TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR GOTOASSIST REMOTE SUPPORT V5

(VOORHEEN BEKEND ALS RESCUEASSIST)

CONTROLEMECHANISMEN VOOR BEVEILIGING EN PRIVACY

Publicatiedatum: Februari 2022

1 Producten en services

In dit document worden de Technische en Organisatorische Maatregelen (TOM's) uiteengezet die zijn geïmplementeerd in de infrastructuur en communicatiekanalen van GoToAssist Remote Support V5 (voorheen bekend als RescueAssist).

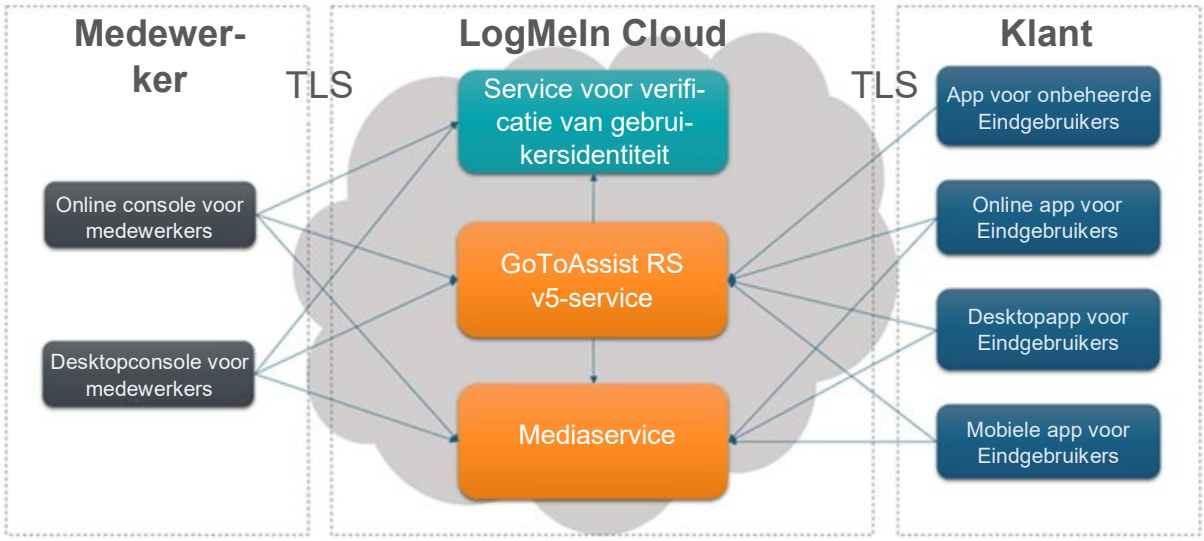
GoToAssist Remote Support V5 stelt IT- en ondersteuningsprofessionals in staat om ondersteuning op afstand te bieden op computers, servers en mobiele apparaten, met de functionaliteit voor externe weergave, besturing op afstand, en het delen van camera's, vanaf een online of desktopconsole van een medewerker. GoToAssist Remote Support V5 maakt gebruik van krachtige gegevensbeveiligingsmaatregelen tegen zowel passieve als actieve aanvallen.

2 Productarchitectuur

GoToAssist Remote Support V5 gebruikt een ASP-model (Application Service Provider) dat ontworpen is om een beveiligde werkomgeving te bieden, terwijl het geïntegreerd wordt met de bestaande netwerk- en beveiligingsinfrastructuur van een bedrijf. De architectuur is ontworpen met het oog op optimale prestaties, betrouwbaarheid en schaalbaarheid. Er zijn redundante switches en routers ingebouwd in de architectuur, waarmee deze vrijwel volledig storingsvrij is. Het systeem is voorzien van geclusterde servers en back-upsystemen met hoge capaciteit, om applicatieprocessen te kunnen blijven uitvoeren in het geval van een zware belasting of systeemstoring. Servicebrokers verdelen daarnaast de belasting van de client/server-sessies over geografisch verspreide communicatieservers. De communicatiearchitectuur van GoToAssist Remote Support V5 wordt hieronder weergegeven in Sectie 2.1.

2.1. Communicatiearchitectuur

De communicatiearchitectuur van GoToAssist Remote Support V5 wordt samengevat in de onderstaande afbeelding.



Voor de verificatie van medewerkers wordt GoTo's eigen service voor verificatie van gebruikersidentiteit ingezet. Communicatie tussen deelnemers in een GoToAssist Remote Support V5-sessie vindt plaats via een overlay-netwerkstack die logisch is gepositioneerd boven het conventionele UDP en TCP/IP. Dit netwerk wordt geleverd door de GoToAssist Remote Support V5-service en de Mediaservice, gehost in Amazon AWS.

Deelnemers aan GoToAssist Remote Support V5-sessies (met de Online console voor Medewerkers, de Desktopconsole voor Medewerkers, Eindpunten van Eindgebruikers (in afbeelding 1 weergegeven als eindpunten van de 'Klant')) communiceren met de GoToAssist Remote Support V5-service en de Mediaservice via uitgaande TCP-verbindingen op poort 443, of UDP-poort 15000, afhankelijk van beschikbaarheid. Omdat GoToAssist Remote Support V5 een gehoste, webgebaseerde service is, kunnen deelnemers een sessie bijwonen vanaf iedere locatie met een internetverbinding; een extern kantoor, een thuiswerkplek, een congrescentrum of het bedrijfsnetwerk van een zakenpartner.

2.2. Desktopconsole voor medewerkers

Medewerkers kunnen de Online console voor Medewerkers of de installeerbare Desktopconsole voor Medewerkers gebruiken om verbinding te maken met de GoToAssist Remote Support V5-service. De Desktopconsole gebruikt de voor alle platforms geschikte Qt-toolkit, om zowel op MacOS als op Windows te kunnen draaien, en de open-sourcewebbrowser Chromium, om onderdelen van de Online console te kunnen gebruiken.

3 Technische besturingselementen van GoToAssist Remote Support v5

GoTo maakt gebruik van technische besturingselementen voor beveiliging die voldoen aan de industriestandaard, en die geschikt zijn voor de aard en het bereik van de services (zoals deze term wordt gedefinieerd in de Servicevoorwaarden). Ze zijn ontworpen om de infrastructuur van de service en de gegevens die zich daarin bevinden optimaal te beschermen. U vindt de Servicevoorwaarden op https://www.goto.com/company/legal/terms-and-conditions.

3.1. Verificatie

Medewerkers en accountbeheerders van GoToAssist Remote Support V5 worden geïdentificeerd aan de hand van hun e-mailadres en geverifieerd met een wachtwoord. Tijdens het verificatieproces wordt het wachtwoord op geen enkel moment onversleuteld overgedragen.

Op de verificatieprocedures zijn de volgende beleidsregels van toepassing:

- **Sterke wachtwoorden:** Een sterk wachtwoord is minimaal 8 tekens lang en heeft voldoende complexiteitsvereisten (d.w.z. moet zowel letters als cijfers bevatten). Wachtwoorden worden op sterkte gecontroleerd wanneer ze worden ingesteld of gewijzigd.
- **Tweeledige verificatie:** Als extra veiligheidsmaatregel is optionele tweeledige verificatie beschikbaar voor elke GoToAssist Remote Support V5-bedrijfsaccount. Wanneer tweeledige verificatie is ingeschakeld moet elke gebruiker zich verifiëren via twee afzonderlijke methoden.

- **Vergrendeling van accounts:** Een gebruikersaccount wordt verplicht 'zacht vergrendeld' na vijf opeenvolgende mislukte aanmeldpogingen. Dit betekent dat de houder van de gebruikersaccount zich gedurende vijf minuten niet kan aanmelden. Na afloop van de vergrendeling kan gebruiker zich opnieuw proberen aan te melden bij zijn account.

3.2. Logische toegangscontrole

Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken. Medewerkers krijgen minimale toegang (met slechts zoveel rechten als nodig zijn) tot specifieke GoTo-systemen, toepassingen, netwerken en apparaten. Verder worden gebruikersrechten gescheiden op basis van functionele rol en omgeving.

Gebruikers aan wie toegang wordt verleend tot onderdelen van GoToAssist Remote Support V5 zijn onder meer geautoriseerde medewerkers van GoTo (zoals van de teams Technische Operaties en Technische Ontwikkeling), beheerders van klanten, of eindgebruikers van het product. De productieservers op locatie zijn alleen beschikbaar vanaf jumphosts of via het virtuele privénetwerk (VPN) van het team Technische Operaties. Cloudgebaseerde productiecomponenten zijn beschikbaar via verificatie met SSU (Self Service Unix).

3.3. Toegangscontrole op basis van toestemming

3.3.1. Bijgewoonde sessie

Een essentieel onderdeel van de beveiliging van GoToAssist Remote Support V5's is het toegangscontrolemodel op basis van toestemming, dat ontworpen is om de toegang tot het computer van de Klant te beschermen. Tijdens live ondersteuningssessies die door een klant worden bijgewoond, wordt de klant voordat de schermdeling, besturing op afstand of bestandsoverdracht wordt gestart, om toestemming gevraagd voor het uitvoeren van dit proces.

Wanneer een Klant tijdens een beheerde sessie toestemming geeft voor besturing op afstand en schermdeling, kan deze alles zien wat de Medewerker doet. Verder is de service zo ingericht dat de Klant op elk moment gemakkelijk de controle terug kan nemen of de sessie kan beëindigen.

3.3.2. Onbeheerde sessie

Voor onbeheerde ondersteuning moet de App voor onbeheerde Eindgebruikers geïnstalleerd zijn op het apparaat van de Klant. De app kan op twee manieren worden ingesteld: installatie tijdens de sessie (i.e. tijdens een Beheerde sessie), of met een Programma voor installatie buiten de sessie om. In beide gevallen is toestemming van de Klant vereist.

Installatie tijdens de sessie: Zodra de Klant en de Medewerker aan een sessie zijn begonnen, kan de Medewerker de Klant toestemming vragen om de App voor onbeheerde Eindgebruikers te installeren. De Klant moet hiervoor vervolgens expliciet toestemming geven via een venster dat verschijnt.

Programma voor installatie buiten de sessie om: Nadat een medewerker veilig is aangemeld bij de GoToAssist Remote Support V5-website of -desktopapplicatie, kan

deze een installatieprogramma downloaden waarmee de App voor onbeheerde Eindgebruikers kan worden geïnstalleerd op elke Windows-pc of Mac waarvoor de Medewerker beheerderstoegang heeft.

3.3.3. Beveiliging tijdens de sessie

GoToAssist Remote Support V5 is niet bedoeld om lokale beveiligingscontroles op de computer van de Klant op te heffen.

Integendeel; de service is juist zo ingericht dat de Klant, wanneer er een Onbeheerde sessie actief is, de sessie te allen tijd kan beëindigen en de supportprivileges van de Medewerker voor de Onbeheerde sessie kan intrekken.

3.4. Rolgebaseerde toegangscontrole

GoToAssist Remote Support V5 biedt toegang tot verschillende bronnen en services beveiligd door een toegangscontrolesysteem op basis van rollen. Een op maat gemaakt toegangsbeleid kan zo worden afgedwongen met behulp van de verschillende onderdelen van de service. De volgende rollen zijn gedefinieerd:

- **Accountbeheerder:** GoToAssist Remote Support V5-gebruiker met volledige beheerdersbevoegdheden om administratieve functies met betrekking tot Medewerkers uit te voeren. Beheerders van accounts kunnen accounts van Medewerkers aanmaken, wijzigen en verwijderen, en de abonnementsgegevens ervan wijzigen.
- **Medewerker:** Een GoToAssist Remote Support V5-gebruiker. De medewerker kan GoToAssist Remote Support V5-sessies starten om technische ondersteuning te bieden aan Klanten via externe weergave, besturing op afstand, en het delen van camera's.
- **Klant:** Niet-geverifieerde persoon die ondersteuning van de Medewerker nodig heeft. De Klant kan sessies beëindigen en moet de Medewerker toestemming verlenen voor toegang tot zijn apparaat.

3.5. Perimeterbescherming en inbraakdetectie

GoTo heeft tools, technieken en services voor perimeterbescherming geïmplementeerd, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie. Cloudbronnen maken ook gebruik van hostgebaseerde firewalls.

3.6. Scheiding van gegevens

GoTo maakt gebruik van een architectuur met meerdere tenants, logisch gescheiden op databaseniveau, en gebaseerd op de GoTo-account van een gebruiker of organisatie. Alleen geverifieerde partijen krijgen toegang tot relevante accounts.

3.7. Fysieke beveiliging

GoTo werkt samen met datacenters om de fysieke beveiliging te waarborgen van serverruimtes waar productieservers staan. Deze beveiligingsmaatregelen omvatten:

- Videobewaking en -opname
- Meervoudige verificatie voor zeer gevoelige ruimtes
- Temperatuurregeling met verwarming, ventilatie en airconditioning
- Brandbestrijding en rookmelders

- Ononderbreekbare stroomvoorziening (UPS)
- 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
- 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. Het GoTo-management controleert minstens elk kwartaal de logbestanden ten aanzien van de fysieke toegang tot datacenters en serverruimtes. Daarnaast verliest eerder geautoriseerd personeel bij ontslag direct het recht op fysieke toegang tot de datacenters.

3.8. 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.

3.9. Versleuteling

GoTo houdt zich aan een cryptografische standaard die overeenkomt met aanbevelingen van brancheverenigingen, overheidspublicaties en andere erkende normgroepen. De cryptografische standaard wordt periodiek herzien en gebruikte technologieën en vercijferingen kunnen worden bijgewerkt in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden.
De versleuteling die wordt gebruikt in GoToAssist Remote Support V5 is gebaseerd op:

- Sessiegegevens van GoToAssist Remote Support V5 worden tijdens de overdracht beschermd met TLS 1.2 (indien ondersteund) en 256-bits AES-codering.
- Sessiesleutels die vanaf de server worden gegenereerd door de medewerker en daar blijven om de klant met de medewerker te kunnen verbinden. De service is zo ontworpen dat deze sleutels nooit openbaar toegankelijk zijn.
- Versleutelde communicatie tussen de klant en de medewerker in GoToAssist Remote Support V5 wordt geregeld via een aangepaste mediaserviceoplossing.
- Eindpunten binnen de infrastructuur van GoToAssist Remote Support V5 maken gebruik van TLS-verbindingen (Transport Layer Security).

3.9.1. Versleuteling tijdens de overdracht

Om de Klantcontent (zoals de term wordt gedefinieerd in de Servicevoorwaarden) tijdens de overdracht nog beter te beschermen, gebruikt GoTo de laatste TLS-protocollen en bijbehorende vercijferingen.

Communicatie tussen Eindpunt en backend van de Klant wordt versleuteld via de OpenSSL. Er zijn via TLS-oplossingen besturingselementen voor beveiliging van communicatie geïmplementeerd op de TCP-laag, waarbij gebruikgemaakt wordt van zeer sterke codering.

Ook worden er sterke verificatiemethoden gebruikt om de kans te verkleinen dat potentiële aanvallers zich voordoen als infrastructuurservers, of de communicatie van supportsessies onderscheppen.

Ter bescherming tegen afluisteren, wijzigingen of replay-aanvallen, worden IETF-standaard TLS-protocollen gebruikt om alle communicatie tussen eindpunten en onze services te beschermen. Gegevens voor schermdeling, gegevens over toetsenbord- en muisbediening, overgedragen bestanden, diagnostische gegevens op afstand en chatinformatie zijn tijdens de overdracht te allen tijde versleuteld met TLS 1.2 (2048-bits RSA, sterke AES-256-versleuteling met een 384-bits SHA-2-algoritme).

Om compatibiliteit en gebalanceerde beveiliging te kunnen garanderen, ondersteunt de GoToAssist Remote Support V5-service ook inkomende verbindingen met behulp van de meeste ondersteunde TLS-vercijferingen in TLS 1.2.

GoTo raadt medewerkers aan hun browser zo te configureren dat er standaard waar mogelijk gebruik wordt gemaakt van sterke cryptografie, om de technische beveiliging van hun apparaten te optimaliseren, en altijd het meest recente besturingssysteem en de laatste beveiligingspatches voor hun browser te installeren.

Wanneer verbindingen tot stand worden gebracht met de GoToAssist Remote Support V5-website en tussen onderdelen van GoToAssist Remote Support V5, verifiëren de GoTo-servers zich bij clients met behulp van openbare-sleutelcertificaten van GlobalSign. Server-to-server-API's zijn alleen toegankelijk binnen het met krachtige firewalls beschermde privénetwerk van GoTo.

3.9.2. Beveiliging TCP-laag

De conform de IETF-standaard (Internet Engineering Task Force) ingerichte TLS-protocollen worden gebruikt om de communicatie tussen eindpunten te beschermen.

Voor de bescherming van klanten zelf adviseert GoTo dat zij hun browser zo te configureren dat er standaard waar mogelijk gebruik wordt gemaakt van sterke cryptografie, en dat zij altijd het meest recente besturingssysteem en de laatste beveiligingspatches voor hun browser installeren.

3.9.3. Bescherming van Eindpunten van Klanten

De Desktopapp voor Eindgebruikers en de App voor onbeheerde Eindgebruikers moeten compatibel zijn zoveel mogelijk verschillende desktopomgevingen. GoToAssist Remote Support V5 voorziet hierin met behulp van een uitvoerbare download waarbij gebruik wordt gemaakt van krachtige versleuteling.

De Desktopapp voor Eindgebruikers en de App voor onbeheerde Eindgebruikers worden op de pc's van klanten gedownload in de vorm van een digitaal ondertekend installatieprogramma. Hiermee is de Klant beschermd tegen het per ongeluk installeren

van een Trojaans paard of andere malware die zich voordoet als GoToAssist Remote Support V5-software.

De eindpuntsoftware bestaat uit verschillende digitaal ondertekende uitvoerbare bestanden en dynamisch gekoppelde bibliotheken. Tijdens de ontwikkeling en implementatie volgt GoTo passende en strikte procedures voor kwaliteitscontrole en configuratiebeheer om de veiligheid van de software te garanderen.

3.10. Beheersing van kwetsbaarheden

Het waarborgen van de veiligheid en bescherming van de Content en systemen van klanten heeft de hoogste prioriteit van GoTo. GoTo implementeert daarom verschillende beveiligingsmaatregelen gedurende de levenscyclus van al zijn producten. Ook tijdens de ontwikkeling en het gebruik van GoToAssist Remote Support V5 wordt zorgvuldig rekening gehouden met alle aspecten van beveiliging.

Er worden periodiek dynamische en statische tests uitgevoerd op de kwetsbaarheid van applicaties, evenals beveiligingstests voor getroffen omgevingen. Relevante kwetsbaarheden worden daarnaast gecommuniceerd en beheerst met maand- en kwartaalrapporten voor zowel de ontwikkelingsteams als het management.

3.10.1. Beveiligingsteam

Het beveiligingsteam van GoTo houdt voortdurend toezicht op de productontwikkeling en -activiteiten, waarbij het nauw samenwerkt met producttechnici om GoToAssist Remote Support V5 veilig te houden, en mogelijke risico's te voorkomen of te verkleinen.

3.10.2. Interne en externe audits

Het interne auditproces van GoTo omvat regelmatige beveiligingsbeoordelingen op zowel infrastructuur- als softwareniveau. Onze interne audits worden aangevuld met verschillende onafhankelijke externe beoordelingen om ervoor te zorgen dat we aan de branchenormen blijven voldoen.

3.11. Rapporteren en waarschuwen

GoTo verzamelt geïdentificeerd afwijkend of verdacht verkeer in de relevante beveiligingslogbestanden van de betreffende productiesystemen.

4 Organisatorische besturingselementen

GoTo biedt een uitgebreide reeks organisatorische en administratieve controlemechanismen om de beveiliging en privacy van GoToAssist Remote Support V5 te beschermen.

4.1. Beveiligingsbeleid en -procedures

GoTo heeft een uitgebreid beveiligingsbeleid, met beleidsregels en procedures die zijn afgestemd op bedrijfsdoelen, nalevingsprogramma's en algemeen verantwoord zakelijk bestuur. Deze beleidsregels en procedures worden periodiek herzien en waar nodig bijgewerkt om de voortdurende naleving ervan te garanderen.

4.2. Naleving van normen

GoTo voldoet aan de van toepassing zijnde wettelijke, financiële, gegevensprivacy- en regelgevende vereisten, en houdt zich aan de volgende certificeringen en externe auditrapporten:

- 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.
- Internationale Organisatie voor Standaardisatie – ISO/IEC 27001:2013 Certificaat Information Security Management System (ISMS), inzake beheersystemen voor informatiebeveiliging.
- Attestatierapport Service Organization Control (SOC) 2 Type II incl. BSI Cloud Computing-catalogus (C5) van het American Institute of Certified Public Accountants (AICPA)
- Attestatierapport Service Organization Control (SOC) 3 Type II 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)

4.3. Het Security Operations Center en incidentbeheer

Het Security Operations Center (SOC) van GoTo wordt beheerd door het Team Beveiligingsoperaties, dat verantwoordelijk is voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het SOC maakt gebruik van beveiligingssensoren en analysesystemen om potentiële problemen te identificeren, en heeft een gedocumenteerd Incidentenbestrijdingsplan om adequaat op incidenten te reageren.

Het Incidentenbestrijdingsplan is afgestemd op de kritieke communicatieprocessen van GoTo, het Beleidsreglement voor Incidentbeheer van Informatiebeveiliging, en de bijbehorende standaardwerkprocedures. Het is ontworpen om verdachte of geïdentificeerde beveiligingsgebeurtenissen in interne systemen en services, te beheren, te identificeren en op te lossen, waaronder de GoToAssist Remote Support V5-service. In het Incidentenbestrijdingsplan is vastgelegd dat er technisch personeel aanwezig moet zijn om mogelijke gebeurtenissen en kwetsbaarheden met betrekking tot informatiebeveiliging te identificeren, en vermoedelijke of bevestigde gebeurtenissen indien nodig naar het management te escaleren. Medewerkers kunnen beveiligingsincidenten melden via e-mail, telefoon en/of tickets, al naargelang het proces dat is gedocumenteerd op de GoTo-intranetsite. Alle geïdentificeerde of verdachte gebeurtenissen worden gedocumenteerd en geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

4.4. Beveiliging van toepassingen

Het applicatiebeveiligingsprogramma van GoTo is gebaseerd op de SDL (Security Development Lifecycle) van Microsoft om productcode te beveiligen. De kernelementen van dit programma zijn handmatige codebeoordelingen, bedreigingsmodellen, statische codeanalyse, en systeemverharding.

4.5. Screening van personeel

Er worden vóór de datum van indiensttreding algemene achtergrondcontroles uitgevoerd ten aanzien van nieuwe werknemers, voor zover toegestaan door de toepasselijke wetgeving en passend bij de functie. De resultaten worden bijgehouden in het functiedossier van de medewerker. De criteria voor achtergrondcontroles variëren afhankelijk van de wetgeving, de functieverantwoordelijkheid en het leiderschapsniveau van de potentiële werknemer, en zijn onderhevig aan de gangbare en aanvaardbare best practices van het betreffende land.

4.6. Bewustzijns- en trainingsprogramma's over beveiliging

Nieuwe medewerkers worden tijdens de oriëntatie geïnformeerd over het beveiligingsbeleid en de Gedragscode en Bedrijfsethiek van GoTo. Deze verplichte jaarlijkse beveiligings- en privacytraining wordt gegeven aan relevant personeel en beheerd door het Team Talentontwikkeling met ondersteuning van het Beveiligingsteam.

Vaste en tijdelijke medewerkers van GoTo worden regelmatig geïnformeerd over richtlijnen, procedures, beleidsregels en normen op het gebied van beveiliging en privacy via verschillende mediakanalen. Dit zijn bijvoorbeeld onboardingkits voor nieuwe medewerkers, bewustmakingscampagnes, webinars met de CISO, een programma voor 'beveiligingskampioenen', en posters en ander materiaal dat minstens twee keer per jaar wordt uitgewisseld en waarop de methoden voor het beveiligen van gegevens, apparaten en faciliteiten worden geïllustreerd.

5 Privacy

GoTo neemt de privacy van zijn klanten, de abonnees van de GoTo-services en eindgebruikers zeer serieus, en zet zich in om relevante best practices voor gegevensverwerking en -beheer op een open en transparante manier bekend te maken.

5.1. AVG

De General Data Protection Regulation (GDPR), in het Nederlands de Algemene Verordening Gegevensbescherming (AVG), is de Europese wet om de privacy en gegevens van alle EU-ingezetenen te beschermen. De GDPR is voornamelijk bedoeld om burgers en ingezetenen controle te geven over hun persoonlijke gegevens en om het regelgevingskader EU-breed te vereenvoudigen. GoToAssist Remote Support v5 voldoet aan de toepasselijke bepalingen van GDPR. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo verklaart en garandeert hierbij dat het voldoet aan de California Consumer Privacy Act (CCPA). Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

5.3. Gegevensbescherming en Privacybeleid

GoTo heeft een uitgebreid en wereldwijd geldend Addendum gegevensverwerking ('DPA'; Data Processing Addendum) opgesteld dat beschikbaar is in het Engels en het Duits en die voldoet aan de eisen van de AVG en CCPA, en deze zelfs overstijgt, en waarin de verwerking van persoonsgegevens door GoTo is geregeld.

Concreet zijn in de DPA verschillende AVG-gerichte beveiligingsmechanismen voor de gegevensprivacy verwerkt, waaronder: (a) details over gegevensverwerking, openbaarmaking aan een andere gegevensverwerkende partij, enzovoorts, zoals vereist onder Artikel 28; (b) Europese modelbepalingen (standaardbepalingen voor overeenkomsten); en (c) de technische en organisatorische maatregelen voor gegevensbeveiliging van GoTo. Om in te spelen op het van kracht worden van de CCPA hebben we onze wereldwijde DPA bijgewerkt om de volgende aspecten hierin op te nemen: (a) aangepaste definities die aansluiten bij de CCPA; (b) recht op toegang en verwijdering; en (c) garanties dat GoTo de persoonlijke gegevens van onze gebruikers niet zal verkopen.

Voor bezoekers van onze webpagina's maakt GoTo in zijn Privacybeleid op de openbare website bekend welke soorten informatie worden verzameld en gebruikt om de Services te leveren, te onderhouden, te verbeteren en te beveiligen. Het bedrijf kan van tijd tot tijd het Privacybeleid bijwerken om wijzigingen in de verwerking van informatie en/of wijzigingen in de toepasselijke wetgeving weer te geven, maar zal op haar website melding maken van eventuele materiële wijzigingen voordat een dergelijke wijziging van kracht wordt.

5.4. Overdrachtskaders

GoTo heeft een krachtig wereldwijd gegevensbeschermingsprogramma ingericht, dat rekening houdt met de toepasselijke wetgeving, en rechtmatige internationale overdrachten binnen de volgende kaders ondersteunt:

5.4.1. Standaardcontractbepalingen

De Standaardbepalingen ('SCC's'; Standard Contractual Clauses) zijn gestandaardiseerde contractbepalingen die zijn erkend en aangenomen door de Europese Commissie. Het hoofddoel van deze bepalingen is om ervoor te zorgen dat alle persoonsgegevens die de Europese Economische Ruimte ('EER') verlaten, worden overgedragen in overeenstemming met de Europese wetgeving voor gegevensbescherming. GoTo heeft geïnvesteerd in een privacyprogramma van wereldklasse om te voldoen aan de strenge vereisten van de SCC's voor de overdracht van persoonsgegevens. GoTo biedt zijn klanten SCC's, soms ook bekend als de Modelbepalingen van de EU, die specifieke garanties bevatten aangaande de overdracht van persoonsgegevens voor de relevante GoTo-services. Ze zijn onderdeel van de wereldwijde DPA. Naleving van de SCC's garandeert dat klanten van GoTo veilig vrijuit gegevens kunnen overdragen vanuit de EER naar de rest van de wereld.

Aanvullende maatregelen

Naast de maatregelen die in deze TOM's zijn gespecificeerd, heeft GoTo de navolgende Veelgestelde vragen en de antwoorden daarop verzameld, om GoTo's aanvullende maatregelen te schetsen die zijn getroffen 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 de SCC's, te bespreken en te begeleiden.

5.4.2. Certificeringen voor de CBPR en PRP van de APEC

GoTo heeft ook de certificeringen 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 leider op het gebied van naleving van gegevensbeveiliging die is goedgekeurd door de APEC.

5.5. Klantcontent retourneren en verwijderen

Klanten van GoToAssist Remote Support V5 kunnen te allen tijde om teruggave of verwijdering van hun Klantcontent vragen via gestandaardiseerde interfaces. Als deze interfaces niet beschikbaar zijn of als GoTo anderszins niet in staat is om een dergelijk verzoek in te willigen, zal GoTo een commercieel redelijke poging doen om de Klant, afhankelijk van de technische haalbaarheid, te helpen bij het ophalen of verwijderen van zijn Content. De Klantcontent van GoToAssist Remote Support V5 zal binnen dertig (30) dagen na het verzoek van de Klant worden verwijderd. De Klantcontent in GoToAssist Remote Support v5 wordt automatisch binnen negentig (90) dagen na afloop of beëindiging van de laatste abonnementstermijn verwijderd. Op schriftelijk verzoek zal GoTo de verwijdering van dergelijke Content bevestigen.

5.6. Gevoelige gegevens

Hoewel GoTo ernaar streeft om alle Klantcontent te beschermen, zijn we door wettelijke en contractuele beperkingen genoodzaakt om het gebruik van GoToAssist Remote Support V5 voor bepaalde soorten informatie te beperken. Tenzij de Klant schriftelijke toestemming van GoTo heeft, mogen de volgende gegevens niet worden geüpload naar of gegenereerd in GoToAssist Remote Support V5 (noch door de Klant, noch door hun eindgebruikers):

- 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) van 1996, en daaraan gerelateerde 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 GoToAssist Remote Support V5 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.

5.7. Volgen en analyseren

GoTo verbetert zijn websites en producten voortdurend met behulp van webanalysetools van derden, waarmee GoTo inzichtelijk maakt hoe bezoekers zijn websites, desktopapplicaties en mobiele toepassingen gebruiken, en wat de voorkeuren en problemen van gebruikers zijn. Voor meer informatie verwijzen wij u naar het Privacybeleid.

6 Derde partijen

6.1. Gebruik van derde partijen

Als onderdeel van de interne beoordeling en processen met betrekking tot leveranciers en derde partijen, kunnen de evaluaties van leveranciers door meerdere teams worden uitgevoerd, afhankelijk van de relevantie en toepasbaarheid. Het Beveiligingsteam evalueert alle relevante leveranciers die op informatiebeveiliging gebaseerde services leveren, en beoordeelt eveneens de hostingfaciliteiten van derde partijen. GoTo's teams Juridische zaken en Inkoop kunnen contracten, werkomschrijvingen en serviceovereenkomsten evalueren, indien vereist volgens interne processen. Er worden indien nodig passende nalevingsdocumentatie of -rapporten verkregen die ten minste jaarlijks worden geëvalueerd, om ervoor te zorgen dat de controleomgeving adequaat functioneert en alle noodzakelijke controles op gebruikersoverwegingen worden uitgevoerd. Daarnaast moeten derde partijen die gevoelige of vertrouwelijke gegevens hosten of die toegangsmachtigingen krijgen van GoTo, een schriftelijk contract ondertekenen waarin de relevante vereisten voor toegang tot of opslag of behandeling van de informatie (zoals van toepassing) zijn opgenomen.

6.2. Best practices bij contractering

Om de bedrijfscontinuïteit te waarborgen en ervoor te zorgen dat er passende maatregelen worden getroffen om de vertrouwelijkheid en integriteit van bedrijfsprocessen en gegevensverwerking van derden te beschermen, beoordeelt GoTo allereerst de voorwaarden van relevante derde partijen. Vervolgens wordt in samenwerking met de teams Beveiliging, Juridische Zaken, Inkoop en Financiën (in elk geval, en naar behoefte) beslist om ofwel GoTo's goedgekeurde inkoopsjablonen te gebruiken, ofwel om te onderhandelen over dergelijke voorwaarden van derden, indien dat nodig blijkt.

7 Contact opnemen met GoTo

Klanten kunnen contact opnemen met GoTo op https://support.goto.com voor algemene vragen of privacy@goto.com voor privacy-gerelateerde vragen.

8 Bijlage – Terminologie

Medewerkers: GoToAssist Remote Support V5-gebruiker, die GoToAssist Remote Support V5-sessies aanmaakt om klanten technische ondersteuning te bieden via externe weergave, besturing op afstand, en het delen van camera's.

Online console voor Medewerkers: Een online toepassing die op een pc, Mac, tablet of Chromebook-apparaat van de Medewerker draait in een van de ondersteunde browsers (Chrome, Firefox, Safari) en verbinding maakt met de GoToAssist Remote Support V5-service. Hiermee kunnen medewerkers GoToAssist Remote Support V5-sessies aanmaken en uitvoeren, evenals verschillende functies voor accountbeheer, servicebeheer en rapportage.

Desktopconsole voor Medewerkers: Een desktoptoepassing die op MacOS en Windows computers draait en verbinding maakt met de GoToAssist Remote Support V5-service. De Desktopconsole voor Medewerkers maakt gebruik van native GoToAssist Remote Support

V5-technologie, Qt en de Chromium-webengine. Deze console biedt dezelfde functionaliteit als de Online console voor Medewerkers, maar heeft een native look en feel.

Beheerde sessie: Een ondersteuningssessie waarbij de Klant aanwezig is tijdens de sessie en eraan kan deelnemen.

Klant: Een persoon die technische support ontvangt van de Medewerker via een sessie met GoToAssist Remote Support V5.

Desktopapp voor Eindgebruikers: Een desktopapplicatie die op de computer van de Eindgebruiker (Windows of Mac) draait en via de GoToAssist Remote Support V5-service verbinding maakt met een GoToAssist Remote Support V5-sessie. De applicatie biedt besturing op afstand en andere geavanceerde functionaliteit, evenals de mogelijkheid om App voor onbeheerde Eindgebruikers op de computer van de klant te installeren.

Klanteneindpunt: Een collectieve term die verwijst naar elk klanteneindpunt; zoals de Online app voor Eindgebruikers, de Desktopapp voor Eindgebruikers, de Mobiele App voor Eindgebruikers, en de App voor onbeheerde Eindgebruikers

Mobiele app voor Eindgebruikers: mobiele applicatie (Android en iOS) die op het mobiele/tabletapparaat van de klant draait en via de GoToAssist Remote Support V5-service Service verbinding kan maken met een GoToAssist Remote Support V5-sessie. De app biedt mogelijkheden voor externe weergave (Android en iOS) en besturing op afstand (alleen Android).

Online app voor Eindgebruikers: Een online applicatie die in elke ondersteunde browser op de computer/het mobiele apparaat van de Eindgebruiker (Windows of Mac) draait, en via de GoToAssist Remote Support V5-service verbinding maakt met een GoToAssist Remote Support V5-sessie. De app biedt mogelijkheden voor chatten, externe weergave, en het delen van camera's, evenals de mogelijkheid om de sessie op elk moment op afstand te besturen, door de Desktopapp voor Eindgebruikers te downloaden of de Mobiele app voor Eindgebruikers te installeren.

Mediaservice: Een vloot van load-balanced, wereldwijd verspreide servers die verschillende unicast- en multicast-communicatieservices bieden, met hoge beschikbaarheid en op basis van WebRTC-protocollen.

GoToAssist Remote Support V5-sessies: beheerde chat, externe weergave, besturing op afstand, het delen van camera's, en onbeheerde besturing op afstand.

GoToAssist Remote Support V5-service: Een vloot van load-balanced, wereldwijd gedistribueerde servers die veilige toegang bieden tot de Online console voor Medewerkers en Eindpunten van de Klant via een versleutelde WebSocket-verbinding en API-aanroepen.

App voor onbeheerde Eindgebruikers: Een installeerbare desktopapplicatie (Windows en Mac) die op de achtergrond op de computer van de Eindgebruiker draait. Deze app kan ook de Desktopapp voor Eindgebruikers downloaden en uitvoeren om verbinding te maken met een geautoriseerde Onbeheerde Sessie.

Onbeheerde Sessie: supportsessie waarbij de Klant niet aanwezig is. De sessie wordt geïnitieerd en tot stand gebracht door de Medewerker zonder tussenkomst van de Klant via een geautoriseerde App voor onbeheerde Eindgebruikers.