Technische en organisatorische maatregelen (TOM's)
Central en Pro

Samenvatting

Dit document met Technische en Organisatorische Maatregelen ('TOM's') beschrijft GoTo's privacy-, beveiligings- en verantwoordingsverplichtingen voor Central en Pro. Specifiek heeft GoTo robuuste wereldwijde privacy- en beveiligingsprogramma's en organisatorische, administratieve en technische beveiligingen die ontworpen zijn om: (i) de vertrouwelijkheid, integriteit en beschikbaarheid van de Klantcontent te waarborgen; (ii) bescherming te bieden tegen bedreigingen en gevaren voor de veiligheid van de Klantcontent; (iii) bescherming te bieden tegen verlies, misbruik, ongeautoriseerde toegang, openbaarmaking, wijziging en vernietiging van Klantcontent; en (iv) naleving van de toepasselijke wet- en regelgeving te handhaven, waaronder wetgeving inzake gegevensbescherming en privacy. Dergelijke maatregelen omvatten:

- **Versleuteling:**
  - *Tijdens de overdracht:* Transport Layer Security (TLS) v1.2 of v1.3, indien ondersteund.
  - *Tijdens de opslag:* Transparent Data Encryption (TDE) en Advanced Encryption Standard (AES) 256-bits voor Klantcontent.
- **Datacenters:** Datacenterlocaties in Duitsland, Australië, het Verenigd Koninkrijk, de Verenigde Staten, Nederland en Ierland ter ondersteuning van redundantie en stabiliteit.
- **Fysieke beveiliging:** Er zijn besturingselementen voor fysieke beveiliging en omgevingen beschikbaar, die zijn ontworpen om fysieke toegang te beschermen, te controleren en te beperken voor systemen en servers die Klantcontent onderhouden, om te kunnen voldoen aan uptime-, prestatie- en schaalbaarheidsverplichtingen.
- **Nalevingsaudits:** Central en Pro beschikken over SOC 2 Type II, BSI C5, PCI DSS, PCAOB, TRUSTe-certificaat inzake privacy van ondernemingen en APEC- CBPR- en PRP-certificeringen.
- **Naleving van wet- en regelgeving:** GoTo heeft een uitgebreid gegevensbeschermingsprogramma met processen en beleidsregels die ervoor zorgen dat de Klantcontent wordt behandeld in overeenstemming met de toepasselijke privacywetgeving, waaronder de AVG, CCPA/CPRA en LGPD.
- **Beveiligingsbeoordelingen**: Naast interne tests sluit GoTo contracten af met externe bedrijven om regelmatig beveiligingsbeoordelingen en/of penetratietests uit te voeren.
- **Logische besturingselementen voor toegang:** Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken.
- **Scheiding van gegevens**: GoTo maakt gebruik van een architectuur met meerdere tenants en scheidt klantaccounts logisch op databaseniveau.
- **Perimeterbescherming en inbraakdetectie**: Er zijn tools, technieken en diensten voor perimeterbescherming beschikbaar, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie.
- **Bewaring van gegevens:**
  - Klanten van Central en Pro kunnen te allen tijde verzoeken om retournering of verwijdering van Klantcontent, waaraan binnen dertig (30) dagen na het verzoek van de klant zal worden voldaan.
  - Klantcontent wordt negentig (90) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant automatisch verwijderd.

Inhoudsopgave

Klik op de paginanummers hieronder om naar het relevante TOM-gedeelte te gaan

1 Productintroductie

Central is een webgebaseerde beheerconsole waarmee IT-professionals externe apparaten kunnen inspecteren, monitoren en beheren, software-updates en patches kunnen toepassen, IT-taken kunnen automatiseren en honderden verschillende versies van antivirussoftware kunnen uitvoeren. Central wordt aangeboden als een premium service met meerdere prijsniveaus op basis van het aantal ondersteunde apparaten en de gewenste functies.

Pro is een dienst voor toegang op afstand die veilige externe toegang biedt tot een computer, of een ander apparaat met internetverbinding, vanaf elk ander online apparaat, evenals de meeste smartphones en tablets. Zodra een Pro-host op een apparaat is geïnstalleerd, is de service zo ontworpen dat een persoon met een subaccount binnen een klantenaccount (de 'Gebruiker') op afstand toegang heeft tot het bureaublad, de bestanden, de toepassingen en de netwerkbronnen van dat apparaat, vanaf de andere apparaten van de Gebruiker met internetverbinding. Pro kan snel worden geïmplementeerd en geïnstalleerd zonder dat enige IT-expertise nodig is.

Central en Pro zijn ontworpen om via een niet-vertrouwd netwerk veilige toegang op afstand mogelijk te maken tot belangrijke bronnen. Beveiliging is een van de belangrijkste overwegingen tijdens de ontwikkeling van deze producten.

Termen in dit document die met een hoofdletter beginnen maar niet in de tekst worden gedefinieerd, worden gedefinieerd in de Servicevoorwaarden.

2 Technische maatregelen

De producten van GoTo zijn ontworpen om oplossingen te bieden die veilig, betrouwbaar en privé zijn. De hieronder gedefinieerde technische maatregelen beschrijven hoe GoTo dat ontwerp implementeert en in de praktijk toepast voor Central en Pro.

2.1 Beveiligingsmechanismen

GoTo's implementatie van beveiligingen, functies en praktijken omvat:

I. Ontwikkeling van producten waarbij beveiliging en privacy de basis vormen van het ontwerp, en waarbij extra beveiligingslagen worden opgenomen om Klantcontent te beschermen;

II. Inrichting van organisatorische besturingselementen voor de vorming van intern beleid en afstemming van interne procedures op naleving van standaarden, incidentbeheer, applicatiebeveiliging, personeelsbeveiliging en regelmatige trainingsprogramma's; en

III. Ervoor zorgen dat er privacyprocedures zijn geïmplementeerd voor gegevensverwerking en -beheer, in overeenstemming met de toepasselijke wetgeving, zoals met de AVG, CCPA/CPRA, LGPD en ons eigen Addendum gegevensverwerking ('DPA'; Data Processing Addendum) en de toepasselijke beleidsregels en verplichtingen van GoTo.

We ontwikkelen producten met beveiligingsmechanismen aan de basis, om Klantcontent van GoTo optimaal tegen bedreigingen te beschermen en ervoor te zorgen dat de voor beveiliging ingerichte besturingselementen ook echt geschikt zijn voor de aard en reikwijdte van de services. Met de configureerbare beveiligingsfuncties van GoTo kunnen beheerders bedreigingen en risico's voor systemen en netwerken, veroorzaakt door gebruikers van GoTo-services, minimaliseren.

3 Productarchitectuur

Central en Pro zijn SaaS-gebaseerde applicaties met een meerlaagse architectuur die gehost wordt in geografisch verspreide datacenters. Beveiligingsmaatregelen op alle niveaus, van de fysieke laag tot de applicatielaag, zijn ontworpen om de meest grondige en optimale bescherming te bieden.

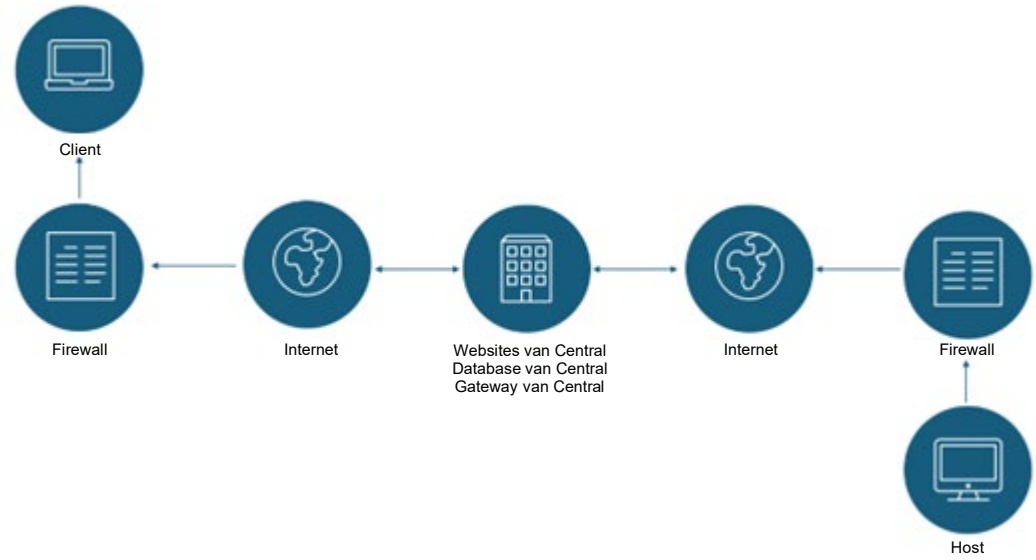
De toepassingen Central en Pro bestaan uit drie hoofdonderdelen die sessies met toegang op afstand mogelijk maken:

- **Client:** de software (zoals de browser, native app, mobiele app) die toegang heeft tot een externe bron;
- **Host of server:** het apparaat waartoe toegang wordt verkregen, of de hostsoftware van het product op dit apparaat; en
- **Central/Pro-gateway:** de service die het verkeer tussen de client en de host verzorgt en beheert.

De Central/Pro-host is ontworpen om een constante met TLS (Transport Layer Security) beveiligde verbinding te onderhouden, met een gatewayserver in een van de GoTo-datacenters. Nadat er een beveiligde verbinding met Central of Pro tot stand is gebracht, wordt de client door de host geverifieerd en geautoriseerd voor toegang tot het apparaat, en kan de sessie op afstand van start gaan. De gatewayserver regelt het versleutelde verkeer tussen de twee entiteiten, maar vereist niet dat de host de client impliciet vertrouwt. Via de Central/Pro-gateway kunnen zowel de client als de host (of beide) een firewall krijgen, zodat Gebruikers zelf geen firewalls hoeven te configureren.

GoTo's eigen protocol voor het doorsturen van sleuteluitwisselingen is ontworpen om de service te beveiligingen tegen het onderscheppen of afluisteren van onze eigen infrastructuur. Specifiek wordt de verbinding tussen de client en de host beheerst door de gateway om ervoor te zorgen dat de client onafhankelijk van de netwerkinstellingen verbinding kan maken met de host.

Als de host al een TLS-verbinding met de gateway tot stand heeft gebracht, stuurt de gateway de TLS-sleuteluitwisseling van de client door naar de host via een verzoek om opnieuw te onderhandelen over de eigen sleutel. De client en de host kunnen zo TLS-sleutels uitwisselen zonder dat de gateway de sleutel te weten komt.



Afbeelding 1: Centrale architectuur

4 Technische beveiligingsmaatregelen

GoTo maakt gebruik van technische besturingselementen voor beveiliging die zijn ontworpen om de infrastructuur van de service en de gegevens daarin te beschermen.

4.1 Versleuteling

GoTo herziet regelmatig zijn standaarden op het gebied van versleuteling, en kan de gebruikte blokvercijferingen en/of technologieën bijwerken in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden, om best practices en versleutelingmethoden voortdurend te verbeteren.

Central- en Pro-services ondersteunen de volgende versleutelingprotocollen (indien van toepassing): TLS 1.2, 2048-bits RSA- en AES256-blokvercijferingen met een 384-bits SHA-2-algoritme.

Central en Pro ondersteunen zowel 128- als 256-bits AES-sleutels, waarbij de client en de server bepalen wat de sterkste compatibele en beschikbare vercijfering van deze twee sleutellengtes is. De client stuurt de server een lijst met vercijferingen die hij wil gebruiken en de server kiest de vercijfering die zijn voorkeur heeft. In Central en Pro selecteert de server de sterkste gedeelde blokvercijfering die de client heeft aangeboden.

4.2 Versleuteling tijdens de overdracht

Al het netwerkverkeer dat de datacenters van Central en Pro in en uit gaat, inclusief Klantcontent, wordt tijdens de overdracht versleuteld met TLS 1.2 of, indien ondersteund, TLS 1.3.

4.3 Versleuteling tijdens de opslag

Alle Klantcontent van Central/Pro wordt bewaard in MSSQL met Transparent Data Encryption (TDE) en tijdens de opslag versleuteld met AES-256.

4.4 Verificatie van gebruikers

Central/Pro gebruikt een eigen algemene aanmeldservice ('CLS'; Common Login Service) voor de verificatie van Gebruikers. De CLS maakt gebruik van eigen aangepaste methodes om verdachte Gebruikerstoegang te voorkomen. Voor accounts met een gekoppeld CIP-account van GoTo (Common Identity Platform) is het aanmeldingsproces nog beter beveiligd, met een risicobeoordelingsservice van een derde partij.

4.5 Meervoudige verificatie

Meervoudige verificatie (ook wel tweeledige of tweestapsverificatie genoemd) voegt een tweede beschermingslaag toe aan een account door twee verschillende vormen van identificatie te vereisen voor aanmelding. Na het instellen van meervoudige verificatie voeren Gebruikers hun aanmeldingsgegevens in, en worden vervolgens gevraagd om hun identiteit te verifiëren aan de hand van een beveiligingscode.

Central-abonnees kunnen een beleidsregel voor aanmelding afdwingen, waarbij alle Gebruikers verplicht worden om meervoudige verificatie te gebruiken om zich aan te melden. Ga voor stapsgewijze instructies naar support.logmeininc.com/central.

4.6 Beveiligingscodes op afdruk

Klanten kunnen ervoor kiezen om gedrukte beveiligingscodes te gebruiken als extra beschermingslaag. Als de Gebruiker deze functie inschakelt, moet hij een lijst met willekeurige wachtwoorden van negen tekens afdrukken die door de gateway zijn gegenereerd. Telkens wanneer de Gebruiker zich aanmeldt bij zijn account op logmein.com, wordt hij gevraagd een van de beveiligingscodes uit de lijst in te voeren om toegang tot zijn account te krijgen. Elke code kan slechts één keer worden gebruikt. Voordat de afgedrukte beveiligingscodes op zijn, moet de Gebruiker nog een vel afdrukken. Beveiligingscodes van de vorige lijst die nog niet zijn gebruikt, worden hiermee ongeldig.

4.7 Beveiligingscodes verzonden via e-mail

Wanneer deze functie is ingeschakeld en de Gebruiker zijn e-mailadres en wachtwoord verifieert bij de Central-gateway, wordt er een toegangscode gegenereerd die naar het e-mailadres wordt verzonden. De Gebruiker ontvangt deze toegangscode in een e-mail en voert de code in in het formulier van de gateway. De toegangscode verloopt direct bij gebruik ervan, of binnen enkele minuten na het aanmaken, afhankelijk van wat zich het eerste voordoet.

4.8 Verificatie van de gateway bij de client

Central en Pro maken gebruik van verificatie conform het TLS 1.2- of TLS 1.3- certificaat (waarbij 1.3 wordt gebruikt wanneer ondersteund en mits niet expliciet uitgeschakeld) om serveridentiteiten te verifiëren en ervoor te zorgen dat wanneer een Gebruiker via een gateway verbinding maakt met een Central- of Pro-server, er verbinding wordt gemaakt met het bedoelde apparaat. Wanneer een verbinding tot stand wordt gebracht, wordt het certificaat van de server gecontroleerd. Er wordt een waarschuwing weergegeven als het certificaat is uitgegeven door een niet-vertrouwde autoriteit. Als de hostnaam in de URL niet overeenkomt met de hostnaam in het certificaat, zelfs als dit certificaat door een vertrouwde autoriteit is uitgegeven, wordt een andere waarschuwing weergegeven.

Als de server door deze controles heen komt, genereert de client van de Gebruiker een 'pre-master secret' (PMS), codeert dit met de openbare serversleutel uit het certificaat, en verzendt het naar de server. Er wordt gebruikgemaakt van versleuteling met openbare sleutels, zodat alleen de server die de bijbehorende persoonlijke sleutel heeft, de PMS kan ontsleutelen. Het 'pre-master secret' wordt vervolgens door zowel de Gebruiker als de server gebruikt om het 'master secret' af te leiden, dat vervolgens wordt gebruikt om initialisatievectoren en sessiesleutels voor de duur van de beveiligde sessie af te leiden.

4.9 One2Many – Verificatie en versleuteling (alleen Central)

De functie One2Many biedt geavanceerde script- en implementatiemogelijkheden waarmee Gebruikers van Central massafuncties kunnen uitvoeren in beheerde organisaties. Met deze tool kunnen Gebruikers administratieve taken op meerdere Windows- en Macapparaten uitvoeren, beheren en monitoren, rechtstreeks vanuit Central.

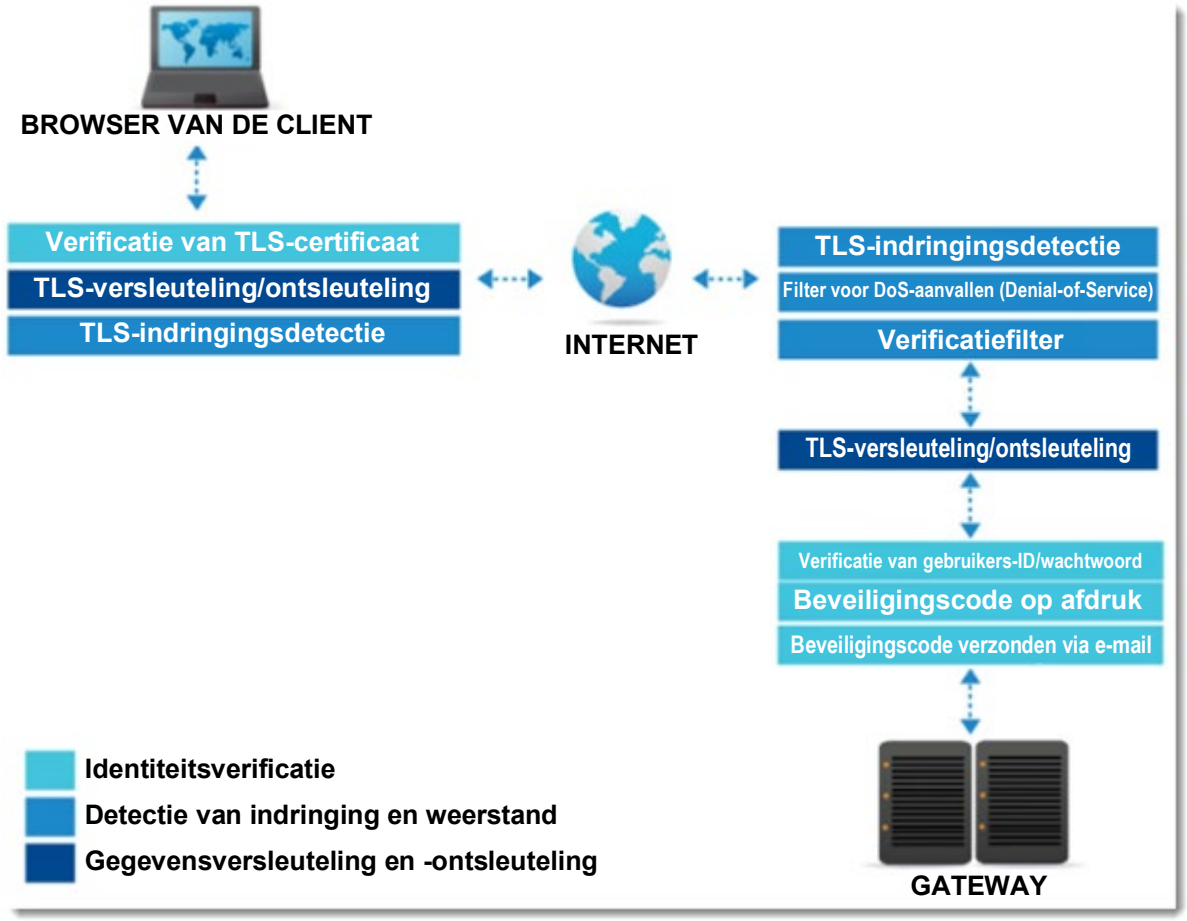
Voor One2Many is meervoudige verificatie vereist. One2Many slaat aanmeldingsgegevens voor meervoudige verificatie op twee verschillende manieren op: wanneer een taak in realtime wordt uitgevoerd, worden de gegevens in de browser opgeslagen; wanneer de taak gepland staat om later uitgevoerd te worden, worden de gegevens in de database van het product opgeslagen.

Aanmeldingsgegevens die in One2Many worden gebruikt, worden eerst versleuteld met de openbare sleutel van de host en vervolgens verder versleuteld door de website. De eerste versleutelingslaag zorgt ervoor dat alleen de host de persoonlijke sleutel kan ontsleutelen; de tweede versleutelingslaag maakt het mogelijk om gegevens van de website te wissen, zelfs als de host offline is.

4.10 Verificatie van Gebruikers bij de gateway

Gebruikers moeten door zowel de gateway als de host worden geverifieerd. Het e-mailadres en wachtwoord van een Gebruiker worden geverifieerd wanneer deze zich aanmeldt bij Central/Pro.

OPMERKING: Gebruikers van Central kunnen met een beleidsregel vereisen dat een sterk wachtwoord wordt gebruikt bij aanmelding. Raadpleeg support.logmeininc.com/central voor meer informatie.



Afbeelding 2: Verificatie tussen Gebruikers en de gateway

4.11 Accountcontrole

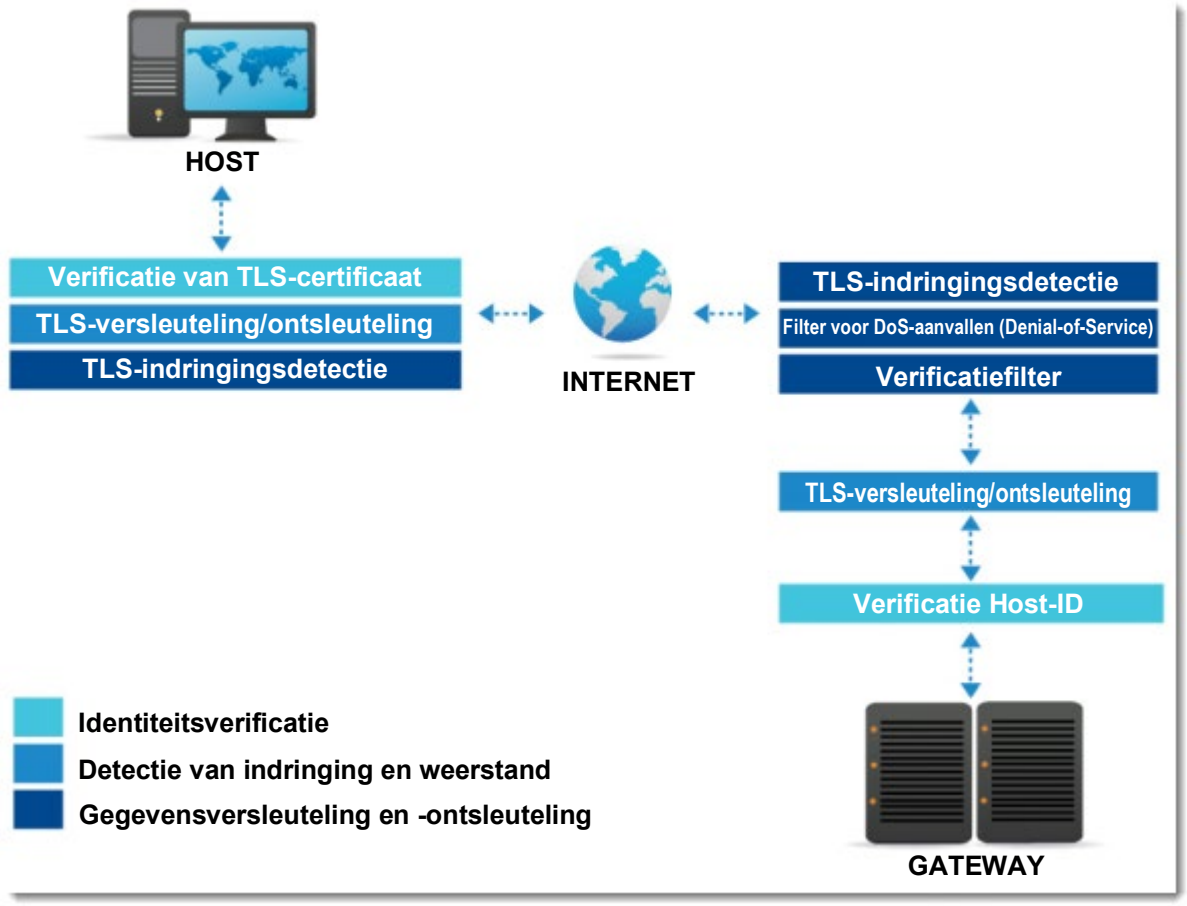
Klanten kunnen de activiteiten in hun Central/Pro-account volgen via e-mailmeldingen. Naast de standaardgebeurtenissen kunnen klanten gebeurtenissen selecteren waarover zij een melding willen ontvangen, zoals mislukte aanmeldpogingen of wijzigingen van wachtwoorden.

4.12 Verificatie van de gateway bij de host

De gateway moet zijn identiteit bewijzen aan de host voordat de toegangscodes eraan kunnen worden toevertrouwd. Wanneer de host verbinding maakt met de gateway, controleert hij het overgedragen certificaat tijdens de 'TLS-handdruk' om er zeker van te zijn dat hij verbinding maakt met een van de GoTo-gatewayservers.

4.13 Verificatie van de host bij de gateway

De gateway verifieert de identiteit van de host aan de hand van een lange unieke identificatiecode. Deze tekenreeks vormt een gedeeld geheim tussen de twee entiteiten en wordt uitgegeven door de gateway wanneer de host geïnstalleerd wordt. Zodra de host de unieke identificatiecode identificeert, communiceert hij de tekenreeks terug naar de gateway via een TLS-beveiligd kanaal. Afbeelding 3 toont hoe de host en de gateway elkaar verifiëren voordat de client toegang kan krijgen tot de host. Voor extra beveiliging kan de host zijn gedeeld geheim wijzigen, met een verzoek van de gateway via de beveiligde verbinding.



Afbeelding 3: Verificatie van host en gateway

4.14 Detectie van indringing

Central en Pro hebben twee beveiligingslagen die ontworpen zijn om indringingspogingen te detecteren: TLS- en GoTo-indringingsfilters.

4.15 TLS

Voor de eerste laag van indringingsdetectie gebruikt Central/Pro verificatie conform de TLS 1.2- of 1.3-certificaten (waarbij 1.3 wordt gebruikt wanneer ondersteund en mits niet expliciet uitgeschakeld) om te kunnen garanderen dat de gegevens tijdens de overdracht niet zijn gewijzigd. Hiervoor worden de volgende technieken gehanteerd:

Record Sequence Numbering (record-volgnummers)	De afzender wijst record-volgnummers toe aan de TLS-records en de volgorde wordt gecontroleerd door de ontvanger. Dit betekent dat een aanvaller geen willekeurige records in de gegevensstroom kan verwijderen of invoegen.
Message Authentication Codes (bericht-verificatie-codes)	Aan elke TLS-record worden Message Authentication Codes (MACs) toegevoegd. Deze code wordt afgeleid van de sessiesleutel (die alleen bekend is bij de twee communicerende partijen) en de gegevens in de record. Als de MAC-verificatie mislukt, wordt aangenomen dat de gegevens tijdens de verzending zijn gewijzigd.

4.16 Indringingsfilters van Central/Pro

De tweede laag wordt geleverd door GoTo zelf en bestaat uit drie indringingsfilters:

4.17 IP-adresfilter

Wanneer Central/Pro een verbindingsverzoek van een client ontvangt, wordt eerst de lijst met vertrouwde en niet-vertrouwde IP-adressen gecontroleerd, en kan de verbinding worden geweigerd als deze niet-vertrouwd is. Een beheerder kan binnen Central/Pro een lijst met IP-adressen instellen op basis waarvan een verbinding met de geselecteerde host wordt toegestaan (vertrouwd) of geweigerd (niet-vertrouwd) (een beheerder kan bijvoorbeeld het interne netwerk van het bedrijf en het IP-adres van de thuisbasis van een andere beheerder als 'toegestaan' aanwijzen).

4.18 Filter voor DoS-aanvallen (Denial-of-Service)

Met het filter voor DoS-aanvallen worden verbindingen geweigerd als het IP-adres waarvan het verzoek afkomstig is, een groot aantal verzoeken zonder verificatie heeft ingediend binnen het tijdsbestek van de observatie, om het hostapparaat te beschermen tegen overbelasting.

4.19 Verificatiefilter

Als de Gebruiker een te groot aantal mislukte aanmeldingspogingen heeft gedaan, wordt de verbinding geweigerd met het Verificatiefilter. Het Verificatiefilter is ontworpen om te voorkomen dat een potentiële indringer toegang krijgt tot een account door de accountnaam en het wachtwoord te raden.

4.20 Verificatie en autorisatie van Gebruikers bij de host

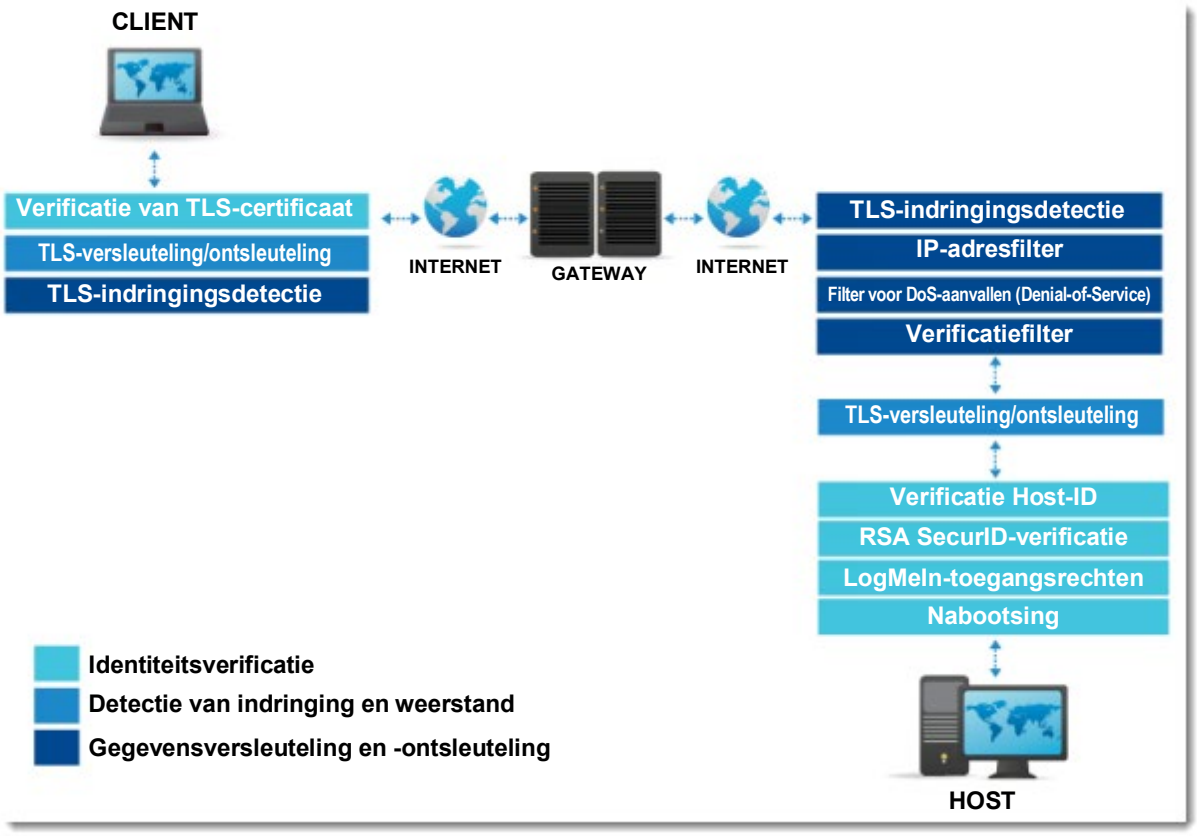
Nadat toegang is verleend door de vorige lagen, moet de Gebruiker zijn identiteit aan de host bewijzen. Dat doet hij via een verplichte verificatiestap op niveau van het besturingssysteem: de Gebruiker wordt bij de host geverifieerd met de gebruikersnaam en het wachtwoord van het apparaat (bijv. Windows of Mac). Waar relevant zal de domeincontroller dit verzoek ontvangen, waarmee de identiteit van de Gebruiker wordt gevalideerd, en netwerkbeheerders kunnen bepalen wie zich bij een specifieke host kan aanmelden.

4.21 Persoonlijk wachtwoord

Een persoonlijk wachtwoord is een andere optionele beveiligingsmaatregel die op de Central/Pro-host kan worden ingesteld. De Gebruiker kan een persoonlijk wachtwoord toewijzen aan de host dat, net als het wachtwoord op niveau van het besturingssysteem, niet door de gateway wordt opgeslagen of geverifieerd. Anders dan bij het wachtwoord voor het besturingssysteem, vraagt de host nooit om het volledige persoonlijke wachtwoord, dus de Gebruiker voert het nooit in zijn geheel in tijdens een verificatiesessie. De Gebruiker wordt gewoonlijk gevraagd om drie willekeurige tekens van het persoonlijke wachtwoord (bijvoorbeeld het eerste, het vierde en het zevende) te verstrekken aan de host nadat de verificatie op niveau van het besturingssysteem is gelukt. Als de Gebruiker de juiste tekens invoert, wordt hem toegang verleend.

4.22 GoTo en RSA SecurID

Als extra beveiligingslaag naast verificatie op basis van gebruikersnaam en wachtwoord, kunnen Gebruikers Central/Pro zo configureren dat verificatie met RSA SecurID verplicht wordt gesteld. Ga voor informatie over het instellen van deze functie op een Central/Pro-host naar https://support.logmeininc.com/pro.



Afbeelding 4: verificatie tussen Gebruikers en de host

4.23 Verificatie en autorisatie van Gebruikers binnen de host

Nadat Central/Pro de identiteit van de Gebruiker heeft vastgesteld met de bovenstaande methoden, bepaalt de eigen interne Gebruikersdatabase tot welke interne modules de Gebruiker toegang heeft.

Systeembeheerders kunnen Central/Pro zo configureren dat gebruikers met bepaalde rollen alleen toegang hebben tot een subset van de hulpprogramma's die GoTo biedt. De configuratie voor de Helpdesk-afdeling kan bijvoorbeeld zo zijn ingesteld dat het scherm van het apparaat en gegevens over de werking worden weergegeven, maar dat de muis en het toetsenbord niet kunnen worden bediend, en er geen wijzigingen kunnen worden aangebracht in de systeemconfiguratie. Een andere mogelijkheid is dat de verkoopafdeling volledige toegang op afstand krijgt tot hun respectieve apparaten, maar niet tot functies zoals prestatiecontrole en beheer op afstand.

Met het toegangstoken voor het besturingssysteem dat is verkregen toen de gebruiker werd geverifieerd, doet Central/Pro zich als de gebruiker voor bij het besturingssysteem voor het uitvoeren van acties uit naam van de gebruiker. Hiermee wordt gegarandeerd dat Central/Pro het beveiligingsmodel van het besturingssysteem volgt, en dat gebruikers toegang hebben tot dezelfde bestanden en netwerkbronnen als wanneer ze zelf achter hun apparaat zouden zitten. Bronnen die niet beschikbaar zijn voor Gebruikers in Windows of OS X zijn ook via Central/Pro niet beschikbaar.

Raadpleeg 'De toegang tot uw host-computers besturen' op de supportwebsite van Central of Pro voor meer informatie.

4.24 Controle en logbestanden

Central en Pro bieden uitgebreide voorzieningen voor logbestanden. In de Central/Pro-directory wordt een zeer gedetailleerd logbestand bijgehouden van de gebeurtenissen in de software. Bepaalde gebeurtenissen worden ook in het gebeurtenissenlogbestand van Windows of OS X opgenomen, zoals registraties van aan- en afmeldingen. Het gedetailleerde logbestand kan ook naar een aangepaste SYSLOG-server naar keuze van de Klant worden gestuurd.

Raadpleeg 'Logbestanden van hostgebeurtenissen weergeven' op de supportwebsite van Pro voor meer informatie. Voor SYSLOG, zie 'Syslog-instellingen voor de host definiëren' op de supportwebsite van Central.

4.25 Gegevens doorsturen

De gateway biedt volledige end-to-endversleuteling door gecodeerde gegevens door te sturen tussen de host en de client.

Daartoe wordt het eerste deel van de TLS-onderhandeling uitgevoerd tussen de gateway en de client. De gateway geeft vervolgens de uitwisseling door aan de host die opnieuw onderhandelt over de TLS-sessie en akkoord gaat met een nieuwe sessiesleutel voor de client, waardoor volledige end-to-endversleuteling tot stand komt.

Als het verkeer door de gateway wordt gevoerd, zet de client een TLS-sessie op met de gateway met behulp van het certificaat van de gateway. De gateway brengt de status van de TLS-sessie (inclusief het 'pre-master secret') over naar de host. Na toestemming voor een nieuwe sessiesleutel verkregen te hebben, gebruikt de host de status van de sessie om de rest van de TLS-sessie direct met de client te behandelen. De sessie is beveiligd door het certificaat van de gateway, waardoor de client direct communiceert met de host – zonder dat de gateway verkeer moet versleutelen en ontsleutelen.

4.26 UDP NAT Traversal

UDP (User datagram protocol) wordt geregeld via de netwerklaag, zoals wordt gedefinieerd door het ISO/OSI-netwerkmodel. Hier bovenop wordt een TCP-achtige transportlaag geplaatst (transmission control protocol), compleet met stroombesturing, dynamische aanpassing van de bandbreedte en pakketvolgnummers. GoTo.com gebruikt UDP-pakketten in plaats van TCP-pakketten (en implementeert daarmee in feite een TCP-achtige transportlaag). Nadat een betrouwbare TCP-achtige stroom is opgezet op basis van onbetrouwbare UDP-pakketten, wordt de stroom verder beveiligd met een TLS-laag, die functies biedt voor volledige versleuteling, integriteitsbeveiliging en eindpuntverificatie.

Voor het instellen van een UDP NAT Traversal-verbinding sturen zowel de client als de host diverse gecodeerde UDP-pakketten naar de gateway. Deze pakketten worden gecodeerd met een geheime sleutel die wordt gedeeld door de gateway en de desbetreffende peer, waarbij de communicatie verloopt via een reeds bestaande TLS-verbinding.

De gateway gebruikt deze pakketten om de externe IP-adressen van de twee entiteiten te bepalen. De gateway probeert ook te voorspellen welke firewallpoort wordt gebruikt voor communicatie wanneer een nieuw UDP-pakket wordt verzonden. De bevindingen worden doorgegeven aan de peers die vervolgens een rechtstreekse verbinding proberen in te stellen. Als de gateway erin geslaagd is om de gebruikte poort vast te stellen, wordt de verbinding tot stand gebracht. De peers verifiëren elkaar met een aanvullend gedeeld geheim dat van de gateway afkomstig is. Er wordt een TLS-sessie tot stand gebracht. Nu kunnen de peers rechtstreeks met elkaar communiceren.

Als er geen directe verbinding kan worden ingesteld, gaan de peers terug naar de gateway via TCP en dienen ze een verzoek in voor een doorgestuurde, volledig versleutelde sessie. Dit proces duurt slechts enkele seconden, is zeer transparant voor de Gebruiker, verbetert de prestaties, en vermindert de latentie wanneer er een directe verbinding wordt gebruikt.[1]

4.27 Software-updates en gatewaybeveiliging

De Central/Pro-host kan, afhankelijk van de voorkeuren van de Gebruiker, zichzelf semi-automatisch of automatisch bijwerken op het apparaat van de gebruiker. De host-software controleert regelmatig op de website logmein.com of er nieuwere versies van de software bestaan. Als een nieuwe versie wordt gevonden, wordt deze automatisch gedownload en wordt er een bericht aan de Gebruiker getoond. Deze kan de update vervolgens toestaan. Het downloadproces gebruikt hierbij maximaal 50% van de beschikbare bandbreedte; de belemmering voor andere netwerktoepassing wordt daardoor minimaal gehouden.

Deze software-updates zijn digitaal ondertekend door logmein.com met een privésleutel, die niet te vinden is op onze systemen die met internet zijn verbonden.

Wachtwoorden voor Central/Pro worden niet opgeslagen in onze database. Central en Pro gebruiken een functie voor cryptografische sleutelafleiding in één richting, en een salt-waarde per account.

5 Bijwerken van beveiliging

GoTo controleert en actualiseert zijn beveiligingsprogramma regelmatig, en schakelt onafhankelijke derden in om relevante besturingselementen voor beveiliging minstens eenmaal per jaar te beoordelen. Zo zorgt GoTo ervoor dat de beveiliging opgewassen blijft tegen actuele bedreigingen en voldoet aan relevante kaders, industrienormen, toezeggingen van klanten en, indien van toepassing, wijzigingen in wet- en regelgeving met betrekking tot de beveiliging van GoTo-gegevens.

6 Back-up van gegevens, noodherstel en beschikbaarheid

De architectuur van GoTo is ontworpen om replicatie bijna in realtime uit te voeren naar geografisch verschillende locaties. Back-ups van databases worden gemaakt met behulp van incrementele back-ups. In het geval van een ramp of een totale uitval van een site op een van de actieve locaties, zijn de resterende locaties ingericht om de belasting van de applicatie in evenwicht te houden. De noodherstelprocedure met betrekking tot deze systemen wordt periodiek getest.

Back-ups van Klantcontent worden iedere 24 uur of iedere zeven dagen gemaakt binnen hetzelfde datacenter. Daarnaast wordt er elke zeven dagen een overeenkomstige back-up gemaakt in een geografisch ver weg gelegen datacenter, die vier weken lang wordt bewaard.

[1] Voor meer informatie, zie VS-patentnr. 7.558.862.

7 Datacenters

De GoTo-infrastructuur is ontworpen om de betrouwbaarheid van de service te verhogen en het risico op uitval door storingen te verminderen, door gebruik te maken van:

a) redundante, actief-actieve datacenters; of
b) datacenters van cloudhostingproviders.

Datacenters bevinden zich in Duitsland, Australië, het Verenigd Koninkrijk, de Verenigde Staten, Nederland of Ierland.

Alle datacenters bewaken de omgevingscondities, en zijn 24 uur per dag voorzien van fysieke beveiligingsmaatregelen.

7.1 Fysieke beveiliging datacenters

GoTo werkt samen met datacenters om de fysieke beveiliging te waarborgen voor systemen en servers die Klantcontent bevatten. Deze beveiligingsmiddelen zijn bijvoorbeeld:

- Videobewaking en -opname;
- Temperatuurregeling met verwarming, ventilatie en airconditioning;
- Brandbestrijding en rookmelders;
- Ononderbreekbare stroomvoorziening;
- Verhoogde vloeren of uitgebreid kabelbeheer;
- Continue monitoring en waarschuwingen;
- Bescherming tegen veel voorkomende natuurrampen en door de mens veroorzaakte rampen, zoals vereist afhankelijk van de locatie van het betreffende datacenter; en
- Gepland onderhoud en validatie van alle kritieke besturingselementen voor fysieke beveiliging.

GoTo biedt uitsluitend fysieke toegang tot productiedatacenters aan daartoe bevoegde personen. Voor toegang tot een fysieke serverruimte of hostingfaciliteit van een derde partij moet een verzoek worden ingediend via het betreffende ticketingsysteem. Vervolgens moet de aanvraag worden goedgekeurd door de betreffende manager, en worden beoordeeld en goedgekeurd door het technische operationele team van GoTo. Alle fysieke toegang tot datacenters en serverruimtes wordt bijgehouden, en de logbestanden worden minstens elk kwartaal gecontroleerd door het GoTo-management. Daarnaast wordt de autorisatie voor fysieke toegang tot het datacenter onmiddellijk opgeheven bij het wijzigen van de rol (wanneer dergelijke toegang niet langer vereist is) of bij het ontslag van eerder geautoriseerd personeel. Toegang met meerdere factoren (zoals biometrische gegevens, een badge of een toetsenblok) is vereist voor zeer gevoelige gebieden, waaronder datacenters.

8 Naleving van normen

GoTo beoordeelt regelmatig of het voldoet aan de toepasselijke wettelijke, financiële, gegevensprivacy- en regelgevingsvereisten. De privacy- en beveiligingsprogramma's van GoTo zijn conform verschillende industriestandaarden gecertificeerd en goedgekeurd volgens externe auditnormen, waaronder:

- **TRUSTe-certificaat inzake privacy en best practices voor gegevensbeheer voor ondernemingen**, voor de operationele besturingselementen voor privacy- en gegevensbescherming die zijn afgestemd op de belangrijkste privacywetten en erkende privacyraamwerken. Raadpleeg voor meer informatie onze blogpost hierover.
- **TRUSTe APEC CBPR- en PRP-certificaten** voor de overdracht van Klantcontent tussen APEC-lidstaten, verkregen en onafhankelijk gevalideerd door TrustArc, een door APEC goedgekeurde derde partij die toonaangevend is op het gebied van naleving van gegevensbescherming. Klik hier voor meer informatie over onze APEC-certificeringen.
- **Attestatierapport Service Organization Control (SOC) 2 Type II** incl. **BSI Cloud Computing-catalogus (C5)** van het American Institute of Certified Public Accountants (AICPA).
- Compliance met de **Payment Card Industry Data Security Standard (PCI DSS)** voor de e-commerce- en betalingsomgevingen van GoTo.
- Beoordeling van interne besturingselementen zoals vereist in het kader van de controle van de jaarrekeningen door de **Public Company Accounting Oversight Board (PCAOB)**.

9 Beveiliging van toepassingen

Het applicatiebeveiligingsprogramma van GoTo volgt de SDL (Security Development Lifecycle) van Microsoft om productcode te beveiligen. Het Microsoft SDL-programma omvat handmatige codebeoordelingen, bedreigingsmodellen, statische codeanalyse, dynamische analyse en systeemverharding. GoTo-teams voeren ook periodiek dynamische en statische tests uit op de kwetsbaarheid van applicaties, evenals penetratietests voor getroffen omgevingen.

10 Rapporteren, monitoren en waarschuwen

GoTo heeft beleidsregels en procedures ingericht voor alle vormen van rapporteren, monitoren en waarschuwen. Hierin worden de principes en besturingselementen beschreven die worden geïmplementeerd om verdachte activiteiten beter te detecteren en hier tijdig op te reageren. GoTo verzamelt geïdentificeerd afwijkend of verdacht verkeer in relevante beveiligingslogbestanden in toepasselijke productiesystemen.

11 Detectie en respons van eindpunten

Software voor detectie en respons van eindpunten (Endpoint Detection and Response (EDR)), inclusief auditrapportage, wordt op alle GoTo-servers gebruikt om onderbrekingen van of impact op de prestaties van de service tot een minimum te beperken. Voor zover van toepassing en noodzakelijk worden er beveiligingsonderzoeken uitgevoerd, in overeenstemming met onze procedures voor het reageren op incidenten, wanneer er verdachte activiteiten worden gedetecteerd. Zie hoofdstuk 17 voor meer informatie over GoTo's Beveiligingscentrum en de procedures voor het reageren op incidenten.

12 Beheren van bedreigingen

GoTo's Cyber Security Incident Respons Team ('CSIRT') bestaat uit meerdere teams en is verantwoordelijk voor de bescherming tegen cyberbedreigingen. Het Cyber Threat Intelligence-team binnen het CSIRT verzamelt, onderzoekt en verspreidt informatie over huidige en opkomende bedreigingen. GoTo blijft op de hoogte van informatie over bedreigingen en risicobeperking door zowel open als gesloten bronnen te bekijken, deel te nemen aan groepen waarin informatie over bedreigingen gedeeld wordt, en via lidmaatschap bij brancheverenigingen (IT-ISAC, FIRST.org, enz.).

13 Scannen op beveiliging en kwetsbaarheid en patchbeheer

GoTo heeft een formeel patchbeheerprogramma ingericht en voert minstens elk kwartaal patchbeheeractiviteiten uit op alle relevante systemen, apparaten, firmware, besturingssystemen, toepassingen en andere software waarmee Klantcontent wordt verwerkt. GoTo beoordeelt en scant op kwetsbaarheden op systeemniveau en in interne en externe hosts/netwerken ('Systemen'), ten minste maandelijks, en na elke wezenlijke verandering aan dergelijke Systemen, en verhelpt relevante ontdekte kwetsbaarheden in overeenstemming met gedocumenteerde Beleidsregels die prioriteit geven aan herstel op basis van risico.

14 Logische toegangscontrole

Er zijn procedures ingericht voor logische toegangscontrole om het risico van onbevoegde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te beperken. Medewerkers krijgen toegang tot specifieke GoTo-systemen, toepassingen, netwerken en apparaten op basis van het principe van de minste rechten. Gebruikersprivileges worden gescheiden op basis van functionele rol (toegangscontrole op basis van rollen) en omgeving, door onderscheid te maken tussen besturingselementen, processen en/of procedures van functies.

15 Scheiding van gegevens

GoTo heeft besturingselementen geïmplementeerd om te voorkomen dat Gebruikers de gegevens van andere Gebruikers zien. GoTo maakt bijvoorbeeld gebruik van een architectuur met meerdere tenants, logisch gescheiden op databaseniveau, gebaseerd op de GoTo-account van een gebruiker of organisatie. Partijen moeten worden geverifieerd om toegang te krijgen tot een account.

16 Perimeterbescherming en inbraakdetectie

De GoTo-netwerkarchitectuur op locatie is onderverdeeld in openbare, privé- en iLO-beheernetwerkzones (Integrated Lights-Out). De openbare zone bevat servers die op het internet zijn gericht, en al het verkeer dat dit netwerk binnenkomt moet door een firewall. Hierbij is alleen vereist netwerkverkeer toegestaan; al het andere netwerkverkeer wordt geweigerd en er wordt geen netwerktoegang toegestaan vanuit de openbare zone naar de privé- of iLO-beheernetwerkzones.

De privénetwerkzone host administratieve en monitoringssystemen op applicatieniveau, en de iLO-beheernetwerkzones zijn ingericht voor het beheren en monitoren van de hardware en netwerken. Toegang tot deze netwerken is beperkt tot bevoegde medewerkers via tweeledige verificatie.

GoTo gebruikt tools, technieken en services voor perimeterbescherming, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Deze beveiligingsmiddelen zijn bijvoorbeeld:

- Intrusiedetectiesystemen die systemen, diensten, netwerken en toepassingen monitoren op ongeautoriseerde toegang;
- Kritische systeem- en configuratiebestandsbewaking;
- Webtoepassingsfirewall (WAF) en DDoS-preventiediensten op de applicatieniveau die fungeren als proxy voor GoTo-verkeer
- Een firewall voor lokale toepassingen die een extra beschermingslaag biedt tegen de top tien van OWASP, en andere kwetsbaarheden van webtoepassingen en kwaadaardig verkeer; en
- Hostgebaseerde firewalls die inkomende en uitgaande verbindingen filteren, inclusief interne verbindingen tussen GoTo-systemen

17 Het Security Operations Center en incidentbeheer

Het Security Operations Center (SOC) van GoTo is verantwoordelijk voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het SOC maakt gebruik van beveiligingssensoren en analysesystemen om potentiële problemen te identificeren, en heeft procedures ontwikkeld om op incidenten te reageren, waaronder een gedocumenteerd Incidentenbestrijdingsplan.

Het Incidentenbestrijdingsplan van GoTo is afgestemd op de kritieke communicatieprocessen, beleidsregels en standaardwerkprocedures van GoTo. Het is ontworpen om relevante verdachte of geïdentificeerde beveiligingsgebeurtenissen in interne systemen en services, inclusief Central en Pro, te beheren, te identificeren en op te lossen. Het Incidentenbestrijdingsplan beschrijft mechanismen voor medewerkers om verdachte beveiligingsgebeurtenissen te melden, evenals escalatiepaden die indien nodig gevolgd moeten worden. Verdachte gebeurtenissen worden gedocumenteerd en indien nodig geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

18 Verwijderen en retourneren van Content

Verwijdering en/of teruggave: Klanten kunnen verzoeken om teruggave en/of verwijdering van hun Klantcontent door een verzoek in te dienen via GoTo's Portaal voor Beheer van Individuele Rechten ('IRM'; Individual Rights Management Portal), via support.goto.com of door een e-mail te sturen naar privacy@goto.com. Verzoeken worden binnen dertig (30) dagen na ontvangst door GoTo verwerkt, maar in het onwaarschijnlijke geval dat we meer tijd nodig hebben, zullen we u zo snel mogelijk op de hoogte stellen van de verwachte termijn.

Schema voor het bewaren van Klantcontent: Tenzij anders vereist door de toepasselijke wetgeving, wordt Klantcontent automatisch verwijderd na negentig (90) dagen na de beëindiging, annulering of afloop ervan, en in elk geval wordt de inrichting van het op dat moment laatste abonnement van de Klant opgeheven. Op schriftelijk verzoek kan GoTo een schriftelijke bevestiging/certificering van de verwijdering van de Content geven.

19 Organisatorische besturingselementen

19.1 Beveiligingsbeleid en -procedures

GoTo heeft een uitgebreide reeks beveiligingsbeleidsregels en -procedures die regelmatig worden herzien en bijgewerkt, ter ondersteuning van de beveiligingsdoelstellingen van GoTo, of wegens wijzigingen in de nalevingsvereisten van toepasselijke wetgeving of industriestandaarden.

19.2 Veranderingsbeheer

GoTo heeft een proces ingericht voor het beheren van veranderingen. Wijzingen in GoTo-systemen worden vóór de implementatie ervan beoordeeld, getest en goedgekeurd om het risico op onderbreking van GoTo-services te beperken.

19.3 Bewustzijns- en trainingsprogramma's over beveiliging

GoTo's heeft een programma ingericht ter vergroting van de bewustwording ten aanzien van privacy en beveiliging. Het programma biedt trainingen aan medewerkers over het belang van de ethische, verantwoordelijke en zorgvuldige behandeling van Persoonsgegevens en vertrouwelijke informatie, en de verwerking ervan conform de toepasselijke wetgeving. Nieuwe medewerkers, contractanten en stagiaires worden tijdens de inwerkperiode geïnformeerd over het beveiligingsbeleid en de Gedragscode en Bedrijfsethiek van GoTo. Medewerkers van GoTo volgen minstens eenmaal per jaar een bewustwordingstraining ten aanzien van privacy en beveiliging. Activiteiten ter vergroting van de bewustwording vinden het hele jaar door plaats. Denk bijvoorbeeld aan campagnes voor Dag van de Gegevensprivacy en Maand van de Cyberveiligheid, webinars van het Hoofd Informatiebeveiliging, en een beloningsprogramma voor 'beveiligingskampioenen'.

Waar nodig kunnen medewerkers ook verplicht worden om rolspecifieke trainingen te volgen. Daarnaast moeten alle medewerkers, contractanten en dochterondernemingen van GoTo het beleid van GoTo met betrekking tot beveiliging en gegevensbescherming doornemen en naleven.

20 Privacy

GoTo neemt de privacy van onze Klanten, Gebruikers en andere personen die GoTo-services gebruiken ('Eindgebruikers') zeer serieus en zet zich in om relevante best practices voor gegevensverwerking en -beheer op een open en transparante manier bekend te maken.

20.1 Privacyprogramma.

GoTo heeft een uitgebreid privacyprogramma waarmee coördinatie van meerdere functies binnen het bedrijf gemoeid is, waaronder de afdelingen Privacy, Beveiliging, Governance, Risico- en nalevingsbeheer, Juridische Zaken, het Productteam, Engineering en Marketing. Dit privacyprogramma is gericht op naleving en omvat de implementatie en het onderhoud van interne en externe beleidsregels, normen en addenda om de best practices van het bedrijf te regelen.

20.2 Naleving van regelgeving

20.2.1 AVG

De Algemene verordening gegevensbescherming (AVG) is een wet van de Europese Unie (EU) met betrekking tot gegevensbescherming en privacy voor personen binnen de EU. GoTo heeft een uitgebreid AVG-nalevingsprogramma, en voor zover GoTo namens de Klant persoonsgegevens verwerkt die onder de AVG vallen, zullen we dit doen in overeenstemming met de toepasselijke vereisten van de AVG. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

De California Consumer Privacy Act, zoals gewijzigd door de California Privacy Rights Act (samen de 'CCPA' genoemd) geeft Californiërs extra rechten en bescherming met betrekking tot de manier waarop bedrijven hun persoonlijke gegevens mogen gebruiken. GoTo heeft een uitgebreid nalevingsprogramma en voor zover GoTo namens de klant persoonsgegevens verwerkt die onder de CCPA vallen, zullen we

dit doen in overeenstemming met de van toepassing zijnde vereisten van de CCPA. Voor meer informatie over onze naleving van de CCPA, zie GoTo's Privacybeleid en Aanvullende Californische Privacywetgeving voor consumenten.

20.2.3 LGPD

De Braziliaanse Wet Bescherming Persoonsgegevens (LGPD) regelt de verwerking van Persoonsgegevens in Brazilië en/of van personen die zich ten tijde van de verzameling in Brazilië bevinden. GoTo heeft een uitgebreid nalevingsprogramma en voor zover GoTo namens de Klant persoonsgegevens verwerkt die onder de LGPD vallen, zullen wij dit doen in overeenstemming met de toepasselijke vereisten van de LGPD. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

20.3 Gegevensverwerkingsaddendum ('DPA')

GoTo biedt een wereldwijd Addendum gegevensverwerking (DPA), dat beschikbaar is in het Engels en Duits. Deze DPA voldoet aan de vereisten voor AVG, CCPA en andere van toepassing zijnde regelgeving, en regelt de verwerking van Klantcontent door GoTo.

Specifiek bevat onze DPA verschillende methoden voor AVG-gerichte bescherming van gegevensprivacy, waaronder:

(a) bekendmaking van de details van de gegevensverwerking en subverwerkers zoals vereist krachtens artikel 28;
(b) de (in 2021) herziene Standaardcontractbepalingen (ook bekend als de EU-modelclausules); en
(c) productspecifieke technische en organisatorische maatregelen van GoTo.

Om te voldoen aan de CCPA-vereisten, omvat onze wereldwijde DPA daarnaast:

(a) herziene definities in kaart gebracht aan de hand van de CCPA;
(b) toegangs- en verwijderingsrechten; en
(c) de garantie dat GoTo de persoonlijke informatie van onze klanten, gebruikers en eindgebruikers niet zal verkopen.

Onze wereldwijde DPA bevat ook bepalingen om:

(a) de naleving van de LGPD door GoTo te realiseren;
(b) rechtmatige overdrachten van Persoonsgegevens van en naar Brazilië ondersteunen; en
(c) ervoor zorgen dat onze Gebruikers dezelfde privacyvoordelen genieten als onze andere wereldwijde Gebruikers.

20.4 Overdrachtskaders

GoTo ondersteunt rechtmatige internationale gegevensoverdrachten onder de volgende kaders:

20.4.1 Standaardcontractbepalingen

De Standaardcontractbepalingen ('SCC's'; Standard Contractual Clauses), soms EU-modelclausules genoemd, zijn gestandaardiseerde contractvoorwaarden, die zijn erkend en aangenomen door de Europese Commissie, om ervoor te zorgen dat alle Persoonsgegevens die de Europese Economische Ruimte (EER) verlaten, worden overgedragen in overeenstemming met de EU-wetgeving inzake gegevensbescherming. De SCC's, herzien en uitgegeven in 2021, zijn opgenomen in de wereldwijde DPA van GoTo, om GoTo-klanten in staat te stellen gegevens buiten de EER over te dragen in overeenstemming met de AVG.

20.4.2 Certificeringen voor de CBPR en PRP van de APEC

GoTo heeft certificeringen behaald van de Asia-Pacific Economic Cooperation ('APEC'), voor de Cross-Border Privacy Rules ('CBPR') en de Privacy Recognition for Processors ('PRP'). De CBPR en de PRP van APEC zijn de eerste standaarden voor gegevensbeveiliging die zijn goedgekeurd voor de overdracht van Persoonsgegevens tussen lidstaten van de APEC. De certificeringen zijn behaald en onafhankelijk gevalideerd door TrustArc, een externe aanbieder op het gebied van naleving van gegevensbeveiliging die is goedgekeurd door de APEC.

20.5 Aanvullende maatregelen

Naast de maatregelen die in deze TOM's zijn gespecificeerd, heeft GoTo Veelgestelde vragen en de antwoorden daarop verzameld, om de aanvullende maatregelen te schetsen die zijn geïmplementeerd om rechtmatige overdrachten, zoals bedoeld in hoofdstuk 5 van de AVG, te ondersteunen. Hiermee bieden we ook de mogelijkheid om case-by-case-analyses, die door het Europese Hof van Justitie worden aanbevolen in verband met het gebruik van de SCC's, te bespreken en te begeleiden.

20.6 Verzoeken om gegevens

GoTo heeft uitgebreide processen ingericht om het ontvangen van verzoeken met betrekking tot gegevensbescherming en beveiliging te vergemakkelijken, waaronder het IRM-portaal, een speciaal privacy-e-mailadres (privacy@goto.com) en de klantenondersteuning op https://support.goto.com.

20.7 Openbaarmakingen van subverwerkers en datacentra

GoTo publiceert openbaarmakingen van subverwerkers in het Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Deze openbaarmakingen specificeren de namen, locaties en verwerkingsdoeleinden van datahostingproviders en andere derden die Klantcontent verwerken als onderdeel van het leveren van de service aan GoTo-klanten.

20.8 Gevoelige gegevens Verwerkingsbeperkingen

Tenzij GoTo hier uitdrukkelijk om heeft verzocht of de Klant hierover anderszins schriftelijke toestemming van GoTo heeft ontvangen, mogen de volgende soorten gevoelige gegevens niet worden geüpload of anderszins aan GoTo worden verstrekt:

- Door de overheid uitgegeven identificatienummers en afbeeldingen van identificatiedocumenten.
- Informatie met betrekking tot de gezondheid van een persoon, inclusief maar niet beperkt tot Beschermde Gezondheidsinformatie (PHI; Protected Health Information), zoals geïdentificeerd in de Amerikaanse Health Insurance Portability and Accountability Act (HIPAA), evenals andere relevante toepasselijke wet- en regelgeving.
- Informatie met betrekking tot financiële rekeningen en betaalinstrumenten, inclusief maar niet beperkt tot creditcardgegevens. De enige algemene uitzondering op deze bepaling betreft expliciet geïdentificeerde betalingsformulieren en -pagina's die door GoTo worden gebruikt om betalingen voor de service te innen.
- Alle informatie die speciaal beschermd wordt door toepasselijke wet- en regelgeving, in het bijzonder informatie over ras, etniciteit, religieuze of politieke overtuigingen, lidmaatschappen van organisaties, etc. van een individu.

20.9 Naleving in gereguleerde omgevingen

Klanten zijn zelf verantwoordelijk voor het implementeren van de juiste beleidsregels, procedures en beveiligingsmechanismen wanneer zij GoTo Resolve gebruiken om apparaten in gereguleerde omgevingen te ondersteunen.

21 Mechanismen voor de controle van beveiliging en privacy van derden

Voordat GoTo externe leveranciers inschakelt die Klantcontent of vertrouwelijke, gevoelige of personeelsgegevens verwerken, controleert en analyseert GoTo de beveiligings- en privacyprocedures van de leverancier via geschikte inkoopkanalen. Indien nodig kan GoTo periodiek nalevingsdocumentatie of -rapporten van leveranciers opvragen en evalueren om ervoor te zorgen dat hun controleomgeving en -normen toereikend blijven.

GoTo sluit schriftelijke overeenkomsten met alle externe leveranciers en gebruikt ofwel door GoTo goedgekeurde inkoopsjablonen of onderhandelt over de standaardvoorwaarden van dergelijke derde partijen om aan de door GoTo geaccepteerde privacy- en beveiligingsnormen te voldoen, waar dat nodig wordt geacht. De teams Financiën, Juridische Zaken, Privacy en Beveiliging zijn betrokken bij het beoordelingsproces van verkopers en controleren waar nodig en/of van toepassing of verkopers voldoen aan bepaalde verplichte vereisten voor gegevensverwerking en contractuele vereisten. GoTo's risicobeleid voor derden regelt de privacy- en beveiligingseisen van leveranciers op basis van het type en de duur van de gegevensverwerking en het toegangsniveau. Waar van toepassing (bijv. waar Klantcontent wordt verwerkt of opgeslagen), bevatten overeenkomsten met verkopers vereisten voor "naleving van toepasselijke wetgeving", een DPA, of vergelijkbaar document waarin onderwerpen zoals AVG, CCPA, LGPD en gebruiks- en verkoopbeperkingen worden behandeld. De DPA voor leveranciers van GoTo regelt bijvoorbeeld beperkingen rond het 'verkopen' van gegevens zoals gedefinieerd onder de CCPA. Op dezelfde manier worden met relevante leveranciers beveiligingsaddenda met passende vereisten voor besturingselementen en systemen opgesteld.

22 Contact opnemen met GoTo

Klanten kunnen voor algemene vragen contact opnemen met GoTo op support.goto.com . Voor vragen of verzoeken met betrekking tot persoonsgegevens of privacy kunt u terecht op ons IRM-portaal of een e-mail sturen naar privacy@goto.com.