Rapport

GoToAssist® CORPORATE

Beveiligingsrapport voor Citrix GoToAssist Corporate

GoToAssist Corporate biedt krachtige maatregelen voor end-to-end gegevensbeveiliging, die bescherming bieden tegen zowel passieve als actieve pogingen tot inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van data.

CITRIX® | online

Inhoudsopgave

Doel en doelgroep 3
Inleiding 3
Servicestructuur van GoToAssist 4
Definities 5
Toepassingsbeveiliging 6
Verificatie 7
Beveiliging van de pc en de gegevens van de klant 7
Functies voor communicatiebeveiliging 8
Vertrouwelijkheid en integriteit van communicatie 9
Beveiliging op de TCP-laag 9
Multicast packet security layer (MPSL) 10
Firewall- en proxy-compatibiliteit 11
Beveiligingsfuncties van het endpoint-systeem 12
Ondertekende endpoint-software 12
Cryptografische subsysteemimplementatie 12
Beveiligingsfuncties van de hosted infrastructuur 13
Schaalbare en betrouwbare infrastructuur 13
Fysieke beveiliging 13
Netwerkbeveiliging 13
Privacy van de klant 13
Gebruik in gereguleerde omgevingen 14
Conclusie 14
Bijlage: Naleving van de beveiligingsstandaarden 15

Doel en doelgroep

Deze handleiding is bestemd voor klanten van Citrix® GoToAssist® Corporate en andere belanghebbenden die willen begrijpen hoe GoToAssist in hun omgeving de risico's en naleving op het gebied van gegevensbeveiliging kan beïnvloeden.

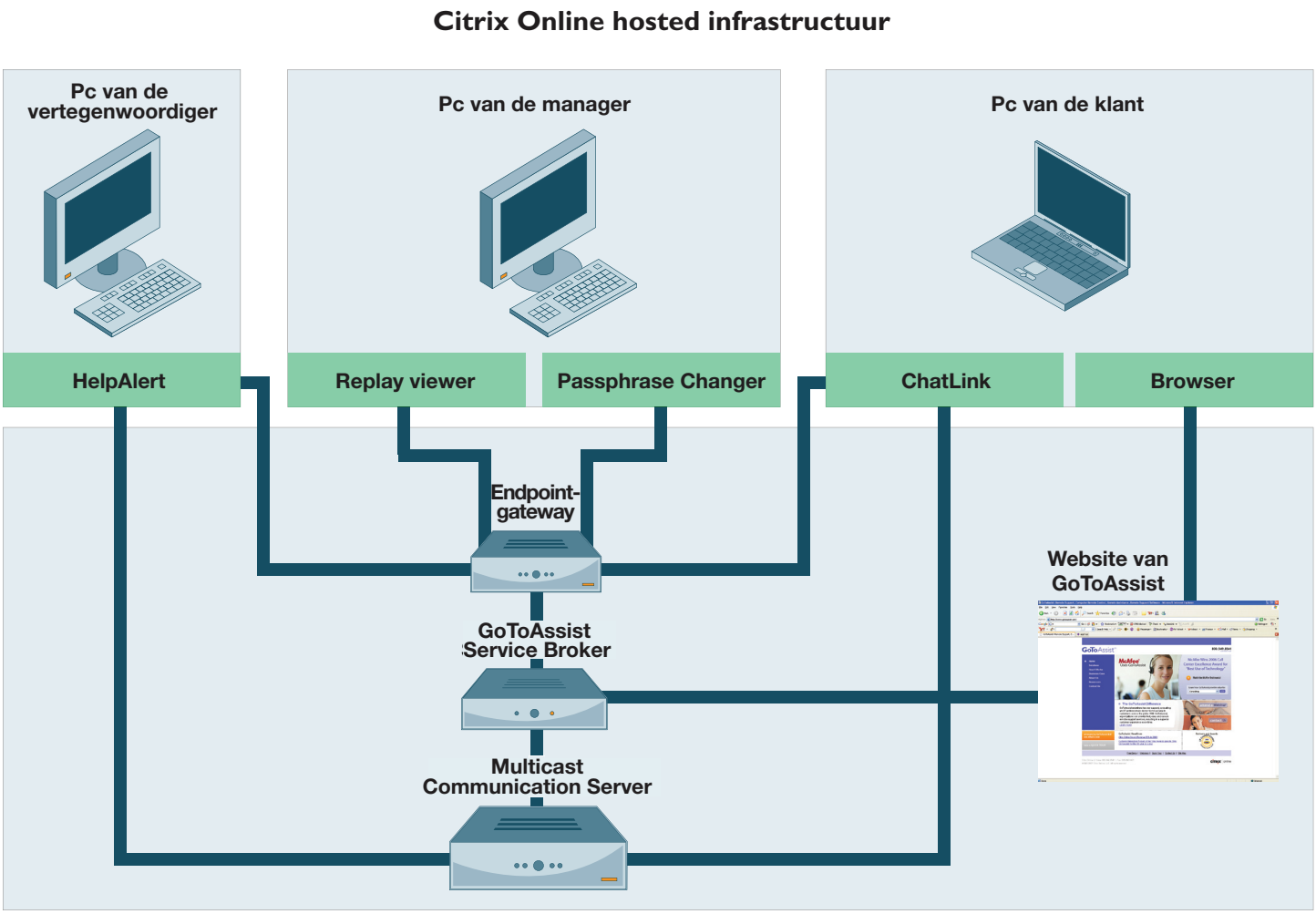
Inleiding

GoToAssist Corporate is een hosted service waarmee Windows-pc's op afstand ondersteuning kunnen ontvangen. Met GoToAssist Corporate kan een gebruiker ondersteuning vragen van een servicemedewerker en deze servicemedewerker vervolgens de computer op afstand laten bekijken en eventueel bedienen.

In dit document worden de functies voor gegevensbeveiliging van GoToAssist Corporate besproken. De lezer wordt geacht te beschikken over basiskennis van het product en zijn functies. Ga voor aanvullende informatie over GoToAssist Corporate naar www.citrixonline.com of neem contact op met een vertegenwoordiger van Citrix Online.

Servicestructuur van GoToAssist Corporate

Onderstaande afbeelding geeft een schematisch overzicht van alle belangrijke servicecomponenten en communicatiekanalen van GoToAssist Corporate.



Definities

HelpAlert: uitvoerbaar win32-bestand op de computer van de servicemedewerker waarmee de medewerker binnenkomende query's van klanten kan ontvangen en beantwoorden.

ChatLink: endpoint-toepassing waarmee de klant en de servicemedewerker via tekst kunnen communiceren.

Browser: standaardwebbrowser zoals Firefox, Internet Explorer etc.

Replay viewer: endpoint-toepassing waarmee managers op bedrijfs-, team- en afdelingsniveau opgenomen GoToAssist Corporate-sessies kunnen afspelen. U kunt gedeelde schermen, chatsessies en diagnostische informatie afspelen met Replay viewer.

Passphrase Changer: endpoint-toepassing waarmee u het wachtwoord kunt wijzigen dat wordt gebruikt om de toegang tot de opgenomen sessies te beveiligen.

Website van GoToAssist: webtoepassing waarmee u toegang krijgt tot de GoToAssist-webpagina en de online interne en externe beheerportals.

GoToAssist Service Broker: webtoepassing voor GoToAssist Corporate-accountbeheer en servicebeheer, met vaste opslag- en rapportagefuncties.

Multicast Communication Server: één van de wereldwijd verspreide servers die worden gebruikt om een scala van breed beschikbare unicast en multicast communicatiediensten te realiseren.

Endpoint-gateway: een speciale gateway die door meerdere endpoint-toepassingen wordt gebruikt om met behulp van externe procedure-oproepen veilig toegang te krijgen tot de GoToAssist Service Broker.

Toepassingsbeveiliging

GoToAssist Corporate biedt toegang tot een uitgebreid pakket hulpmiddelen en services. Het maakt hierbij gebruik van een op rollen gebaseerd toegangscontrolesysteem dat onder toezicht staat van de verschillende serviceonderdelen. De rollen en bijbehorende termen worden in onderstaande tabel gedefinieerd:

Rollen

Beheerder	De Citrix Online-medewerker die groepen en portals maakt in het GoToAssist Corporate Management Center van een bedrijf. Beheerders kunnen GoToAssist Corporate-accounts, portals, bedrijfsmanagers en teammanagers maken, aanpassen en verwijderen, alsmede abonnementsgegevens en prijsgegevens aanpassen en overige administratieve functies uitvoeren.
Bedrijf	Klant van GoToAssist Corporate waarvoor portals worden opgezet.
Bedrijfsmanager	Een medewerker van het bedrijf van de klant die toegang heeft tot het GoToAssist Corporate Management Center. Mag accounts, portals, teams en medewerkers van het account aanpassen.
Klant	De persoon in het bedrijf van de klant die ondersteuning aanvraagt via GoToAssist Corporate.
Groep/team	Verzameling van servicemedewerkers die aan een specifieke portal zijn toegewezen. Elke servicemedewerker behoort tot exact één groep of team, elke groep of elk team wordt toegewezen aan exact één portal. Groepen/teams bevatten enkele standaardinstellingen voor servicemedewerkers.
Groepsmanager/teammanager	Een medewerker bij de klant, die van een bedrijfsmanager de bevoegdheid heeft gekregen om bepaalde aspecten van een team en de portal en servicemedewerkers van dat team aan te passen.
Vertegenwoordiger	De servicemedewerker die query's van de klant beantwoordt via HelpAlert.

Verificatie

Beheerders, managers en servicemedewerkers van GoToAssist Corporate worden door middel van een accountnaam en een sterk wachtwoord geverifieerd.

Wachtwoorden zijn gebonden aan de volgende regels:

Sterke wachtwoorden: een sterk wachtwoord is tussen 8 en 32 karakters lang en moet tenminste drie van de volgende vier tekensoorten bevatten: hoofdletters [A-Z], kleine letters [a-z], cijfers [0-9], en speciale symbolen [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Sterke wachtwoorden mogen niet gelijk zijn aan de aanmeldingsnaam of de voor- of achternaam die bij het account hoort. De kwaliteit van het wachtwoord wordt getest bij het eerste gebruik of bij wijziging van het wachtwoord.

Geldigheidsperiode wachtwoord: de geldigheidsperiode van het wachtwoord is in te stellen (min.: 10 dagen, max.: 120 dagen, standaard: 90 dagen). Als de houder van het wachtwoord zich aanmeldt en het wachtwoord is verlopen, is de houder van het wachtwoord gedwongen zijn of haar wachtwoord te wijzigen.

Wachtwoordgeschiedenis: er wordt een geschiedenis van wachtwoorden bijgehouden. Een wachtwoord kan niet gewijzigd worden in een wachtwoord dat al in de wachtwoordgeschiedenis bestaat. De grootte van de wachtwoordgeschiedenis is in te stellen (min.: 1, max.: 5, standaard: 3).

Accountblokkering: na drie opeenvolgende mislukte aanmeldpogingen krijgt het account een verplichte zogenaamde zachte blokkeringsstatus. Dit betekent dat de houder van het account zich gedurende een in te stellen tijd niet kan aanmelden (min.: 5 minuten, max.: 30 minuten, standaard: 5 minuten). Na afloop van de blokkeringsperiode kan de houder van het account zich weer op zijn of haar account aanmelden.

Indien gewenst kunt u ook een zogenaamde harde blokkering instellen. Na een in te stellen aantal mislukte aanmeldpogingen krijgt het account dan de zogenaamde harde blokkeringsstatus. Dit houdt in dat de houder van het account zich niet meer kan aanmelden totdat zijn of haar wachtwoord opnieuw is ingesteld door een andere houder van een account met speciale bevoegdheden. Het account krijgt de harde blokkeringsstatus na een in te stellen aantal aanmeldpogingen (min.: 10, max.: 50, standaard: 10).

Beveiliging van de pc en de gegevens van de klant

Het op toestemming gebaseerde toegangscontrolemodel dat de toegang tot de pc en de gegevens van de klant hierin beveiligt, vormt een essentieel onderdeel van de beveiliging van GoToAssist Corporate.

Ten eerste moeten GoToAssist Corporate-sessies gestart worden door de klant. GoToAssist Corporate is niet ontwikkeld voor supportscenario's zonder toezicht.

Ten tweede wordt de klant altijd om toestemming gevraagd voordat er wordt gestart met schermdeling, externe pc-besturing of het overbrengen van bestanden, diagnostische gegevens of andere informatie.

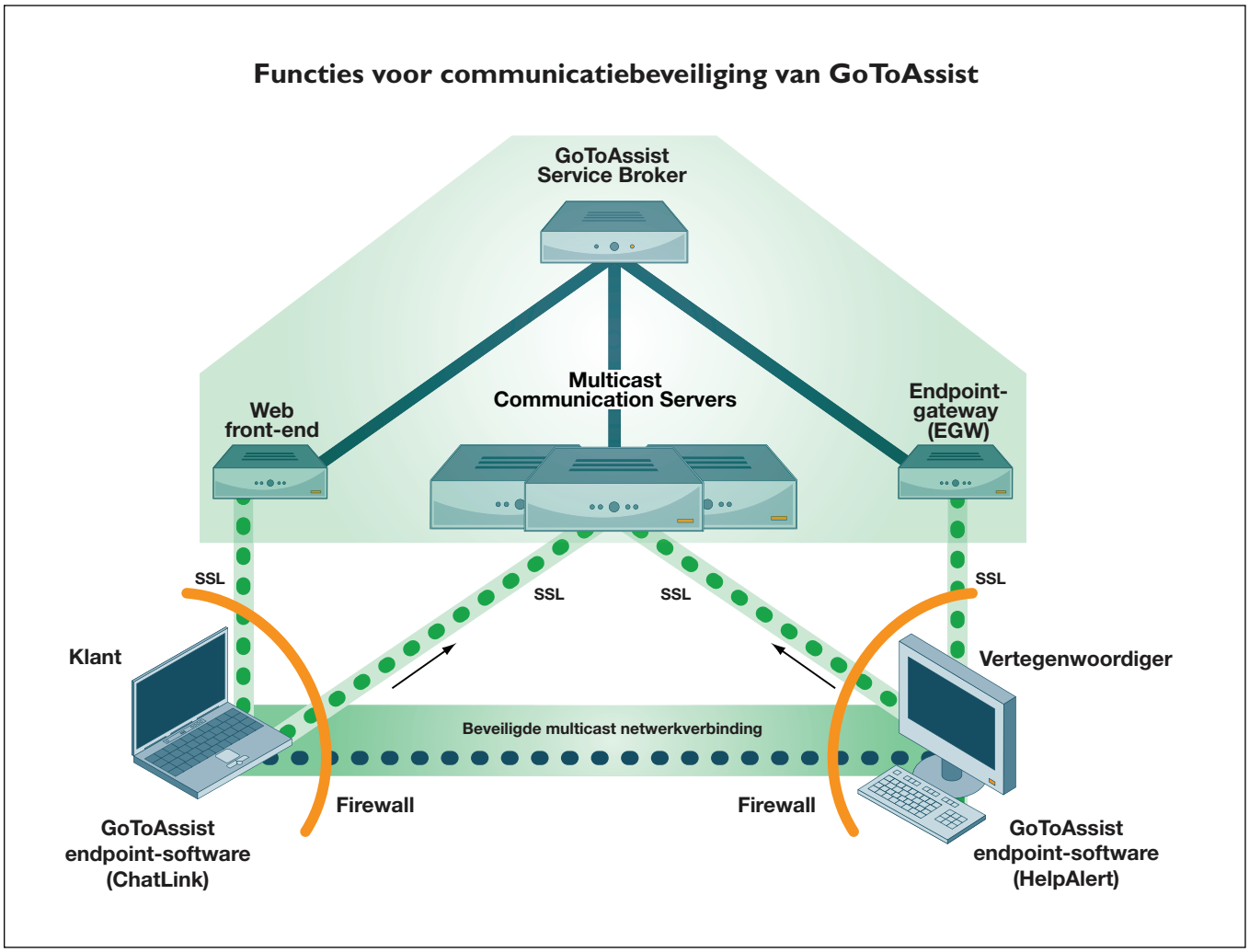
Als de klant toestemming heeft gegeven voor externe pc-besturing en schermdeling, kan hij te allen tijde zien wat de servicemedewerker doet. Verder kan de klant op elk moment de besturing weer overnemen of de sessie beëindigen.

Lokale beveiligingscontroles op de pc van de klant worden nooit opgeheven; de klant of de servicemedewerker moet alle gebruikelijke verificatiegegevens voor Windows of toepassingen invoeren.

Bovendien worden alle verbindingsactiviteiten bijgehouden en kunnen schermdeling- en chatsessies optioneel worden opgenomen en afgespeeld voor controle op een later tijdstip.

Functies voor communicatiebeveiliging

Communicatie tussen deelnemers in een GoToAssist Corporate-sessie vindt plaats via een multicast netwerkstack, die logisch over de conventionele TCP/IP-stack in elke pc van de gebruiker wordt geplaatst. Dit netwerk bestaat uit een verzameling Multicast Communication Servers (MCS) onder beheer van Citrix Online. In de onderstaande afbeelding is de communicatiestructuur samengevat.



Deelnemers aan GoToAssist Corporate-sessies (“endpoints”) communiceren via comunicatieservers en gateways van de CitrixOnline-infrastructuur via uitgaande TCP/IP-verbindingen op de poorten 8200, 443 en 80. Omdat GoToAssist Corporate een hosted online service is, kunnen deelnemers zich overal op internet bevinden: in een willekeurig kantoor, thuis, in een businesscenter of op het netwerk van een ander bedrijf.

Toegang tot de GoToAssist Corporate-service biedt maximale flexibiliteit en connectiviteit. Altijd, overal. Om de vertrouwelijkheid en integriteit van bedrijfscommunicatie te kunnen garanderen, beschikt GoToAssist Corporate echter ook over krachtige functies ter beveiliging van communicatie.

Vertrouwelijkheid en integriteit van communicatie

GoToAssist Corporate biedt krachtige maatregelen voor sterke end-to-end gegevensbeveiliging, die bescherming bieden tegen zowel passieve als actieve pogingen tot inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van data. Alle GoToAssist Corporate-verbindingen zijn “end-to-end” gecodeerd en alleen toegankelijk voor bevoegde deelnemers van supportsessies.

De gegevens van de schermdeling, keyboard-/muisbesturing en tekstchats worden nooit in een ongecodeerde vorm weergegeven tijdens een tijdelijk verblijf op Citrix Online-communicatieservers of tijdens de overdracht tussen openbare of beveiligde netwerken.

Als de opnamefunctie is uitgeschakeld, wordt de sleutel van de GoToAssist Corporate-sessie in geen enkele vorm op een Citrix Online-server opgeslagen. Een indringer op een server kan dus op geen enkele manier de sleutel van eventueel onderschepte gecodeerde gegevens bekendmaken.

Als de opnamefunctie is ingeschakeld, worden de gegevens van de chatsessies, schermdeling en schermweergave gecodeerd opgeslagen. De sessiesleutel wordt ook opgeslagen, maar deze wordt beschermd door een 1024-bits RSA-openbare/persoonlijke sleutelcodering. De sessiesleutel wordt door middel van een portalspecifieke openbare sleutel gecodeerd voordat deze wordt opgeslagen. Voor het afspelen hebt u drie dingen nodig: de sessieopname, de gecodeerde sessiesleutel en de persoonlijke sleutel van de portal.

Sterk gecodeerde elementen voor communicatiebeveiliging kunnen op twee lagen geïmplementeerd worden: TCP en MPSL (Multicast Packet Security Layer).

Beveiliging op de TCP-laag

Er worden IETF-normatieve SSL- (Secure Sockets Layer) en TLS-protocollen (Transport Layer Security) gebruikt om de communicatie tussen de endpoints te beveiligen. Om maximale bescherming te bieden tegen afluisteren, manipulatie of herhaald afspelen, is 1024-bits RSA met 128-bits AES-CBC en HMAC-SHA1 de enige SSL-cipher-suite die wordt ondersteund voor TCP-verbindingen met andere locaties dan websites. Voor maximale compatibiliteit met vrijwel elke webbrowser op vrijwel alle desktops ondersteunt de GoToAssist-website inkomende verbindingen met vrijwel alle ondersteunde SSL-cipher-suites. Voor optimale beveiliging raadt Citrix Online haar klanten aan hun browsers zodanig te configureren dat, waar mogelijk, standaard sterke codering wordt gebruikt, en om verder altijd de laatste beveiligingspatches voor het besturingssysteem en de browser te installeren.

Bij het maken van SSL/TLS-verbindingen met de GoToAssist-website en tussen GoToAssist Corporate-componenten, worden Citrix Online-servers door middel van openbare VeriSign/Thawte-certificaten bij de klant geverifieerd. Voor aanvullende bescherming tegen aanvallen op de infrastructuur wordt wederzijdse verificatie op basis van certificaten ingezet op alle server-to-server-verbindingen (bijv. MCS – MCS, MCS – verbindingsserver). Deze sterke verificatiemaatregelen voorkomen dat mogelijke aanvallers zich voordoen als infrastructuurservers of tussenbeide komen tijdens supportsessies.

Multicast packet security layer (MPSL)

Aanvullende functies bieden complete “end-to-end” beveiliging voor multicast pakketgegevens, die naast de beveiligingsfuncties van SSL/TLS functioneren. Met name worden alle multicast sessiegegevens beveiligd door “end-to-end” coderings- en integriteitsmechanismen. Op deze manier wordt voorkomen dat iemand met toegang tot onze communicatieservers kan meeluisteren met een GoToAssist Corporate-sessie of gegevens kan manipuleren zonder ontdekt te worden. Dit extra niveau van vertrouwelijkheid en integriteit van communicatie maakt GoToAssist Corporate uniek. Bedrijfscommunicatie is nooit zichtbaar voor een derde partij; noch voor gebruikers die niet voor een bepaalde supportsessie zijn uitgenodigd, noch voor Citrix Online zelf.

De MPSL-sleutel wordt samengesteld door een op een openbare sleutel gebaseerde, door SRP-6 geverifieerde sleutelindeling te gebruiken. Hierbij wordt de coderingssleutel gegenereerd middels een 1024-bits module. (Zie http://srp.stanford.edu/design.html.) Deze coderingssleutel wordt vervolgens met behulp van het AES-algoritme IETF RFC 3394 gebruikt voor de symmetrische sleutelgroepdistributie. Alle sleutelgegevens worden gegenereerd met een FIPS-compatibele PRNG (Pseudorandom Number Generator), die bevolkt is met entropiegegevens die tijdens de uitvoering uit meerdere bronnen op de hostcomputer worden verzameld. Met deze krachtige, dynamische methoden voor het genereren en uitwisselen van sleutels bent u verzekerd van een hoog beveiligingsniveau, die het raden en kraken van sleutelcombinaties vrijwel onmogelijk maakt.

MPSL beveiligt multicast pakketgegevens verder tegen afluisteren met behulp van 128-bits AES-codering in Counter Mode. Platte tekstgegevens worden gecomprimeerd voor ze worden gecodeerd met behulp van onze eigen krachtige technieken voor de optimalisatie van bandbreedte. Beveiliging van gegevensintegriteit wordt bereikt door het opnemen van een controlewaarde voor integriteit; deze wordt gegenereerd middels het HMAC-SHA-1-algoritme. Omdat GoToAssist Corporate gebruikmaakt van zeer sterke, op industrienormen gebaseerde coderingsmaatregelen, kunnen klanten erop vertrouwen dat hun multicast supportsessiegegevens beveiligd zijn tegen onbevoegde publicatie of onontdekte manipulatie.

Bovendien zijn aan deze essentiële functies voor communicatiebeveiliging geen extra kosten verbonden, gaan de prestaties niet achteruit en leveren ze geen problemen op bij het gebruik. Hoge prestaties en op normen gebaseerde beveiliging van gegevens is een ingebouwde eigenschap van elke GoToAssist Corporate-sessie.

Hoofdpunten

- De vertrouwelijkheid van de sessie wordt bewaakt middels 128-bits AES-codering.
- De initiële sessiesleutel wordt willekeurig gekozen door de verbindingsserver en vervolgens doorgegeven aan de endpoints via geverifieerde en gecodeerde kanalen.
- De endpoints bepalen vervolgens onder elkaar een uiteindelijke sessiesleutel.
- De uiteindelijke sessiesleutel is niet bekend bij de verbindingsserver.
- Communicatieservers verzenden alleen gecodeerde pakketten en beschikken niet over de coderingssleutel van de sessie.
- De GoToAssist Corporate-architectuur minimaliseert het risico op blootstelling van de sessiegegevens en maximaliseert de mogelijkheid om medewerkers aan gebruikers te koppelen die hulp nodig hebben.

Firewall- en proxy-compatibiliteit

Net als de overige onlineproducten van Citrix beschikt GoToAssist Corporate over een ingebouwde beheerlogica voor proxydetectie en -verbindingen. Deze beheerlogica zorgt ervoor dat de software automatisch wordt geïnstalleerd, zonder dat daarvoor een complexe configuratie/herconfiguratie van het netwerk is vereist, en maximaliseert tevens de gebruikersproductiviteit. Firewalls en proxy's die al op uw netwerk zijn geïnstalleerd hoeven voor het gebruik van GoToAssist Corporate normaal gesproken niet opnieuw te worden geconfigureerd.

Wanneer de endpoint-software van GoToAssist Corporate wordt gestart, wordt via de EGW (Endpoint Gateway) contact gemaakt met de GoToAssist-verbindingsserver door een of meer uitgaande SSL-beveiligde TCP-verbindingen op de poorten 8200, 443 en/of 80 te starten. De verbinding die hier het eerst op reageert, wordt gebruikt en de andere verbindingen worden genegeerd. Deze verbinding vormt de basis voor deelname aan alle toekomstige ondersteuningssessies door communicatie tussen de hosted servers en de computer van de gebruiker mogelijk te maken.

Als een gebruiker deel wil gaan nemen aan een ondersteuningssessie, genereert de endpoint-software van GoToAssist Corporate een of meer extra verbindingen met de Citrix Online-communicatieservers, waarbij opnieuw gebruik wordt gemaakt van SSL-beveiligde TCP-verbindingen op de poorten 8200, 443 en/of 80. Deze verbindingen verzenden de gegevens van de actieve ondersteuningssessie.

Voor een optimale verbinding worden door de endpoint-software een of meer kortstondige niet-SSL-beveiligde TCP-verbindingen gestart op de poorten 8200, 443 en/of 80. Deze 'netwerkprobes' bevatten geen vertrouwelijke gegevens of gegevens die kunnen worden misbruikt en vormen dan ook geen risico met betrekking tot het openbaar raken van vertrouwelijke gegevens.

Op www.citrixonline.com/iprange vindt u de volledige lijst met de IP-adressen die door Citrix Online worden gebruikt.

Door het lokale netwerk automatisch in te laten stellen door uitsluitend uitgaande verbindingen te gebruiken en een poort te kiezen die al voor de meeste firewalls en proxy's is geopend, bent u verzekerd van een uitstekende compatibiliteit tussen GoToAssist Corporate en uw bestaande netwerkbeveiligingsmaatregelen. In tegenstelling tot bepaalde andere producten hoeft u met GoToAssist Corporate de bestaande netwerkbeveiliging niet uit te schakelen om communicatie voor online ondersteuningssessies mogelijk te maken. Zo worden zowel de compatibiliteit als de algehele netwerkbeveiliging gemaximaliseerd.

Beveiligingsfuncties van het endpoint-systeem

Software voor online ondersteuningssessies moet compatibel zijn met een groot aantal verschillende computeromgevingen, maar moet tegelijkertijd een veilig endpoint vormen op de computer van de gebruiker. GoToAssist Corporate bereikt dit door gebruik te maken van uitvoerbare bestanden die van internet worden gedownload en die voorzien zijn van geavanceerde coderingsmaatregelen.

Ondertekende endpoint-software

De endpoint-software van GoToAssist Corporate is een uitvoerbaar Win32-bestand dat naar de computer van de gebruiker wordt gedownload. Met behulp van een digitaal ondertekende Java-applet wordt het downloadproces beheerd en wordt de integriteit geverifieerd van de endpoint-software die van de Citrix-servers wordt gedownload. Hiermee wordt voorkomen dat de gebruiker per ongeluk een trojan of andere schadelijke software installeert die zich voordoet als endpoint-software van GoToAssist Corporate.

De endpoint-software omvat een aantal uitvoerbare Win32-bestanden en dynamisch gekoppelde bibliotheken. Om de veiligheid van de software te waarborgen worden er door Citrix Online tijdens de ontwikkeling en de implementatie strikte kwaliteitscontroles en configuratiebeheerprocedures opgevolgd. De endpoint-software maakt geen extern beschikbare netwerkinterfaces openbaar en kan niet door schadelijke software of virussen worden gebruikt om externe systemen te misbruiken of te infecteren. Hierdoor worden de computers van deelnemers aan een ondersteuningssessie beschermd tegen infecties afkomstig van een besmette host die door een andere deelnemer wordt gebruikt.

Cryptografische subsysteemimplementatie

Alle cryptografische functies en beveiligingsprotocollen die door de endpoint-clientsoftware van GoToAssist Corporate worden gebruikt, worden door middel van geavanceerde Certicom Security Builder® Crypto™- en Certicom Security Builder® SSL™-bibliotheken geïmplementeerd. Dit zorgt voor superieure prestaties. (Zie www.certicom.com voor meer informatie.)

Het gebruik van de cryptografische bibliotheken is volledig beperkt tot de endpoint-toepassing van GoToAssist Corporate; de andere software die op de computer wordt uitgevoerd heeft geen toegang tot de externe API's. Alle coderings- en integriteitsalgoritmen, de sleutelgrootte en overige cryptografische beleidsparameters worden tijdens de samenstelling van de toepassing op een statische manier gecodeerd. Omdat er geen cryptografische instellingen zijn die door de eindgebruiker kunnen worden geconfigureerd, wordt voorkomen dat gebruikers het beveiligingsniveau van een GoToAssist Corporate-sessie per ongeluk kunnen verlagen. Een bedrijf dat gebruikmaakt van GoToAssist Corporate is ervan verzekerd dat het beveiligingsniveau van een online ondersteuningssessie voor alle deelnemende endpoints even hoog is, ongeacht wie elke computer bestuurt.

Beveiligingsfuncties van de hosted infrastructuur

Citrix GoToAssist Corporate maakt gebruik van een ASP-model (Application Service Provider) dat speciaal is ontwikkeld om een krachtige en veilige omgeving te garanderen, terwijl het systeem tegelijkertijd naadloos integreert met het bestaande bedrijfsnetwerk en de beveiligingsinfrastructuur.

Schaalbare en betrouwbare infrastructuur

De servicearchitectuur van Citrix Online is speciaal ontwikkeld voor optimale prestaties, betrouwbaarheid en schaalbaarheid. De GoToAssist Corporate-service wordt aangestuurd door algemeen gebruikte, hoogwaardige servers en netwerkapparatuur waarop de allernieuwste beveiligingspatches zijn geïnstalleerd. De architectuur omvat ook redundante schakelaars en routers, zodat u ervan verzekerd bent er nooit een storing zal optreden. Geclusterde servers en back-upsystemen dragen bij aan een naadloze verwerking van de toepassingsprocessen – zelfs bij een zware belasting of als het systeem uitvalt. Voor optimale prestaties verdeelt de GoToAssist Service Broker de client/server-sessies over geografisch gedistribueerde communicatieservers.

Fysieke beveiliging

De web-, toepassings-, communicatie- en databaseservers van GoToAssist Corporate bevinden zich in beveiligde datacenters op verschillende locaties. Fysieke toegang tot de servers is strikt beperkt en daarop wordt constant toezicht gehouden. Alle faciliteiten zijn voorzien van redundante stroomvoorziening en er worden omgevingscontroles uitgevoerd.

Netwerkbeveiliging

Citrix Online maakt gebruik van firewall-, router- en VPN-toegangscontroles om onze eigen servicenetwerken en backend-servers te beveiligen. De infrastructuurbeveiliging wordt constant in de gaten gehouden en de beveiliging wordt regelmatig op kwetsbaarheid getest door onze interne beveiligingsafdeling en externe partijen.

Privacy van de klant

Omdat het vertrouwen van onze gebruikers voor ons een prioriteit is, neemt Citrix Online het beschermen van uw privacy zeer serieus. Op onze servicewebsite www.citrixonline.com vindt u een koppeling naar het huidige privacybeleid van Citrix GoToAssist Corporate.

Gebruik in gereguleerde omgevingen

Vanwege de uitgebreide beveiligingscontroles voor toepassingen en communicatie, zoals het door de klant geautoriseerde, op toestemming gebaseerde beveiligingsmodel, kunt u GoToAssist Corporate zorgeloos gebruiken op computers en toepassingen in omgevingen die onder de HIPAA-, de Gramm-Leach-Bliley Act- of de Sarbanes-Oxley-regelgeving vallen. Daarbij staan vertrouwelijkheid en gegevensintegriteit voorop.

Citrix Online raadt organisaties aan alle standaard en configureerbare beveiligingsfuncties van GoToAssist Corporate nauwgezet te controleren op de vereisten die van toepassing zijn op de organisatie, de gebruikers en het beleid, om te bepalen welke functies moeten worden ingeschakeld en hoe deze moeten worden geconfigureerd. In sommige gevallen is het aan te bevelen gebruikers te voorzien van aanvullende gebruiksrichtlijnen om ervoor te zorgen dat de beveiliging voor alle belanghebbenden in orde is. U kunt bij het professionele serviceteam van Citrix Online terecht voor aanvullende informatie met betrekking tot de implementatie en het gebruik van GoToAssist Corporate.

Conclusie

Dankzij de intuïtieve en beveiligde interface en functies van GoToAssist Corporate beschikt u over de meest efficiënte oplossing voor het houden van online ondersteuningssessies. Met GoToAssist Corporate kunnen ondersteuningsmedewerkers, adviseurs en IT-professionals snel en eenvoudig wereldwijd technische hulp bieden aan klanten.

Dankzij deze veilige en betrouwbare omgeving biedt de hosted-servicearchitectuur van Citrix Online achter de schermen ondersteuning voor transparante, meervoudige samenwerking. Zoals u in dit document kunt zien, bevordert GoToAssist Corporate het gebruiksgemak en de flexibiliteit zonder dat de integriteit, de privacy of het beheer van de bedrijfscommunicatie of de IT-apparatuur daaronder lijdt.

Bijlage:
Naleving van de beveiligingsstandaarden

GoToAssist Corporate is compatibel met de volgende algemene en Amerikaanse overheidsstandaarden voor cryptografische algoritmen en beveiligingsprotocollen:

- Het TLS/SSL-protocol, versie 1.0 IETF RFC 2246
- AES (Advanced Encryption Standard), FIPS 197
- (FIPS-gevalideerde implementatie, NIST-certificaat 175)
- AES-cipher-suites voor TLS, IETF RFC 3268
- AES-algoritme voor de coderingssleutel, IETF RFC 3394
- RSA, PKCS #1
- SHA-1, FIPS 180-1 (FIPS-gevalideerde implementatie, NIST-certificaat 89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- PRNG (Pseudorandom Number Generation), ANSI X9.62 en FIPS 140-2

Citrix Online

Divisie Citrix Online

Productinformatie:
www.citrixonline.com

Verkoopinformatie:
Benelux@citrixonline.com
Telefoon: +353 (0) 1 254 3901

Persinformatie:
pr@citrixonline.com
Telefoon: +441 49 454 1715

www.citrixonline.com

Ga naar www.citrixonline.com voor meer informatie over Citrix GoToAssist Corporate.

Informatie over Citrix Online

Citrix Online biedt veilige, gebruiksvriendelijke online oplossingen waarmee gebruikers vanaf alle mogelijke plekken met anderen kunnen samenwerken. Of u nu GoToMyPC® gebruikt voor toegang tot een externe computer, GoToAssist® voor ondersteuning aan klanten of GoToMeeting® voor het houden van online meetings en webinars, u zult – net als ruim 35.000 bedrijven en honderdduizenden andere gebruikers – ervaren dat de productiviteit stijgt, de reiskosten afnemen en de omzet, training en service wereldwijd verbeteren. Een divisie van Citrix Systems, Inc. (Nasdaq: CTXS). Citrix Online is gevestigd in Santa Barbara, Californië, Verenigde Staten. Voor meer informatie kunt u terecht op www.citrixonline.com of bellen naar 805-690-6400.

18191/11.17.08/PDF