TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR GOTOASSIST REMOTE SUPPORT V5

(FRÜHER „RESCUEASSIST“)

DOKUMENTATION ZU ORGANISATORISCHEN SICHERHEITS- UND DATENSCHUTZKONTROLLEN

Datum der Veröffentlichung: Februar 2022

1 Produkte und Dienste

Dieses Dokument konzentriert sich auf die technischen und organisatorischen Maßnahmen (TOMs) der Infrastruktur und Kommunikationskanäle von GoToAssist Remote Support V5 (früher „RescueAssist“).

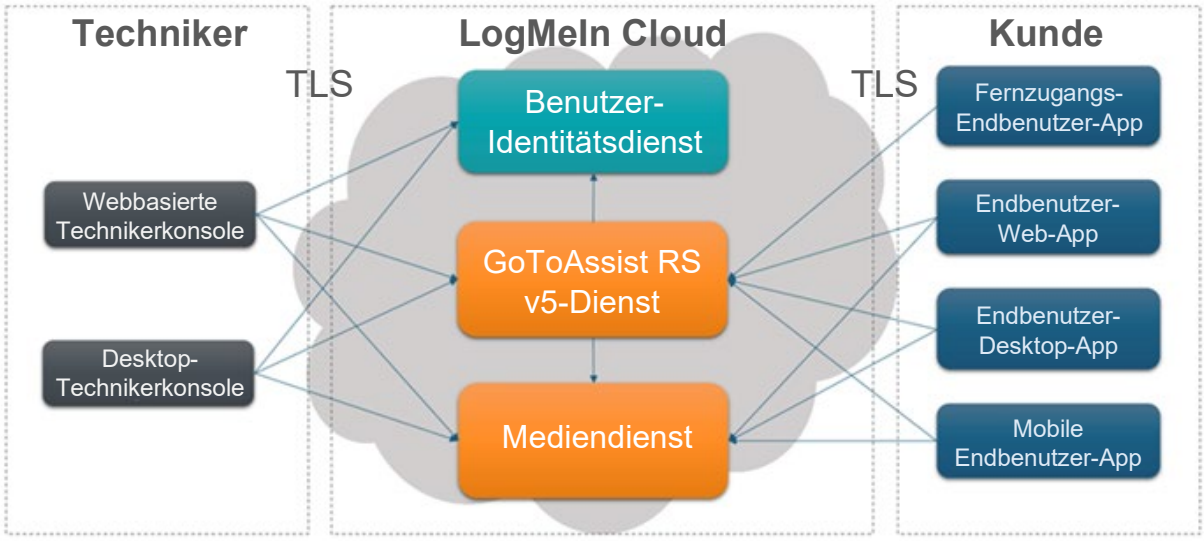
GoToAssist Remote Support V5 ermöglicht es IT- und Support-Fachkräften, über eine Web- oder Desktop-Technikerkonsole mit Funktionen für Bildschirmanzeige, Remotesteuerung und Kameraübertragung Remotesupport für Computer, Server und Mobilgeräte zu leisten. GoToAssist Remote Support V5 setzt Sicherheitsmaßnahmen zum Schutz von Daten ein, die sowohl passive als auch aktive Angriffe abwehren.

2 Produktarchitektur

GoToAssist Remote Support V5 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 für optimale Leistung, Zuverlässigkeit und Skalierbarkeit konzipiert. Redundante Switches und Router sind Teil der Architektur, damit es keinen „Single Point of Failure“ geben kann. Kapazitätsstarke, geclusterte Server und Backup-Systeme stellen sicher, dass Anwendungsprozesse im Falle einer hohen Auslastung oder eines Systemausfalls weiter ausgeführt werden. Service Broker verteilen die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver. Die Kommunikationsarchitektur für GoToAssist Remote Support V5 ist in Abschnitt 2.1 unten dargestellt.

2.1. Kommunikationsarchitektur

Die Kommunikationsarchitektur von GoToAssist Remote Support V5 ist in der folgenden Abbildung zusammengefasst.



Die Authentifizierung von Technikern erfolgt über den Benutzer-Identitätsdienst von GoTo. Die Kommunikation zwischen den Teilnehmern einer GoToAssist Remote Support V5-Sitzung erfolgt über einen Overlay-Netzwerkstapel, der logisch über dem konventionellen UDP- und TCP/IP-Stapel angeordnet ist. Dieses Netzwerk wird vom Dienst und Mediendienst von GoToAssist Remote Support V5 bereitgestellt, der in Amazon AWS gehostet wird.

Die GoToAssist Remote Support V5-Sitzungsteilnehmer (Webbasierte Technikerkonsole, Desktop-Technikerkonsole und Endbenutzer-Endgeräte) kommunizieren mit dem Dienst und Mediendienst von GoToAssist Remote Support V5 über ausgehende TCP-Verbindungen an Port 443 oder UDP-Port 15000, je nach Verfügbarkeit. Da GoToAssist Remote Support V5 ein webbasierter Dienst ist, können sich die Teilnehmer an jedem beliebigen Ort mit Internetzugang befinden – in einem Außenbüro, zu Hause, in einem Business-Center oder im Netzwerk eines anderen Unternehmens.

2.2. Desktop-Technikerkonsole

Die Techniker können die webbasierte Technikerkonsole oder eine installierbare Desktop-Technikerkonsole verwenden, um sich mit dem GoToAssist Remote Support V5-Dienst zu verbinden. Die Desktopkonsole verwendet das plattformübergreifende Qt-Toolkit zur Ausführung unter MacOS und Windows und nutzt den Open-Source-Webbrowser Chromium zur Verwendung von Komponenten der Webkonsole.

3 GoToAssist Remote Support V5 – Technische Kontrollen

GoTo setzt branchenübliche technische Sicherheitskontrollen ein, die der Art und dem Umfang der Dienste (wie in den Nutzungsbedingungen definiert) angemessen sind, um die Infrastruktur der Dienste und die darin enthaltenen Daten zu schützen. Die Nutzungsbedingungen finden Sie unter https://www.goto.com/company/legal/terms-and-conditions.

3.1. Authentifizierung

Techniker und Kontoadministratoren werden in GoToAssist Remote Support V5 anhand ihrer E-Mail-Adresse identifiziert und mit einem Passwort authentifiziert. Bei der autorisierten Authentifizierung wird das Passwort während der Übertragung immer verschlüsselt.

Die Authentifizierungsverfahren werden durch die folgenden Richtlinien geregelt:

- **Starke Passwörter:** Ein starkes Passwort muss mindestens 8 Zeichen lang sein und eine ausreichende Komplexität aufweisen (d. h. es muss sowohl Buchstaben als auch Zahlen enthalten). Passwörter werden bei der Einrichtung oder Änderung auf ihre Stärke überprüft.
- **Zwei-Faktor-Authentifizierung:** Als zusätzliche Sicherheitsmaßnahme ist die optionale Zwei-Faktor-Authentifizierung für jedes GoToAssist Remote Support V5-Unternehmenskonto verfügbar. Falls die Zwei-Faktor-Authentifizierung aktiviert ist, muss jeder Benutzer seinen Zugriff über zwei separate Methoden autorisieren.
- **Kontosperrung:** Nach fünf aufeinander folgenden fehlgeschlagenen Anmeldeversuchen wird für das Benutzerkonto eine obligatorische „sanfte Sperre“ verhängt. Das bedeutet, dass sich der Benutzer fünf Minuten lang nicht bei seinem Konto anmelden

kann. Nach Ablauf der Sperrfrist kann der Benutzer erneut versuchen, sich bei seinem Konto anzumelden.

3.2. Logische Zugriffskontrolle

Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollverfahren sollen die Bedrohungen des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden. Mitarbeitern wird nach Bedarf minimaler Zugriff (oder „geringste Rechte“) auf bestimmte GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte gewährt. Außerdem werden die Berechtigungen der Benutzer je nach funktionaler Rolle und Umgebung getrennt.

Zu den Benutzern, die zum Zugriff auf die Produktkomponenten von GoToAssist Remote Support V5 berechtigt sind, gehören möglicherweise die technischen Mitarbeiter von GoTo (z. B. Technical Operations und Engineering DevOps), Kundenadministratoren oder End-benutzer des Produkts. On-Premise-Produktionsserver sind nur über Jump-Hosts oder das virtuelle private Netzwerk (VPN) des Betriebs verfügbar. Cloudbasierte Produktions-komponenten sind über die SSU(Self Service Unix)-Authentifizierung verfügbar.

3.3. Berechtigungsbasierte Zugriffskontrolle

3.3.1. Interaktive Sitzung

Ein wesentlicher Bestandteil des Sicherheitskonzepts von GoToAssist Remote Support V5 ist das auf Berechtigungen basierende Zugriffskontrollmodell, das den Zugriff auf Computer und Daten des Kunden schützt. Bei interaktiven Live-Supportsitzungen (an denen der Kunde teilnimmt) wird der Kunde 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 Benutzer alles beobachten, was der Techniker tut. Außerdem ist der Service so konzipiert, dass der Kunde jederzeit die Kontrolle zurückerlangen oder die Sitzung beenden kann.

3.3.2. Fernzugangssitzung

Für den Fernzugang muss die Fernzugangs-Kunden-App auf dem Gerät des Kunden 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 Kunden erforderlich ist.

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

Installationsprogramm außerhalb der Sitzung: Nachdem sich der Techniker sicher bei der GoToAssist Remote Support V5-Website oder der Desktop-Anwendung angemeldet hat, kann er ein Installationsprogramm herunterladen, das die Installation der Fernzugangs-Kunden-App auf jedem Windows-PC oder Mac ermöglicht, auf dem der Techniker Administratorzugriff hat.

3.3.3. Sicherheit während der Sitzung

GoToAssist Remote Support V5 ist nicht dafür vorgesehen, die lokalen Sicherheitskontrollen auf dem Computer des Kunden außer Kraft zu setzen.

Insbesondere kann der Kunde, wenn er während einer interaktiven Sitzung zum Rechner zurückkehrt, die Sitzung jederzeit beenden und dem Techniker die Berechtigungen für den interaktiven Support dauerhaft entziehen.

3.4. Rollenbasierte Zugriffskontrolle

GoToAssist Remote Support V5 ermöglicht den Zugriff auf eine Vielzahl von Ressourcen und Diensten mithilfe eines rollenbasierten Zugriffskontrollsystems, das von den verschiedenen Komponenten der Dienstbereitstellung durchgesetzt wird. Die folgenden Rollen sind definiert:

- **Kontoadministrator:** GoToAssist Remote Support V5-Benutzer mit vollen Administratorrechten zur Durchführung von Administrationsfunktionen in Bezug auf Techniker. Kontoadministratoren können Technikerkonten erstellen, ändern und löschen und Abonnementdaten ändern.
- **Techniker:** Benutzer von GoToAssist Remote Support V5. Der Techniker kann GoToAssist Remote Support V5-Sitzungen initiieren, um Kunden per Bildschirmanzeige, Remotesteuerung oder Kameraübertragung technische Unterstützung zu leisten.
- **Kunde:** Nicht authentifizierte Person, die den Techniker um Unterstützung bittet. Der Kunde kann Sitzungen schließen und muss dem Techniker Berechtigungen zum Zugreifen auf sein Gerät gewähren.

3.5. Perimeterabwehr und Erkennung von Eindringversuchen

GoTo setzt branchenübliche Perimeterabwehr-Tools, Techniken und Dienste zum Schutz des Perimeters ein, die verhindern sollen, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch hostbasierte Firewalls.

3.6. Datentrennung

GoTo nutzt eine logisch auf Datenbankebene getrennte Multi-Tenant-Architektur, die auf dem GoTo-Konto eines Benutzers oder einer Organisation basiert. Nur authentifizierte Parteien erhalten Zugriff auf die entsprechenden Konten.

3.7. Physische Sicherheit

GoTo schließt Verträge mit Rechenzentren ab, um die physische Sicherheit und Umgebungskontrollen für Serverräume zu gewährleisten, in denen Produktionsserver untergebracht sind. Zu diesen Kontrollen gehören die folgenden:

- Videoüberwachung und -aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- HLK-Temperaturregelung (Heizung, Lüftung und Klimatisierung)
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (UPS)
- 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 überprüft und genehmigt werden muss. Das GoTo-Management überprüft mindestens vierteljährlich die Protokolle des physischen Zugangs zu den Rechenzentren und Serverräumen. Außerdem wird der physische Zugang zu den Rechenzentren widerrufen, wenn ein zuvor autorisierter Mitarbeiter entlassen wird.

3.8. Daten-Backup, Notfallwiederherstellung, 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.

3.9. Verschlüsselung

GoTo nutzt einen kryptografischen Standard, der den Empfehlungen von Branchenverbänden, behördlichen Veröffentlichungen und anderen angesehenen Standardverbänden entspricht. Der kryptografische Standard wird regelmäßig überprüft, und die ausgewählten Technologien und Verschlüsselungsverfahren können je nach Risikobewertung und Marktakzeptanz neuer Standards aktualisiert werden.
Die wichtigsten Punkte bei der Verschlüsselung in GoToAssist Remote Support V5 sind:

- Die Sitzungsdaten von GoToAssist Remote Support V5 sind mittels TLS 1.2 (falls unterstützt) 256-Bit-AES-Verschlüsselung geschützt.
- Die Sitzungsschlüssel werden serverseitig vom Techniker generiert und verbleiben dort, um den Kunden mit dem Techniker verbinden zu können. Der Dienst ist so konzipiert, dass diese Schlüssel weder offengelegt werden noch öffentlich einsehbar sind.
- Die verschlüsselte Kommunikation zwischen dem Kunden und dem Techniker in GoToAssist Remote Support V5 erfolgt über eine kundenspezifische Mediendienstlösung.
- Die Endpunkte innerhalb der GoToAssist Remote Support V5-Infrastruktur verwenden TLS-Verbindungen (Transport Layer Security).

3.9.1. Verschlüsselung während der Übertragung

Um Kundeninhalte während der Übertragung zusätzlich zu schützen (wie in den Nutzungsbedingungen definiert), verwendet GoTo aktuelle TLS-Protokolle und zugehörige Verschlüsselungssammlungen.

Die Kommunikation zwischen Kundenendpunkt und Backend wird über OpenSSL verschlüsselt. Sicherheitskontrollen für die Kommunikation, die auf starker Kryptographie basieren, werden auf der TCP-Ebene über TLS-Standardlösungen implementiert.

Es werden sichere Authentifizierungsmethoden genutzt, um die Wahrscheinlichkeit zu verringern, dass sich potenzielle Angreifer als Infrastrukturserver ausgeben oder sich in die Supportsitzungskommunikation einschalten.

Zum Schutz vor Abhör-, Änderungs- oder Wiederholungsangriffen werden TLS-Protokolle nach IETF-Standard verwendet, um die gesamte Kommunikation zwischen Endpunkten und unseren Diensten zu schützen. Daten in Bildschirmübertragungen, Tastatur-/Maussteuerungsdaten, übertragene Dateien, Daten von Remotediagnosen und Informationen aus Text-Chats werden bei der Übertragung mit TLS 1.2 verschlüsselt (2048-Bit RSA, sichere AES-256-Verschlüsselungs-Chiffren mit 384 Bit SHA-2 Algorithmus).

Um angemessene Kompatibilität und Sicherheit zu gewährleisten, unterstützt der GoToAssist Remote Support V5-Dienst auch eingehende Verbindungen durch die meisten unterstützten TLS-Cipher-Suites in TLS 1.2.

GoTo empfiehlt Technikern außerdem, ihre Browser so zu konfigurieren, dass sie standardmäßig eine starke Verschlüsselung verwenden, um die technischen Sicherheitsvorkehrungen auf dem Rechner des Technikers zu erhöhen, und immer die neuesten Sicherheitspatches für Betriebssystem und Browser zu installieren.

Wenn Verbindungen zur GoToAssist Remote Support V5-Website und zwischen den Komponenten von GoToAssist Remote Support V5 hergestellt werden, authentifizieren sich die GoTo-Server gegenüber den Clients mit GlobalSign-Zertifikaten mit öffentlichem Schlüssel. Der Zugriff auf Server-zu-Server-APIs ist nur innerhalb des durch eine robuste Firewall geschützten privaten Netzwerks von GoTo möglich.

3.9.2. Sicherheit der TCP-Schicht

Zum Schutz der Kommunikation zwischen Endpunkten werden TLS-Standardprotokolle der Internet Engineering Task Force (IETF) verwendet.

Zu ihrer eigenen Sicherheit empfiehlt GoTo seinen Kunden, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden, und stets die aktuellsten Sicherheitspatches für ihr Betriebssystem und ihre Browser zu installieren.

3.9.3. Endgeräteschutz für Kunden

Endbenutzer-Desktop-Apps und nicht betreute Endbenutzer-Apps müssen mit einer Vielzahl von Desktop-Umgebungen kompatibel sein. GoToAssist Remote Support V5 erreicht dies durch einen ausführbaren Download, der starke kryptografische Maßnahmen umsetzt.

Die Endbenutzer-Desktop-Apps und nicht betreuten Endbenutzer-Apps werden als digital signiertes Installationsprogramm auf die Kunden-PCs heruntergeladen. Dies

schützt den Kunden davor, versehentlich einen Trojaner oder andere Malware zu installieren, die sich als GoToAssist Remote Support V5-Software ausgibt.

Die Endpunkt-Software besteht aus mehreren digital signierten ausführbaren Dateien und dynamisch verknüpften Bibliotheken. Während der Entwicklung und Verteilung befolgt GoTo entsprechende Maßnahmen zur Qualitätskontrolle und zum Konfigurationsmanagement, um die Sicherheit der Software zu verbessern.

3.10. Schwachstellenmanagement

Die Gewährleistung der Sicherheit und des Schutzes der Inhalte und Systeme der GoTo-Kunden hat höchste Priorität. GoTo implementiert während des gesamten Lebenszyklus seiner Produkte verschiedene Sicherheitsmaßnahmen. Sicherheitsaspekte werden bei der Entwicklung und dem Betrieb von GoToAssist Remote Support V5 berücksichtigt und miteinbezogen.

Dynamische und statische Schwachstellenprüfungen von Anwendungen sowie Tests zur Sicherheitsbewertung bestimmter Zielumgebungen werden ebenfalls regelmäßig durchgeführt. Relevante Schwachstellen werden darüber hinaus durch monatliche und vierteljährliche Berichte an die Entwicklungs- und Verwaltungsteams kommuniziert und verwaltet.

3.10.1. Sicherheitsteam

Das Sicherheitsteam von GoTo überwacht in enger Zusammenarbeit mit den Produktentwicklern kontinuierlich die Produktentwicklung und den Betrieb, um die Sicherheit von GoToAssist Remote Support V5 zu gewährleisten und mögliche Risiken zu vermeiden oder deren Wahrscheinlichkeit zu verringern.

3.10.2. Interne und externe Audits

Das interne Audit-Verfahren von GoTo umfasst regelmäßige Sicherheitsbewertungen, sowohl auf Infrastruktur- als auch auf Software-Ebene. Unsere internen Audits werden durch verschiedene unabhängige externe Bewertungen ergänzt, um sicherzustellen, dass wir die Branchenstandards einhalten.

3.11. Protokollierung und Warnmeldungen

GoTo sammelt identifizierten anomalen oder verdächtigen Datenverkehr in den entsprechenden Sicherheitsprotokollen der jeweiligen Produktionssysteme.

4 Organisatorische Kontrollen

GoTo setzt eine umfassende Reihe von organisatorischen und administrativen Kontrollen ein, um die Sicherheit und den Datenschutz von GoToAssist Remote Support V5 zu gewährleisten.

4.1. Sicherheitsrichtlinien und -verfahren

GoTo setzt eine umfassende Reihe von Sicherheitsrichtlinien und -verfahren ein, die den Geschäftszielen, Compliance-Programmen und den Interessen der allgemeinen Unternehmensführung entsprechen. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um ihre Einhaltung zu gewährleisten.

4.2. Einhaltung von Standards

GoTo erfüllt die geltenden rechtlichen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen und hält sich an die folgenden Zertifikate und externen Prüfberichte:

- 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.
- 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 2 Zertifizierungsbericht inkl. BSI Cloud Computing Katalog (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Typ II Zertifizierungsbericht
- 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

4.3. Sicherheitsmaßnamen und Incident-Management

Das Security-Operations-Team des GoTo Security Operations Centers (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 einen Plan zur Reaktion auf Vorfälle entwickelt, der angemessene Reaktionen vorschreibt.

Der Plan zur Reaktion auf Vorfälle ist auf die kritischen Kommunikationsprozesse von GoTo, die Richtlinie für das Management von Vorfällen im Bereich der Informationssicherheit sowie die zugehörigen Standardbetriebsverfahren abgestimmt. Er wurde entwickelt, um mutmaßliche oder identifizierte Sicherheitsereignisse in den Systemen und Diensten des Unternehmens zu verwalten, zu identifizieren und zu beheben, einschließlich GoToAssist Remote Support V5. Gemäß dem Plan für die Antwort auf Vorfälle gibt es technische Mitarbeiter, die potenzielle Ereignisse und Schwachstellen im Zusammenhang mit der Informationssicherheit identifiziert und vermutete oder bestätigte Ereignisse gegebenenfalls an die Verwaltung weiterleitet. Mitarbeiter können Sicherheitsvorfälle per E-Mail, Telefon und/oder Ticket melden, entsprechend dem auf der GoTo-Intranetseite dokumentierten Verfahren. Alle identifizierten oder vermuteten Ereignisse werden dokumentiert und über standardisierte Ereignistickets eskaliert und nach ihrer Kritikalität eingestuft.

4.4. Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL), um den Produktcode zu abzusichern. Die Kernelemente dieses Programms sind manuelle Codeprüfungen, Bedrohungsmodellierung, statische Codeanalyse und Systemhärtung.

4.5. Mitarbeitersicherheit

Hintergrundüberprüfungen werden, soweit gesetzlich zulässig und für die jeweilige Position angemessen, bei neuen Mitarbeitern vor dem Einstellungsdatum global durchgeführt. Die Ergebnisse werden in der Personalakte des Mitarbeiters hinterlegt. Die Kriterien für die

Hintergrundüberprüfung hängen von den Gesetzen, der beruflichen Verantwortung und der Führungsebene des potenziellen Mitarbeiters ab und unterliegen den üblichen und angemessenen Praktiken des jeweiligen Landes.

4.6. Programme für Sicherheitssensibilisierung und -schulung

Neu eingestellte Mitarbeiter werden bei der Einarbeitung über die Sicherheitsrichtlinien und den betrieblichen Verhaltenskodex und die ethischen Grundsätze von GoTo informiert. Diese obligatorische jährliche Sicherheits- und Datenschutzschulung wird den betreffenden Mitarbeitern bereitgestellt und vom Talent-Development-Team mit Unterstützung des Sicherheitsteams verwaltet.

GoTo-Mitarbeiter und Zeitarbeitskräfte werden regelmäßig über Sicherheits- und Datenschutzleitfäden, -verfahren, -richtlinien und -standards informiert, u. a. durch Onboarding-Kits für neue Mitarbeiter, Sensibilisierungskampagnen, Webinare mit dem CISO, ein Security-Champion-Programm und mindestens halbjährlich wechselnde Poster und andere Ressourcen, die Methoden zur Sicherung von Daten, Geräten und Einrichtungen erläutern.

5 Datenschutzpraktiken

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

5.1. DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) über den Schutz der Daten und der Privatsphäre aller Personen in der EU. Hauptziel der DSGVO ist es, den Bürgern und Einwohnern mehr Kontrolle über ihre personenbezogenen Daten zu geben und das regulatorische Umfeld innerhalb der EU zu vereinfachen. GoToAssist Remote Support V5 hält die geltenden Bestimmungen der DSGVO ein. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo versichert und garantiert hiermit, dass es den California Consumer Privacy Act (CCPA) einhält. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3. Datenschutzrichtlinien

GoTo bietet einen umfassenden globalen Datenverarbeitungsnachtrag (DVN), der in Englisch und Deutsch verfügbar ist und die Anforderungen der DSGVO, CCPA erfüllt bzw. sie übertrifft und die Verarbeitung personenbezogener Daten durch GoTo regelt.

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) zur Regelung der gesetzeskonformen Übermittlung gemäß der DSGVO mittels Anwendung der 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 legt GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Dienste bereitzustellen, zu pflegen, zu verbessern und zu sichern, in seiner Datenschutzrichtlinie auf der öffentlichen Website offen. Das Unternehmen kann die Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen seiner Informationspraktiken und/oder Änderungen des anwendbaren Rechts zu reflektieren, wird jedoch auf seiner Website über alle wesentlichen Änderungen informieren, bevor diese in Kraft treten.

5.4. Abkommen zur Datenübertragung

GoTo verfügt über ein robustes globales Datenschutzprogramm, das die geltenden Gesetze berücksichtigt und rechtmäßige internationale Datenübertragungen unter den folgenden Rahmenbedingungen 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 DNV von GoTo spezifische Garantien betreffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Dienste. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

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

5.4.2. Zertifizierung nach APEC CBPR und PRP

GoTo hat außerdem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft), CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC CBPR und PRP wurden als erste ihrer Art für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt und durch den APEC-konformen Datenschutzmanagement-Anbieter TrustArc erworben und unabhängig validiert.

5.5. Rückgabe und Löschung von Kundeninhalten

GoToAssist Remote Support V5-Kunden können jederzeit die Rückgabe oder Löschung ihrer Inhalte über standardisierte Benutzeroberflächen beantragen. Wenn diese Oberflächen nicht zur Verfügung stehen oder GoTo aus anderen Gründen nicht in der Lage ist, die Anfrage zu bearbeiten, wird GoTo im Rahmen der technischen Möglichkeiten alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um den Kunden bei der Abfrage oder Löschung

seiner Inhalte zu unterstützen. Die Kundeninhalte für GoToAssist Remote Support V5 werden innerhalb von dreißig (30) Tagen nach Aufforderung durch den Kunden gelöscht. Die Inhalte von GoToAssist Remote Support V5-Kunden werden automatisch innerhalb von neunzig (90) Tagen nach Ablauf oder Beendigung der letzten Abonnementlaufzeit gelöscht. Auf schriftliche Anfrage wird GoTo die Löschung dieser Inhalte bestätigen.

5.6. Vertrauliche Daten

Obwohl GoTo bestrebt ist, alle Kundeninhalte zu schützen, sind wir aufgrund regulatorischer und vertraglicher Bestimmungen dazu gezwungen, die Verwendung von GoToAssist Remote Support V5 für bestimmte Arten von Informationen einzuschränken. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die folgenden Daten nicht in GoToAssist Remote Support V5 (durch den Kunden oder seine Endbenutzer) hochgeladen oder generiert werden:

- 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) von 1996 und verwandte Gesetze 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 GoToAssist Remote Support V5 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.

5.7. Tracking und Analyse

GoTo verbessert seine Websites und Produkte kontinuierlich mithilfe von Webanalyse-Tools von Drittanbietern, die GoTo dabei helfen, zu verstehen, wie Besucher seine Websites, Desktop-Tools und mobilen Anwendungen nutzen und welche Benutzereinstellungen und Probleme sie haben. Weitere Informationen entnehmen Sie bitte der Datenschutzrichtlinie.

6 Drittanbieter

6.1. Einsatz von Drittanbietern

Im Rahmen der internen Beurteilung und der Prozesse in Bezug auf Anbieter bzw. Drittanbieter können Anbieterbeurteilungen je nach Relevanz und Anwendbarkeit von mehreren Teams durchgeführt werden. Das Sicherheitsteam evaluiert relevante Anbieter, die auf Informationssicherheitsdienste anbieten, dazu gehört auch die Beurteilung von Hosting-Einrichtungen Dritter. Die Rechts- und Beschaffungsabteilungsteams von GoTo können Verträge, Leistungsbeschreibungen (Statements of Work, SOW) und Dienstleistungsvereinbarungen nach Bedarf im Rahmen interner Prozesse beurteilen. Angemessene Unterlagen oder Berichte über die Einhaltung der Vorschriften können mindestens einmal jährlich eingeholt und ausgewertet werden, um sicherzustellen, dass das Kontrollumfeld

angemessen funktioniert und alle notwendigen Kontrollen zwecks Berücksichtigung der Benutzer durchgeführt werden. Darüber hinaus müssen Dritte, die sensible oder vertrauliche Daten von GoTo hosten oder denen von GoTo Zugang zu diesen gewährt wird, einen schriftlichen Vertrag unterzeichnen, in dem die entsprechenden Anforderungen für den Zugang zu, die Speicherung oder den Umgang mit den Informationen (je nach Fall) dargelegt sind.

6.2. Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität der Geschäftsprozesse und der Verarbeitung von Daten Dritter getroffen werden, prüft GoTo die Geschäftsbedingungen relevanter Dritter und verwendet entweder von GoTo genehmigte Beschaffungsvorlagen oder handelt in Zusammenarbeit mit den Abteilungen Sicherheit, Recht, Beschaffung und Finanzen (in jedem Fall, je nach Bedarf) die Bedingungen dieser Drittparteien aus, sofern dies für erforderlich gehalten wird.

7 Kontaktaufnahme mit GoTo

Kunden können GoTo unter https://support.goto.com für allgemeine Anfragen oder privacy@goto.com für Fragen zum Datenschutz kontaktieren.

8 Anhang – Begriffserklärungen

Techniker: Ein Benutzer von GoToAssist Remote Support V5, der GoToAssist Remote Support V5-Sitzungen initiieren kann, um Kunden per Bildschirmanzeige, Remotesteuerung oder Kameraübertragung technische Unterstützung zu leisten.

Webbasierte Technikerkonsole: Eine Webanwendung, 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 GoToAssist Remote Support V5-Dienst herstellt. Mit dieser Anwendung kann der Techniker GoToAssist Remote Support V5-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 GoToAssist Remote Support V5-Dienst herstellt. Sie nutzt die Technologie der Web-Technikerkonsole für GoToAssist Remote Support V5, Qt und die Chromium-Web-Engine. Sie bietet dieselbe Funktionalität wie die webbasierte Technikerkonsole, aber in einem nativen Erscheinungsbild.

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

Kunde: Person, die vom Techniker über eine GoToAssist Remote Support V5-Sitzung technische Unterstützung erhält.

Endbenutzer-Desktop-App: Eine Desktop-Anwendung, die auf dem Computer des Kunden (Windows oder Mac) ausgeführt wird und über den GoToAssist Remote Support V5-Dienst eine Verbindung zu einer GoToAssist Remote Support V5-Sitzung herstellt. Sie bietet eine

Remotesteuerungsfunktion sowie andere erweiterte Funktionen und die Möglichkeit, die Fernzugangs-App auf dem Computer des Kunden zu installieren.

Kundenendpunkt: Sammelbegriff, der sich auf einen beliebigen Kundenendpunkt bezieht: Endbenutzer-Web-App, Endbenutzer-Desktop-App, Mobile Endbenutzer-App, Fernzugangs-Endbenutzer-App.

Mobile Endbenutzer-App: Eine mobile Anwendung (Android oder iOS), die auf dem Mobilgerät/Tablet des Kunden ausgeführt wird und über den GoToAssist Remote Support V5-Dienst eine Verbindung zu einer GoToAssist Remote Support V5-Sitzung herstellt. Sie bietet Funktionen zur Bildschirmanzeige (Android und iOS) und zur Remotesteuerung (nur Android).

Endbenutzer-Web-App: Eine Webanwendung, die in einem unterstützten Browser auf dem Computer/Mobilgerät des Kunden ausgeführt wird und über den GoToAssist Remote Support V5-Dienst eine Verbindung zu einer GoToAssist Remote Support V5-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.

GoToAssist Remote Support V5-Sitzungen: Interaktive Sitzung mit Chat, Bildschirmanzeige, Remotesteuerung oder Kameraübertragung und Remotesteuerung per Fernzugang.

GoToAssist Remote Support V5-Dienst: Eine Gruppe von global verteilten Servern mit Lastausgleich, die über eine verschlüsselte WebSocket-Verbindung und API-Aufrufe einen sicheren Zugriff für die webbasierte Technikerkonsole und die Kunden-Endgeräte bieten.

Fernzugangs-Kunden-App: Eine installierbare Desktop-Anwendung (Windows und Mac), die im Hintergrund auf dem Computer des Kunden 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 Kunde nicht anwesend ist. Die Sitzung wird vom Techniker ohne Beteiligung des Kunden über eine autorisierte Fernzugangs-Kunden-App initiiert und aufgebaut.