TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR GOTO MEETING, GOTO WEBINAR, GOTO TRAINING UND GOTO STAGE

Operative Sicherheits- und Datenschutzkontrollen

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

Dieses Dokument behandelt die technischen und organisatorischen Maßnahmen (TOMs) für GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage (zusammenfassend als „UCC-Lösungen von GoTo“ bezeichnet).

Bei den GoTo-Produkten der UCC-Lösungen handelt es sich um Online-Kommunikationsservices, die es Einzelpersonen und Organisationen ermöglichen, je nach Service-Angebot mit zahlreichen Funktionen zu interagieren. Dazu gehören Bildschirmfreigabe, Videokonferenzen und integriertes Audio. Die GoTo-Services der UCC-Lösungen werden mit Hilfe eines Webbrowsers oder eines Client-Programms über ein global verteiltes Netzwerk proprietärer Hardware und Software bereitgestellt.

- GoTo Meeting ermöglicht es Benutzern, Sitzungen über die GoTo Meeting-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren.

- GoTo Webinar ermöglicht es Unternehmen, über das Internet Events und Präsentationen für ein größeres lokales oder globales Publikum durchzuführen. Webinare werden über die GoTo Webinar-Website und/oder die Client-Software geplant, einberufen und moderiert.

- GoTo Training ermöglicht es Benutzern, Schulungssitzungen über die GoTo Training-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren. Es bietet spezielle Funktionen für webbasierte Schulungen wie Online-Zugang zu Tests und Schulungsmaterialien und ein gehostetes Kursverzeichnis.

- GoTo Stage ist ein Online-Portal, in dem GoTo Webinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo Stage-Homepage vorgestellt. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoTo Webinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo Stage-Umgebung gelöscht werden.

2 Produktarchitektur

Die Bildschirmübertragung zwischen den Teilnehmern in Sitzungen der UCC-Lösungen von GoTo erfolgt über einen Overlay Networking Stack, der logisch über dem konventionellen TCP/IP-Stack auf den Computern der einzelnen Benutzer angeordnet ist (siehe Abbildung 1).

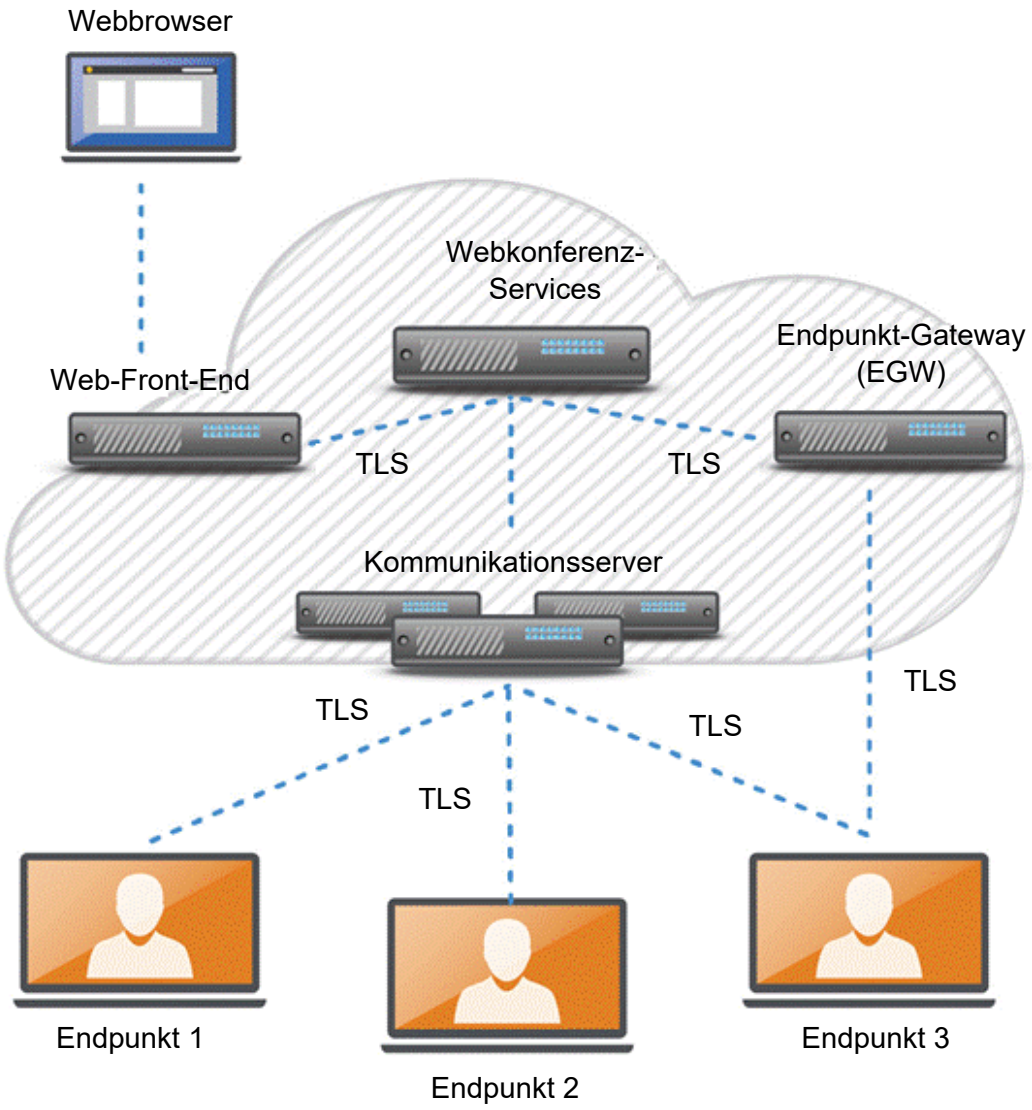

Abbildung 1 – Architektur von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage.

***Web-Front-End** – Portal-Webseite der GoTo-Suite, wird in Co-Location-Rechenzentren an Tier 1 und auf AWS gehostet*

***WCS** – Sitzungsplanung, Meetingchronik, GTM-Organisatoreinstellungen, wird in Co-Location-Rechenzentren an Tier 1 gehostet*

***Kommunikationsserver** – inkl. Server für Bildschirmfreigabe, Audio Bridges und Voice Gateways (als Proxy), H.323-Gateways – gehostet auf Amazon Web Services/**Multicast-Kommunikationsserver** und Video Cluster Server in Co-Location-Rechenzentren an Tier 1 gehostet*

***Endpunkt-Gateway (EGW)** – verarbeitet Organisator- und Endpunktverbindungen und Verschlüsselungsmechanismen – EGW auf Amazon Web Services gehostet*

Die Teilnehmer (Sitzungsendpunkte) verwenden ausgehende TCP/IP-Verbindungen über den Port 443, um mit den Kommunikationsservern und Gateways der Infrastruktur zu kommunizieren. Dabei können sich die Teilnehmer überall im Internet befinden. Clients kommunizieren in der Regel über das Endpunkt-Gateway mit den UCC-Lösungen von GoTo. Neue Clients kommunizieren jedoch direkt mit Hilfe von REST-Aufrufen (Representational

State Transfer) über Lastenausgleiche mit den Back-End-Services. Die Service-Infrastruktur ermöglicht es Benutzern des Telefonnetzes, sich in ein Meeting einzuwählen.

GoTo-Produkte von UCC-Lösungen verwenden ein ASP-Modell (Application Service Provider), das einen sicheren Betrieb gewährleistet und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt.

Die Architektur ist für eine hohe Leistung, Zuverlässigkeit und Skalierbarkeit konzipiert und wird auf Hochleistungsservern betrieben, auf denen die entsprechenden Sicherheitspatches installiert sind. Redundante Switches und Router sind so konzipiert, dass „Single Points of Failure“ ausgeschlossen werden. Geclusterte Server und Backup-Systeme stellen selbst bei hoher Auslastung oder einem Systemausfall sicher, dass die Anwendungsprozesse funktionieren. Webkonferenz-Services verteilen die Last der Client/Server-Sitzungen auf geografisch verteilte Kommunikationsserver, um die Leistung und eine angemessene Latenz sicherzustellen.

Die Service-Infrastruktur wird hauptsächlich in Co-Location-Rechenzentren an Tier 1 gehostet, wobei einige Komponenten-Services bei Cloud-Hosting-Anbietern gehostet werden. Die Audio Bridge-Services werden vollständig von Cloud-Anbietern gehostet, während einige der Webkonferenz-Services für Produkte teilweise von Cloud-Anbietern gehostet werden. Die Daten, die mit einem von einem Cloud-Anbieter gehosteten Service verbunden sind, werden auch bei diesem Anbieter gespeichert.

Der physische Zugriff auf Co-Location Hosted Servern ist eingeschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante Stromversorgungen und entsprechende Einrichtungen zur Kontrolle der Umgebungsbedingungen. Die privaten Netzwerke und Back-End-Server von GoTo sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und externe Prüfer führen regelmäßige Tests auf Schwachstellen durch.

Weitere Informationen finden Sie im Whitepaper zur UCC-Sicherheit.

3 Technische Sicherheitskontrollen für UCC-Lösungen von GoTo

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

3.1 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um 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.

3.2 Perimeterverteidigung und Erkennung von Eindringversuchen

GoTo setzt Standard-Tools, -Techniken und -Services für den Perimeterschutz ein, die verhindern sollen, dass nicht autorisierter Netzwerkdatenverkehr in unsere Produktinfrastruktur gelangt. Das GoTo-Netzwerk enthält nach außen gerichtete Firewalls und eine interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch Host-basierte Firewalls. Außerdem wird ein Cloud-basierter DDoS-Schutzservice (Distributed Denial of Service) eines Drittanbieters zum Schutz vor umfangreichen DDoS-Angriffen verwendet. Dieser Service wird mindestens einmal pro Jahr getestet. Wichtige Systemdateien werden vor böswilliger oder unbeabsichtigter Infizierung oder Zerstörung geschützt.

3.3 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.

3.4 Physische Sicherheit

Physische Rechenzentrumssicherheit

GoTo arbeitet mit Rechenzentren zusammen, um physische Sicherheits- und Umgebungskontrollen für Serverräume mit Produktionsservern zu bieten. Zu diesen Kontrollen gehören:

- Videoüberwachung und Aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- Temperaturregelung von Heizung, Lüftung und Klimaanlage
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (USV)
- Zwischenböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen Naturkatastrophen und vom Menschen verursachten Katastrophen entsprechend der Geografie und des Standorts des jeweiligen Rechenzentrums
- Geplante Wartung und Validierung aller wichtigen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu Produktionsrechenzentren nur auf autorisierte Einzelpersonen. Für den Zugang zu einer Hosting-Einrichtung ist die Einreichung eines Antrags über das entsprechende Ticketing-System und die Genehmigung des jeweiligen Managers sowie eine Überprüfung und Genehmigung der Technikabteilung erforderlich. Die GoTo-Verwaltung überprüft die Protokolle für den physischen Zugang zu Rechenzentren und Serverräumen mindestens auf vierteljährlicher Basis. Außerdem wird der physische Zugang zu Rechenzentren bei Kündigung von bereits autorisiertem Personal entfernt.

3.5 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

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

3.6 Malware-Schutz

Malware-Schutzsoftware mit Überwachungsprotokollen wird auf allen Servern der UCC-Lösungen von GoTo eingesetzt. Warnmeldungen, die auf mögliche böswillige Aktivitäten hinweisen, werden an ein entsprechendes Reaktionsteam gesendet.

3.7 Vertraulichkeit und Authentizität der Daten

GoTo verfügt über einen kryptografischen Standard, der sich nach Empfehlungen von Branchengruppen, staatlichen Veröffentlichungen und anderen für Standards relevanten Gruppen 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.

3.7.1 Übertragene Daten

GoTo Meeting, GoTo Webinar und GoTo Training umfassen Sicherheitsmaßnahmen für übertragene Daten zum Schutz vor und zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten. Bildschirm- und Videofreigabe, VoIP, Webcam-Video, Tastatur-/Maussteuerung und textbasierte Chat-Informationen („Sitzungsdaten“) weisen Kommunikationssicherheitskontrollen nach Branchenstandard auf.

Sitzungsdaten werden bei der Übertragung zwischen Endpunkten und GoTo-Kommunikationsservern nie in Klartext offengelegt.

In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: (i) auf dem TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) und (ii) in der MPSL (Multicast Packet Security Layer).

TCP- und UDP-Sicherheit

Die TCP-Kommunikation zwischen Endpunkten wird durch TLS-Protokolle (Transport Layer Security) 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 Verschlüsselung verwenden und sicherstellen, dass die Sicherheitspatches für ihr Betriebssystem und ihre Browser aktuell sind.

Beim Herstellen einer TLS-Verbindung zur Website sowie zwischen den GoTo Meeting-, GoTo Webinar- oder GoTo Training-Komponenten authentifizieren sich die GoTo-Server mit Hilfe von Public-Key-Zertifikaten bei den Clients. Als zusätzlicher Schutz vor Infrastrukturangriffen erfolgt eine gegenseitige zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z.B. Kommunikations-server zu Webkonferenz-Services).

Für mit UDP gesendete Daten wird eine vorhandene TLS-Verbindung genutzt, um kryptografische Schlüssel zum Verschlüsseln und Authentifizieren von UDP-Daten sicher auszutauschen.

Sicherheit der Multicast Packet Layer

Multicast-Daten wie Tastatur-/Maussteuerung, Chat und Statusinformationen in der Sitzung sind durch Verschlüsselung bei der Übertragung und Integritätsmechanismen geschützt, die jeden mit Zugriff auf die Kommunikationsserver – egal ob Freund oder Feind – daran hindern sollen, eine Sitzung abzuhören oder Daten unerkannt zu manipulieren. Die MPSL bietet speziell für GoTo-Produkte eine zusätzliche Ebene der Kommunikationsvertraulichkeit und -integrität. Diese zusätzliche Sicherheitsschicht verwendet AES-Verschlüsselung mit 128 Bit im Abwehrmodus für weiteren Schutz vor Abhörung und Manipulation.

Zur Optimierung der Bandbreite werden Klartextdaten in der Regel vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert. Der Schutz der Datenintegrität wird durch eine ICV-Prüfsumme gewährleistet, die derzeit mit dem HMAC-SHA-1-Algorithmus generiert wird.

Die Schlüsselvereinbarung erfolgt mittels eines zufällig generierten 128-Bit-Startwerts („Seed“), der vom GoTo-Service ausgewählt und über TLS an alle Endpunkte verteilt wird. Er dient als Eingabe für eine vom NIST genehmigte Schlüsselableitungsfunktion. Bei Beendigung der Sitzung wird der Seed-Wert aus dem Arbeitsspeicher des Service gelöscht.

Audiosicherheit

GoTo Meeting, GoTo Webinar und GoTo Training unterstützen integrierte Audiokonferenzen sowohl über das herkömmliche Telefonnetz als auch über VoIP (Voice over Internet Protocol). Das herkömmliche Telefonnetz gewährleistet von vornherein die Vertraulichkeit und Integrität der Sprachkommunikation. Zum Schutz der Vertraulichkeit und Integrität der VoIP-Verbindungen zwischen Endpunkten und Sprachservern kommt sowohl über UDP als auch TCP ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1 zum Einsatz. Client und Server tauschen die Schlüssel über die hergestellte TLS-Verbindung aus.

Videosicherheit

Zum Schutz der Vertraulichkeit und Integrität von Videoverbindungen zwischen Endpunkten und Videoservern nutzt GoTo ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1. Client und Server tauschen die Schlüssel über die hergestellte TLS-Verbindung aus.

Webcast-Sicherheit

GoTo Webinar-Webcasts nutzen Kommunikationsserver, Broadcast-Gateways, Streaming Engines und Content Delivery Networks von Drittanbietern, um die Bildschirm-, Ton- und Videoübertragung für Teilnehmer, die über einen Browser beitreten, zu ermöglichen. Die Gateways empfangen Mediendaten von den Kommunikationsservern, transcodieren sie in Standard-Codecs und leiten sie an die Streaming Engine über RTP weiter − alles in unserem sicheren internen Netzwerk. Die Streaming Engine erzeugt HTTP Live Streaming (HLS) mit mehreren Bitraten, um eine adaptive Zustellung für Clients mit nicht ganz optimalen Netzwerkverbindungen zu ermöglichen. CDNs wurden eingerichtet, um Daten aus der Streaming Engine über HTTPS sicher abrufen. Die Clients rufen Daten auch sicher von CDNs über HTTPS ab.

GoTo Stage

GoTo Stage ist ein Online-Portal, in dem GoTo Webinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo Stage-Homepage vorgestellt. Ein auf GoTo Stage veröffentlichtes Video ist über die GoTo Stage-Homepage und über Suchmaschinen auffindbar, sofern der Organisator die Auffindbarkeit nicht mit Hilfe der Administratoreinstellungen auf seiner Kanalseite eingeschränkt. Andernfalls können alle bei GoTo Stage registrierten Personen mit einem direkten Link zum Kanal oder zur individuellen „Watch Now"-Seite des Videos die Aufzeichnung ansehen. Besucher registrieren sich mit ihrem Namen und ihrer E-Mail-Adresse bei GoTo Stage oder stellen über Konten in sozialen Netzwerken wie LinkedIn, Facebook und Gmail eine Verbindung her. Nach der Registrierung erfolgt die Wiedergabe des aufgezeichneten Webinars über eine signierte S3-URL mit einer festgelegten TTL. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoTo Webinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo Stage-Umgebung gelöscht werden. Zum Schutz der GoTo Stage-Administrationsfunktionen werden Passwörter verwendet, und alle Verbindungen im GoTo Stage-Portal sind mittels TLS geschützt.

3.7.2 Daten im Ruhezustand

In GoTo Meeting, GoTo Webinar und GoTo Training können Organisatoren ihre Live-Sitzungen einschließlich Audio-, Video- und Bildschirminhalten aufzeichnen. Sobald ein Organisator die Aufzeichnung startet, werden die Teilnehmer dazu benachrichtigt. Dass eine Aufzeichnung läuft, wird ihnen dann auf dem Bedienpanel angezeigt. Kunden können Sitzungsaufzeichnungen auf ihrem lokalen Rechner oder in der Cloud speichern.

Cloud-Aufzeichnungen

Cloud-Aufzeichnungen werden auf AWS S3 gespeichert. Dateien werden im Ruhezustand unter Verwendung von serverseitiger Verschlüsselung mit 256-Bit-AES gespeichert

Transkripte

Wenn vom Organisator aktiviert, wird Cloud Speech-to-Text-Technologie von Google verwendet, um Sitzungsaufzeichnungen zu transkribieren. Audiodateien werden mit TLS für die Transkription übertragen, wobei die Datei mit 256-Bit-AES verschlüsselt und direkt nach der Verarbeitung von Sprache zu Text gelöscht wird. Transkripts werden von GoTo mithilfe der AWS S3-Instanz aufbewahrt und dem Organisator bei den Cloud-Aufzeichnungen zur Verfügung gestellt.

Upload von Inhalten

Einige der GoTo-Services bieten Funktionen, mit denen Organisatoren Videos für den Einsatz in Live-Sitzungen hochladen können. Auch diese Uploads werden in AWS S3 gespeichert, wenn AES-Verschlüsselung (256 Bit) im Ruhezustand und bei der Übertragung aktiviert ist.

3.8 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden monatlich auf Schwachstellen überprüft. Es werden auch regelmäßig Schwachstellenprüfungen dynamischer und statischer

Anwendungen vorgenommen und Penetrationstestaktivitäten für bestimmte Umgebungen ausgeführt. Für die Ergebnisse dieser Überprüfungen und Tests werden in Netzwerküberwachungstools Berichte erstellt, und wo dies basierend auf der Wichtigkeit der identifizierten Schwachstellen erforderlich ist, werden Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.9 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 der UCC-Lösungen von GoTo.

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 wahrt Compliance mit den folgenden Zertifizierungen und externen Audit-Berichten:

- TRUSTe Enterprise Privacy & Data Governance Practices Certification, 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.
- Service Organization Control (SOC) 2 Type 2-Bericht des American Institute of Certified Public Accountants (AICPA)
- 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 Security Operations und Incident-Management

Das Security Operations Center (SOC) von GoTo ist mit dem Security Operations-Team besetzt und ist 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. Diese Richtlinien und Verfahren wurden entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services von GoTo, einschließlich der UCC-Lösungen von GoTo 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 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, Abonnenten der UCC-Lösungen von GoTo 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. Die UCC-Lösungen von GoTo sind 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. Es regelt die Verarbeitung personenbezogener Daten durch GoTo, um die Anforderungen von DSGVO, CCPA und mehr zu erfüllen.

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 Inkrafttreten des 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 Abkommen zur Datenübertragung

GoTo hat ein robustes globales Data Protection-Programm, das das geltende Recht 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 der UCC-Lösungen von GoTo können jederzeit die Rückgabe oder Löschung ihres Inhalts anfordern. Derartige Anfragen werden innerhalb von dreißig (30) Tagen der Anfrage ausgeführt (oder früher, wo durch geltendes Recht erforderlich). Zudem werden GoTo Meeting-Meetingchronik und Cloud-Aufzeichnungen automatisch auf rollierender 1-Jahres-Basis während eines aktiven Abonnementzeitraums des Kunden gelöscht.

Nach Ende eines zahlungspflichtigen Abonnements für GoTo Meeting werden die Konten des Kunden in ein kostenloses Konto umgewandelt. Wenn ein Konto explizit gekündigt oder aufgelöst wird, wird der Inhalt innerhalb von 90 Tagen der Kündigung oder Auflösung gelöscht. Kostenlose GoTo Meeting-Konten unterliegen der rollierenden 1-Jahres-Löschung, die oben beschrieben ist. Kostenlose GoTo Meeting-Konten werden zudem nach zwei (2) Jahren Inaktivität des Benutzers (z. B. keine Anmeldungen) automatisch gelöscht.

Zur Berücksichtigung eines saisonalen Benutzerstamms werden GoTo Webinar- und GoTo Training-Konten zwei (2) Jahre nach Ablauf oder Beendigung der jeweiligen Endlaufzeit gelöscht. GoTo Stage-Benutzer können ihre veröffentlichten Webinare während eines aktiven GoTo Webinar-Abonnements jederzeit per Self-Service über die GoTo Webinar-Service-Umgebung und/oder durch Einreichen einer Supportanfrage bei GoTo entfernen oder die Veröffentlichung rückgängig machen. Auf schriftliche Anfrage bestätigt GoTo die Löschung des betreffenden Kontos und des Inhalts.

5.6 Sensible Daten

Es ist das Ziel von GoTo, den gesamten Kundeninhalt zu schützen, und regulatorische und vertragliche Beschränkungen verlangen, dass die Verwendung von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die

folgenden Daten nicht in GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage 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, die im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) und damit verbundenen Gesetzen und Vorschriften festgelegt sind.
- 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 GoTo Meeting, GoTo Training, GoTo Webinar und GoTo Stage 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 Anbietern und Dritten 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. Die Teams für Recht und Beschaffung können 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.