Technische und organisatorische Maßnahmen
GoTo Resolve

Zusammenfassung

In diesem Dokument zu technischen und organisatorischen Maßnahmen (TOMs) werden die Verpflichtungen von GoTo in Bezug auf Datenschutz, Sicherheit und Verantwortlichkeit für GoTo Resolve dargelegt. Insbesondere unterhält GoTo robuste globale Datenschutz- und Sicherheitsprogramme sowie organisatorische, administrative und technische Schutzmaßnahmen, um: (i) die Vertraulichkeit, Integrität und Verfügbarkeit von Kundeninhalten sicherzustellen; (ii) vor Bedrohungen und Gefahren für die Sicherheit von Kundeninhalten zu schützen; (iii) vor Verlust, Missbrauch, unbefugtem Zugriff, Offenlegung, Veränderung und Zerstörung von Kundeninhalten zu schützen; und (iv) die Einhaltung geltender Gesetze und Vorschriften, einschließlich Datenschutzgesetzen, zu gewährleisten. Solche Maßnahmen umfassen:

- **Verschlüsselung:**
  - *Während der Übertragung* Transport Layer Security (TLS) Version 1.2.
  - *Im Ruhezustand* Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte.
- **Rechenzentren:**[1] Standorte in den USA, Deutschland, Irland, Schweden, Singapur, Indien und den Niederlanden, um Redundanz und Stabilität zu gewährleisten.
- **Physische Sicherheit:** Geeignete physische Sicherheits- und Umgebungskontrollen sind vorhanden und darauf ausgelegt, den physischen Zugang zu Systemen und Servern mit Kundeninhalten zu schützen, zu kontrollieren und einzuschränken, um die Verpflichtungen hinsichtlich Betriebszeit, Leistung und Skalierbarkeit einhalten zu können.
- **Compliance-Audits:** GoTo Resolve ist nach ISO/IEC 27001:2013, SOC 2 Typ II, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy sowie APEC CBPR und PRP zertifiziert.
- **Einhaltung gesetzlicher/behördlicher Vorschriften:** GoTo unterhält ein umfassendes Datenschutzprogramm mit Prozessen und Richtlinien, die sicherstellen sollen, dass Kundeninhalte in Übereinstimmung mit den geltenden Datenschutzgesetzen, einschließlich DSGVO, CCPA/CPRA und LGPD, behandelt werden.
- **Sicherheitsprüfungen**: GoTo führt nicht nur interne Tests durch, sondern beauftragt zusätzlich externe Firmen mit der regelmäßigen Durchführung von Sicherheitsprüfungen und/oder Penetrationstests.
- **Logische Zugriffskontrollen:** Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollen soll die Bedrohung des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden.
- **Datentrennung**: GoTo verwendet eine Multi-Tenant-Architektur und trennt Kundenkonten logisch auf der Datenbankebene.
- **Perimeterabwehr und Erkennung von Eindringversuchen**: Tools, Techniken und Dienste zum Schutz des Perimeters sollen verhindern, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung.
- **Datenaufbewahrung:**
  - Kunden von GoTo Resolve können jederzeit einen Antrag auf Rückgabe oder Löschung von Kundeninhalten stellen, der innerhalb von dreißig (30) Tagen nach Antragstellung des Kunden bearbeitet wird.
  - Kundeninhalte werden nach folgenden Kriterien automatisch gelöscht: (a) neunzig (90) Tage nach Ablauf der letzten bezahlten Abonnementlaufzeit eines Kunden oder (b) kostenlose Konten nach zwei (2) Jahren Inaktivität (z. B. keine Anmeldungen). Aufzeichnungen werden rollierend nach neunzig (90) Tagen gelöscht.

[1] Die Hosting-Standorte können variieren (d. h. abhängig von der Wahl des Datenspeicherorts verschieden sein). Lesen Sie die entsprechende Offenlegung der Unterauftragsverarbeiter für GoTo Resolve (GoTo Resolve Sub-Processor Disclosure), die Sie im Abschnitt „Product Resources“ des GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center) finden.

Inhalt

Klicken Sie auf die Seitenzahlen unten, um zum entsprechenden Abschnitt der TOMs zu gelangen.

1 Produkteinführung

GoTo Resolve ermöglicht es IT- und Support-Experten, über eine Web- oder Desktop-Technikerkonsole mit Funktionen für Bildschirmanzeige, Remotesteuerung und Kameraübertragung Remotesupport für Computer, Server und Mobilgeräte zu leisten. GoTo Resolve setzt Sicherheitsmaßnahmen zum Schutz von Daten ein, die sowohl passive als auch aktive Angriffe abwehren sollen.

In diesem Dokument verwendete Begriffe, die nicht im Text definiert sind, werden entweder in den Nutzungsbedingungen erklärt oder in Abschnitt 23 erläutert.

2 Technische Maßnahmen

Die Produkte von GoTo sind so konzipiert, dass sie Lösungen bieten, die sicher, zuverlässig und privat sind. Die im Folgenden definierten technischen Maßnahmen beschreiben, wie GoTo dieses Konzept umsetzt und in der Praxis für GoTo Resolve anwendet.

2.1 Schutzmaßnahmen

Die Implementierung von Schutzmaßnahmen, Funktionen und Praktiken durch GoTo beinhaltet Folgendes:

I. Entwicklung von Produkten, bei denen Sicherheit und Datenschutz standardmäßig integriert sind, und Einbeziehung zusätzlicher Sicherheitsebenen zum Schutz von Kundeninhalten

II. Durchführung organisatorischer Kontrollen, die interne Richtlinien und Verfahren in Bezug auf die Einhaltung von Standards, Incident-Management, Anwendungssicherheit, Personalsicherheit und regelmäßige Schulungsprogramme operationalisieren

III. Sicherstellung, dass Datenschutzpraktiken vorhanden sind, die den Umgang mit und die Verwaltung von Daten in Übereinstimmung mit geltenden Gesetzen, einschließlich DSGVO, CCPA/CPRA, LGPD, sowie mit unserem eigenen Datenverarbeitungsnachtrag (DVN) und den geltenden Richtlinien und Verpflichtungen von GoTo regeln.

Durch Einbau von Sicherheitsvorkehrungen in das Produkt bemühen wir uns, GoTo-Kundeninhalte vor Bedrohungen zu schützen und sicherzustellen, dass die Sicherheitskontrollen der Art und dem Umfang der Dienste angemessen sind. Die konfigurierbaren Sicherheitsfunktionen von GoTo können Administratoren dabei helfen, Bedrohungen und Risiken, die von Benutzern der GoTo-Dienste ausgehen, für Systeme und Netzwerke zu minimieren.

3 Produktarchitektur

GoTo Resolve verwendet ein ASP-Modell (Application Service Provider), das für einen sicheren Betrieb sorgt und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt. Die Architektur ist so konzipiert, dass sie optimale Leistung, Zuverlässigkeit und Skalierbarkeit bietet. GoTo Resolve nutzt die Cloud-Ressourcen von Amazon Web Services und Microsoft Azure, um eine skalierbare, hochverfügbare Lösung ohne Single Point of Failure bereitzustellen. GoTo Resolve verwendet Backup-Systeme, die in mehreren Regionen gehostet werden, um bei hoher Auslastung oder bei einem Systemausfall den fortlaufenden Betrieb von Anwendungsprozessen zu ermöglichen.

3.1 Kommunikationsarchitektur

Eine Übersicht der Kommunikationsarchitektur von GoTo Resolve ist in der folgenden Abbildung dargestellt:

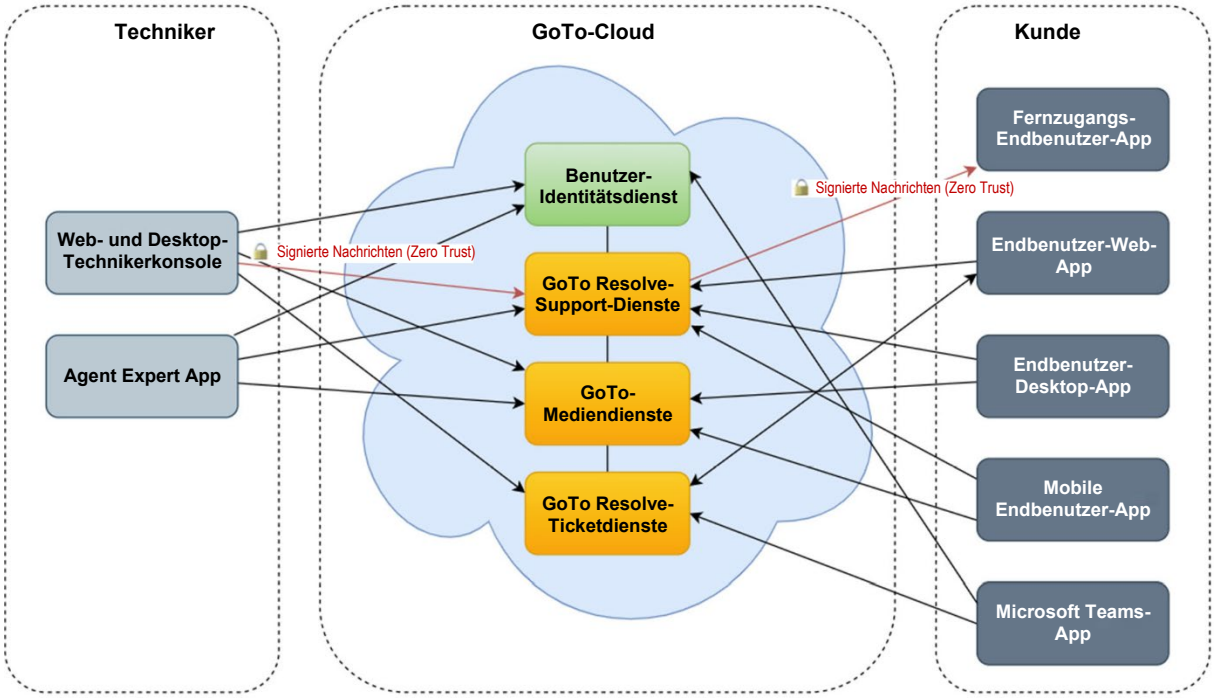

Abbildung 1: Kommunikationsarchitektur von GoTo Resolve

Die Authentifizierung von Technikern erfolgt über den GoTo-eigenen Benutzer-Identitätsdienst. Die Kommunikation zwischen den Teilnehmern einer GoTo Resolve-Sitzung erfolgt über einen Overlay-Netzwerkstack, der logisch über dem herkömmlichen User Datagram Protocol (UDP) und Transmission Control Protocol/Internet Protocol (TCP/IP) angeordnet ist. Dieses Netzwerk wird von GoTo Resolve und GoTo-Mediendiensten bereitgestellt, die auf Amazon Web Services und Microsoft Azure gehostet werden.

GoTo Resolve-Sitzungsteilnehmer (Web-Technikerkonsole, Desktop-Technikerkonsole, Agent Expert App und Endbenutzer-Endpunkte (in Abbildung 1 als „Kunden"-Endpunkte dargestellt)) kommunizieren mit GoTo Resolve und dem GoTo-Mediendienst über ausgehende TCP-Verbindungen an Port 443 oder UDP-Port 15000, je nach Verfügbarkeit. Da GoTo Resolve ein webbasierter Dienst ist, können die Teilnehmer von fast überall aus darauf zugreifen, sofern sie mit dem Internet verbunden sind – in einem Außenbüro, zu Hause, in einem Business Center oder im Netzwerk eines anderen Unternehmens.

3.2 Desktop-Technikerkonsole

Techniker können die Web-Technikerkonsole oder eine installierbare Desktop-Technikerkonsole verwenden, um sich mit GoTo Resolve zu verbinden. Die Desktopkonsole verwendet das plattformübergreifende Qt-Toolkit zur Ausführung unter MacOS und Windows und nutzt den Open-Source-Webbrowser Chromium zur Unterstützung von Komponenten der Webkonsole.

3.3 Zero-Trust-Modell

3.3.1 Architektur

GoTo Resolve basiert auf einer Zero-Trust-Architektur: Techniker, die GoTo Resolve verwenden, erstellen einen privaten Signaturschlüssel, der bei der Durchführung sensibler Aufgaben eine zusätzliche erforderliche Form der Verifizierung darstellt.

Wenn die Anwendung GoTo Resolve auf einem Remotegerät bereitgestellt wird, erstellt der Schlüssel einen Link zwischen dem Techniker und dem Gerät und identifiziert den Techniker eindeutig. Der Schlüssel verschlüsselt jeden Befehl, der an das bereitgestellte Remotegerät gesendet wird, und zeigt, wer die einzelnen Befehle sendet. Die Autorisierung von Befehlen basiert auf asymmetrischen Paaren aus privaten und öffentlichen Schlüsseln, wobei der private Schlüssel zum Signieren von Befehlen verwendet wird und nur dem Techniker bekannt ist (d. h. die GoTo Resolve-Dienste- oder Kunden-Endpunkte kennen ihn nicht). Der öffentliche Schlüssel wird auf jedem Endbenutzer-Endpunkt bereitgestellt und verwendet, um die Signatur jedes vom Techniker empfangenen Befehls zu verifizieren. Bei diesem Modell „vertrauen“ die Endbenutzer-Endpunkte nicht den GoTo Resolve-Diensten, sondern den Befehlen, die von einem Techniker mit einem autorisierten Schlüssel stammen.

3.3.2 Signaturschlüsseltypen

Der Kern des Signaturschlüssels ist ein Paar aus privatem und öffentlichem Schlüssel: Der öffentliche Schlüssel wird im Backend gespeichert und mit jedem Gerät geteilt, während der private Schlüssel seinen Rechner/Browser nie unverschlüsselt verlässt. Das Schlüsselpaar wird nach dem Zufallsprinzip im Browser des Technikers mit nativen Methoden in der elliptischen Kurve P-384 generiert.

Die kryptografischen Schlüsselpaare werden mit einem Passwort verschlüsselt und dann im Backend gespeichert, sodass der Techniker von jedem Browser aus darauf zugreifen kann. Der Verschlüsselungsschlüssel wird aus dem Passwort abgeleitet und ist für jedes Unternehmen und jeden Techniker unterschiedlich.

3.3.3 Verschlüsselungssammlungen

In den Verschlüsselungsoperationen der Zero-Trust-Architektur werden die folgenden Algorithmen verwendet:

- ECDSA mit elliptischer Kurve P-384 (für die Generierung privater und öffentlicher Schlüssel)
- Hash-Algorithmus SHA-256/512
- HMAC-SHA-256 (für die Authentifizierung von Nachrichten)
- AES256 mit GCM-Betriebsmodus für Blockchiffren (für die Schlüsselverschlüsselung)
- Schlüsselableitungsfunktion PBKDF2

Diese Kryptosysteme und Verschlüsselungsverfahren werden vom Betriebssystem oder der OpenSSL-Bibliothek verwaltet.

3.4 Problemdefinition

Die folgenden Diagramme (Abbildungen 2, 3 und 4) veranschaulichen, wie die Zero-Trust-Architektur von GoTo Resolve zum Schutz von Personen konzipiert ist. Abbildung 2 zeigt ein hypothetisches Szenario, das eintreten könnte, wenn ein Backend in einer Architektur ohne Zero Trust kompromittiert wird. Ein Angreifer wäre dann in der Lage, bösartige Inhalte auf den Runner-Instanzen bereitzustellen, indem er Aufträge erstellt.

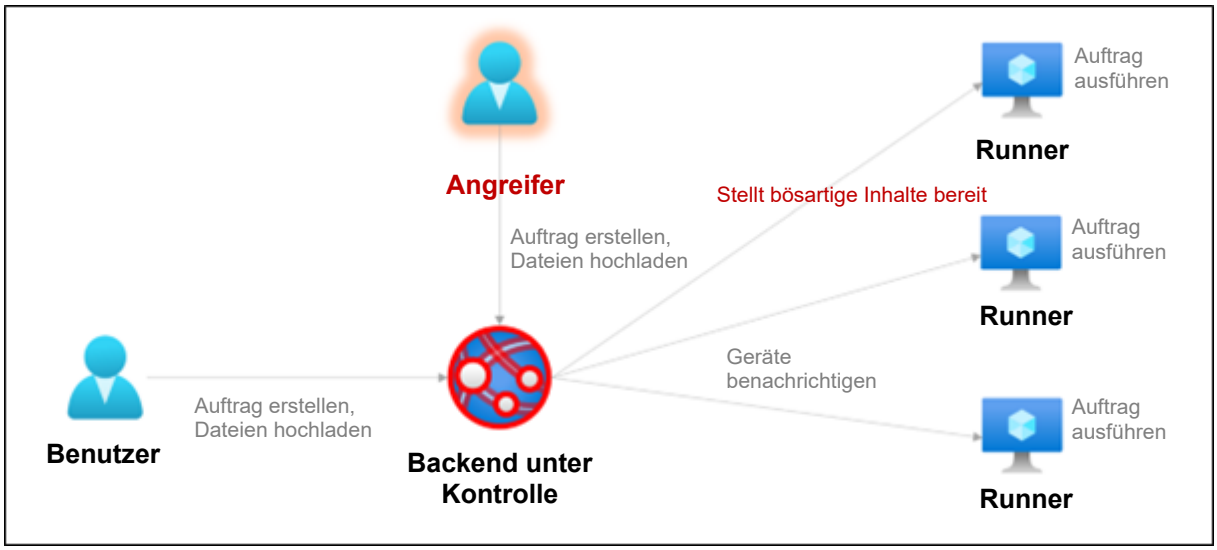

Abbildung 2: Kompromittiertes Backend-System ohne Zero Trust

Die Abbildungen 3 und 4 zeigen die Vorteile des Zero-Trust-Modells, bei dem jeder Auftrag mit dem (privaten) Signaturschlüssel des Benutzers signiert wird, bevor er an das Backend gesendet wird. Signierte Aufträge werden an die Runner-Instanzen weitergeleitet, die sie dann mit dem öffentlichen Schlüssel verifizieren können. Die Aufträge werden erst ausgeführt, wenn die Verifizierung des privaten und öffentlichen Schlüssels erfolgreich war. Abbildung 3 zeigt, wie Zero Trust einige dieser potenziellen Risiken zu vermeiden hilft.

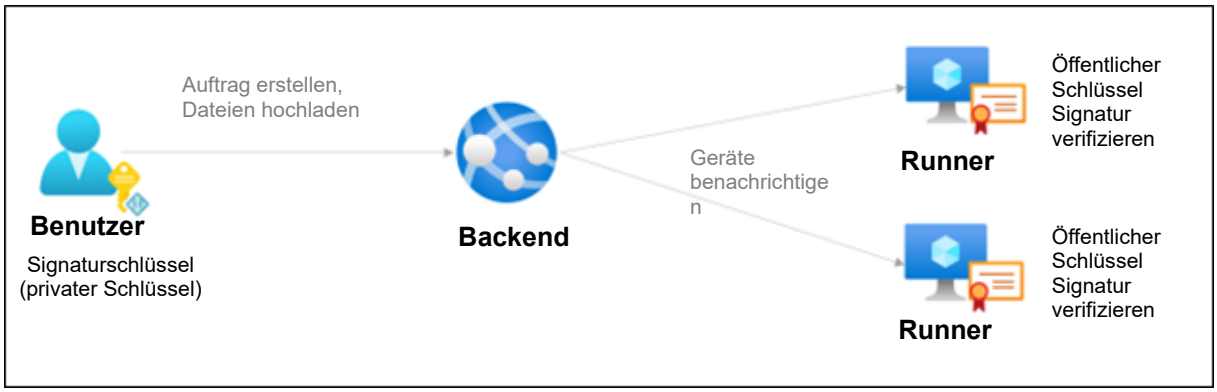

Abbildung 3 Auftragssignatur und Signaturverifizierung in Zero-Trust-Umgebung

Abbildung 4 zeigt ein hypothetisches Szenario, das eintreten könnte, wenn ein Backend in einer Zero-Trust-Umgebung kompromittiert wird. In diesem Szenario könnte der Angreifer nicht auf den Signaturschlüssel zugreifen und wäre daher nicht in der Lage, bösartige Inhalte bereitzustellen oder mit den Runner-Instanzen zu interagieren. In diesem Szenario würde die Verifizierung des privaten und öffentlichen Schlüssels fehlschlagen, und der Runner würde den Auftrag oder den Befehl verwerfen. Der Signaturschlüssel kann nicht aus dem öffentlichen Schlüssel wiederhergestellt werden.

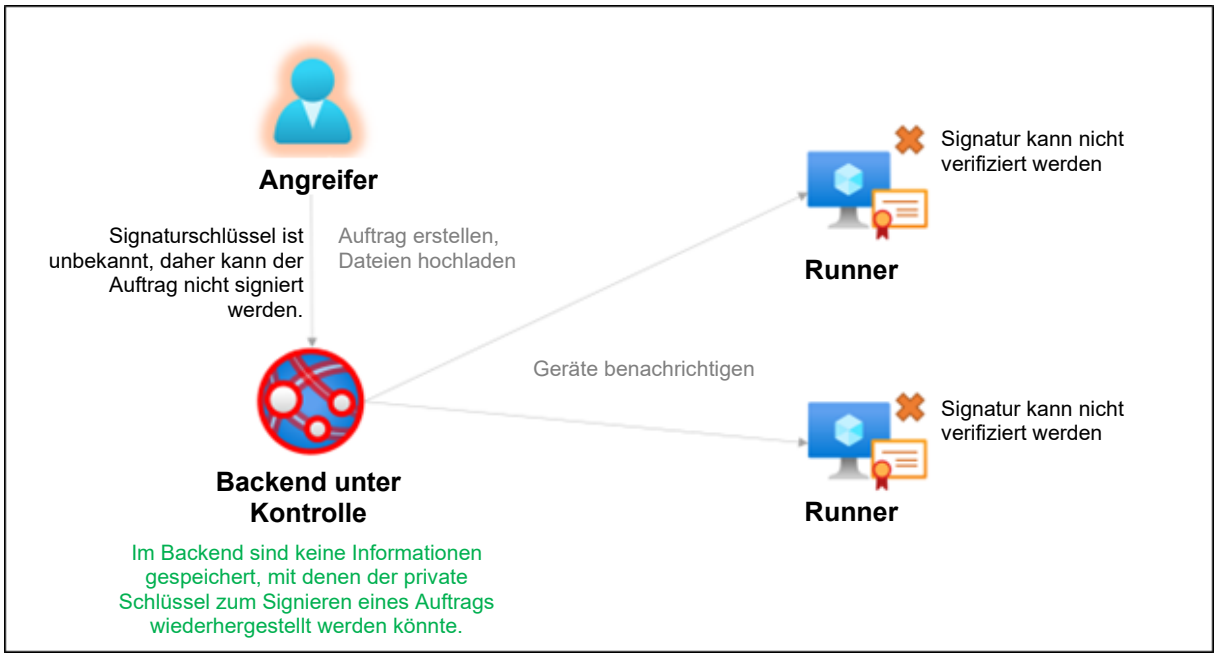

Abbildung 4: Kompromittiertes Backend in einer Zero-Trust-Umgebung

3.5 Infrastruktur für Mediendienste

Die Medieninfrastruktur besteht aus den folgenden Servern/Protokollen:

- Signalisierungsserver
- Session Traversal Utilities for NAT (STUN)- und Traversal Using Relay around NAT Secure (TURN(S))-Server

Der Signalisierungsserver verwendet sichere WebSockets (Vollduplex-Kommunikationskanäle), um gleichzeitig mit dem Endbenutzer und dem Techniker zu kommunizieren und die für den Aufbau der Peer-to-Peer-Verbindung erforderlichen Metadaten und Kontrollinformationen auszutauschen. Nach dem Upgrade der HTTPS-Verbindung kommunizieren der Client und der Server über dieselbe TCP-Verbindung und verwenden TLS 1.2 zur Absicherung der Verbindung.

WebRTC wird verwendet, um Echtzeitkommunikation (Real-Time Communication, RTC) für Webbrowser und Remotesupport-Anwendungen bereitzustellen. Alle WebRTC-Sitzungen verwenden die SRTP-Verschlüsselung (Secure Real-Time Transport Protocol). WebRTC verschlüsselt Informationen (insbesondere Datenkanäle) mit Datagram Transport Layer Security (DTLS) 1.2 im Fall von UDP- und TLS 1.2 im Fall von TCP-Verbindungen. Alle über den RTCDataChannel gesendeten Daten werden mit DTLS abgesichert.

DTLS-SRTP wird als sicheres Protokoll zum Austausch von Verschlüsselungsschlüsseln verwendet und erfordert die Übertragung von Verschlüsselungsschlüsseln von Peer zu Peer auf der Medienebene. Der TURNS-Server verwendet TLS 1.2 über TCP, um Daten zwischen den Peers weiterzuleiten.

4 Technische Sicherheitskontrollen

GoTo setzt technische Sicherheitskontrollen ein, die dafür entwickelt wurden, die Dienstinfrastruktur und die darin enthaltenen Daten zu schützen.

4.1 Verschlüsselung

GoTo überprüft regelmäßig seine Verschlüsselungsstandards und aktualisiert gegebenenfalls die verwendeten Verschlüsselungsverfahren und/oder Technologien entsprechend der Risikobewertung und der Marktakzeptanz neuer Standards.

4.1.1 Verschlüsselung während der Übertragung

GoTo verwendet TLS-Protokolle und zugehörige Verschlüsselungssammlungen, um Kundeninhalte während der Übertragung zu schützen.

Die Kommunikation zwischen Endbenutzer-Endpunkt und Backend wird über die OpenSSL-Bibliothek verschlüsselt. Die Sicherheitskontrollen für Kommunikation werden auf der TCP-Ebene über TLS-Lösungen implementiert.

Daten in Bildschirmübertragungen, Tastatur-/Maussteuerungsdaten, übertragene Dateien, Daten von Remotediagnosen und Informationen aus Text-Chats werden während der Übertragung mit TLS 1.2 verschlüsselt (ECDHE, DHE und RSA für den Schlüsselaustausch, RSA für die Authentifizierung, AES256 für die Datenverschlüsselung mit 384 oder 256-Bit-SHA-2-HMAC-Algorithmus). Sitzungsschlüssel werden serverseitig generiert und verbleiben dort, um die Verbindung mit dem Endbenutzer zu ermöglichen.

GoTo-Server authentifizieren sich bei Clients mit Zertifikaten mit öffentlichem Schlüssel, die von der globalen Stammzertifizierungsstelle DigiCert oder GlobalSign signiert werden, wenn Verbindungen zur GoTo Resolve-Website und zwischen GoTo Resolve-Komponenten hergestellt werden. Der Zugriff auf Server-zu-Server-APIs ist nur innerhalb des durch eine Firewall geschützten privaten Netzwerks von GoTo möglich.

4.1.2 Verschlüsselung ruhender Daten

Auf der Serverseite werden ruhende Kundeninhalte mit AES256 verschlüsselt, wobei der Galois Counter Mode (GCM) oder ähnliche moderne Betriebsmodi für Blockchiffren für zum Einsatz kommen. Auf der Client-Seite wurde die Client-Anwendung von GoTo so konfiguriert, dass sie die Zugangsdaten speichert und absichert, die die Verbindung zum Dienst über die Kryptografie-APIs des Betriebssystems ermöglichen. Kundeninhalte werden nicht clientseitig gespeichert.

4.2 Sicherheit der TCP-Schicht

TLS-Protokolle werden verwendet, um die Kommunikation zwischen öffentlichen Endpunkten zu schützen.

4.3 Schutz des Endbenutzer-Endpunkts

Endbenutzer-Desktop-Apps und Fernzugangs-Endbenutzer-Apps werden über ein digital signiertes Installationsprogramm heruntergeladen und installiert.

Das Installationsprogramm verwendet einen ausführbaren Download, der starke Verschlüsselungsmechanismen einsetzt, um den Endbenutzer davor zu schützen, versehentlich einen Trojaner oder andere Malware zu installieren, die sich als GoTo Resolve-Software ausgibt.

Die Endpunkt-Software von GoTo Resolve besteht aus mehreren digital signierten ausführbaren Dateien und dynamisch verknüpften Bibliotheken. In den Phasen der

Softwareentwicklung und -bereitstellung hat GoTo Verfahren zur Qualitätskontrolle und Konfigurationsverwaltung implementiert.

4.4 Benutzerauthentifizierung

Techniker und Kontoadministratoren werden anhand ihrer E-Mail-Adresse identifiziert und mit einem Passwort authentifiziert. Bei der autorisierten Authentifizierung wird das Passwort während der Übertragung verschlüsselt.

Die Authentifizierungsverfahren werden durch die folgenden Richtlinien geregelt:

Anforderungen an starke Passwörter: Die Passwörter müssen mindestens 8 Zeichen lang sein und sowohl Buchstaben als auch Ziffern enthalten. Passwörter müssen diese Mindestanforderungen erfüllen, wenn sie erstellt oder geändert werden.

Zwei-Faktor-Authentifizierung: Die optionale Zwei-Faktor-Authentifizierung kann auf Kontoebene aktiviert werden. Falls die Zwei-Faktor-Authentifizierung aktiviert ist, muss jeder Benutzer oder Endbenutzer innerhalb des Kontos seinen Zugriff über zwei separate Methoden autorisieren.

Kontosperrung: Nach fünf aufeinander folgenden fehlgeschlagenen Anmeldeversuchen wird für das Konto eines Benutzers oder Endbenutzers eine obligatorische „sanfte Sperre“ verhängt. Die sanfte Sperre verhindert fünf Minuten lang den Zugriff auf das Konto. Nach Ablauf der Sperrfrist kann der Benutzer oder Endbenutzer erneut versuchen, sich bei seinem Konto anzumelden.

4.5 Sicherheit während der Sitzung

Ein Benutzer kann eine laufende Fernzugangssitzung jederzeit beenden und die Fernzugangsberechtigungen des Technikers dauerhaft widerrufen.

5 Aktualisierungen des Sicherheitsprogramms

Mindestens einmal jährlich überprüft und aktualisiert GoTo sein Sicherheitsprogramm und beauftragt unabhängige Dritte mit der Bewertung seiner maßgeblichen Sicherheitskontrollen, um sicherzustellen, dass es sich an die aktuelle Bedrohungslage anpasst und mit den relevanten Rahmenwerken, Branchenstandards, Kundenverpflichtungen und ggf. Änderungen von Gesetzen und Vorschriften in Bezug auf die Sicherheit der GoTo-Daten konform ist.

6 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo ist so konzipiert, dass eine Replikation in nahezu Echtzeit an geografisch verteilten Standorten erfolgt. Datenbanken werden mit einer rollierenden inkrementellen Backup-Strategie gesichert. Im Notfall oder bei einem Totalausfall an einem der zahlreichen aktiven Standorte sind die verbleibenden Standorte so konzipiert, dass sie die Anwendungslast ausgleichen. Die Notfallwiederherstellung für diese Systeme wird regelmäßig getestet.

7 Rechenzentren

Die GoTo-Infrastruktur setzt auf die folgenden Komponenten, um die Zuverlässigkeit des Diensts zu erhöhen und das Risiko von Ausfallzeiten aufgrund eines Single Point of Failure zu verringern:

a) redundante, aktiv-passive Rechenzentren oder
b) Rechenzentren von Cloud-Hosting-Anbietern

Bei der Kontoerstellung können GoTo Resolve-Kunden wählen, ob sie ihre Kundeninhalte in der Dateninfrastruktur von GoTo in der Europäischen Union oder an einem globalen Standort speichern möchten. Die Hosting-Standorte sind unten aufgeführt[2]:

- **Europäische Union:** Deutschland, Irland, Schweden und die Niederlande
- **Global:** USA, Deutschland, Singapur, Indien und die Niederlande

In allen Rechenzentren werden die Umgebungsbedingungen überwacht und Daten rund um die Uhr durch die nachfolgend erläuterten physischen Sicherheitsvorkehrungen geschützt.

7.1 Physische Sicherheit im Rechenzentrum

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungskontrollen für Systeme und Server mit Kundeninhalten zu gewährleisten. Zu diesen Kontrollen gehören die folgenden:

- Videoüberwachung und -aufzeichnung
- HLK-Temperaturregelung (Heizung, Lüftung und Klimatisierung)
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung
- Doppelböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen natürlichen und vom Menschen verursachten Katastrophen, je nach Geografie und Standort des jeweiligen Rechenzentrums
- Planmäßige Wartung und Validierung aller kritischen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu den Produktionsdatenzentren auf autorisierte Personen. Um Zugang zu einem On-Premise-Serverraum oder zu einer Hosting-Einrichtung eines Drittanbieters zu erhalten, muss ein Antrag über das entsprechende Ticketsystem gestellt werden, der vom zuständigen Manager genehmigt und vom technischen Betriebsteam von GoTo überprüft und genehmigt werden muss. Der gesamte physische Zugang zu Rechenzentren und Serverräumen wird protokolliert, und die Protokolle werden vom GoTo-Management mindestens vierteljährlich überprüft. Darüber hinaus wird die Autorisierung für den physischen Zugang zum Rechenzentrum bei einem Rollenwechsel (wenn ein solcher Zugang nicht mehr erforderlich ist) oder bei Kündigung oder Austritt eines zuvor autorisierten Mitarbeiters umgehend aufgehoben. Für hochsensible Bereiche, zu denen auch Rechenzentren gehören, ist eine Multifaktor-Authentifizierung (z. B. Biometrie, Ausweis und Tastatur) erforderlich, um Zugang zu erhalten.

[2] Die Hosting-Standorte können variieren (d. h. abhängig von der Wahl des Datenspeicherorts verschieden sein). Lesen Sie die entsprechende Offenlegung der Unterauftragsverarbeiter für GoTo Resolve (GoTo Resolve Sub-Processor Disclosure), die Sie im Abschnitt „Product Resources“ des GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center) finden.

8 Einhaltung von Standards

GoTo prüft regelmäßig die Einhaltung der geltenden rechtlichen, sicherheitstechnischen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen. Die Datenschutz- und Sicherheitsprogramme von GoTo erfüllen strenge und international anerkannte Standards, wurden nach umfassenden externen Audit-Standards bewertet und haben wichtige Zertifizierungen erhalten, darunter:

- **TRUSTe Enterprise Privacy- und Data Governance Practices-Zertifizierung** für betriebliche Datenschutz- und Datensicherheitskontrollen, die mit den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzrahmenwerken übereinstimmen. Um mehr zu erfahren, besuchen Sie unseren Blogbeitrag.
- **TRUSTe APEC CBPR- und PRP-Zertifizierungen** für die Übertragung von Kundeninhalten zwischen APEC-Mitgliedsländern, erworben und unabhängig validiert von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für Datenschutz-Compliance. Um mehr über unsere APEC-Zertifizierungen zu erfahren, klicken Sie hier.
- Internationale Organisation für Normung – **ISO/IEC 27001:2013** ISMS-Zertifizierung (Managementsystem für Informationssicherheit).
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Typ II** Zertifizierungsbericht inkl. **BSI Cloud Computing Katalog (C5)**.
- **Payment Card Industry Data Security Standard (PCI DSS)**-Compliance für die E-Commerce- und Zahlungsumgebungen von GoTo.
- Bewertung der internen Kontrollen, wie im Rahmen einer Jahresabschlussprüfung des **Public Company Accounting Oversight Board (PCAOB)** erforderlich.

9 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo folgt dem Microsoft Security Development Lifecycle (SDL), um den Produktcode zu abzusichern. Das Microsoft SDL-Programm umfasst manuelle Codeprüfungen, Bedrohungsmodellierung, statische Codeanalyse, dynamische Analyse und Systemhärtung. GoTo-Teams führen außerdem regelmäßig dynamische und statische Schwachstellenprüfungen von Anwendungen und Penetrationstests für bestimmte Umgebungen durch.

10 Protokollierung, Überwachung und Warnmeldungen

GoTo unterhält Richtlinien und Verfahren für Protokollierung, Überwachung und Warnmeldungen, in denen die Grundsätze und Kontrollen festgelegt werden, die implementiert wurden, um unsere Fähigkeit zur Erkennung verdächtiger Aktivitäten und zur rechtzeitigen Reaktion darauf zu verbessern. GoTo sammelt identifizierten anomalen oder verdächtigen Datenverkehr in den entsprechenden Sicherheitsprotokollen der jeweiligen Produktionssysteme.

11 Endpoint Detection and Response (EDR)

EDR-Software (Endpoint Detection and Response) mit Audit-Protokollierung wird auf allen GoTo-Servern eingesetzt, um Unterbrechungen oder Auswirkungen auf die Leistung des Diensts zu minimieren. Wenn verdächtige Aktivitäten entdeckt werden, werden Sicherheitsuntersuchungen gemäß unseren Verfahren zur Reaktion auf Vorfälle eingeleitet, sofern dies angemessen und notwendig ist. In Abschnitt 17 finden Sie weitere Informationen über das GoTo Security Operations Center und die Verfahren zur Reaktion auf Vorfälle.

12 Bedrohungsmanagement

Das Cyber Security Incident Antwort-Team („CSIRT“) von GoTo besteht aus mehreren Teams und ist für den Schutz vor Cyberbedrohungen zuständig. Speziell das Cyber Threat Intelligence-Team innerhalb des CSIRT sammelt, prüft und verbreitet Informationen über aktuelle und neu auftretende Bedrohungen. Durch ständige Überprüfung von Open- und Closed-Source-Software und sowie die Teilnahme an Austauschgruppen und Mitgliedschaft in Branchenverbänden (IT-ISAC, FIRST.org usw.) hält sich GoTo über Bedrohungsforschung und -abwehr auf dem Laufenden.

13 Sicherheits- und Schwachstellenscans sowie Patch-Management

GoTo unterhält ein formelles Patch-Management-Programm und führt mindestens vierteljährlich Patch-Management-Aktivitäten für alle relevanten Systeme, Geräte, Firmware, Betriebssysteme, Anwendungen und andere Software durch, die Kundeninhalte verarbeiten. Mindestens einmal im Monat sowie nach jeder wesentlichen Änderung dieser Systeme führt GoTo Bewertungen durch und sucht nach Schwachstellen auf Systemebene sowie in internen und externen Hosts/Netzwerken („Systeme“) und behebt die betreffenden entdeckten Schwachstellen in Übereinstimmung mit dokumentierten Richtlinien, die die Abhilfemaßnahmen auf Basis des Risikos priorisieren.

14 Logische Zugriffskontrolle

Verfahren zur logischen Zugriffskontrolle sollen das Risiko eines unbefugten Anwendungszugriffs und des Datenverlusts in Unternehmens- und Produktionsumgebungen verringern. Mitarbeitern wird der Zugriff auf bestimmte GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte nach dem Prinzip der geringsten Rechte gewährt. Benutzerberechtigungen werden auf der Grundlage der funktionalen Rolle (rollenbasierte Zugriffskontrolle) und der Umgebung unter Verwendung von Kontrollen, Prozessen und/oder Verfahren zur Aufgabentrennung getrennt.

Die Produktionsserver sind nur über ein virtuelles privates Netzwerk (VPN) verfügbar. Für den Zugriff auf cloudbasierte Produktionskomponenten ist eine Authentifizierung über Self Service Unix (SSU) erforderlich.

14.1 Berechtigungsbasierte Zugriffskontrolle

14.1.1 Interaktive Sitzung

Ein wesentlicher Bestandteil des Sicherheitskonzepts von GoTo Resolve ist das auf Berechtigungen basierende Zugriffskontrollmodell, das den Zugriff auf das System und die Daten des Endbenutzers schützen soll. Bei interaktiven Live-Supportsitzungen (an denen der Endbenutzer teilnimmt), wird der Endbenutzer um Erlaubnis gebeten, bevor eine Bildschirmübertragung oder Remotesteuerung eingeleitet wird oder Dateien übertragen werden.

Sobald die Remotesteuerung und die Bildschirmübertragung während einer interaktiven Sitzung genehmigt wurden, kann der Endbenutzer alles beobachten, was der Techniker tut. Der Endbenutzer kann jederzeit wieder die Kontrolle übernehmen oder die Sitzung beenden.

14.1.2 Fernzugangssitzung

Für den Fernzugang muss die Fernzugangs-Endbenutzer-App auf dem Gerät des Endbenutzers installiert sein. Sie kann auf zwei Arten eingerichtet werden: Setup in Sitzung (während einer interaktiven Sitzung) oder mit einem Installationsprogramm außerhalb der Sitzung, wobei in beiden Fällen die Genehmigung des Endbenutzers erforderlich ist.

Setup in Sitzung: Sobald der Endbenutzer und der Techniker einer interaktiven Sitzung beigetreten sind, kann der Techniker eine spezielle Berechtigung zur Installation der Fernzugangs-Endbenutzer-App anfordern. Der Endbenutzer wird um Genehmigung gebeten und muss diese ausdrücklich erteilen.

Installationsprogramm außerhalb der Sitzung: Nachdem sich der Techniker sicher bei GoTo Resolve-Website oder in der Desktop-Anwendung angemeldet hat, kann er ein Installationsprogramm herunterladen, das die Installation der Fernzugangs-Endbenutzer-App auf jedem Windows-PC oder Mac ermöglicht, auf den der Techniker Administratorzugriff hat.

14.1.3 Rollenbasierte Zugriffskontrolle

GoTo Resolve ermöglicht den Zugriff auf eine Vielzahl von Ressourcen und Diensten mithilfe eines rollenbasierten Zugriffskontrollsystems. Die folgenden Rollen sind definiert:

Kontoadministrator: GoTo Resolve-Benutzer mit vollen Administratorrechten zur Durchführung von Administrationsfunktionen in Bezug auf Techniker. Kontoadministratoren können Technikerkonten erstellen, ändern und löschen und Abonnementdaten ändern.

Techniker: GoTo Resolve-Benutzer, der GoTo Resolve-Sitzungen initiieren kann, um Endbenutzern per Bildschirmanzeige, Remotesteuerung oder Kameraübertragung technische Hilfe zu leisten.

Endbenutzer: Benutzer und andere Personen, die GoTo-Dienste nutzen (z. B. eine nicht authentifizierte Person, die den Techniker um Support bittet). Der Endbenutzer kann Sitzungen schließen und muss dem Techniker Berechtigungen zum Zugreifen auf sein Gerät gewähren.

15 Datentrennung

GoTo hat Kontrollen implementiert, um zu verhindern, dass Benutzer die Daten anderer Benutzer sehen können. GoTo nutzt zum Beispiel eine logisch auf Datenbankebene getrennte Multi-Tenant-Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Die Parteien müssen sich authentifizieren, um Zugriff auf ein Konto zu erhalten.

16 Perimeterabwehr und Erkennung von Eindringversuchen

GoTo verwendet Tools, Techniken und Dienste zum Schutz des Perimeters, um zu verhindern, dass unbefugter Netzwerkdatenverkehr in die Produktinfrastruktur von GoTo gelangt. Zu diesen Maßnahmen zählen unter anderem:

- Systeme zur Erkennung von Eindringversuchen, die Systeme, Dienste, Netzwerke und Anwendungen auf unbefugten Zugriff überwachen
- Überwachung kritischer System- und Konfigurationsdateien
- Web Application Firewall (WAF) und DDoS-Präventionsdienste auf der Anwendungsschicht, die als Proxy für den GoTo-Datenverkehr fungieren
- AWS-Sicherheitsgruppen auf GoTo-Webservern, die eingehende und ausgehende Verbindungen filtern, darunter auch interne Verbindungen zwischen GoTo-Systemen
- Interne Netzwerksegmentierung

17 Sicherheitsmaßnamen und Incident-Management

Das GoTo Security Operations Center (SOC) ist für die Erkennung von und die Reaktion auf Sicherheitsereignisse zuständig. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um potenzielle Probleme zu identifizieren, und hat Verfahren zur Reaktion auf Vorfälle entwickelt, einschließlich eines dokumentierten Notfallplans.

Der GoTo-Notfallplan ist auf die Prozesse, Richtlinien und Standardbetriebsverfahren von GoTo für kritische Kommunikation abgestimmt. Er wurde entwickelt, um relevante mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten des Unternehmens (einschließlich GoTo Resolve) zu verwalten, zu identifizieren und zu beheben. Im Notfallplan sind Mechanismen festgelegt, mit denen Mitarbeiter mutmaßliche Sicherheitsereignisse melden können, sowie Eskalationswege, die gegebenenfalls zu befolgen sind. Mutmaßliche Ereignisse werden dokumentiert und ggf. über standardisierte Ereignistickets eskaliert und nach ihrer Kritikalität eingestuft.

18 Löschung und Rückgabe von Inhalten

Löschung und/oder Rückgabe: Kunden können die Rückgabe und/oder Löschung ihrer Kundeninhalte anfordern, indem sie einen Antrag über das Portal zur Verwaltung individueller Rechte (Individual Rights Management Portal, IRM) von GoTo stellen, und zwar über support.goto.com oder per E-Mail an privacy@goto.com. Anträge werden innerhalb von dreißig (30) Tagen nach Eingang bei GoTo bearbeitet. Sollten wir jedoch mehr Zeit benötigen, werden wir Sie so schnell wie möglich über die voraussichtliche Verzögerung und den neuen Abschlusstermin informieren.

Zeitplan für die Aufbewahrung von Kundeninhalten: Sitzungsaufzeichnungen werden rollierend nach jeweils 90 Tagen gelöscht.[3] Darüber hinaus werden die Kundeninhalte nach folgenden Kriterien automatisch gelöscht, sofern das geltende Recht nichts anderes vorschreibt: 1) kostenpflichtige Konten neunzig (90) Tage nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden oder 2) kostenlose Konten nach zwei (2) Jahren Inaktivität (z. B. keine Anmeldungen).

Auf schriftliche Anfrage kann GoTo die Löschung von Inhalten schriftlich bestätigen/bescheinigen.

19 Organisatorische Kontrollen

19.1 Sicherheitsrichtlinien und -verfahren

GoTo unterhält einen umfassenden Satz von Sicherheitsrichtlinien und -verfahren, die regelmäßig überprüft und bei Bedarf aktualisiert werden, um den Sicherheitszielen von GoTo, Änderungen der geltenden Gesetze, Branchenstandards und Compliance-Bemühungen zu entsprechen.

19.2 Änderungsmanagement

GoTo unterhält ein geeignetes Änderungsmanagement-Verfahren. Änderungen an GoTo-Systemen werden vor der Implementierung bewertet, getestet und genehmigt, um das Risiko einer Unterbrechung der GoTo-Dienste zu verringern.

19.3 Programme für Sicherheitssensibilisierung und -schulung

Das GoTo-Programm zur Sensibilisierung für Datenschutz und Sicherheit beinhaltet die Schulung der Mitarbeiter über die Bedeutung eines ethisch korrekten, verantwortungsvollen, gesetzeskonformen und sorgfältigen Umgangs mit personenbezogenen Daten und vertraulichen Informationen. Neu eingestellte Mitarbeiter, Vertragspartner und Praktikanten werden beim Onboarding über die Sicherheitsrichtlinien und den betrieblichen Verhaltenskodex und die ethischen Grundsätze von GoTo informiert. GoTo-Mitarbeiter absolvieren mindestens einmal jährlich eine Schulung zum Thema Datenschutz und Sicherheit. Sensibilisierungsmaßnahmen finden das ganze Jahr über statt und können Kampagnen zum Datenschutztag, zum Cybersecurity Awareness Month, Webinare mit dem Chief Information Security Officer und ein Programm für Sicherheits-Champions umfassen.

Gegebenenfalls müssen die Mitarbeiter auch rollenspezifische Schulungen absolvieren. Darüber hinaus müssen alle Mitarbeiter, Vertragspartner und Tochtergesellschaften von GoTo die Richtlinien von GoTo in Bezug auf Sicherheit und Datenschutz lesen und befolgen.

20 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten unserer Kunden, Benutzer und Endbenutzer sehr ernst und verpflichtet sich, relevante Praktiken zur Datenverarbeitung und -verwaltung offen und transparent darzulegen.

20.1 Datenschutzprogramm

GoTo unterhält ein umfassendes Datenschutzprogramm, für das Koordination mehrerer Funktionen innerhalb des Unternehmens erforderlich ist, darunter Datenschutz, Sicherheit, Governance, Risiko und Compliance (GRC), Recht, Produkt, Technik und Marketing. Dieses Datenschutzprogramm konzentriert sich auf die Einhaltung von Vorschriften und

[3] Kunden mit anderen Aufbewahrungsanforderungen können sich dafür entscheiden, Aufzeichnungen lokal an einem Speicherort ihrer Wahl außerhalb der GoTo-Umgebung zu speichern. Weitere Informationen finden Sie hier im Abschnitt „Abspielen von Sitzungsaufzeichnungen“.

umfasst die Implementierung und Pflege interner und externer Richtlinien, Standards und Ergänzungen zur Regelung der Praktiken des Unternehmens.

20.2 Einhaltung behördlicher Vorschriften

20.2.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) bzgl. des Schutzes der Daten und der Privatsphäre aller Personen in der EU. GoTo unterhält ein umfassendes Programm zur Sicherstellung der DSGVO-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die der DSGVO unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen der DSGVO tun. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

Der California Consumer Privacy Act in der Fassung des California Privacy Rights Act (gemeinsam als „CCPA“ bezeichnet), gewährt den kalifornischen Bürgern zusätzliche Rechte und zusätzlichen Schutz in Bezug auf die Verwendung ihrer persönlichen Informationen durch Unternehmen. GoTo unterhält ein umfassendes Programm zur Sicherstellung der CCPA-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die dem CCPA unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen des CCPA tun. Weitere Informationen über die Einhaltung des CCPA finden Sie in der Datenschutzrichtlinie von GoTo und den Ergänzenden Offenlegungen nach dem California Consumer Privacy Act.

20.2.3 LGPD

Das brasilianische Datenschutzgesetz (LGPD) regelt die Verarbeitung personenbezogener Daten in Brasilien und/oder von Personen, die sich zum Zeitpunkt der Datenerfassung in Brasilien befinden. GoTo unterhält ein umfassendes Programm zur Sicherstellung der LGPD-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten verarbeitet, die dem LGPD unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen des LGPD tun. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

20.3 Datenverarbeitungsnachtrag

GoTo bietet einen globalen Datenverarbeitungsnachtrag (DVN) an, der auf Englisch und Deutsch verfügbar ist. Dieser DVN erfüllt die Anforderungen von DSGVO, CCPA, LGPD und anderen geltenden Vorschriften und regelt die Verarbeitung von Kundeninhalten durch GoTo.

Unser DVN enthält mehrere auf die DSGVO ausgerichtete Datenschutzmaßnahmen, darunter:

(a) Details zur Datenverarbeitung und Offenlegungen der Unterauftragsverarbeiter unter Artikel 28
(b) überarbeitete (2021) Standardvertragsklauseln (auch bezeichnet als EU-Musterklauseln) und
(c) produktspezifische technische und organisatorische Maßnahmen von GoTo.

Um den Anforderungen des CCPA Rechnung zu tragen, umfasst unser globaler DVN außerdem:

(a) überarbeitete Definitionen, die dem CCPA zugeordnet sind
(b) Zugriffs- und Löschrechte

(c) Garantien, dass GoTo die persönlichen Informationen unserer Kunden, Benutzer und Endbenutzer nicht verkauft

Unser globaler DVN enthält außerdem Bestimmungen zu folgenden Punkten:

(a) Einhaltung des LGPD durch GoTo
(b) Unterstützung der rechtmäßigen Übertragung personenbezogener Daten nach/aus Brasilien
(c) Sicherstellung, dass unsere Benutzer die gleichen Vorteile beim Datenschutz genießen wie unsere anderen Benutzer in aller Welt.

20.4 Abkommen zur Datenübertragung

GoTo unterstützt die rechtmäßige internationale Übertragung von Daten im Rahmen der folgenden Abkommen:

20.4.1 Standardvertragsklauseln

Die Standardvertragsklauseln (Standard Contractual Clauses, SCCs), die manchmal auch als EU-Musterklauseln bezeichnet werden, sind standardisierte Vertragsbedingungen, die von der Europäischen Kommission anerkannt und übergenommen wurden, um sicherzustellen, dass alle personenbezogenen Daten, die den Europäischen Wirtschaftsraum (EWR) verlassen, in Übereinstimmung mit dem EU-Datenschutzrecht übertragen werden. Die 2021 überarbeiteten und herausgegebenen SCCs wurden in den globalen DVN von GoTo integriert, um GoTo-Kunden die Übertragung von Daten aus dem EWR in Übereinstimmung mit der DSGVO zu ermöglichen.

20.4.2 Ergänzende Maßnahmen

Zusätzlich zu den in diesen TOMs genannten Maßnahmen hat GoTo eine FAQ erstellt, die die zusätzlichen Maßnahmen zur Unterstützung rechtmäßiger Übertragungen gemäß Kapitel 5 der DSGVO darlegt und alle vom Europäischen Gerichtshof in Verbindung mit der Verwendung der SCCs empfohlenen Einzelfallanalysen behandelt und leitet.

20.4.3 Zertifizierung nach APEC CBPR und PRP

GoTo ist gemäß APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft) CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) zertifiziert. Die APEC CBPR- und PRP-Rahmenwerke wurden als erste ihrer Art für die Übertragung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt und von TrustArc, einem von der APEC anerkannten Drittanbieter für Datenschutz-Compliance, erworben und unabhängig validiert.

20.5 Datenanfragen

GoTo unterhält umfassende Prozesse, um die Entgegennahme von datenschutz- und sicherheitsbezogenen Anfragen zu erleichtern. Dazu gehören das IRM-Portal, die Datenschutz-E-Mail-Adresse (privacy@goto.com) und der Kundensupport unter https://support.goto.com.

20.6 Offenlegungen der Unterauftragsverarbeiter und Rechenzentren

GoTo veröffentlicht die Offenlegungen der Unterauftragsverarbeiter in seinem Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Diese Offenlegungen enthalten die Namen, Standorte und Verarbeitungszwecke von Datenhosting-Anbietern und anderen Drittanbietern, die Kundeninhalte im Rahmen der Bereitstellung des Diensts für GoTo-Kunden verarbeiten.

20.7 Einschränkungen bei der Verarbeitung sensibler Daten

Die folgenden Arten von sensiblen Daten dürfen nicht in GoTo Resolve hochgeladen oder GoTo auf andere Weise zur Verfügung gestellt werden, es sei denn, GoTo hat dies ausdrücklich verlangt oder der Kunde hat eine anderweitige schriftliche Genehmigung von GoTo erhalten:

- Von der Regierung ausgestellte Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen, die sich auf die Gesundheit einer Person beziehen, einschließlich, aber nicht beschränkt auf geschützte Gesundheitsinformationen (Protected Health Information, PHI) gemäß Definition im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) sowie anderen einschlägigen geltenden Gesetzen und Vorschriften.
- Informationen im Zusammenhang mit Finanzkonten und Zahlungsinstrumenten, einschließlich, aber nicht beschränkt auf, Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung bezieht sich auf ausdrücklich gekennzeichnete Zahlungsformulare und -seiten, die von GoTo verwendet werden, um Zahlungen für den Dienst einzuziehen.
- Alle Informationen, die durch geltende Gesetze und Vorschriften besonders geschützt sind, insbesondere Informationen über Rasse, ethnische Zugehörigkeit, religiöse oder politische Überzeugung, Mitgliedschaften einer Person in Organisationen usw.

20.8 Compliance in regulierten Umgebungen

Es liegt in der Verantwortung der Kunden, angemessene Richtlinien, Verfahren und andere Schutzmaßnahmen in Bezug auf die Verwendung von GoTo Resolve zur Unterstützung von Geräten in regulierten Umgebungen einzuführen.

21 Kontrollen der Sicherheits- und Datenschutzpraktiken von Drittanbietern

Vor der Beauftragung von Drittanbietern, die Kundeninhalte oder vertrauliche, sensible oder Mitarbeiterdaten verarbeiten, überprüft und analysiert GoTo die Sicherheits- und Datenschutzpraktiken des Anbieters über die entsprechenden Beschaffungskanäle. Gegebenenfalls holt GoTo in regelmäßigen Abständen Compliance-Dokumente oder -Berichte von Anbietern ein und wertet diese aus, um sicherzustellen, dass das Kontrollumfeld und die Standards der Anbieter weiterhin ausreichend sind.

GoTo schließt mit allen Drittanbietern schriftliche Vereinbarungen ab und verwendet entweder von GoTo genehmigte Beschaffungsvorlagen oder verhandelt die Standardbedingungen dieser Drittanbieter, um die von GoTo akzeptierten Datenschutz- und Sicherheitsstandards zu erfüllen, sofern dies für erforderlich gehalten wird. Die Teams für Finanzen, Recht, Datenschutz und Sicherheit sind an der Überprüfung der Anbieter beteiligt und verifizieren, ob die Anbieter die spezifischen obligatorischen Anforderungen für den Umgang mit Daten und die vertraglichen Anforderungen erfüllen, sofern dies erforderlich und/oder angemessen ist. Die GoTo-Richtlinien in Bezug auf Drittanbieterrisiken regeln die Anforderungen an den Datenschutz und die Sicherheit von Anbietern auf der Grundlage der Art und Dauer der Datenverarbeitung und der Zugriffsebene. Gegebenenfalls (z. B. wenn Kundeninhalte verarbeitet oder gespeichert werden) beinhalten die Vereinbarungen mit Anbietern Anforderungen zur „Einhaltung der geltenden Gesetze“, einen DVN oder ein ähnliches Dokument, das Themen wie DSGVO, CCPA, LGPD sowie Nutzungs- und Verkaufsbeschränkungen behandelt, je nach Bedarf. Der GoTo-DVN für Lieferanten enthält beispielsweise Beschränkungen bzgl. des „Verkaufs“ von Daten gemäß der Definition des CCPA. Entsprechend werden ergänzende Sicherheitsmaßnahmen mit geeigneten Kontrollen und Systemanforderungen mit den betreffenden Anbietern vereinbart.

22 Kontaktaufnahme mit GoTo

Für allgemeine Fragen können Kunden GoTo unter support.goto.com kontaktieren. Bei Fragen oder Anfragen in Bezug auf personenbezogene Daten oder Datenschutz besuchen Sie bitte unser IRM-Portal oder senden Sie eine E-Mail an privacy@goto.com.

23 Begriffserklärungen

Web-Technikerkonsole: Eine Web-Anwendung, die auf dem PC, Mac, Android- oder iOS-Tablet oder Chromebook des Technikers in einem der unterstützten Browser (Chrome, Firefox, Safari) ausgeführt wird und eine Verbindung zum GoTo Resolve-Dienst herstellt. Mit dieser Anwendung kann der Techniker GoTo Resolve-Sitzungen erstellen und abhalten sowie verschiedene Funktionen zur Kontoverwaltung, Dienstverwaltung und Berichterstellung ausführen.

Desktop-Technikerkonsole: Eine Desktop-Anwendung, die auf MacOS- und Windows-Computern ausgeführt wird und eine Verbindung zum GoTo Resolve-Dienst herstellt. Sie nutzt die Technologie der Web-Technikerkonsole für GoTo Resolve, Qt und die Chromium-Web-Engine. Sie bietet dieselbe Funktionalität wie die Web-Technikerkonsole, aber in einem nativen Erscheinungsbild.

Interaktive Sitzung: Eine Supportsitzung, bei der der Endbenutzer während der Sitzung anwesend ist und daran teilnehmen kann.

Endbenutzer-Desktop-App: Eine Desktop-Anwendung, die auf dem Computer des Endbenutzers (Windows oder Mac) ausgeführt wird und über den GoTo Resolve-Dienst eine Verbindung zu einer GoTo Resolve-Sitzung herstellt. Sie bietet eine Remotesteuerungsfunktion sowie andere erweiterte Funktionen und die Möglichkeit, die Fernzugangs-App auf dem Computer des Endbenutzers zu installieren.

Endbenutzer-Endpunkt: Ein Sammelbegriff, der sich auf jeden Endbenutzer-Endpunkt bezieht: Endbenutzer-Web-App, Endbenutzer-Desktop-App, Mobile Endbenutzer-App, Fernzugangs-Endbenutzer-App.

Mobile Endbenutzer-App: Eine mobile Anwendung (Android und iOS), die auf dem Mobilgerät/Tablet des Endbenutzers ausgeführt wird und über den GoTo Resolve-Dienst eine Verbindung zu einer GoTo Resolve-Sitzung herstellen kann. Sie bietet Funktionen zur Bildschirmanzeige (Android und iOS) und zur Remotesteuerung (nur Android).

Endbenutzer-Web-App: Eine Web-Anwendung, die in einem beliebigen unterstützten Browser auf dem Computer/Mobilgerät des Endbenutzers ausgeführt wird und über den GoTo Resolve-Dienst eine Verbindung zu einer GoTo Resolve-Sitzung herstellt. Sie bietet Funktionen für Chat, Bildschirmanzeige und Kameraübertragung sowie die Möglichkeit, die Sitzung jederzeit in eine Remotesteuerungssitzung umzuwandeln, indem die Endbenutzer-Desktop-App heruntergeladen oder die mobile Endbenutzer-App installiert wird.

Mediendienst: Eine Gruppe von global verteilten Servern mit Lastausgleich, die eine Vielzahl von hochverfügbaren Unicast- und Multicast-Kommunikationsdiensten auf der Grundlage von WebRTC-Protokollen bereitstellen.

GoTo Resolve-Sitzungen: Interaktive Sitzung mit Chat, Bildschirmanzeige, Remotesteuerung oder Kameraübertragung und Remotesteuerung per Fernzugang.

GoTo Resolve-Dienst: Eine Gruppe von global verteilten Servern mit Lastausgleich, die über eine verschlüsselte WebSocket-Verbindung und API-Aufrufe einen sicheren Zugriff für die Web-Technikerkonsole und die Endbenutzer-Endpunkte bieten.

Fernzugangs-Endbenutzer-App: Eine installierbare Desktop-Anwendung (Windows und iOS), die im Hintergrund auf dem Computer des Endbenutzers ausgeführt wird. Mit dieser App kann eine Endbenutzer-Desktop-App herunterladen und ausgeführt werden, um eine Verbindung zu einer autorisierten Fernzugangssitzung herzustellen.

Fernzugangssitzung: Eine Supportsitzung, bei der der Endbenutzer nicht anwesend ist. Die Sitzung wird vom Techniker ohne Beteiligung des Endbenutzers über eine autorisierte Fernzugangs-Endbenutzer-App initiiert und aufgebaut.

Benutzer: Personen mit Unterkonten innerhalb eines Kundenkontos (z. B. Mitarbeiter, Administratoren).

GoTo Resolve-Ticketdienste: Eine Backend-Anwendung, die die Helpdesk-Funktion von GoTo Resolve unterstützt. Außerdem ermöglicht sie die Kommunikation zwischen der MS Teams-App und GoTo Resolve.