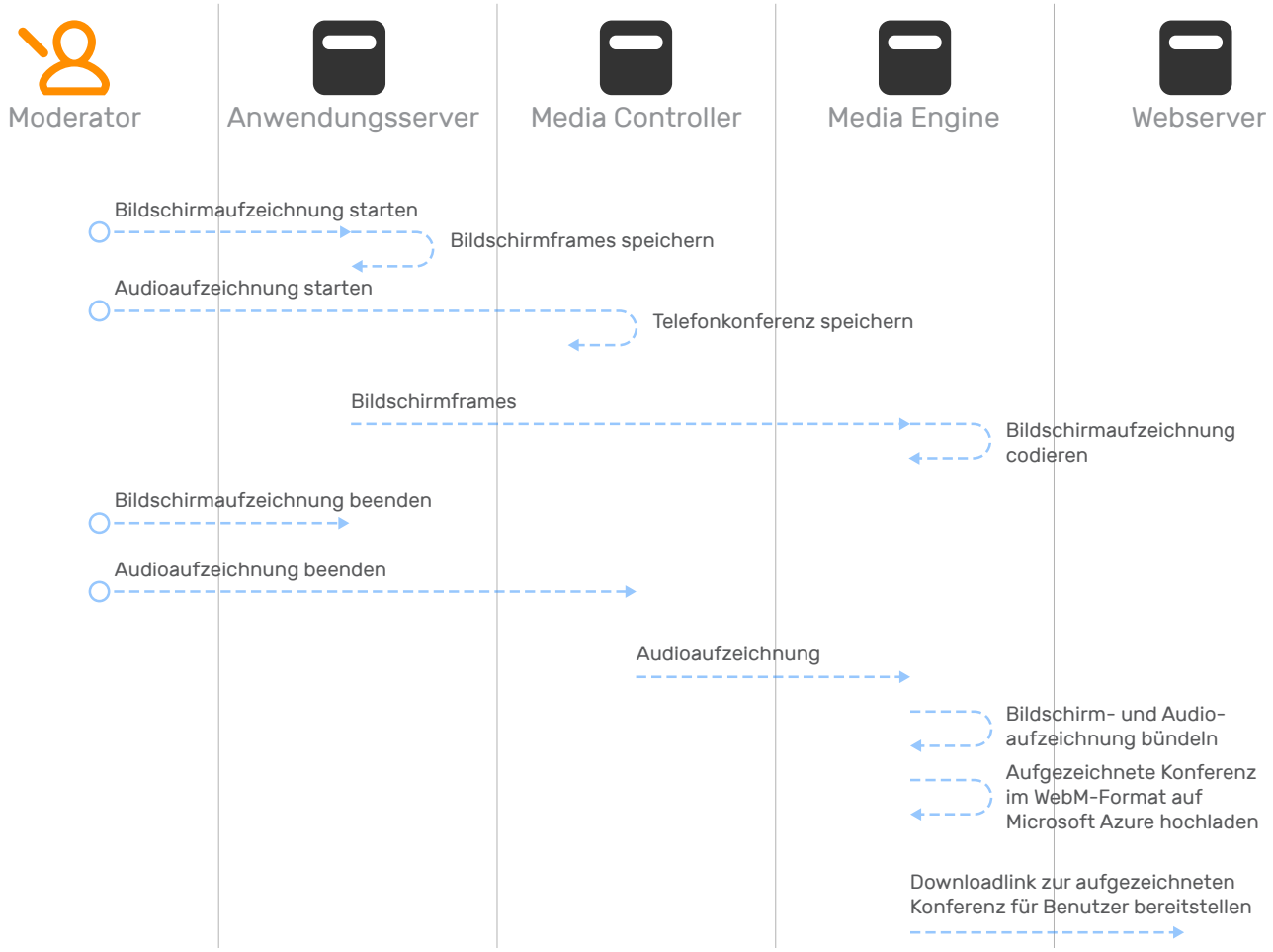
Funktionsweise (Fortsetzung)

Aufzeichnung von Besprechungen

Die Aufzeichnung von **join.me**-Besprechungen erfolgt in der Infrastruktur von LogMeIn, was dem Organisator der Besprechung den rechenintensiven Prozess des Aufzeichnens, Kodierens und Speichern eines hochauflösenden Videos erspart. Da die Videodatei bereits während der Besprechung kodiert wird, können die Benutzer die Aufzeichnung für gewöhnlich wenige Minuten nach der Videokonferenz herunterladen und für andere freigeben.

Die Aufzeichnungen werden im WebM-Videoformat gespeichert und können mit HTML5 ohne Plugins direkt in einem Webbrowser wiedergegeben werden. Die WebM-Videos werden in Microsoft Azure Storage gespeichert. Standardmäßig werden sie sowohl in jener Azure-Speicherregion gespeichert, die dem Standort des Moderators zum Zeitpunkt der Aufzeichnung am nächsten liegt, sowie in einer zweiten Region. Diese geografische Redundanz gewährleistet eine lange Haltbarkeit und eine hohe Verfügbarkeit der Videos. Auf Anfrage lässt sich das Konto auch so konfigurieren, dass die Dateien ausschließlich in einer Region gespeichert werden. Wenden Sie sich hierzu an Ihren **join.me**-Kundenbetreuer. Für jedes Speicherkonto gibt es ein Content Delivery Network (CDN), welches die Antwortzeiten für die Benutzer beim Zugriff auf die aufgezeichneten Inhalte optimiert.

Hier eine Darstellung dieses komplexen Ablaufs:



Datensicherheit

join.me erfüllt folgende Voraussetzungen, um eine sichere Datenübertragung zu gewährleisten:

- Authentifizierung der kommunizierenden Parteien
- vertraulicher Nachrichtenaustausch
- Erkennung kompromittierter Nachrichten

Auf Protokollebene nutzt **join.me** TLS, um die Sicherheit des Datenaustauschs zu gewährleisten. Als Protokoll für den Schlüsselaustausch wird ECDHE verwendet, während für die Datenverschlüsselung AES (vorzugsweise AES256-SHA384) zum Einsatz kommt. Alle modernen Browser, darunter die aktuellen Versionen von Internet Explorer, Firefox und Chrome, unterstützen AES256-SHA384.

Alle Sitzungen sind durch das TLS-Zertifikat des Anwendungsservers geschützt. Die Verwendung von SSLv2 und SSLv3 ist in allen join.me-Komponenten untersagt. Die vom Teilnehmer und dem Moderator aufgebauten gesicherten Verbindungen enden am Anwendungsserver. Der Grund dafür liegt auf der Hand: Ein einzelnes Teilnehmer-Moderator-Paar könnte potentiell eine Ende-zu-Ende-Verschlüsselung einsetzen und den Anwendungsserver als einfaches Vernetzungsrelay nutzen; bei mehreren Teilnehmern ist dies jedoch nicht möglich. Das System ist so konzipiert, dass mehrere Personen an einer Sitzung teilnehmen können, ohne dass dem Moderator Bandbreitenbeschränkungen auferlegt werden.

Die gesamte Datenübertragung mit **join.me**, darunter auch der Zugriff auf die Website selbst, wird mittels TLS geschützt.

Sitzungsdaten wie Screenshots, Videos oder Chatprotokolle werden nie auf unseren Servern gespeichert. Die einzige Ausnahme hierbei ist die Aufzeichnung von Besprechungen unter Verwendung der Aufzeichnungsfunktion von **join.me**. Die Aufzeichnungen werden im Cloud-Speicher-Dienst Microsoft Azure Storage gespeichert. Microsoft Azure Storage erfüllt verschiedene behördliche Auflagen, darunter auch die Anforderungen des US-amerikanischen Health Insurance Portability and Accountability Acts (HIPAA). Sie können Ihre Aufzeichnungen jederzeit löschen.

Profildaten von Kunden

join.me ermöglicht es den Anwendern, Profildaten aus Windows- und Mac-OS-X-Clients zu speichern. Zu den speicherbaren Informationen zählen der Spitzname, der Vorname, der Nachname und ein Avatarbild (eine hochgeladene Datei oder eine Kameraaufnahme). Der Client kommuniziert mit dem Server über eine sichere HTTPS-Verbindung, die anerkannten Webstandards entspricht. Avatarbilder werden binär im Azure Blob Storage gespeichert, während Metadaten im Tabellenspeicher und der SQL-Datenbank abgelegt werden.

Unbefugte Persionen haben keinen Zugriff auf Profildaten von Kunden oder zugehörige Infrastruktur.

Die Lösung setzt sich aus drei Diensten zusammen:

- Identitätsanbieter: für die Benutzerauthentifizierung und die Profilspeicherung zuständig. Bei der Authentifizierung kommen OAuth, JWT (JSON Web Token) und standardmäßige Verschlüsselungsalgorithmen zum Einsatz.
- Dateispeicherdienst: zur Speicherung der Avatarbilder, Binär- und Metadaten in Azure Storage.
- Chatthread-Dienst: wird zum Führen des Teilnehmerverzeichnisses und Speichern von Profildaten in Azure Redis Cache genutzt, was die Leistung verbessert.

Weitere Details finden Sie in den rechtlichen Informationen zu Microsoft Azure:
https://azure.microsoft.com/de-de/support/legal/

Sitzungs- und Website-Sicherheit

Sitzungen werden mit Hilfe von Sitzungscodes identifiziert und geschützt. Diese kurzlebigen, neunstelligen Codes werden nach dem Ende einer Sitzung wiederverwertet. Zum Veröffentlichungszeitpunkt hatte LogMeIn auf Basis der aktuellen Nutzungstrends festgestellt, dass neun Stellen das Risiko einer Code-Kollision auf das Vernachlässigbare minimierten. Im Zuge der zunehmenden Nutzung von **join.me** ist es möglich, dass die Länge der kurzlebigen Sitzungscodes über die derzeitigen neun Stellen hinaus ausgeweitet wird.

Für zahlende Kunden werden statische Sitzungscodes (auch als „persönliche Links“ bezeichnet) angeboten. Dabei handelt es sich um eine vom Benutzer definierte alphanumerische Zeichenfolge mit bis zu 127 Zeichen. Ein gut gewählter persönlicher Link ist kaum zu erraten; wegen seines statischen Charakters ist sein Einsatz jedoch auf vertrauenswürdige Teilnehmer beschränkt. Bei Verwendung eines statischen Codes werden die Besprechungen gesperrt gestartet und der Moderator muss jeden Teilnehmer genehmigen.

Die Teilnehmer authentisieren sich mit Hilfe des Sitzungscodes beim System. Ihre Authentisierung dem Moderator gegenüber erfolgt in der Regel implizit („wenn der Teilnehmer den Code hat, muss er ihn wohl vom Moderator erhalten haben“). Die Teilnehmer können jedoch auch einen Anzeigenamen eingeben, was besonders in einer größeren Gruppe nützlich ist. Die Moderatoren können die Website für spontane Besprechungen ohne Anmeldung nutzen. In diesem Fall sind sie anonym und die Authentifizierung erfolgt nur über den vom System erstellten Sitzungscode. Wenn sie sich für eine Anmeldung entscheiden (um auf Besprechungen aus dem Terminplaner zuzugreifen oder einen statischen Code zu nutzen), identifizieren sie sich mit Hilfe einer Kombination aus E-Mail-Adresse und Passwort. **join.me** erfordert eine gültige und verifizierte E-Mail-Adresse. Das Passwort muss mindestens sechs Stellen lang sein. Bei der Registrierung regt eine einfache Anzeige für die Passwortqualität den Benutzer dazu an, ein komplizierteres Passwort zu wählen.

Auf Wunsch können die Moderatoren ihre Zugangsdaten speichern und stets auf der Website angemeldet bleiben. So sind sie auch beim nächsten Besuch auf der **join.me**-Website bereits eingeloggt – vorausgesetzt, sie verwenden denselben Browser und dasselbe Gerät. Diese „Merkfunktion“ nutzt kryptographisch sichere zufällige Zeichenfolgen. Es werden keine Benutzer-IDs in Cookies gespeichert und es kommt keine

AES- oder andere Verschlüsselung zum Einsatz. Das Cookie für die automatische Anmeldung enthält den Schlüssel für einen SQL-Server-Datensatz mit der Benutzer-ID. Die Merkfunktion steht für risikoreiche Funktionen wie etwa die Änderung von Kontodaten nicht zur Verfügung. Bei der Ausführung risikoreicher Funktionen muss der Benutzer immer ein gültiges Passwort eingeben.

Die Moderatoren können außerdem Software auf ihren Computer herunterladen und dort installieren. Für Bildschirmfreigabesitzungen ist dann kein Website-Besuch mehr erforderlich. Diese Software (allgemein als die **join.me**-Computer-App bekannt) lässt sich mit dem Konto eines Moderators verknüpfen und bietet so Zugriff auf Besprechungen aus dem Terminplaner sowie statische Codes (persönlicher Link). Wenn die Präsentationssoftware mit einem Konto verknüpft wird, wird ihr ein 32-stelliges Token zugewiesen, das von einem kryptographischen Zufallsalgorithmus aus einem aus 62 Zeichen bestehenden Alphabet (Ziffern sowie Groß- und Kleinbuchstaben) erstellt wurde. Dieses Token wird dauerhaft auf dem Computer des Moderators gespeichert und von der Software zur Authentisierung beim System verwendet.

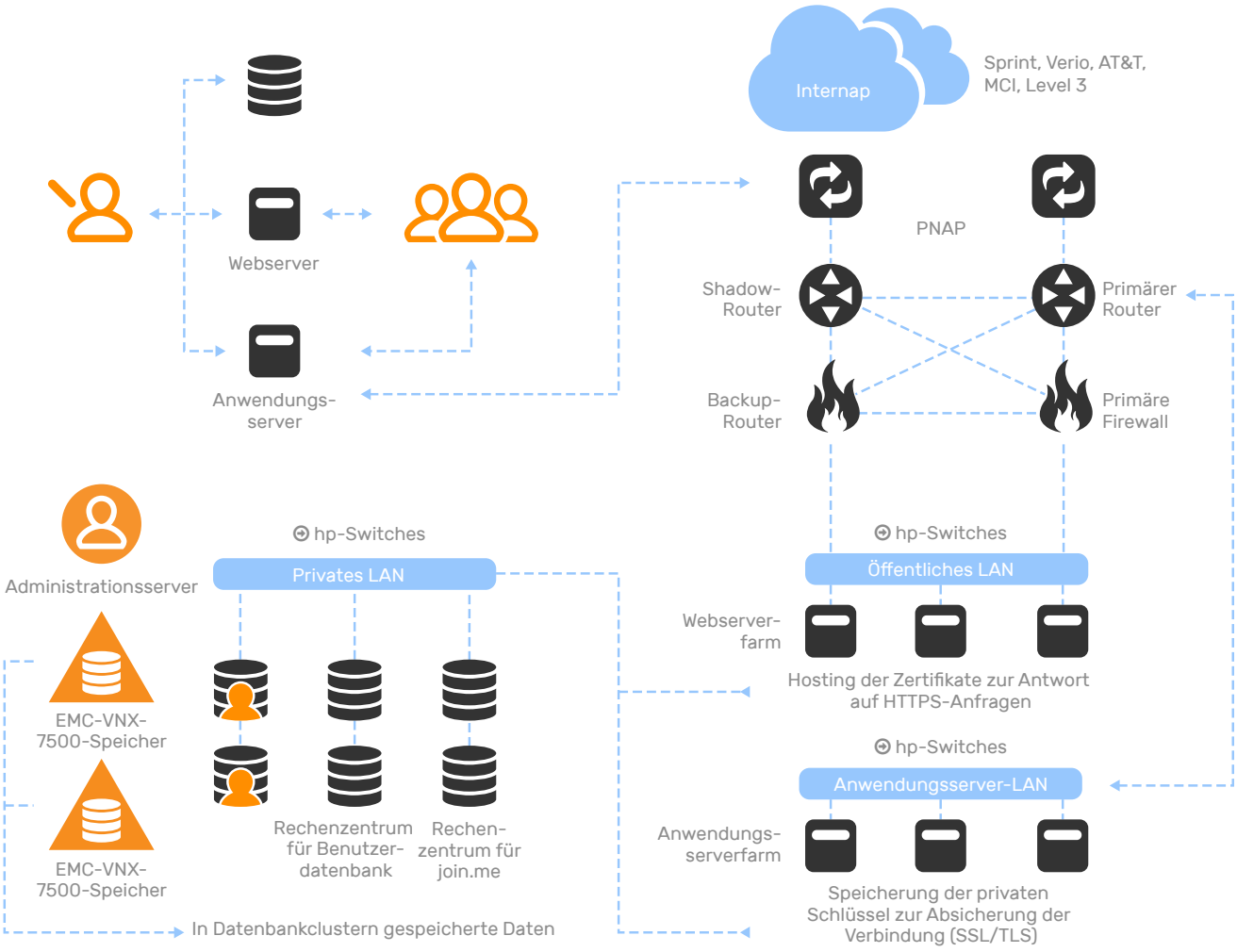
Für die Anmeldung auf der Website oder in den nativen Apps bietet **join.me** die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA). Für den zweiten Verifizierungsschritt stehen dabei folgende Optionen zur Auswahl: LogMeIn Authenticator (für Android und iOS verfügbar), TOTP (Google Authenticator und andere Apps), SMS (textbasiert) oder E-Mail.

Single Sign-On (SSO) ist ebenfalls verfügbar.

Überblick über die Hosting-Einrichtungen

Der **join.me**-Dienst nutzt dieselben Hosting-Einrichtungen wie die restlichen LogMeIn-Dienste. Dabei handelt es sich um Tier-1-Serverhousing-Einrichtungen mit folgenden Ausstattungsmerkmalen:

- mehrstufige Sicherheitskontrollen, biometrische Zugangskontrollsysteme, Rund-um-die-Uhr-Video-überwachung und Alarmüberwachung
- unterbrechungsfreie und redundante Stromversorgung (Gleich- und Wechselstrom), Notstromgenera-toren vor Ort
- redundante HLK-Konstruktion mit Unterbodenlüftung für ideale Temperaturregelung
- Rauchmelder über und unter dem Doppelboden; doppelt gesicherte, vorgesteuerte Trocken-sprinkleranlage



Überblick über die Hosting-Einrichtungen (Fortsetzung)

Die LogMeIn-Server (einschließlich aller **join.me**-Server) befinden sich in jedem Rechenzentrum in eigenen Cages. Diese „Käfige“ sind zweifach elektronisch verriegelt (biometrisch und per PIN).

Die LogMeIn-Infrastruktur in jedem Rechenzentrum ist über mehrere 10-GB-Uplinks und Tier-1-NSPs an das Internet angebunden. Die Grenzrouter sind als Aktiv/Passiv-Cluster konfiguriert und vollvermascht mit einem Aktiv/Passiv-Firewallcluster verbunden.

Diese wiederum sind vollvermascht mit einem Aktiv/Passiv-Lastenausgleichscluster auf IP-Ebene verbunden.

Hinter den Firewalls befindet sich eine DMZ mit den Web- und den Anwendungsservern sowie der Audio- und der Videoinfrastruktur. Die Datenbankserver kommunizieren mit den Servern in der DMZ über ein privates, nicht routbares LAN. Zur Warnung und zum Schutz vor böswilligem Zugriff wurde ein internes Angriffserkennungssystem (IDS) eingerichtet.

Der Zugang zu den Cages selbst wird streng kontrolliert und ist auf ein Team von Netzwerktechnikern beschränkt. Der logische Zugriff zu Zwecken der Fernverwaltung und Softwareverteilung erfolgt über LogMeIns eigene Dienste (LogMeIn Pro) sowie ein SSH-Gateway auf einem separaten Kanal. Der Fernzugriff ist für Administratoren nur nach der Zwei-Faktor-Authentifizierung (Benutzername/Passwort-Kombination und ein Hardware- bzw. Software-Token) möglich.

Alle Server werden monatlich intern sowie vierteljährlich und jährlich von Drittanbietern geprüft. Dabei werden unter anderem Netzwerk-Penetrationstests durchgeführt und die Serverkonfigurationen überprüft.

Schlussbemerkung

Der **join.me**-Dienst mag sehr einfach wirken, baut jedoch auf einer hochentwickelten Architektur auf, die selbst den Ansprüchen der besorgtesten Nutzer gerecht wird.

Weitere Informationen werden unter Umständen nach Unterzeichnung einer Vertraulichkeitsvereinbarung bekanntgegeben.

Fragen? Tel.: +**1 877 251 8373**
oder **help.join.me**