Technische und organisatorische Maßnahmen
Central und Pro

Zusammenfassung

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

- **Verschlüsselung:**
  - *Während der Übertragung* Transport Layer Security (TLS) Version 1.2 oder 1.3, wenn unterstützt.
  - *Im Ruhezustand* Transparent Data Encryption (TDE) und Advanced Encryption Standard (AES) 256-Bit für Kundeninhalte.
- **Rechenzentren:** Standorte in Deutschland, Australien, im Vereinigten Königreich, in den USA, den Niederlanden und Irland, um Redundanz und Stabilität zu gewährleisten.
- **Physische Sicherheit:** Geeignete physische Sicherheits- und Umgebungskontrollen sind vorhanden und darauf ausgelegt, den physischen Zugang zu Systemen und Servern mit Kundeninhalten zu schützen, zu kontrollieren und einzuschränken, um die Verpflichtungen hinsichtlich Betriebszeit, Leistung und Skalierbarkeit einhalten zu können.
- **Compliance-Audits:** Central und Pro sind nach SOC 2 Typ II, C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy sowie APEC CBPR und PRP zertifiziert.
- **Einhaltung gesetzlicher/behördlicher Vorschriften:** GoTo unterhält ein umfassendes Datenschutzprogramm mit Prozessen und Richtlinien, die sicherstellen sollen, dass Kundeninhalte in Übereinstimmung mit den geltenden Datenschutzgesetzen, einschließlich DSGVO, CCPA/CPRA und LGPD, behandelt werden.
- **Sicherheitsprüfungen**: GoTo führt nicht nur interne Tests durch, sondern beauftragt zusätzlich externe Firmen mit der regelmäßigen Durchführung von Sicherheitsprüfungen und/oder Penetrationstests.
- **Logische Zugriffskontrollen:** Durch Implementierung entsprechend konzipierter logischer Zugriffskontrollen soll die Bedrohung des unbefugten Anwendungszugriff und des Datenverlusts in Unternehmens- und Produktionsumgebungen verhindert oder gemindert werden.
- **Datentrennung**: GoTo verwendet eine Multi-Tenant-Architektur und trennt Kundenkonten logisch auf der Datenbankebene.
- **Perimeterabwehr und Erkennung von Eindringversuchen**: Tools, Techniken und Dienste zum Schutz des Perimeters sollen verhindern, dass nicht autorisierter Netzwerk-Datenverkehr in die Produktinfrastruktur gelangt. Das GoTo-Netzwerk ist mit externen Firewalls ausgestattet und verfügt über interne Netzwerksegmentierung.
- **Datenaufbewahrung:**
  - Kunden von Central und Pro können jederzeit einen Antrag auf Rückgabe oder Löschung von Kundeninhalten stellen, der innerhalb von dreißig (30) Tagen nach Antragstellung des Kunden bearbeitet wird.
  - Kundeninhalte werden neunzig (90) Tage nach Ablauf der letzten Abonnementlaufzeit eines Kunden automatisch gelöscht.

Inhalt

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

1 Produkteinführung

Central ist eine webbasierte Verwaltungskonsole, die es IT-Experten ermöglicht, auf Remotegeräte zuzugreifen, sie zu verwalten und zu überwachen, Software-Updates und Patches zu installieren, IT-Aufgaben zu automatisieren und hunderte Versionen von Virenschutzsoftware auszuführen. Central wird als Premium-Dienst mit mehreren Preisstufen angeboten, die sich nach der Anzahl der unterstützten Geräte und den gewünschten Funktionen richten.

Pro ist ein Remotezugriffsdienst, der von jedem mit dem Internet verbundenen Gerät sowie den meisten Smartphones und Tablets aus sicheren Zugriff auf Remotecomputer und andere internetfähige Geräte gewährt. Nachdem ein Pro-Host auf einem Gerät installiert wurde, ermöglicht es der Dienst einer Person mit einem Unterkonto innerhalb eines Kundenkontos („Benutzer“), von den anderen internetfähigen Geräten des Benutzers aus remote auf den Desktop, die Dateien, Anwendungen und Netzwerkressourcen des Pro-Geräts zuzugreifen. Pro kann schnell bereitgestellt und installiert werden, ohne dass IT-Kenntnisse erforderlich sind.

Central und Pro sind so konzipiert, dass sie den sicheren Remotezugriff auf kritische Ressourcen über ein nicht als vertrauenswürdig eingestuftes Netzwerk ermöglichen. Sicherheit spielt eine wichtige Rolle bei der Produktentwicklung.

In diesem Dokument verwendete Begriffe, die nicht im Text definiert sind, werden in den Nutzungsbedingungen erklärt.

2 Technische Maßnahmen

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

2.1 Schutzmaßnahmen

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

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

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

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

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

3 Produktarchitektur

Central und Pro sind SaaS-basierte Anwendungen mit einer mehrstufigen Architektur, die in geografisch verteilten Rechenzentren gehostet werden. Die Sicherheitsmaßnahmen auf allen Ebenen, von der Bitübertragungsschicht bis hin zur Anwendungsschicht, sind so konzipiert, dass sie umfassenden Schutz bieten.

Die Anwendungen Central und Pro bestehen aus drei Schlüsselkomponenten, die eine erfolgreiche Remotezugriffssitzung ermöglichen:

- **Client:** die Software (z. B. Browser, native App, mobile App), die auf eine Remoteressource zugreift
- **Host oder Server:** das Gerät, auf das zugegriffen wird, oder die Host-Software des Produkts auf diesem Gerät
- **Central/Pro-Gateway:** der Dienst, der den Datenverkehr zwischen dem Client und dem Host vermittelt

Der Central/Pro-Host ist so konzipiert, dass er eine ständige, mit Transport Layer Security (TLS) gesicherte Verbindung zu einem Gateway-Server in einem der GoTo-Rechenzentren aufrechterhält. Nachdem eine sichere Verbindung zu Central oder Pro hergestellt wurde, wird der Client vom Host authentifiziert und autorisiert, auf das Gerät zuzugreifen, und die Remotezugriffssitzung beginnt. Der Gateway-Server vermittelt den verschlüsselten Datenverkehr zwischen den beiden Entitäten, setzt aber nicht voraus, dass der Host dem Client implizit vertraut. Über das Central/Pro-Gateway kann entweder der Client oder der Host (oder beide) mit einer Firewall versehen werden, sodass Benutzer keine Firewalls konfigurieren müssen.

Das GoTo-eigene Weiterleitungsprotokoll für den Schlüsselaustausch schützt unsere eigene Infrastruktur vor dem Abfangen oder Abhören von Daten. Insbesondere ermöglicht das Gateway die Verbindung zwischen dem Client und dem Host, damit sichergestellt ist, dass sich der Client unabhängig von der Netzwerkkonfiguration mit dem Host verbinden kann.

Wenn der Host bereits eine TLS-Verbindung zum Gateway aufgebaut hat, leitet das Gateway den TLS-Schlüsselaustausch des Clients über eine proprietäre Anforderung zur Neuaushandlung des Schlüssels an den Host weiter. So tauschen der Client und der Host TLS-Schlüssel aus, ohne dass das Gateway den Schlüssel erfährt.

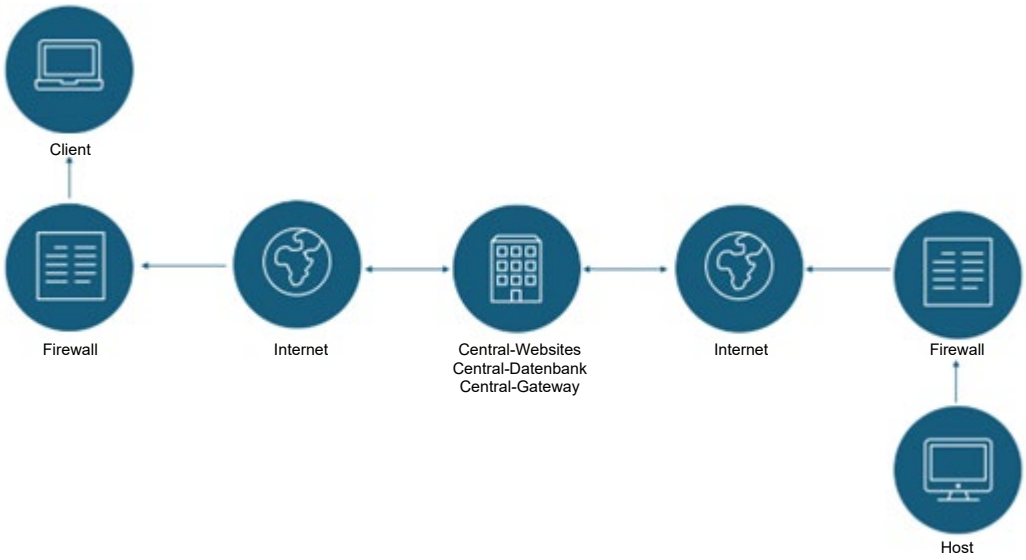

Abbildung 1: Central-Architektur

4 Technische Sicherheitskontrollen

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

4.1 Verschlüsselung

GoTo überprüft regelmäßig seine Verschlüsselungsstandards und aktualisiert gegebenenfalls die verwendeten Verschlüsselungsverfahren und/oder Technologien entsprechend der Risikobewertung und der Marktakzeptanz neuer Standards, um seine Verfahren und Verschlüsselungsmethoden fortlaufend zu verbessern.

Die Dienste Central und Pro unterstützen die folgenden Verschlüsselungsprotokolle (soweit zutreffend): TLS 1.2, 2048-Bit-RSA- und -AES256-Verschlüsselung mit 384-Bit-SHA-2-Algorithmus.

Central und Pro unterstützen sowohl AES 128- als auch 256-Bit-Schlüssel, und der Client und der Server einigen sich auf den stärksten kompatiblen und verfügbaren Verschlüsselungscode zwischen diesen beiden Schlüssellängen. Der Client sendet dem Server eine Liste der Verschlüsselungscodes, die er verwenden möchte, und der Server sucht sich den gewünschten Verschlüsselungscode aus. Bei Central und Pro sucht der Server die stärkste gemeinsame Verschlüsselungssammlung aus, die vom Client angeboten wurde.

4.2 Verschlüsselung während der Übertragung

Der gesamte Netzwerk-Datenverkehr, der in Central/Pro-Rechenzentren ein- und ausgeht, wird während der Übertragung mit TLS 1.2 oder, wo unterstützt, mit TLS 1.3 verschlüsselt. Dies schließt auch Kundeninhalte ein.

4.3 Verschlüsselung ruhender Daten

Alle Central/Pro-Kundeninhalte werden in MSSQL mit Transparent Data Encryption (TDE) gespeichert und im Ruhezustand mit AES-256 verschlüsselt.

4.4 Benutzerauthentifizierung

Central/Pro verwendet einen proprietären Common Login Service („CLS“) zur Benutzerauthentifizierung. CLS verwendet benutzerdefinierte Heuristiken, um verdächtige Benutzerzugriffe zu verhindern. Bei Konten, die mit einem GoTo Common Identity Platform („CIP“)-Konto verknüpft sind, wird die Anmeldung durch einen Risikobewertungsdienst eines Drittanbieters zusätzlich geschützt.

4.5 Multifaktor-Authentifizierung

Die Multifaktor-Authentifizierung (auch als zweistufige Verifizierung oder Zwei-Faktor-Authentifizierung bezeichnet) erweitert den Schutz für ein Konto, indem sie zwei verschiedene Arten der Identifizierung zum Anmelden beim Konto gefordert werden. Nach der Einrichtung der Multifaktor-Authentifizierung geben Benutzer ihre Zugangsdaten ein und werden dann aufgefordert, ihre Identität durch einen Sicherheitscode zu verifizieren.

Central-Abonnenten können Login-Regeln durchsetzen, die alle Benutzer ihres Kontos zwingen, die Multifaktor-Authentifizierung zu verwenden. Eine schrittweise Anleitung finden Sie unter support.logmeininc.com/central.

4.6 Gedruckte Sicherheitscodes

Kunden können sich für die Verwendung von gedruckten Sicherheitscodes als zusätzlichen Schutz entscheiden. Wenn der Benutzer diese Funktion aktiviert, wird er aufgefordert, eine Liste mit neunstelligen zufälligen Passwörtern auszudrucken, die vom Gateway generiert wurden. Wenn sich ein Benutzer auf logmein.com bei seinem Konto anmeldet, wird er zur Eingabe eines dieser Sicherheitscodes aus der Liste aufgefordert, um Zugriff auf sein Konto zu erhalten. Jeder Code kann nur einmal verwendet werden. Bevor alle gedruckten Sicherheitscodes aufgebraucht sind, muss der Benutzer ein neues Blatt ausdrucken. Alle bis dahin nicht benutzten Sicherheitscodes werden dadurch ungültig.

4.7 E-Mail-Sicherheitscodes

Wenn diese Funktion aktiviert ist und sich der Benutzer erfolgreich mit seiner E-Mail-Adresse und seinem Passwort beim Central/Pro-Gateway authentifiziert hat, wird ein Passcode generiert und an die E-Mail-Adresse gesendet. Der Benutzer muss den per E-Mail erhaltenen Code in das vom Gateway bereitgestellte Formular eingeben. Der Passcode läuft entweder bei Verwendung oder einige Minuten nach der Erstellung ab (je nachdem, was zuerst eintritt).

4.8 Authentifizierung des Gateways gegenüber dem Client

Central und Pro verwenden die zertifikatsbasierte Authentifizierung mit TLS 1.2 oder 1.3 (wobei 1.3 verwendet wird, wenn es unterstützt wird und nicht explizit deaktiviert ist), um die Identitäten von Servern zu verifizieren und sicherzustellen, dass ein Benutzer, der sich über ein Gateway mit einem Central- oder Pro-Server verbindet, eine Verbindung zum vorgesehenen Gerät herstellt. Wenn eine Verbindung hergestellt wird, wird das Zertifikat des Servers überprüft. Falls das Zertifikat von einer nicht als vertrauenswürdig eingestuften Zertifizierungsstelle ausgegeben wurde, wird ein Warnhinweis angezeigt. Sollte der Hostname in der URL nicht mit dem Hostnamen im Zertifikat übereinstimmen, wird ein anderer Warnhinweis angezeigt, selbst wenn das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt.

Nachdem die Identität des Servers bestätigt wurde, erstellt der Client des Benutzers ein so genanntes „Pre-Master Secret“ (PMS, Vorstufe des geheimen Hauptschlüssels), verschlüsselt es mit dem öffentlichen Schlüssel des Servers laut dessen Zertifikat und sendet es an den Server. Durch die Verschlüsselung mit dem öffentlichen Schlüssel wird sichergestellt, dass nur der Server das PMS entschlüsseln kann, der den dazugehörigen

privaten Schlüssel besitzt. Das PMS wird anschließend sowohl vom Benutzer als auch vom Server zur Ableitung des geheimen Hauptschlüssels verwendet, welcher wiederum dazu dient, für die Dauer der sicheren Sitzung die Initialisierungsvektoren und die Sitzungsschlüssel abzuleiten.

4.9 One2Many – Authentifizierung und Verschlüsselung (nur Central)

Die Funktion One2Many unterstützt erweiterte Skripterstellungs- und Bereitstellungsfunktionen, mit denen Central-Benutzer Massenvorgänge in verwalteten Unternehmen ausführen können. Mit diesem Tool können Benutzer Administrationsaufgaben direkt von Central aus auf mehreren Windows- und Mac-Geräten ausführen, verwalten und überwachen.

Für One2Many ist eine Multifaktor-Authentifizierung erforderlich. One2Many speichert die Zugangsdaten für die Multifaktor-Authentifizierung auf zwei verschiedene Arten: Wenn eine Aufgabe in Echtzeit ausgeführt wird, werden die Zugangsdaten im Browser gespeichert; wenn die Ausführung der Aufgabe für einen späteren Zeitpunkt geplant ist, werden die Zugangsdaten in der Datenbank des Produkts gespeichert.

Die in One2Many verwendeten Zugangsdaten werden zuerst mit dem öffentlichen Schlüssel des Hosts verschlüsselt und dann von der Website weiter verschlüsselt. Die erste Verschlüsselungsebene stellt sicher, dass nur der Host die Zugangsdaten mit seinem privaten Schlüssel entschlüsseln kann. Die zweite Verschlüsselungsebene aktiviert die Option zum Löschen von Daten von der Website, selbst wenn der Host offline ist.

4.10 Authentifizierung der Benutzer gegenüber dem Gateway

Benutzer müssen sowohl vom Gateway als auch vom Host authentifiziert werden. Die E-Mail-Adresse und das Passwort eines Benutzers werden jedes Mal verifiziert, wenn er sich bei Central/Pro anmeldet.

HINWEIS: Central-Kunden können eine Richtlinie für starke Passwörter erzwingen. Weitere Informationen finden Sie auf support.logmeininc.com/central.

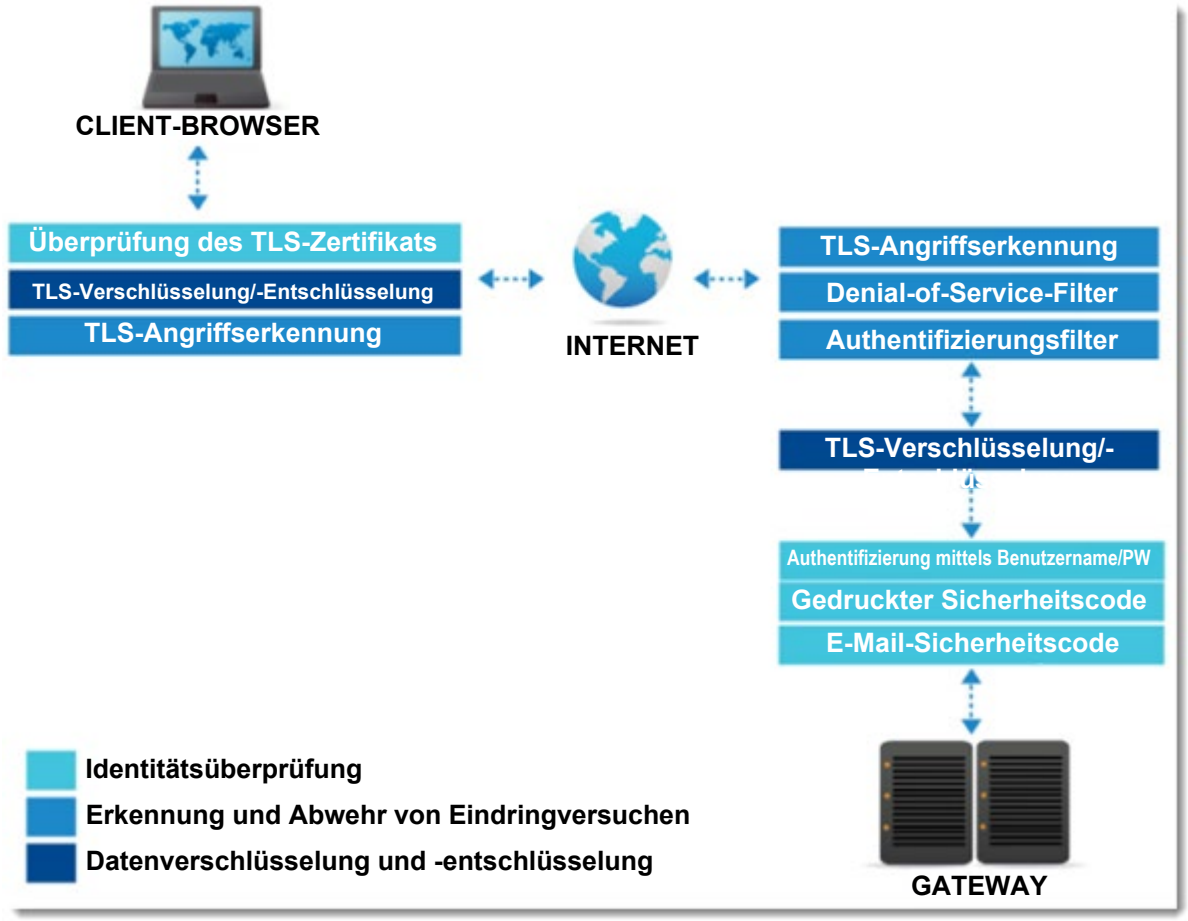

Abbildung 2: Authentifizierung zwischen Benutzern und Gateway

4.11 Kontoüberwachung

Kunden können die Aktivitäten in ihrem Central/Pro-Konto durch E-Mail-Benachrichtigungen nachverfolgen. Zusätzlich zu den Standardereignissen können Kunden Ereignisse auswählen, über die sie benachrichtigt werden möchten, z. B. fehlgeschlagene Anmeldeversuche oder Passwortänderungen.

4.12 Authentifizierung des Gateways gegenüber dem Host

Das Gateway muss seine Identität dem Host gegenüber nachweisen, bevor ihm Zugriffscodes anvertraut werden. Wenn der Host eine Verbindung zum Gateway herstellt, überprüft er das während des TLS-„Handshakes“ übertragene Zertifikat, um sicherzugehen, dass es sich tatsächlich um einen der GoTo-Gateway-Server handelt.

4.13 Authentifizierung des Hosts gegenüber dem Gateway

Das Gateway verifiziert die Identität des Hosts mithilfe einer langen, eindeutigen Identifizierungszeichenkette. Diese Zeichenkette ist ein gemeinsamer geheimer Schlüssel der beiden Entitäten und wird bei der Installation des Hosts vom Gateway ausgegeben. Sobald der Host die eindeutige Identifizierungszeichenkette identifiziert hat, übermittelt er die Zeichenkette über einen TLS-verschlüsselten Kanal zurück an das Gateway. Abbildung 3 zeigt, wie sich der Host und das Gateway gegenseitig authentifizieren, bevor der Client Zugriff auf den Host erhält. Als weitere Sicherheitsmaßnahme kann der Host seinen gemeinsamen geheimer Schlüssel über die sichere Verbindung mit einer Anfrage des Gateways ändern.

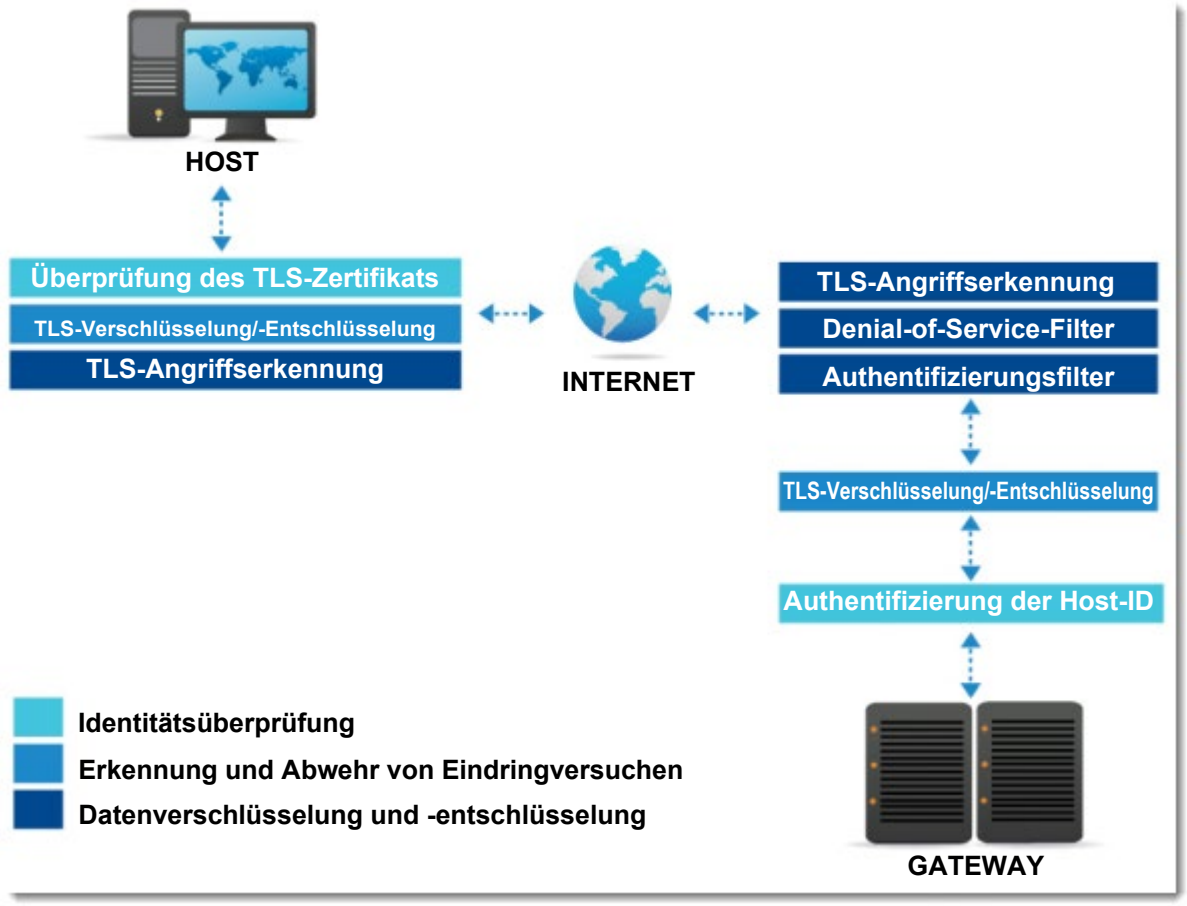

Abbildung 3: Authentifizierung von Host und Gateway

4.14 Erkennung von Eindringversuchen

Central und Pro verfügen über zwei Sicherheitsschichten zur Erkennung von Eindringversuchen: TLS und GoTo-Angriffsfilter.

4.15 TLS

Auf der ersten Schicht zur Erkennung von Eindringversuchen verwenden Central und Pro die zertifikatsbasierte Authentifizierung mit TLS 1.2 oder 1.3 (wobei 1.3 verwendet wird, wenn es unterstützt wird und nicht explizit deaktiviert ist), um sicherzustellen, dass die Daten während der Übertragung nicht verändert wurden. Dies wird durch folgende Verfahren erreicht:

Nummerierung der Datensatzsequenzen	Bei der Sequenznummerierung werden die TLS-Datensätze vom Sender nummeriert und die Reihenfolge wird vom Empfänger überprüft. Dadurch wird sichergestellt, dass ein Angreifer keine willkürlichen Datensätze in den Datenstrom einfügen bzw. daraus löschen kann.
Nachrichtenauthentifizierungscodes	An jeden TLS-Datensatz werden so genannte Nachrichtenauthentifizierungscodes (Message Authentication Codes, MACs) angehängt. Diese werden vom Sitzungsschlüssel (der nur den beiden kommunizierenden Parteien bekannt ist) und den im Datensatz enthaltenen Daten abgeleitet. Wenn die MAC-Verifizierung fehlschlägt, wird angenommen, dass die Daten während der Übertragung verändert wurden.

4.16 Central/Pro-Angriffsfilter

Die zweite Schicht wird von GoTo selbst bereitgestellt und besteht aus drei Angriffsfiltern:

4.17 IP-Adressen-Filter

Wenn Central/Pro eine Verbindungsanfrage von einem Client erhält, überprüft es zunächst seine Liste mit vertrauenswürdigen und nicht vertrauenswürdigen IP-Adressen und lehnt die Verbindung ggf. ab, wenn sie nicht vertrauenswürdig ist. Administratoren können in Central/Pro eine Liste mit IP-Adressen einrichten, die beim Verbindungsaufbau mit dem gewählten Host zugelassen (vertrauenswürdig) oder verweigert (nicht vertrauenswürdig) werden sollen (Administratoren können beispielsweise das interne Netzwerk oder die private IP-Adresse eines anderen Administrators als zulässig definieren).

4.18 Denial-of-Service-Filter

Ein Denial-of-Service-Filter („Dienstverweigerungsfilter“) lehnt Verbindungen ab, wenn die anfordernde IP-Adresse im Beobachtungszeitraum überdurchschnittlich viele Anforderungen ohne Authentifizierung gesendet hat. Damit soll eine Überlastung des Hostgeräts verhindert werden.

4.19 Authentifizierungsfilter

Wenn der Benutzer übermäßig viele fehlgeschlagene Anmeldeversuche durchgeführt hat, wird die Verbindung vom Authentifizierungsfilter abgelehnt. Der Authentifizierungsfilter soll verhindern, dass ein potenzieller Angreifer sich Zugriff auf ein Konto verschafft, indem er den Kontonamen und das dazugehörige Passwort errät.

4.20 Authentifizierung und Autorisierung der Benutzer gegenüber dem Host

Nachdem dem Benutzer von den vorherigen Schichten der Zugriff gewährt wurde, muss er seine Identität dem Host gegenüber nachweisen. Dies erfolgt über einen obligatorischen Authentifizierungsschritt auf Betriebssystemebene: Der Benutzer authentifiziert sich beim Hos mit seinem Benutzernamen und Passwort für das Gerät (z. B. Windows oder Mac). Gegebenenfalls erhält der Domänencontroller diese Anfrage, mit der die Identität des Benutzers validiert und sichergestellt wird, dass Netzwerkadministratoren steuern können, wer sich bei einem bestimmten Host anmelden kann.

4.21 Persönliches Passwort

Ein persönliches Passwort ist eine weitere optionale Sicherheitsmaßnahme, die auf dem Central/Pro-Host eingerichtet werden kann. Der Benutzer kann dem Host ein persönliches Passwort zuweisen, das – so wie das Betriebssystempasswort – vom Gateway weder gespeichert noch überprüft wird. Anders als beim Betriebssystempasswort fragt der Host nie nach dem vollständigen persönlichen Passwort. Der Benutzer muss es also in einer bestimmten Authentifizierungssitzung nie vollständig eingeben. Nachdem die Authentifizierung auf Betriebssystemebene erfolgreich war, wird der Benutzer vom Host normalerweise zur Eingabe von drei zufällig ausgewählten Zeichen des persönlichen Passworts aufgefordert (z. B. das erste, vierte und siebte Zeichen). Wenn der Benutzer die richtigen Zeichen eingibt, wird ihm der Zugriff gewährt.

4.22 GoTo und RSA SecurID

Um zusätzlich zur einfachen Authentifizierung mittels Benutzername und Passwort eine weitere Sicherheitsschicht zu implementieren, können Benutzer Central/Pro so konfigurieren, dass eine RSA SecurID-Authentifizierung erforderlich ist. Informationen zur Einrichtung dieser Funktion auf einem Central/Pro-Host finden Sie unter https://support.logmeininc.com/pro.

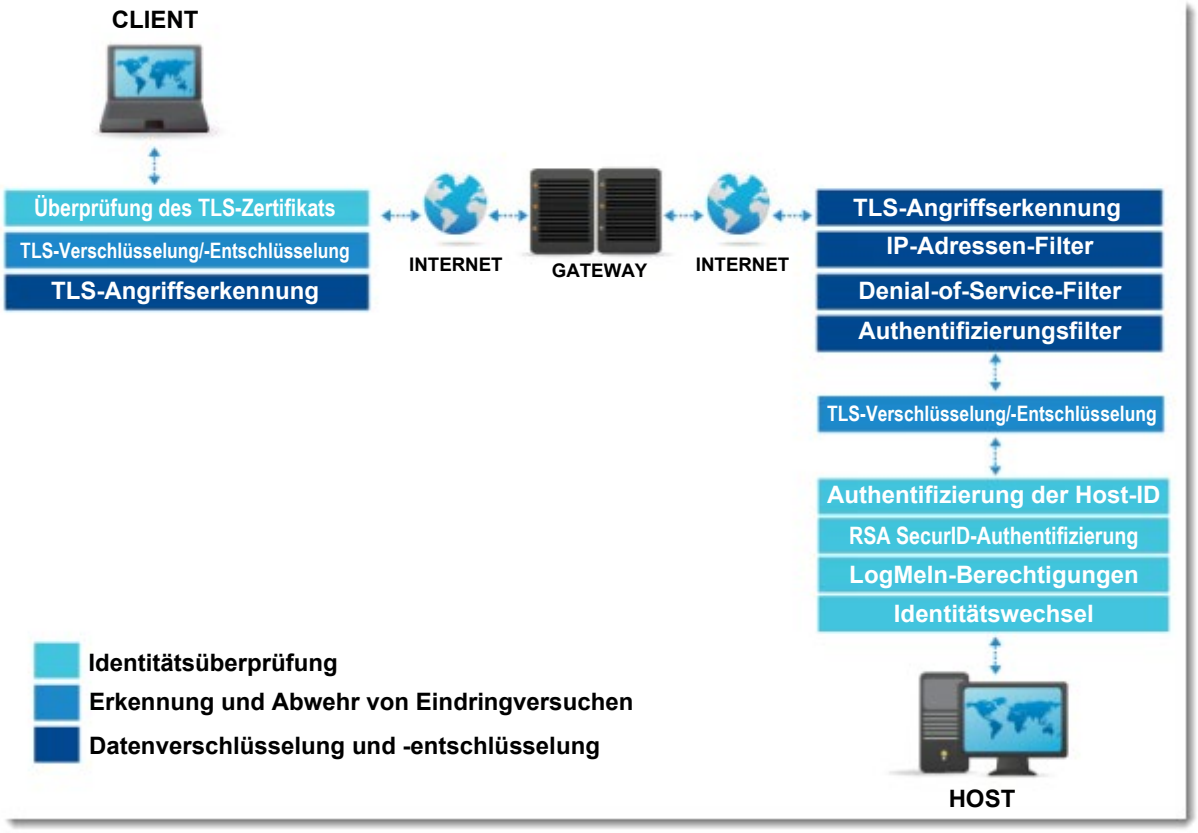

Abbildung 4: Authentifizierung zwischen den Benutzern und dem Host

4.23 Authentifizierung und Autorisierung der Benutzer innerhalb des Hosts

Nachdem Central/Pro die Identität des Benutzers mithilfe der oben beschriebenen Methoden verifiziert hat, sieht das Tool in seiner eigenen internen Benutzerdatenbank nach, auf welche internen Module der Benutzer zugreifen darf.

Systemadministratoren können Central/Pro so konfigurieren, dass Benutzer mit bestimmten Rollen nur auf eine Teilmenge der von GoTo angebotenen Tools zugreifen können. So kann z. B. der Zugriff der Helpdesk-Abteilung so konfiguriert werden, dass die Mitarbeiter lediglich die Bildschirm- und Leistungsdaten eines Geräts sehen, nicht jedoch die Kontrolle über Maus und Tastatur übernehmen oder Änderungen an der Systemkonfiguration vornehmen können. Alternativ könnte die Vertriebsabteilung vollen Remotesteuerungszugriff auf ihre jeweiligen Geräte erhalten, jedoch nicht auf Funktionen wie Leistungsüberwachung und Remoteadministration.

Mit dem Betriebssystem-Zugriffstoken, das Central/Pro bei der Authentifizierung des Benutzers erhalten hat, gibt sich die Anwendung gegenüber dem Betriebssystem als der Benutzer aus und führt in seinem Namen Aktionen durch. Dadurch wird sichergestellt, dass Central/Pro das Sicherheitsmodell des Betriebssystems befolgt und die Benutzer Zugriff auf dieselben Dateien und Netzwerkressourcen haben, als würden sie direkt vor

dem Gerät sitzen. Die den Benutzern in Windows oder OS X nicht zugänglichen Ressourcen sind auch über Central/Pro nicht verfügbar.

Weitere Informationen finden Sie unter „Steuern der Personen, die Zugriff auf Ihre Hostcomputer haben“ auf der Supportwebsite von Central oder Pro.

4.24 Überwachung und Protokollierung

Central und Pro bieten umfangreiche Protokollierungsfunktionen. Ein detailliertes Protokoll der Ereignisse in der Software wird im „data log“-Verzeichnis von Central/Pro gespeichert. Bestimmte wichtige Ereignisse wie z. B. An- und Abmeldungen werden auch im Anwendungsereignisprotokoll von Windows oder OS X gespeichert. Das detaillierte Protokoll kann auch an einen benutzerdefinierten, vom Kunden gewählten SYSLOG-Server gesendet werden.

Weitere Informationen finden Sie unter „How to View Host Event Log Files“ auf der Supportwebsite von Pro. Informationen zu SYSLOG finden Sie unter „Define Syslog Settings for the Host“ auf der Supportwebsite von Central.

4.25 Datenweiterleitung

Das Gateway sorgt für eine Ende-zu-Ende-Verschlüsselung zwischen den Endpunkten, indem zwischen dem Host und dem Client verschlüsselte Daten übermittelt werden.

Hierzu findet der erste Teil der TLS-Aushandlung zwischen dem Gateway und dem Client statt. Dann leitet das Gateway den Informationsaustausch an den Host weiter, welcher die TLS-Sitzung neu aushandelt und sich mit dem Client auf einen neuen Sitzungsschlüssel einigt. Somit ist für eine echte Ende-zu-Ende-Verschlüsselung zwischen Ausgangs- und Zielgerät gesorgt.

Wenn die Daten per Relay durch das Gateway übertragen werden, richtet der Client unter Verwendung des Gateway-Zertifikats eine TLS-Sitzung mit dem Gateway ein. Das Gateway überträgt den Status dieser TLS-Sitzung (einschließlich des Pre-Master Secret (PMS)) an den Host. Nachdem ein neuer Sitzungsschlüssel vereinbart wurde, verwendet der Host den Status dieser Sitzung, um den Rest der TLS-Sitzung direkt mit dem Client abzuwickeln. Die Sitzung ist durch das Zertifikat des Gateways geschützt; der Client kommuniziert dabei direkt mit dem Host, ohne dass das Gateway die übertragenen Daten ent- und erneut verschlüsseln muss.

4.26 UDP-NAT-Traversal

Auf der Vermittlungsschicht wird das User Datagram Protocol (UDP) gemäß Definition im ISO/OSI-Netzwerkmodell verwendet. Darauf setzt eine TCP-ähnliche (Transmission Control Protocol) Transportschicht mit Flusssteuerung, dynamischer Bandbreitenskalierung und Paketfolgenummerierung auf. Logmein.com verwendet UDP- anstelle von TCP-Paketen (und implementiert damit effektiv eine TCP-ähnliche Transportschicht). Nachdem aus den unzuverlässigen UDP-Paketen ein zuverlässiger TCP-ähnlicher Datenstrom erzeugt wurde, wird dieser über eine TLS-Schicht zusätzlich geschützt, sodass eine vollständige Verschlüsselung, Schutz der Integrität und Endpunkt-Überprüfungsmöglichkeiten gewährleistet sind.

Zur Erstellung einer UDP-NAT-Traversal-Verbindung senden sowohl der Client als auch der Host mehrere verschlüsselte UDP-Pakete an das Gateway. Diese Pakete werden mit einem geheimen Schlüssel verschlüsselt, der nur dem Gateway und dem entsprechenden Peer bekannt ist, und über die bereits bestehende TLS-Verbindung übertragen.

Das Gateway verwendet diese Pakete, um die externen (Internet-)IP-Adressen der beiden Entitäten zu bestimmen. Es versucht außerdem vorherzusagen, welcher Firewall-Port beim Senden eines neuen UDP-Pakets zur Kommunikation verwendet wird. Danach leitet das Gateway die ermittelten Informationen an die Peers weiter, welche daraufhin versuchen, eine direkte Verbindung aufzubauen. Wenn das Gateway den verwendeten Port bestimmen kann, ist der Verbindungsaufbau erfolgreich. Die Peers authentifizieren sich gegenseitig mithilfe eines weiteren gemeinsamen geheimen Schlüssels, der vom Gateway gesendet wird. Eine TLS-Sitzung wird eingerichtet. Anschließend kommunizieren die Peers direkt miteinander.

Wenn keine direkte Verbindung hergestellt werden kann, stellen die Peers wieder eine TCP-Verbindung zum Gateway her und fordern eine Sitzung mit Datenweiterleitung und Ende-zu-Ende-Verschlüsselung an. Dieser Vorgang dauert nur wenige Sekunden, ist für den Benutzer transparent, verbessert die Leistung und verringert die Latenzzeit, wenn eine direkte Verbindung verwendet wird.[1]

4.27 Software-Updates und Gateway-Sicherheit

Der Central/Pro-Host kann sich je nach den Benutzereinstellungen halbautomatisch oder automatisch auf dem Gerät des Benutzers aktualisieren. Die Hostsoftware sucht regelmäßig auf der Website logmein.com nach neuen Versionen der Software. Wenn eine neue Version gefunden wird, wird sie automatisch heruntergeladen, und dem Benutzer wird eine Meldung angezeigt, sodass dieser die Aktualisierung genehmigen kann. Der Downloadvorgang nimmt höchstens 50 % der verfügbaren Bandbreite in Anspruch und hat daher so gut wie keine Auswirkungen auf andere Netzwerkanwendungen.

Diese Software-Updates werden von logmein.com mit einem privaten Schlüssel digital signiert, der auf keinem unserer mit dem Internet verbundenen Systeme zu finden ist.

Central/Pro-Passwörter werden nicht in unserer Datenbank gespeichert: Central und Pro verwenden eine Funktion zur Ableitung kryptographischer Schlüssel, die nur in eine Richtung funktioniert, sowie eine kontospezifische Bitfolge („Salt“).

5 Aktualisierungen des Sicherheitsprogramms

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

6 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

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

[1] Für nähere Einzelheiten siehe US-Patent Nr. 7.558.862.

Kundeninhalte werden im selben Rechenzentrum in 24-Stunden- und 7-Tage-Intervallen gesichert. Zusätzlich wird alle 7 Tage ein entsprechendes Backup in einem geografisch entfernten Rechenzentrum erstellt und 4 Wochen lang aufbewahrt.

7 Rechenzentren

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

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

Rechenzentren befinden sich entweder in Deutschland, Australien, dem Vereinigten Königreich, den USA, den Niederlanden oder Irland.

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

7.1 Physische Sicherheit im Rechenzentrum

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

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

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

8 Einhaltung von Standards

GoTo prüft regelmäßig die Einhaltung der geltenden rechtlichen, finanziellen, datenschutzrechtlichen und regulatorischen Anforderungen. Die Datenschutz- und Sicherheitsprogramme von GoTo haben verschiedene Zertifizierungen erhalten und wurden nach externen Audit-Standards bewertet, darunter:

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

9 Anwendungssicherheit

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

10 Protokollierung, Überwachung und Warnmeldungen

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

11 Endpoint Detection and Response (EDR)

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

12 Bedrohungsmanagement

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

13 Sicherheits- und Schwachstellenscans sowie Patch-Management

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

14 Logische Zugriffskontrolle

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

15 Datentrennung

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

16 Perimeterabwehr und Erkennung von Eindringversuchen

Die On-Premise-Netzwerkarchitektur von GoTo ist in drei Netzwerkzonen unterteilt: öffentlich, privat und Integrated Lights-Out (iLO)-Management. Die öffentliche Zone enthält Server mit Internetzugriff, und der gesamte eingehende Datenverkehr dieses Netzwerks muss eine Firewall passieren. Nur der erforderliche Netzwerkverkehr wird zugelassen, jeglicher andere Netzwerkverkehr wird abgelehnt. Von der öffentlichen Zone aus ist kein Netzwerkzugriff auf die private oder die iLO-Management-Netzwerkzone zulässig.

In der privaten Netzwerkzone werden Administrations- und Überwachungssysteme auf Anwendungsebene gehostet, während die iLO-Management-Netzwerkzone für die Administration und Überwachung von Hardware und Netzwerk zuständig ist. Der Zugriff auf diese Netzwerke wird durch Zwei-Faktor-Authentifizierung auf autorisierte Mitarbeiter beschränkt.

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

- Systeme zur Erkennung von Eindringversuchen, die Systeme, Dienste, Netzwerke und Anwendungen auf unbefugten Zugriff überwachen
- Überwachung kritischer System- und Konfigurationsdateien
- Web Application Firewall (WAF) und DDoS-Präventionsdienste auf der Anwendungsschicht, die als Proxy für den GoTo-Datenverkehr fungieren
- Eine lokale Anwendungs-Firewall, die als zusätzlicher Schutz vor den OWASP Top Ten und anderen Schwachstellen in Webanwendungen sowie vor bösartigem Datenverkehr dient
- Host-basierte Firewalls, die eingehende und ausgehende Verbindungen filtern, darunter auch interne Verbindungen zwischen GoTo-Systemen

17 Sicherheitsmaßnamen und Incident-Management

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

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

18 Löschung und Rückgabe von Inhalten

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

Zeitplan für die Aufbewahrung von Kundeninhalten: Sofern das geltende Recht nichts anderes vorschreibt, werden Kundeninhalte neunzig (90) Tage nach Kündigung, Stornierung oder Ablauf und – in jedem Fall – nach Aufhebung des letzten Abonnements des Kunden automatisch gelöscht. Auf schriftliche Anfrage kann GoTo die Löschung von Inhalten schriftlich bestätigen/bescheinigen.

19 Organisatorische Kontrollen

19.1 Sicherheitsrichtlinien und -verfahren

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

19.2 Änderungsmanagement

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

19.3 Programme für Sicherheitssensibilisierung und -schulung

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

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

20 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten unserer Kunden, Benutzer und anderer Personen, die GoTo-Dienste nutzen („Endbenutzer“) sehr ernst und verpflichtet sich, relevante Praktiken zur Datenverarbeitung und -verwaltung offen und transparent darzulegen.

20.1 Datenschutzprogramm

GoTo unterhält ein umfassendes Datenschutzprogramm, für das Koordination mehrerer Funktionen innerhalb des Unternehmens erforderlich ist, darunter Datenschutz, Sicherheit, Governance, Risiko und Compliance (GRC), Recht, Produkt, Technik und Marketing. Dieses Datenschutzprogramm konzentriert sich auf die Einhaltung von Vorschriften und umfasst die Implementierung und Pflege interner und externer Richtlinien, Standards und Ergänzungen zur Regelung der Praktiken des Unternehmens.

20.2 Einhaltung behördlicher Vorschriften

20.2.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) bzgl. des Schutzes der Daten und der Privatsphäre aller Personen in der EU. GoTo unterhält ein umfassendes Programm zur Sicherstellung der DSGVO-Compliance. Soweit GoTo im Auftrag des Kunden personenbezogene Daten

verarbeitet, die der DSGVO unterliegen, werden wir dies in Übereinstimmung mit den geltenden Anforderungen der DSGVO tun. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

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

20.2.3 LGPD

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

20.3 Datenverarbeitungsnachtrag

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

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

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

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

(a) überarbeitete Definitionen, die dem CCPA zugeordnet sind
(b) Zugriffs- und Löschrechte
(c) Garantien, dass GoTo die persönlichen Informationen unserer Kunden, Benutzer und Endbenutzer nicht verkauft

Unser globaler DVN enthält außerdem Bestimmungen zu folgenden Punkten:

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

20.4 Abkommen zur Datenübertragung

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

20.4.1 Standardvertragsklauseln

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

20.4.2 Zertifizierung nach APEC CBPR und PRP

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

20.5 Ergänzende Maßnahmen

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

20.6 Datenanfragen

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

20.7 Offenlegungen der Unterauftragsverarbeiter und Rechenzentren

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

20.8 Einschränkungen bei der Verarbeitung sensibler Daten

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

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

20.9 Compliance in regulierten Umgebungen

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

21 Kontrollen der Sicherheits- und Datenschutzpraktiken von Drittanbietern

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

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

Sicherheitsmaßnahmen mit geeigneten Kontrollen und Systemanforderungen mit den betreffenden Anbietern vereinbart.

22 Kontaktaufnahme mit GoTo

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