TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR GOTO RESOLVE

OPERATIVE SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

Dieses Dokument hebt die technischen und organisatorischen Maßnahmen (TOMs) hervor, um Datenschutz und Sicherheit der Infrastruktur und Kommunikationskanäle von GoTo Resolve sicherzustellen.

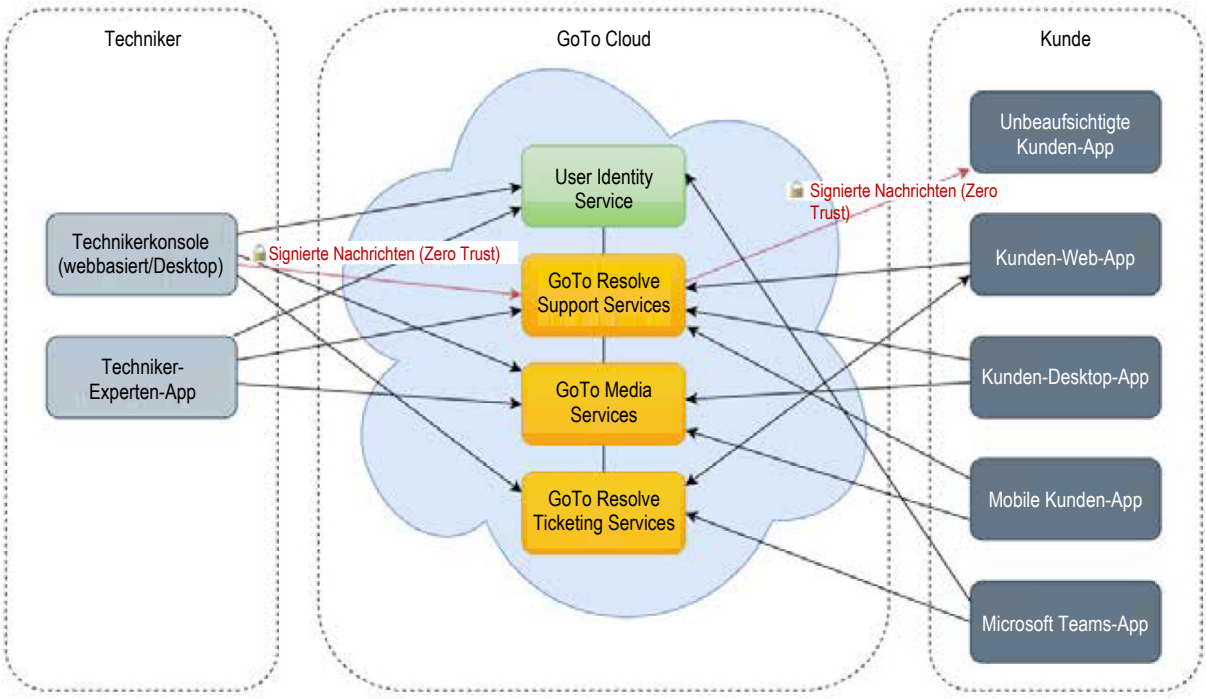
GoTo Resolve ermöglicht IT und Support-Mitarbeitern Fernsupport für Computer, Server und Mobilgeräte per Bildschirmanzeige, Fernsteuerung oder Kameraübertragung über eine Technikerkonsole (webbasiert oder Desktop). GoTo Resolve führt robuste Datensicherheits-maßnahmen durch, um vor passiven und aktiven Angriffen zu schützen.

2 Produktarchitektur

GoTo Resolve verwendet ein ASP-Modell (Application Service Provider), um für sichere Vorgänge bei der Integration mit einer vorhandenen Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens zu sorgen. Die Architektur ist auf optimale Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt. GoTo Resolve nutzt Amazon Web Services und Cloud-Ressourcen von Microsoft Azure, um eine skalierbare, hoch verfügbare Lösung ohne „Single Point of Failure“ bereitzustellen. Es verwendet in mehreren Regionen gehostete Backup-Systeme, um selbst bei hoher Last oder einem Systemausfall sicherzustellen, dass die Anwendungsprozesse weiterhin funktionieren.

2.1 Kommunikationsarchitektur

Die GoTo Resolve-Kommunikationsarchitektur ist in der Abbildung unten zusammengefasst.



Bei der Techniker-Authentifizierung kommt der User Identity Service von GoTo zum Einsatz. Die Kommunikation zwischen Teilnehmern in einer GoTo Resolve-Sitzung erfolgt über einen Overlay Networking Stack, der logisch auf dem konventionellen UDP und TCP/IP aufsetzt. Dieses Netzwerk wird vom GoTo Resolve Service und Media Service bereitgestellt (gehostet von Amazon Web Services und Microsoft Azure). Teilnehmer an GoTo Resolve-Sitzungen (webbasierte Technikerkonsole, Desktop-Technikerkonsole und Kunden-Endpunkte) kommunizieren mit dem GoTo Resolve Service und dem Media Service unter Verwendung ausgehender TCP-Verbindungen auf Port 443 oder UDP-Port 15000, abhängig von der Verfügbarkeit. Da GoTo Resolve ein webbasierter Service ist, können Teilnehmer sich nahezu überall befinden, wo es Internet gibt − im Remote Office, zu Hause, in einem Business Center oder verbunden mit dem Netzwerk eines anderen Unternehmens.

2.2 Desktop-Technikerkonsole

Die Techniker können die webbasierte Technikerkonsole oder die installierbare Desktop-Technikerkonsole verwenden, um sich mit dem GoTo Resolve-Service zu verbinden. Die Desktop-Konsole verwendet das plattformübergreifende Qt-Toolkit zur Ausführung unter MacOS und Windows und nutzt den Open-Source-Webbrowser Chromium für Komponenten der Webkonsole.

3 GoTo Resolve – technische Kontrollen

GoTo nutzt technische Kontrollen nach Branchenstandard gemäß der Art und Weise und des Umfangs der Services (gemäß Definition in den Nutzungsbedingungen). Diese Kontrollen wurden zum Schutz der Service-Infrastruktur und des darin enthaltenen Kundeninhalts entwickelt. Sie finden die Nutzungsbedingungen unter https://www.goto.com/company/legal/terms-and-conditions.

3.1 Authentifizierung

GoTo Resolve-Techniker und -Kontoadministratoren werden durch ihre E-Mail-Adresse identifiziert und unter Verwendung eines Passworts authentifiziert. Bei der autorisierten Authentifizierung wird das Passwort nie in unverschlüsseltem Zustand übertragen.

Authentifizierungsverfahren sind durch folgende Richtlinien geregelt:

Starke Passwörter: Ein starkes Passwort muss mindestens 8 Zeichen lang sein und ausreichende Komplexitätsanforderungen erfüllen (d. h. Buchstaben und Zahlen aufweisen). Passwörter werden beim Erstellen oder Ändern auf ihre Stärke überprüft.

Zwei-Faktor-Authentifizierung: Als zusätzliche Sicherheitsmaßnahme ist optional Zwei-Faktor-Authentifizierung für jedes GoTo Resolve-Unternehmenskonto verfügbar. Bei Aktivierung erfordert die Zwei-Faktor-Authentifizierung, dass sich jeder Benutzer beim Zugriff über zwei separate Methoden autorisiert.

Kontosperre: Nach fünf aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen wird das Benutzerkonto in einen obligatorischen Soft Lockout-Zustand versetzt. Das bedeutet, dass der Inhaber des Benutzerkontos sich fünf Minuten nicht anmelden kann. Nach Ablauf des Sperrzeitraums kann der Inhaber des Benutzerkontos versuchen, sich erneut anzumelden.

3.2 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt. Sie dienen dazu, die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen und einen Datenverlust in Unternehmens- und Produktionsumgebungen zu verhindern oder zu minimieren. Mitarbeiter erhalten bei Bedarf minimalen Zugriff (oder „Least Privilege“-Zugriff) auf angegebene GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte. Zudem sind Benutzerrechte basierend auf der funktionalen Rolle und Umgebung voneinander getrennt.

Benutzer, die zum Zugriff auf GoTo Resolve-Produktkomponenten autorisiert sind, können autorisierte technische Mitarbeiter von GoTo (z. B. Technikabteilung und Engineering DevOps), Kundenadministratoren oder Endbenutzer des Produkts sein. Produktionsserver sind nur über das Virtual Private Network (VPN) von Operations verfügbar. Zudem sind sie durch die rollenbasierte Zugriffskontrolle geschützt, um nicht autorisierten Zugriff zu verhindern. Cloud-basierte Produktionskomponenten sind über SSU-Authentifizierung (Self Service Unix) verfügbar.

3.2.1 Zugriffskontrolle nach dem Zero-Trust-Prinzip

In diesem Modell sind die GoTo Resolve-Services nicht vertrauenswürdig. Sie dienen nur als Kanal zum Weiterleiten von Befehlen an Kunden-Endpunkte. Die Autorisierung basiert auf Kryptografie nach Branchenstandard. Jeder Techniker hat ein asymmetrisches Paar aus privatem und öffentlichem Schlüssel, wobei der private Schlüssel zum Signieren von Befehlen verwendet wird und nur dem Techniker bekannt ist (nicht den GoTo Resolve-Services oder dem Kunden-Endpunkt). Der öffentliche Schlüssel wird jedem Kunden-Endpunkt bereitgestellt und verwendet, um die Signatur jedes Befehls vom Techniker zu verifizieren. Daher vertrauen die Kunden-Endpunkte GoTo Resolve-Services nicht, sondern nur dem Techniker.

Alle Kryptografievorgänge verwenden sichere Algorithmen nach Branchenstandard (beispielsweise EC-DSA, SHA-256/512, HMAC-SHA-256, AES-256-GCM, PBKDF2). Diese Kryptosysteme und Cipher werden vom Betriebssystem oder der OpenSSL-Bibliothek verarbeitet. Im Fall der Webkonsole bietet der Browser des Endbenutzers native Funktionen zum sicheren Generieren oder Manipulieren von Daten.

3.3 Berechtigungsbasierte Zugriffskontrolle

3.3.1 Beaufsichtigte Sitzung

Ein wichtiger Bestandteil der GoTo Resolve-Sicherheit ist das berechtigungsbasierte Zugriffskontrollmodell zum Schutz des Zugriffs auf Computer und Daten des Kunden. Während Live-Supportsitzungen muss der Kunde vor Initiierung der Bildschirmübertragung, Fernsteuerung oder Übertragung von Dateien zustimmen.

Nach der Autorisierung von Fernsteuerung und Bildschirmübertragung während einer beaufsichtigten Sitzung kann der Kunde alles sehen, was der Techniker tut. Zudem können Kunden einfach jederzeit wieder die Kontrolle übernehmen oder die Sitzung beenden.

3.3.2 Unbeaufsichtigte Sitzung

Unbeaufsichtigter Support erfordert die Installation der unbeaufsichtigten Kunden-App auf dem Kundengerät. Sie kann auf zwei Arten eingerichtet werden: Setup in Sitzung (während beaufsichtigter Sitzung) oder unter Verwendung eines Out-of-Session Installer. Für beides ist die Genehmigung des Kunden erforderlich.

Setup in Sitzung: Wenn Kunde und Techniker einer beaufsichtigten Sitzung beitreten, kann der Techniker eine zusätzliche Genehmigung anfordern, um die unbeaufsichtigte Kunden-App zu installieren. Der Kunde muss dies genehmigen und explizit autorisieren.

Out-of-Session Installer: Nach der sicheren Anmeldung auf der GoTo Resolve-Website oder bei der Desktop-Anwendung kann der Techniker ein Installationsprogramm herunterladen. Es ermöglicht die Installation der unbeaufsichtigten Kunden-App auf jedem Windows-PC oder Mac, auf den der Techniker Administratorzugriff hat.

3.3.3 Sicherheit in der Sitzung

GoTo Resolve überschreibt keine lokalen Sicherheitskontrollen auf dem Kundencomputer. Insbesondere, wenn der Kunde während einer unbeaufsichtigten Sitzung an den Rechner zurückkehrt, kann er diese jederzeit beenden und die Privilegien des Technikers für den unbeaufsichtigten Support permanent zurücknehmen.

3.4 Rollenbasierte Zugriffskontrolle

GoTo Resolve bietet Zugriff auf eine Vielzahl von Ressourcen und Services unter Verwendung eines rollenbasierten Zugriffskontrollsystems, das durch seine unterschiedlichen Komponenten für die Servicebereitstellung erzwungen wird. Die folgenden Rollen sind definiert:

Kontoadministrator: GoTo Resolve-Benutzer mit vollständigen Administratorprivilegien zur Durchführung administrativer Funktionen von Technikern. Kontoadministratoren können Techniker-Konten erstellen, modifizieren und löschen sowie Abonnementdaten ändern.

Techniker: GoTo Resolve-Benutzer. Der Techniker kann GoTo Resolve-Sitzungen initiieren, um Kunden technische Unterstützung per Bildschirmanzeige, Fernsteuerung oder Kameraübertragung bereitzustellen.

Kunde: nicht authentifizierte Person, die Support vom Techniker anfordert. Der Kunde kann Sitzungen schließen und muss dem Techniker den Zugriff auf sein Gerät gewähren.

3.5 Perimeterverteidigung und Erkennung von Eindringversuchen

GoTo setzt Standard-Tools, -Techniken und -Services für den Perimeterschutz ein, die verhindern sollen, dass nicht autorisierter Netzwerkdatenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk enthält nach außen gerichtete Firewalls und eine interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch Host-basierte Firewalls.

3.6 Datentrennung

GoTo nutzt eine Architektur mit mehreren Mandanten, die basierend auf dem GoTo-Konto eines Benutzers oder einer Organisation logisch auf Datenbankebene getrennt ist. Nur authentifizierten Parteien wird Zugriff auf die relevanten Konten gewährt.

3.7 Physische Sicherheit

Da die gesamte Infrastruktur für Public Cloud-Anbieter bereitgestellt wird, ist physische Sicherheit für GoTo kein Problem.

3.8 Daten-Backup, Notfallwiederherstellung, Verfügbarkeit

Die Architektur von GoTo wurde so konzipiert, dass die Replikation zu geografisch verteilten Standorten nahezu in Echtzeit erfolgt. Datenbanken werden mit Hilfe einer rollierende inkrementelle Backup-Strategie gesichert. Im Falle eines Notfalls oder eines Totalausfalls eines der vielen aktiven Standorte können die übrigen Standorte die Anwendungslast ausgleichen. Die Notfallwiederherstellung dieser Systeme wird regelmäßig getestet.

3.9 Verschlüsselung

GoTo verfügt über einen kryptografischen Standard, der sich nach Empfehlungen von Branchengruppen, staatlichen Veröffentlichungen und anderen seriösen Gruppen für Standards richtet. Der kryptografische Standard wird regelmäßig überprüft und ausgewählte Technologien und Cipher werden in Einklang mit dem bewerteten Risiko und der Marktakzeptanz neuer Standards aktualisiert.
Zentrale Punkte hinsichtlich der Verschlüsselung in GoTo Resolve sind u. a.:

- GoTo Resolve-Sitzungsdaten sind während der Übertragung durch Transport Layer Security (TLS) 1.2 und AES-Verschlüsselung (256 Bit) geschützt.
- Sitzungsschlüssel werden serverseitig durch den Techniker generiert und bleiben dort, um eine Verbindung zwischen Kunde und Techniker zu ermöglichen. Der Service soll sicherstellen, dass diese Schlüssel nie der Öffentlichkeit preisgegeben werden oder für diese sichtbar sind.
- Verschlüsselte Medienkommunikation zwischen Kunde und Techniker in GoTo Resolve erfolgt über eine benutzerdefinierte Media Service-Lösung.
- Endpunkte in der öffentlichen GoTo Resolve-Infrastruktur verwenden TLS-Verbindungen.

3.9.1 Verschlüsselung während der Übertragung

Um Kundeninhalt zusätzlich zu sichern, verwendet GoTo aktuelle TLS-Protokolle und verknüpfte Cipher Suites.
Kunden-Endpunkt und Back-End-Kommunikation sind über die OpenSSL-Bibliothek verschlüsselt. Sicherheitskontrollen für die Kommunikation basierend auf starker Kryptografie werden auf der TCP-Schicht über TLS-Standardlösungen implementiert.

Starke Authentifizierungsmaßnahmen sollen die Wahrscheinlichkeit potenzieller Angreifer reduzieren, sich als Infrastrukturserver auszugeben oder sich in die Kommunikation der Supportsitzung einzuschalten.

Um Schutz vor Abhörung, Modifizierung oder Replay-Angriffen zu bieten, werden TLS-Protokolle nach IETF-Standard zum Schutz der gesamten Kommunikation zwischen Endpunkten und unseren Services verwendet. Daten zu Bildschirmübertragung, Tastatur-/Maussteuerung, Diagnose und Text-Chat sowie übertragene Dateien werden während der Übertragung mit TLS 1.2 (ECDHE, DHE und RSA für Schlüsselaustausch, RSA für Authentifizierung, starken AES-256-Ciphern für Datenverschlüsselung mit SHA-2 HMAC-Algorithmus mit 384 Bit).

Um für ein angemessenes Gleichgewicht zwischen Kompatibilität und Sicherheit zu sorgen, unterstützt der GoTo Resolve-Service auch eingehende Verbindungen unter Verwendung der am häufigsten unterstützten TLS Cipher Suites in TLS 1.2.

GoTo empfiehlt auch, dass Techniker ihre Browser standardmäßig für die Verwendung starker Kryptografie konfigurieren (wenn möglich), um technische Schutzmaßnahmen auf dem Techniker-Rechner zu erhöhen, und immer die aktuellen Sicherheitspatches für Betriebssystem und Browser zu installieren.

Beim Herstellen von Verbindungen zur GoTo Resolve-Website und zwischen den GoTo Resolve-Komponenten authentifizieren sich die GoTo-Server mit Hilfe von Public-Key-Zertifikaten (signiert von der DigiCert oder GlobalSign Global Root CA) bei den Clients. APIs zwischen Servern sind nur im privaten Netzwerk von GoTo hinter robusten Firewalls zugänglich.

3.9.2 Sicherheit der TCP-Schicht

Die Kommunikation zwischen öffentlichen Endpunkten wird durch TLS-Protokolle nach IETF-Standard (Internet Engineering Task Force) geschützt.

GoTo empfiehlt Kunden zu ihrer eigenen Sicherheit, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Kryptografie verwenden und sicherstellen, dass die Sicherheitspatches für ihr Betriebssystem und ihre Browser aktuell sind.

3.9.3 Schutz des Kunden-Endpunkts

Kunden-Desktop-Apps und nicht unbeaufsichtigte Kunden-Apps müssen mit einer Vielzahl von Desktop-Umgebungen kompatibel sein. GoTo Resolve erreicht dies durch den Download einer ausführbaren Datei, die starke kryptografische Maßnahmen anwendet.

Kunden-Desktop-Apps und unbeaufsichtigte Kunden-Apps werden auf den Kunden-PC als digital signiertes Installationsprogramm heruntergeladen. Dies schützt den Kunden vor der versehentlichen Installation eines Trojaners oder anderer Malware, die sich als GoTo Resolve-Software ausgibt. Die Endpunkt-Software besteht aus verschiedenen digital signierten ausführbaren Dateien und dynamisch verknüpften Bibliotheken. GoTo hält entsprechende Verfahren zur Qualitätskontrolle und Konfigurationsverwaltung während der Entwicklung und Bereitstellung ein, um die Softwaresicherheit zu verbessern.

3.10 Schwachstellen-Management

Sicherheit und Schutz des Inhalts der GoTo-Kunden und -Systeme haben oberste Priorität. GoTo implementiert verschiedene Sicherheitsmaßnahmen während des Lebenszyklus aller Produkte. Sicherheitsaspekte werden bei der Entwicklung und beim Betrieb von GoTo Resolve berücksichtigt.

Dynamische und statische Tests von Anwendungsschwachstellen sowie Sicherheitsbewertungstests für anvisierte Umgebungen werden ebenfalls regelmäßig durchgeführt. Relevante Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.10.1 Sicherheitsteam

Das Sicherheitsteam von GoTo überwacht fortlaufend Produktentwicklung und -betrieb in enger Zusammenarbeit mit den Product Engineers, damit GoTo Resolve sicher bleibt und um mögliche Risiken zu vermeiden oder zu reduzieren.

3.10.2 Interne und externe Audits

Der interne Auditprozess von GoTo beinhaltet regelmäßige Sicherheitsbewertungen auf Infrastruktur- und Software-Ebene. Unsere internen Audits werden anhand verschiedener unabhängiger externer Bewertungen durchgeführt, um die Einhaltung der Branchenstandards durch uns sicherzustellen.

3.11 Protokollierung und Warnmeldungen

GoTo erfasst identifizierten anomalen oder verdächtigen Datenverkehr in entsprechenden Sicherheitsprotokollen in den jeweiligen Produktionssystemen.

4 Organisatorische Kontrollen

GoTo bietet einen umfassenden Satz an organisatorischen und administrativen Kontrollen zum Schutz des Sicherheits- und Datenschutzstatus von GoTo Resolve.

4.1 Sicherheitsrichtlinien und -verfahren

GoTo pflegt umfangreiche Sicherheitsrichtlinien und -verfahren, die an Geschäftszielen, Compliance-Programmen und der allgemeinen Unternehmensführung ausgerichtet sind. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um die Einhaltung von Vorschriften stets sicherzustellen.

4.2 Einhaltung der Standards

GoTo hält geltende rechtliche, finanzielle, datenschutzrechtliche und regulatorische Anforderungen ein und erfüllt die folgenden Compliance-Zertifizierungen und externen Audit-Berichte:

- TRUSTe Enterprise Privacy & Data Governance Practices Zertifizierung, um operative Datenschutz- und Data Protection-Kontrollen zu adressieren, die sich an

den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzabkommen orientieren. Weitere Informationen finden Sie in unserem Blog-Beitrag.

- Internationale Organisation für Normung – ISO/IEC 27001:2013 Information Security Management System-Zertifizierung (ISMS)
- Service Organization Control (SOC) 2 Type II-Bericht des American Institute of Certified Public Accountants (AICPA) inkl. BSI Cloud Computing Catalogue (C5)
- Service Organization Control (SOC) 3 Type II-Bericht des American Institute of Certified Public Accountants (AICPA)
- Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) bei den E-Commerce- und Zahlungsumgebungen von GoTo
- Interne Kontrollenbewertung wie im Rahmen der Jahresrechnungsprüfung durch das Public Company Accounting Oversight Board (PCAOB)

4.3 Sicherheitsvorgänge und Incident-Management

Das Security Operations Center (SOC) von GoTo ist mit dem Security Operations-Team besetzt und für das Erkennen von und Reagieren auf Sicherheitsereignisse verantwortlich. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um mögliche Probleme zu identifizieren und hat einen Vorfallsreaktionsplan entwickelt, der die entsprechenden Reaktionen vorgibt.

Der Vorfallsreaktionsplan ist auf die wichtigen GoTo-Kommunikationsprozesse, die Incident-Management-Richtlinie für Informationssicherheit sowie standardmäßige Betriebsvorgänge ausgerichtet. Er wurde entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services, einschließlich der GoTo Resolve, zu verwalten, zu identifizieren und zu beheben. Laut Vorfallsreaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicherheit von Informationen identifizieren und alle vermuteten oder bestätigten Ereignisse gegebenenfalls an das Management eskalieren. Mitarbeiter können Sicherheitsvorfälle gemäß des auf der Intranet-Seite von GoTo dokumentierten Prozesses per E-Mail, Telefon und/oder Ticket melden. Alle identifizierten oder vermuteten Ereignisse werden über standardisierte Ereignistickets dokumentiert, eskaliert und je nach Wichtigkeit selektiert.

4.4 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL) für einen sicheren Produktcode. Zu den Hauptelementen dieses Programms gehören manuelle Codeüberprüfungen, Bedrohungsmodellierung, statische Codeanalysen, dynamische Analysen für ausgeführte Anwendungen und Systemhärtung.

4.5 Personalsicherheit

Überprüfungen der Mitarbeiter – soweit dies nach geltendem Recht zulässig und für die Position angemessen ist – werden weltweit bei neuen Mitarbeitern vor dem Datum ihrer Einstellung vorgenommen. Die Ergebnisse werden im Personalstammblatt des Mitarbeiters hinterlegt. Die Kriterien der Mitarbeiterüberprüfung variieren in Abhängigkeit der Gesetze, der Arbeitsverantwortung und dem Führungsniveau des potenziellen Mitarbeiters und unterliegen den üblichen und zulässigen Praktiken des jeweiligen Lands.

4.6 Sicherheitsbewusstsein und Schulungsprogramme

Neu eingestellte Mitarbeiter werden zur Orientierung über die Sicherheitsrichtlinien und den Verhaltenskodex und Geschäftsethik von GoTo informiert. Diese obligatorische jährliche Schulung zu Sicherheit und Datenschutz wird für die entsprechenden Mitarbeiter durch das Talentförderungsteam und mit Unterstützung des Sicherheitsteams durchgeführt.

Die Mitarbeiter und Zeitarbeiter von GoTo werden regelmäßig über die Anweisungen, Verfahren, Richtlinien und Standards zu Sicherheit und Datenschutz informiert. Dazu werden verschiedene Medien wie Einarbeitungsunterlagen für Neueingestellte, Aufklärungs-kampagnen, Webinare mit dem CISO, ein Sicherheits-Champion-Programm und der Aushang von Plakaten oder anderes Begleitmaterial genutzt, die mindestens halbjährlich ausgetauscht werden und Methoden zum Schutz von Daten, Geräten und Anlagen veranschaulichen.

5 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten seiner Kunden (in diesem Abschnitt die Abonnenten der GoTo-Services) und Endbenutzer sehr ernst und verpflichtet sich, entsprechende Praktiken zur Verarbeitung und Verwaltung von Daten offen und transparent preiszugeben.

5.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die sich mit dem Schutz der Daten und der Privatsphäre von Einzelpersonen in der Europäischen Union befasst. Sie zielt primär darauf ab, ihren Bürgern und Bewohnern Kontrolle über ihre personenbezogenen Daten zu geben und die regulative Umgebung in der EU zu vereinfachen. GoTo Resolve ist mit den anwendbaren DSGVO-Bestimmungen kompatibel. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2 CCPA

GoTo sichert hiermit zu, dass es mit dem California Consumer Privacy Act (CCPA) konform ist. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3 Data Protection- und Datenschutzerklärung

GoTo freut sich, einen umfassenden, globalen Datenverarbeitungsnachtrag (DVN) in Englisch und Deutsch bereitzustellen, um die Anforderungen von DSGVO, CCPA und mehr zu erfüllen und die GoTo-Verarbeitung personenbezogener Daten zu regeln.

Der DVN schließt folgende Datenschutz-Anforderungen in Bezug auf die DSGVO ein: (a) Details zur Datenverarbeitung, Offenlegung bzgl. Auftragsverarbeiter-Partnerunternehmen etc. gemäß Artikel 28 (b) EU-Standardvertragsklauseln (auch als EU-Modellklauseln bekannt) und (c) die technischen und organisatorischen Maßnahmen von GoTo. Im Zusammenhang mit dem CCPA haben wir zusätzlich in unserem globalen DVN Folgendes aktualisiert: (a) Definitionen im Zusammenhang mit dem CCPA (b) Zugriffs- und Löschrechte und (c) Garantien, dass GoTo keine persönlichen Daten von Benutzern verkaufen wird.

Für Besucher unserer Webseiten veröffentlicht GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Services bereitzustellen, aufrechtzuerhalten, zu verbessern und zu sichern, in seiner Datenschutzerklärung auf der öffentlichen Website. Das Unternehmen kann seine Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen an seinen Informationspraktiken und/oder Änderungen geltender Gesetze zu berücksichtigen, weist aber auf seiner Website auf jegliche Materialänderungen hin, bevor diese wirksam werden.

5.4 Übertragung

GoTo hat ein robustes globales Data Protection-Programm, das anwendbare Gesetze berücksichtigt und rechtmäßige internationale Datenübertragungen im Rahmen der folgenden Abkommen unterstützt:

5.4.1 Standardvertragsklauseln

Die Standardvertragsklauseln („SCC“) sind standardisierte Vertragsbestandteile, die von der Europäischen Kommission anerkannt und übernommen wurden und vorrangig dem Zweck dienen, eine EU-datenschutzkonforme Übermittlung personenbezogener Daten in Regionen außerhalb des Europäischen Wirtschaftsraums („EWR“) sicherzustellen. GoTo hat ein ausgefeiltes Datenschutzprogramm eingerichtet, das die Ausführungsbestimmungen der SCC für die Übermittlung personenbezogener Daten einhält. GoTo bietet Kunden SCC (andere Bezeichnung: EU-Modellklauseln) an. Diese leisten als Bestandteil des globalen DVN von spezifische Garantien betreffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Services im Rahmen des globalen DVN. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Neben den in diesen TOMs angegebenen Maßnahmen hat GoTo die folgenden FAQ erstellt, um seine ergänzenden Maßnahmen zur Unterstützung rechtmäßiger Datenübertragungen gemäß Kapitel 5 der DSGVO zu skizzieren und alle Analysen zu adressieren und anzuleiten, die vom Europäischen Gerichtshof zusammen mit den SCCs empfohlen werden.

5.4.2 Zertifizierungen zu APEC, CBPR und PRP

GoTo hat zudem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft), CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC-, CBPR- und PRP-Rahmenregelungen sind die ersten Datenregelungen, die für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt wurden. Sie wurden von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für die Einhaltung von Datenschutzbestimmungen, eingeholt und unabhängig validiert.

5.5 Rückgabe und Löschung von Kundeninhalt

Kunden können die Rückgabe oder Löschung ihres Inhalts jederzeit über standardisierte Schnittstellen anfordern. Wenn diese Schnittstellen nicht verfügbar sind oder GoTo anderweitig nicht in der Lage ist, der Anfrage gerecht zu werden, ergreift GoTo wirtschaftlich zumutbare Maßnahmen, um den Kunden im Rahmen der technischen Möglichkeiten beim

Abrufen oder Löschen seines Inhalts zu unterstützen. Der Kundeninhalt wird innerhalb von dreißig (30) Tagen nach der Anfrage des Kunden gelöscht. Bei Ablauf oder Kündigung eines Kundenkontos wird Kundeninhalt automatisch dreißig (30) Tage nach dem tatsächlichen Datum des Ablaufs oder der Kündigung des Kontos gelöscht. Bei einer schriftlichen Anfrage bestätigt GoTo eine derartige Inhaltslöschung.

5.6 Sensible Daten

Es ist das Ziel von GoTo, den gesamten Kundeninhalt zu schützen und zu sichern. Regulatorische und vertragliche Beschränkungen verlangen jedoch, dass die Verwendung von GoTo Resolve für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoTo Resolve hochgeladen oder dort generiert werden:

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, wie im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) sowie anderen relevanten anwendbaren Gesetzen und Vorschriften festgelegt.
- Informationen über Finanzkonten und Zahlungsinstrumente, einschließlich − aber nicht beschränkt auf − Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung betrifft ausdrücklich gekennzeichnete Zahlungsformulare und Seiten, die von GoTo verwendet werden, um Zahlungen für den Service zu erheben.
- Alle Informationen, die besonders durch geltende Gesetze und Vorschriften geschützt sind, insbesondere Informationen über die Rasse, die ethnische Zugehörigkeit, religiöse oder politische Überzeugungen, organisatorische Mitgliedschaften der Person usw.

5.7 Nachverfolgung und Analysen

GoTo verbessert kontinuierlich seine Websites und Produkte mit Hilfe von Webanalysetools von Drittanbietern, um Folgendes besser zu verstehen: Nutzung der Websites, Desktop-Tools und mobilen Anwendungen durch Besucher, Benutzerpräferenzen und Probleme. Weitere Einzelheiten finden Sie in der Datenschutzrichtlinie.

6 Drittanbieter

6.1 Nutzung von Drittanbietern

Im Rahmen der internen Bewertung und der Prozesse im Zusammenhang mit Anbieter- und Drittanbieter-Verwaltung von GoTo können Anbieterbewertungen je nach Relevanz und Anwendbarkeit von mehreren Teams vorgenommen werden. Das Sicherheitsteam bewertet Anbieter von Services, die auf Informationssicherheit basieren, und nimmt auch die Bewertung der Hosting-Einrichtungen von Drittanbietern vor. Das Team für Recht und Beschaffung kann bei Bedarf nach internen Prozessen Verträge, Leistungsbeschreibungen und Servicevereinbarungen bewerten. Angemessene Konformitätsdokumente oder -berichte können mindestens einmal jährlich eingeholt und bewertet werden, sofern dies für angemessen erachtet wird, um sicherzustellen, dass die Kontrollumgebung ordnungsgemäß funktioniert und alle erforderlichen benutzerbezogenen Kontrollen durchgeführt werden.

Zudem müssen Drittanbieter, die sensible oder vertrauliche Daten hosten oder von GoTo Zugriff darauf erhalten haben, einen schriftlichen Vertrag zu unterzeichnen, in dem die relevanten Anforderungen für den Zugriff auf die Informationen sowie deren Speicherung oder Verarbeitung (sofern zutreffend) festgelegt sind.

6.2 Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Geschäftsprozessen und Datenverarbeitung durch Drittanbieter getroffen werden, überprüft GoTo die jeweiligen Nutzungsbedingungen von Drittanbietern und nutzt entweder von GoTo genehmigte Beschaffungsvorlagen oder verhandelt die Bedingungen dieser Drittanbieter, wenn dies als notwendig erachtet wird.

7 GoTo kontaktieren

Kunden können sich bei allgemeinen Anfragen an https://support.goto.com oder bei Fragen zum Datenschutz an privacy@goto.com wenden.

8 Anhang – Terminologie

Techniker: GoTo Resolve-Benutzer, der GoTo Resolve-Sitzungen erstellt, um Kunden technische Unterstützung per Bildschirmanzeige, Fernsteuerung oder Kameraübertragung bereitzustellen.

Webbasierte Technikerkonsole: Webanwendung, die auf dem PC, Mac, Tablet oder Chromebook in einem beliebigen der unterstützten Browser (Chrome, Firefox, Safari) ausgeführt wird und eine Verbindung zum GoTo Resolve-Service herstellt. Sie ermöglicht dem Techniker das Erstellen und Durchführen von GoTo Resolve-Sitzungen per Kameraübertragung sowie verschiedene Funktionen für Kontoverwaltung, Serviceverwaltung und Berichterstattung.

Desktop-Technikerkonsole: Desktop-Anwendung, die auf MacOS- und Windows-Computern ausgeführt wird, sich mit dem GoTo Resolve-Service verbindet und die webbasierte Technikerkonsole von GoTo Resolve, Qt und die Chromium-Webengine nutzt. Bietet dieselbe Funktionalität wie die webbasierte Technikerkonsole, aber in einem nativen Look and Feel.

Beaufsichtigte Sitzung: Supportsitzung, bei der der Kunde anwesend ist und partizipieren kann.

Kunde: Person, die technischen Support vom Techniker über eine GoTo Resolve-Sitzung erhält.

Kunden-Desktop-App: Desktop-Anwendung, die auf dem Kundencomputer (Windows oder Mac) ausgeführt wird und sich mit einer GoTo Resolve-Sitzung über den GoTo Resolve-Service verbindet. Sie ermöglicht Fernsteuerung sowie andere erweiterte Funktionalitäten und die Fähigkeit, die unbeaufsichtigte App auf dem Kundencomputer zu installieren.

Kunden-Endpunkt: kollektiver Begriff für jeden Kunden-Endpunkt: Kunden-Web-App, Kunden-Desktop-App, mobile Kunden-App, unbeaufsichtigte Kunden-App.

Mobile Kunden-App: mobile Anwendung (Android und iOS), die auf dem Mobilgerät/Tablet des Kunden ausgeführt wird und sich mit einer GoTo Resolve-Sitzung über den GoTo Resolve-Service verbinden kann. Sie ermöglicht Bildschirmanzeige (Android und iOS) und Fernsteuerung (nur Android).

Kunden-Desktop-App: Web-Anwendung, die auf jedem unterstützen Browser auf dem Computer/Mobilgerät des Kunden ausgeführt wird und sich mit einer GoTo Resolve-Sitzung über den GoTo Resolve-Service verbindet. Sie ermöglicht Chat, Bildschirmanzeige und Kameraübertragung sowie die Sitzung jederzeit auf Fernsteuerung hochzustufen, indem die Kunden-Desktop-App heruntergeladen oder die mobile App installiert wird.

Media Service: mehrere global verteilte Server mit Lastenausgleich, die eine Vielzahl von hoch verfügbaren Unicast- und Multicast-Kommunikationsservices basierend auf WebRTC-Protokollen bieten.

GoTo Resolve-Sitzungen: interaktiver Chat, Bildschirmanzeige, Fernsteuerung oder Kameraübertragung und unbeaufsichtigte Fernsteuerung.

GoTo Resolve-Service: mehrere global verteilte Server mit Lastenausgleich, die sicheren Zugriff für die webbasierte Technikerkonsole und Kunden-Endpunkte über verschlüsselte Web Socket-Verbindungen und API-Aufrufe bieten.

Unbeaufsichtigte Kunden-App: installierbare Desktop-Anwendung (Windows und Mac), die im Hintergrund auf dem Kundencomputer ausgeführt wird. Es kann eine Kunden-Desktop-App für eine Verbindung mit einer autorisierten unbeaufsichtigten Sitzung heruntergeladen und ausgeführt werden.

Unbeaufsichtigte Sitzung: Supportsitzung, bei der der Kunde nicht anwesend ist. Die Sitzung wird ohne Einbeziehung des Kunden vom Techniker über eine unbeaufsichtigte Kunden-App initiiert und erstellt.

GoTo Resolve Ticketing Services: Back-End-Anwendung, die das HelpDesk-Feature von GoTo Resolve unterstützt. Sie vereinfacht auch die Kommunikation zwischen der MS Teams-App und GoTo Resolve.