Sicherheitshandbuch

Zoom Video Communications Inc.

Zoom unterstützt Unternehmen und Organisationen dabei, ihre Teams in einer reibungslosen Umgebung zusammenzubringen, damit sie mehr leisten können. Unsere problemlose, zuverlässige Cloud-Plattform für Video, Sprache, Inhaltsfreigabe und Chatausführungen wird von Mobilgeräten, Desktops, Telefonen und Raumsystemen unterstützt.

Für Zoom steht Sicherheit bei der Ausführung all seiner Produkte und Dienste an erster Stelle. Zoom folgt dem Anspruch, ständig robuste Sicherheitsfunktionen und -praktiken bereitzustellen, die die Anforderungen von Unternehmen für eine sichere Zusammenarbeit erfüllen.

Der Zweck dieses Dokuments ist die Bereitstellung von Informationen über die bei Zoom verfügbaren Sicherheitsfunktionen. Der Ausgangspunkt ist, dass der Leser dieses Dokuments mit den Zoom-Funktionen für Meetings, Webinare, Chat, Dateifreigabe und Sprachanrufe vertraut ist.

Wenn nicht anders angegeben, treffen die Sicherheitsfunktionen in diesem Dokument auf alle Produkte von Zoom Meetings, Zoom Video Webinars, Zoom Rooms und Zoom Voice zu, die von Endpunkten wie Mobiltelefonen, Tablets, Desktops, Laptops und SIP/H.323-Raumsystemen unterstützt werden.

Infrastruktur

Die Zoom-Cloud ist ein eigens entwickeltes globales Netzwerk, das von Grund auf aufgebaut wurde, um hochwertige Kommunikationserlebnisse bieten zu können. Zoom wird in einem skalierbaren Hybridmodus betrieben. Webbasierte Dienste wie Funktionen zur Einrichtung von Meetings, Benutzerverwaltung, Aufzeichnungen von Konferenzen, Chats und Sprachnachrichten werden in der Cloud gehostet, während Echtzeit-Konferenzmedien in global verteilten Tier-1-Colocation-Rechenzentren mit SSAE 16 SOC 2 Type 2-Zertifikaten verarbeitet werden.

Echtzeit-Medienverarbeitung

Ein verteiltes Netzwerk mit Multimedia-Softwareroutern mit niedrigen Latenzzeiten verknüpft die Kommunikationsinfrastruktur von Zoom. Durch diese Multimediarouter werden alle Sitzungsdaten, die vom Gerät des Hosts stammen und bei den Geräten der Teilnehmer ankommen, dynamisch zwischen den Endpunkten übermittelt. Zoom-Echtzeitsitzungen funktionieren analog zum beliebten mobilen Gespräch über das öffentliche Mobilfunknetz.

zoom | Authorised Reseller

Firewall-Kompatibilität

Während der Einrichtung einer Sitzung verbindet sich der Zoom-Client via HTTPS (Port 443/TLS) mit Servern von Zoom, um die Daten abzurufen, die für die Verbindung mit dem entsprechenden Meeting oder Webinar benötigt werden, und um die aktuelle Netzwerkumgebung zu untersuchen und so den geeigneten Multimediarouter zu verwenden, dessen Ports offen sind, und um zu überprüfen, ob ein SSL Proxy verwendet wird. Mit diesen Metadaten bestimmt der Zoom-Client die beste Methode für die Echtzeit-Kommunikation. Dabei versucht er automatisch, sich mit bevorzugten UDP und TCP-Ports 8801, 8802 und 8804 zu verbinden. Für eine erhöhte Kompatibilität und Unterstützung von Enterprise SSL-Proxys kann die Verbindung auch via HTTPS (Port 443/TLS) aufgebaut werden. Auch für Benutzer, die sich über den Zoom Webbrowser-Client anschließen, wird eine HTTPS-Verbindung hergestellt.

Client-Anwendung

Rollenbasierte Benutzersicherheit

Die folgenden Sicherheitsfunktionen für Meetings stehen dem Host vor dem Meeting zur Verfügung:

- Sichere Anmeldung mit Standard-Benutzername und Kennwort oder einmaliges Anmelden mit SAML
- Start eines gesicherten Meetings mit Kennwort
- Planung eines gesicherten Meetings mit Kennwort

Ausgewählte Einladung zum Meeting: Der Host kann ausgewählte Teilnehmer per E-Mail, IM oder SMS einladen. Dadurch erhält der Host mehr Kontrolle über die Verbreitung der Zugriffsdaten zum Meeting. Der Host kann das Meeting auch so erstellen, dass nur Mitglieder einer bestimmten Domain-E-Mail teilnehmen können.

Sicherheit der Meeting-Informationen: Zoom speichert zu einer Sitzung gehörende Event-Informationen zu Abrechnungs- und Berichtszwecken. Die Event-Informationen werden in einer gesicherten Datenbank von Zoom gespeichert und können nach sicherer Anmeldung vom Kontoadministrator des Kunden über die Kundenportalseite eingesehen werden.

Anwendungssicherheit: Zoom kann alle Präsentationsinhalte auf Anwendungsebene mit dem AES-256-Bit-Algorithmus verschlüsseln (AES, Advanced Encryption Standard).

Gruppenrichtlinienkontrollen für den Zoom-Client: Insbesondere im Zoom Meetings-Client für Windows und in Zoom Rooms für Windows können Administratoren ein breites Spektrum an Client-Konfigurationseinstellungen festsetzen, die durch Active Directory Gruppenrichtlinienkontrollen erzwungen werden.

Chat-Verschlüsselung: Die Chat-Verschlüsselung von Zoom ermöglicht eine sichere Kommunikation, bei der nur der vorgesehene Empfänger die gesicherte Nachricht lesen kann. Zoom verwendet öffentliche und private Schlüssel, um Chatsitzungen mit Advanced Encryption Standard (AES-256) zu verschlüsseln. Sitzungsschlüssel werden mit einer gerätespezifischen Hardware-ID generiert, um zu verhindern, dass Daten von anderen Geräten gelesen werden. Dies stellt sicher, dass die Sitzung nicht abgehört oder manipuliert werden kann.

Sicherheit von Meetings

Rollenbasierte Benutzersicherheit

Die folgenden Sicherheitsfunktionen für Meetings stehen dem Host während des Meetings zur Verfügung:

- Standardmäßige Verschlüsselung von Meetings
- Warteraum
- Aktivierung der Funktion „Zur Teilnahme auf Host warten“
- Ausschluss einzelner oder aller Teilnehmer
- Beenden eines Meetings
- Sperren eines Meetings
- Chat mit einem Teilnehmer oder allen Teilnehmern
- Stummschalten/Deaktivierung der Stummschaltung für einen oder alle Teilnehmer
- Wasserzeichen für Bildschirmfreigaben
- Audiosignaturen
- Aktivierung/Deaktivierung eines oder aller Teilnehmer für die Aufzeichnung
- Vorübergehendes Anhalten der Bildschirmfreigabe bei Öffnen eines neuen Fensters

Die folgenden Sicherheitsfunktionen für Meetings stehen den Teilnehmern während des Meetings zur Verfügung:

- Stumm-/Einschalten des Audiosignals
- Ein-/Ausschalten des Videos
- Weichzeichnung der Momentaufnahme auf der iOS-Aufgabenumschaltfunktion

Durch Host und Client authentifiziertes Meeting: Ein Host muss sich (per https) mit seinen Benutzerinformationen (ID und Kennwort) auf der Zoom-Website authentifizieren, um ein Meeting zu starten. Für den Client-Authentifizierungsvorgang wird ein einmaliger Token pro Client und pro Sitzung verwendet, mit dem die Identität jedes Teilnehmers, der dem Meeting beitreten will, bestätigt wird. Jede Sitzung verfügt über einen eindeutigen Satz von Sitzungsparametern, die von Zoom generiert werden. Jeder authentifizierte Teilnehmer muss Zugriff auf diese Sitzungsparameter sowie den einmaligen Sitzungstoken haben, um am Meeting teilnehmen zu können.

Offenes oder kennwortgeschütztes Meeting: Der Host kann von den Teilnehmern verlangen, vor Teilnahme am Meeting ein Kennwort einzugeben. Dies gewährleistet eine bessere Zugriffskontrolle und verhindert, dass ungebetene Gäste an einem Meeting teilnehmen.

Bearbeiten oder Löschen eines Meetings: Der Host kann kommende oder vergangene Meetings bearbeiten oder löschen. Dies gewährleistet eine bessere Kontrolle über die Verfügbarkeit von Meetings.

Durch den Host kontrollierter Beitritt zum Meeting: Zu einer besseren Kontrolle des Meetings kann der Host entscheiden, dass Teilnehmer dem Meeting erst beitreten können, nachdem er es gestartet hat. Für höhere Flexibilität kann der Host Teilnehmern gestatten, vor ihm selbst beizutreten. Wenn Teilnehmer vor dem Host beitreten, können sie ein höchstens 30 Minuten langes Meeting abhalten.

Sicherheit in Meetings: Während des Meetings stellt Zoom allen Teilnehmern des Zoom-Meetings Rich Media-Inhalte in Echtzeit bereit. Alle Inhalte, die in einem Meeting für die Teilnehmer freigegeben werden, sind nur eine Abbildung der Originaldaten. Diese Inhalte sind mittels einer sicheren Implementierung für die Freigabe wie folgt kodiert und optimiert:

- Sie ist die einzige Möglichkeit, an einem Zoom-Meeting teilzunehmen.
- Sie ist vollständig von Verbindungen abhängig, die für jede einzelne Sitzung hergestellt werden.
- Sie führt einen eigens entwickelten Vorgang aus, der alle freigegebenen Daten kodiert.
- Sie kann alle Inhalte der Bildschirmübertragung mit dem AES-256-Verschlüsselungsstandard verschlüsseln.
- Sie kann die Netzwerkverbindung zu Zoom mit einem 256-Bit-TLS-Verschlüsselungsstandard verschlüsseln.
- Sie bietet eine optische Identifizierung jedes einzelnen Meeting-Teilnehmers.

Durch den Host kontrollierter Beitritt zum Meeting
Die Authentifizierungsmethoden umfassen einmaliges Anmelden (SSO) mit SAML oder OAuth.

Mit SSO meldet sich der Benutzer einmal an und erhält Zugriff zu zahlreichen Anwendungen, ohne sich für jede einzelne erneut anmelden zu müssen. Zoom unterstützt SAML 2.0, das die webbasierte Authentifizierung und Berechtigung, SSO inbegriffen, ermöglicht. SAML 2.0 ist ein XML-basiertes Protokoll, dass Sicherheitstokens, die Assertionen enthalten, einsetzt, um Daten über einen Benutzer zwischen einer SAML-Stelle (einem Identitätsanbieter) und einem webbasierten Dienst (z. B. Zoom) zu vermitteln. Zoom arbeitet mit Exchange ADFS 2.0 sowie mit Enterprise Identity Management wie Centrify, Fugen, Gluu, Okta, OneLogin, PingOne, Shibboleth, Symplified und vielen weiteren. Zoom kann Attribute zuordnen, um einem Benutzer einer anderen Gruppe Funktionsbedienelementen zuzuweisen.

Die OAuth-basierte Bereitstellung funktioniert mit Google oder Facebook OAuth für die sofortige Bereitstellung. Zoom bietet auch einen API-Aufruf an, um Benutzer aus jedem Datenbank-Backend vorab zu versorgen.

Darüber hinaus kann Ihre Organisation oder Universität Benutzer mit verwalteten Domains automatisch zu Ihrem Konto hinzufügen. Sobald Ihre Anwendung für verwaltete Domains genehmigt wurde, werden alle vorhandenen und neuen Benutzer mit Ihrer E-Mail-Domain Ihrem Konto hinzugefügt.

Administrative Bedienelemente

Die folgenden Sicherheitsfunktionen stehen dem Kontoadministrator zur Verfügung:

- Sichere Anmeldungsoptionen mit Standard-Benutzername und-Kennwort oder SAML SSO
- Hinzufügen von Benutzer und Admin zu einem Konto
- Upgrade oder Downgrade des Benutzerabos
- Entfernen von Benutzern aus einem Konto

- Einsehen von Abrechnungen und Berichten
- Verwaltung des Konto-Dashboards und der Cloud-Aufzeichnungen

API für spezielle Sicherheitsfunktionen/-optionen

Für die Integration von Zoom mit benutzerdefinierten Kundenanwendungen und Drittanwendungen stehen APIs zur Verfügung. Jedes Kundenkonto kann Anmeldeinformationen für API-Integrationsschlüssel enthalten, die vom Administrator des Kundenkontos verwaltet werden. API-Aufrufe werden sicher über sichere webbasierte Dienste übermittelt und eine API-Authentifizierung ist erforderlich.

Meeting-Connector

Der Meeting-Connector von Zoom ist eine hybride Cloud-Bereitstellungsmethode, mit welcher ein Kunde einen Zoom-Multimediarouter (Software) in seinem internen Netzwerk einsetzen kann.

Die Metadaten über Benutzer und Meetings werden in der Kommunikationsinfrastruktur von Zoom verwaltet, aber das Meeting selbst wird im internen Netzwerk des Kunden gehostet. Der gesamte Echtzeit-Meeting-Verkehr, wie Audio, Video und Datenfreigabe läuft über das interne Netzwerk des Unternehmens. So kann die bestehende Sicherheitskonfiguration Ihres Netzwerks den Datenverkehr Ihrer Meetings schützen.

Wenn sich Kunden für einen hybriden Einsatz entscheiden, haben sie die Option, nach Benutzertyp zu unterscheiden. Hier verwenden die Benutzertypen Pro und Basic (kostenfrei) die Cloud, während die Benutzertypen Business und Enterprise die On-Premise-Infrastruktur verwenden.

Wenn die On-Premise-Infrastruktur offline ist, wird das Meeting automatisch über die Cloud durchgeführt. Sowohl unsere Cloud- als auch unsere On-Premise-Lösung ist mit Failover- und Lastenausgleichsmechanismen ausgestattet.

Zoom Rooms

Zoom Rooms ist das softwarebasierte Konferenzraumsystem von Zoom. Es bietet Video- und Audiokonferenzen, drahtlose Inhaltsfreigabe und integrierte Kalenderfunktionen, die auf handelsüblicher Hardware ausgeführt werden. Die Kommunikation wird mit einer 256-Bit-TLS-Verschlüsselung hergestellt. Alle freigegebenen Inhalte werden mit der AES-256-Verschlüsselung verschlüsselt. Die Zoom Rooms-App wird durch den Anwendungssperrcode gesichert. Der Anwendungssperrcode für Zoom Rooms ist ein erforderter 1-16-stelliger Ziffernsperrcode, der zur Sicherung Ihrer Zoom Rooms-Anwendung verwendet wird. Er verhindert, dass unautorisierte Änderungen an Ihrer Zoom Rooms-Anwendung und den Einstellungen Ihrer begleitenden Hardware vorgenommen werden.

Zoom Chat

Mit der durchgängigen, plattformübergreifenden Chat-Funktion der Zoom Meetings können Benutzer unter vier Augen oder in Gruppen chatten und Dateien freigeben. Benutzer können in jedem Chatfenster auf „Treffen“ klicken und sofort ein Zoom Videomeeting mit den Chatteilnehmern starten. Der Chat kann für HIPAA-konforme Einstellungen verschlüsselt werden.

Zoom Phone

Zoom Phone ist ein Cloud-Telefonsystem, das zur Zoom-Plattform hinzugefügt werden kann. Es unterstützt ein- und ausgehende Anrufe über das öffentliche Telefonfestnetz (PSTN) und nahtlos integrierte Telefoniefunktionen ermöglichen Kunden, ihre bestehenden PSTN-Lösung zu ersetzen und all ihre Geschäftskommunikation und Zusammenarbeitsanforderungen in ihrer Lieblingsvideoplattform zusammenzulegen.

Durch den Einsatz auf Normen basierte Voice-over-Internet-Protocol (VoIP) liefert Zoom Phone erstklassige Sprachdienste und eine sichere und verlässliche Alternative zu herkömmlichen On-Premise-PBX-Lösungen. Rufaufbau und Funktionen für eingehende Gespräche werden über Session Initiation Protocol (SIP) bereitgestellt. Zur Gewährleistung der höchstmöglichen Qualität wird OPUS als bevorzugter Codec eingesetzt. Zoom Phone unterstützt aber auch weitere branchenübliche Codecs (G.722, G.711 und G.729) für die Transcodierung von Medien.

Authentifizierung

- Die SIP-Registrierung von Zoom Phone authentifiziert mithilfe der Verschlüsselung AES-128 Bit TLS 1.2.

Medienverschlüsselung

- VoIP-Medien werden vom Secure Real-time Transport Protocol (SRTP) mit AES-128-Verschlüsselung übermittelt und geschützt.

Privates Netzwerk-Peering

- Zoom hat direkte private Netzwerk-Peering-Verbindungen zwischen den Rechenzentren von Zoom Phone und den PSTN-Dienstleisternetzwerken hergestellt, um höchstmögliche Sicherheit zu gewährleisten.

Notrufe

- Zoom Phone unterstützt die mit E911 (USA/Kanada) erweiterten Notrufdienste, um, wie gesetzlich vorgeschrieben, der Notrufleitstelle den Standort des Anrufers mitzuteilen. Die vom Anruf ausgehenden Standortadressen können auf Ebene des Kontos und des einzelnen Benutzers eingestellt und zugewiesen werden.
- Notrufe aus der Zoom Mobile App auf iOS- und Android-Smartphones verweisen automatisch auf die ausgehende Mobiltelefoniefunktionen des Smartphones und umgehen den Dienst von Zoom Phone, um den Notruf direkt an die Notrufleitstelle des Mobilfunkbetreibers weiterzuleiten.
- Zoom Phone-Administratoren können Notrufe wahlweise automatisch abfangen und an firmeneigene Sicherheitsdienste weiterleiten.

Gebührenbetrug

- Zoom Phone verhindert Gebührenbetrug durch Zugriffskontrolle und automatische Erkennungsfunktionen. Unsere Sicherheitsabteilung überwacht die Kundenkonten aktiv, um irreguläre Anrufmuster zu erkennen und benachrichtigt Kunden über potenzielle betrügerische Tätigkeiten.

Schwarze Listen aufrufen

- Mithilfe anpassbarer allgemeiner und persönlicher Schwarze Listen können Benutzer und Administratoren einfach gesperrte Telefonnummern hinzufügen und verwalten.

Aufruf der Funktion „in ein Meeting verwandeln“

- Wenn Zoom Phone-Anrufe in Zoom-Meetings umgewandelt werden, gelten alle verfügbaren Sicherheitsfunktionen für Zoom-Meetings für das Gespräch.

Zoom Video-Webinare

In Zoom Video-Webinaren können bis zu 100 Video-Diskussionsteilnehmer vor bis zu 10.000 Teilnehmern, die nur zusehen können, mit Video, Audio und Bildschirmübertragung präsentieren. Für diese Webinare stehen Registrierungsoptionen, Berichterstattung, Fragen und Antworten, Umfragen, Wortmeldungen, Aufmerksamkeitsanzeigen, und MP4/M4A-Aufzeichnung zur Verfügung. Zoom Video-Webinare können auf YouTube und Facebook Live übertragen werden, um ein unbegrenztes Live-Publikum zu erreichen. Diskussionsteilnehmer sind vollwertige Meeting-Teilnehmer. Sie können Videos ansehen und senden, den Bildschirm freigeben, Anmerkungen machen usw. Die Einladungen an Diskussionsteilnehmer werden getrennt von den Einladungen an Webinar-Teilnehmer gesendet. Inhalte und Bildschirmübertragung in Webinaren werden durch AES 256 gesichert und über ein geschütztes Netzwerk mit 256-Bit-Verschlüsselungsstandard übermittelt.

Webinar mit Registrierung

- Manuell genehmigte Registrierung – der Host des Webinars wird manuell genehmigen oder ablehnen, ob ein Registrant die Informationen erhält, um am Webinar teilzunehmen.
- Registranten automatisch genehmigen – alle Registranten des Webinars erhalten die Informationen, um am Webinar teilzunehmen, automatisch.

Webinar ohne Registrierung

- Einmalig – Teilnehmer nehmen nur einmal am Webinar teil. Nach Ende des Webinars können die Teilnehmer dieselben Informationen zur Teilnahme am Webinar nicht noch einmal nutzen.
- Wiederkehrend – Teilnehmer können mit den bereitgestellten Informationen wiederholt am gleichen Webinar teilnehmen.

Speicherung der Aufzeichnungen

Zoom bietet Kunden die Möglichkeit, ihre Meetings, Webinare und Zoom Phone-Telefonate aufzuzeichnen und freizugeben. Aufzeichnungen von Meetings und Webinaren können mit der lokalen Aufzeichnungsoption auf dem lokalen Gerät des Hosts gespeichert werden oder Meetings, Webinare und Zoom Phone-Telefonate können mit der Cloud-Aufzeichnungsoption (für zahlende Kunden verfügbar) in der Zoom-Cloud gespeichert werden. Aufzeichnungen, die lokal auf dem Gerät des Hosts gespeichert sind, können auf Wunsch mit verschiedenen kostenlosen oder im Handel erhältlichen Tools verschlüsselt werden.

Cloud-Aufzeichnungen werden nach Beendigung des Meetings in der Zoom-Cloud verarbeitet und gespeichert. Die Aufzeichnungen können kennwortgeschützt sein oder nur für Zuschauer, die unter einer bestimmten E-Mail-Domain eingeloggt sind, verfügbar sein. Die Aufzeichnungen werden sowohl im Video-/Audio-Format als auch nur im Audio-Format gespeichert. Nachrichten im Meeting, freigegebene Dateien und Abschriften von Meetings können optional in der Zoom-Cloud gespeichert werden, wo sie auch verschlüsselt sind. Der Meeting-Host kann seine Aufzeichnungen über die gesicherte Weboberfläche verwalten. Aufnahmen können heruntergeladen, freigegeben oder gelöscht werden. Aufzeichnungen von Zoom Phone-Sprachnachrichten werden in der Zoom-Cloud verarbeitet und gespeichert und können über den gesicherten Zoom-Client verwaltet werden.

Zählung von Teilnehmern in Zoom Rooms

Die Funktion „Zählung von Teilnehmern in Zoom Rooms“ ist standardmäßig ausgeschaltet, kann aber von den Raumadministratoren eingeschaltet werden. Mit dieser Funktion können Administratoren Daten über die Anzahl der Teilnehmer des Meetings, die von Zoom Rooms aus teilgenommen haben, einsehen.

Diese Funktion erfasst Bilder während der gesamten Dauer des Meetings. Bilder werden vorübergehend auf der lokalen Festplatte von Zoom Rooms gespeichert und nie an die Cloud gesendet. Nach Ende des Meetings wird mithilfe der lokal gespeicherten Bilder die maximale Anzahl der sichtbaren Teilnehmer des Meetings errechnet. Während dieses Vorgangs wird die Gesichtserkennung (ohne Verknüpfungen zu persönlichen Informationen) verwendet, um die einzelnen Personen anhand der aufgenommenen Bilder zu zählen. Wenn die Verarbeitung der Bilder zur Erfassung der Anzahl der Personen abgeschlossen ist, werden die Bilder permanent gelöscht.

Wenn Sie die Funktion zur Zählung der Teilnehmer in Zoom Rooms aktivieren, bestätigen Sie Ihre Verpflichtung zur Einhaltung aller Gesetze und Ihre Verantwortung, sicherzustellen, dass Sie Benutzern hinreichende Informationen darüber geben, dass diese Funktion eingeschaltet ist, und dass Sie die entsprechenden Genehmigungen von Datensubjekten in Übereinstimmung mit den entsprechenden Aufzeichnungs- und/oder Datenschutzbestimmungen für die Erfassung und die Speicherung dieser Daten eingeholt haben.

Datenschutz

Zoom speichert nur grundlegende Daten unter den Benutzerkonto-Profilinformationen:

- E-Mail-Adresse
- Benutzerkennwort – mit Salt und Hash
- Vorname
- Nachname
- Name des Unternehmens (optional)
- Telefonnummer des Unternehmens (optional)
- Profilbild (optional)

Weitere Informationen zu unseren Datenschutzbestimmungen finden Sie unter https://zoom.us/de-de/privacy.html.

Abrechnungsdaten

Zoom verwendet einen PCI-konformen Drittanbieter zur Zahlungsverarbeitung und zur Abwicklung aller Aspekte der Rechnungsstellung. Wir speichern keinerlei Kreditkarten- oder Abrechnungsdaten von Benutzern in unserer Datenbank.

Sicherheits- und Datenschutzzertifizierungen

SOC 2:

Der SOC 2-Bericht bietet eine Zusicherung durch Dritte, dass der Aufbau von Zoom und unsere internen Prozesse und Kontrollen die strengen Prüfungsanforderungen, die von den Standards für Sicherheit, Betriebsbereitschaft, Vertraulichkeit und Datenschutz des American Institute of Certified Public Accountants (AICPA) festgelegt wurden, erfüllen. Der SOC 2-Bericht ist der De-Facto-Zusicherungsstandard für Clouddienstanbieter.

TRUSTe:

TRUSTe hat die Datenschutzpraktiken und die Datenschutzerklärung von Zoom zertifiziert und wird bei Datenschutzklagen als Dienstanbieter für die Streitbeilegung fungieren. Zoom verpflichtet sich, Ihre Privatsphäre zu respektieren. Wenn Sie ein ungelöstes Anliegen hinsichtlich Datenschutz oder Datennutzung haben, das wir nicht zu Ihrer Zufriedenheit behandelt haben, wenden Sie sich bitte an unseren beauftragten Dienstanbieter für die Streitbeilegung in den USA (kostenlos) unter https://feedback-form.truste.com/watchdog/request.

EU-USA Datenschutzschild:

Zoom bestätigt die Teilnahme an der Erfüllung der Rahmenbedingungen des EU-US Datenschutzschilds. Zoom hat sich dazu verpflichtet, alle persönlichen Daten von Mitgliedsstaaten der Europäischen Union (EU) in Anlehnung an die Rahmenbedingungen des Datenschutzschilds den entsprechenden Grundsätzen der Rahmenbedingungen zu unterziehen. Für mehr Informationen über die Rahmenbedingungen des Datenschutzschilds besuchen Sie die Datenschutzschildliste des U.S. Department of Commerce. https://www.privacyshield.gov/list.

FedRAMP:

Zoom ist dazu berechtigt, unter dem Federal Risk and Authorization Management Program (FedRAMP), tätig zu sein. FedRAMP ist ein Programm der US-Regierung, das einen standardisierten Ansatz für die Sicherheitseinschätzung, die Genehmigung und die kontinuierliche Überwachung von Cloudprodukten und -diensten bereitstellt, die von Behörden der US-amerikanischen Bundesstaaten genutzt werden.

Unternehmen, Gesundheits- und Bildungseinrichtungen weltweit nutzen die Zoom-Plattform tagtäglich, um ihre Abteilungen miteinander zu verbinden, ihre Organisationen auszubauen und die Welt zu verändern. Datenschutz und Sicherheit stehen bei den Lebenszyklus-Operationen von Zoom an erster Stelle unserer Kommunikationsinfrastruktur und der Meeting-Connectornetzwerke. Außerdem setzen wir uns dafür ein, ständig ein stabiles Set von Sicherheitsfunktionen bereitzustellen, um unser Ziel zu erreichen, das effizienteste und sicherste einheitliche Video-First-Kommunikationssystem zu liefern.