Whitepaper

GoToAssist® CORPORATE

GoToAssist Corporate whitepaper om sikkerhed

GoToAssist Corporate leverer robuste end-to-end-datasikkerhedsmetoder, der forhindrer såvel passive som aktive angreb mod fortrolighed, integritet og tilgængelighed.

CITRIX® | online

Indholdsfortegnelse

Rækkevidde og publikum

Denne guide er beregnet til de Citrix® GoToAssist® Corporate-kunder og andre, der har brug for at forstå, hvordan GoToAssist indvirker på sikkerhedsricisi og overensstemmelser i deres miljø.

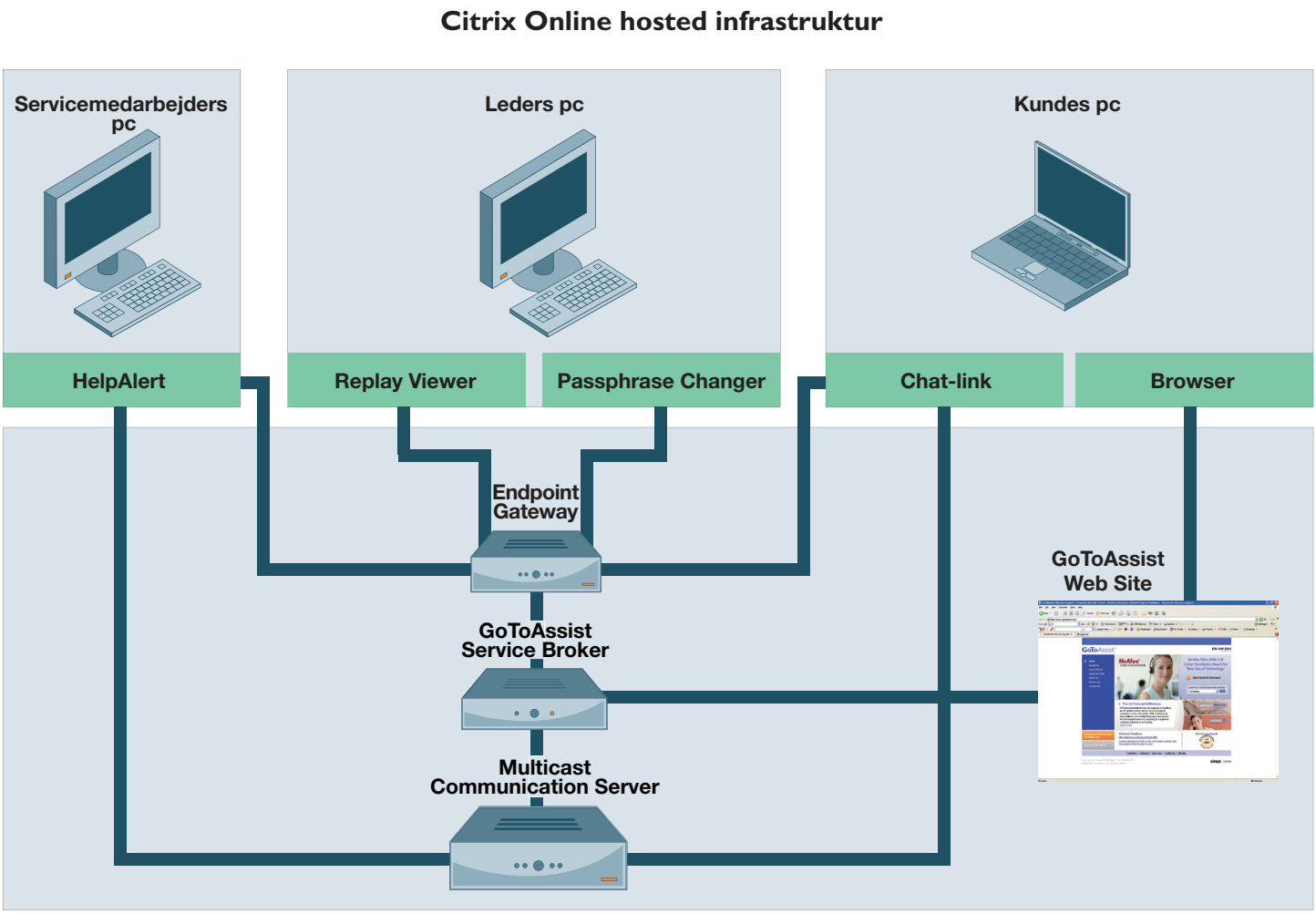
Introduktion

GoToAssist Corporate er en hostet service, der indeholder en måde at levere fjernsupport til Windows-baserede computere. GoToAssist Corporate lader en bruger anmode om support fra en supportmedarbejder og giver derefter denne medarbejder mulighed for at vise og evt. kontrollere slutbrugerens pc eksternt.

Dette dokument fokuserer på funktionerne til informationssikkerhed i GoToAssist Corporate. Det forudsættes, at læseren har en grundlæggende forståelse af produktet og dets funktioner. Man kan finde andet materiale om GoToAssist Corporate online på www.citrixonline.com eller ved at kontakte en Citrix Online-medarbejder.

Leveringsarkitektur for GoToAssist Corporate-service

Nedenstående diagram viser en skematisk oversigt over de vigtigste leveringskomponenter og kommunikationsstier i GoToAssist Corporate-service.



Definitioner

HelpAlert: Win32-eksekverbare filer, som findes på servicemedarbejderens computer og gør det muligt for medarbejderen at modtage og svare på indgående kundeforespørgsler.

ChatLink: Slutpunkt-applikation, som gør det let for kunden og en servicemedarbejder at kommunikere.

Browser: Standardinternetbrowser, f.eks. Firefox, Internet Explorer osv.

Replay Viewer: Slutpunkt-applikation, som lader virksomhedsledere, teamledere og medarbejderledere afspille optagne GoToAssist Corporate-sessioner. Fremviseren kan afspille fjernskærmdeling, lokal skærmdeling, chat og fjerndiagnosticering.

Passphrase Changer: Slutpunk-applikation, der gør det nemt at ændre den adgangskode, der bruges til at beskytte kryptografisk adgang til sessionsoptagelser.

GoToAssist Web Site: Webapplikation, der giver adgang til GoToAssist-webstedet og webbaserede interne og eksterne administrationsportaler.

GoToAssist Service Broker: Webapplikation, der udfører GoToAssist Corporate-konto- og serviceadministration, fillagring og rapportfunktioner.

Multicast Communication Server: En af en række af globalt distribuerede servere, der bruges til at virkeliggøre en lang række unicast- og multicast-kommunikationsservices med høj tilgængelighed.

Endpoint Gateway: En special-gateway, der bruges af mange slutpunkt-applikationer til sikkert at få adgang til GoToAssist Service Broker for en lang række formål ved kald til fjernprocedurer.

Applikationssikkerhed

GoToAssist Corporate giver adgang til en lang række ressourcer og services ved at bruge et rollebaseret adgangskontrolsystem, der håndhæves af de forskellige komponenter til servicelevering. Rollerne og de beslægtede udtryk er defineret i nedenstående tabel:

Roller

Administrator (eller admin)	Den Citrix Online-medarbejder, der opretter grupper og portaler i et firmas GoToAssist Corporate Administrationscenter. Administratorer kan oprette, ændre og slette GoToAssist Corporate-konti, portaler, virksomhedsledere og teamledere, ændre data for abonnement og pris samt udføre andre administrative funktioner.
Firma	Den GoToAssist Corporate-kunde, som portalerne opsættes til.
Virksomhedsleder	En medarbejder hos en virksomhedskunde, der har adgang til dets GoToAssist Corporate Administrationscenter. Kan ændre konti, portal-teams og -medarbejdere tilknyttet hans eller hendes konto.
Kunden	Den person, der anmoder om support fra virksomhedskunden via GoToAssist Corporate.
Gruppe / team	Gruppe af medarbejdere, der er tilknyttet en bestemt portal. Hver medarbejder hører til nøjagtig én gruppe eller ét team, og hver gruppe eller team er tilknyttet præcis én portal. Grupper/teams indeholder nogle standardindstillinger for medarbejdere.
Gruppeleder / teamleder	En medarbejder hos kunden, der er autoriseret af virksomhedslederen til at ændre visse aspekter af et team og dette teams tilknyttede portal og medarbejdere.
Medarbejder	Den supportperson, der besvarer en kundes forespørgsel via HelpAlert.

Godkendelse

GoToAssist Corporate-administratorer, -ledere og -medarbejdere godkendes vha. et kontonavn og en stærk adgangskode.

Adgangskode styres ud fra følgende regler:

Stærke adgangskoder: En stærk adgangskode indeholder mellem 8-32 tegn og skal indeholde mindst tre af følgende fire: store bogstaver [A-Z], små bogstaver [a-z], tal [0-9] og specialsymboler [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Stærke adgangskoder må ikke være det samme som logonnavnet eller kontoens rigtige fornavn eller efternavn. Adgangskoder kontrolleres for styrke, når de initialiseres eller ændres.

Udløbsperiode for adgangskode: Man kan angive adgangskodens udløbsperiode (min.: 10 dage, maks.: 120 dage, standard: 90 dage). Hvis kontoholderen logger på, og adgangskoden er udløbet, skal kontoholderen ændre sin adgangskode.

Historik for adgangskode: En historik over adgangskoder opretholdes. Man kan ikke ændre en adgangskode til en adgangskode, der findes i historikken. Man kan konfigurere dybden på historikken for adgangskode (min.: 1, maks.: 5, standard: 3).

Konto-lockout: Efter 3 gentagne mislykkede login-forsøg, sættes kontoen i en obligatorisk soft-lockout-tilstand. Det betyder, at kontoholderen ikke vil kunne logge på inden for det konfigurere tidsrum (min.: 5 minutter, maks.: 30 minutter, standard: 5 minutter). Når lockout-perioden udløber, kan kontoholderen logge på kontoen igen.

Desuden kan man konfigurere hard-lockout. Efter det konfigurerede antal mislykkede login-forsøg, sættes kontoen i hard-lockout-tilstand. Det betyder, at kontoholderen ikke kan logge på, før kontoens adgangskode er nulstillet af en anden kontoholder med de fornødne rettigheder. En hard-lockout aktiveres efter det konfigurerede antal forsøg (min.: 10, maks.: 50, standard: 10).

Beskyttelse af kundens pc og data

En vigtig del af GoToAssist Corporates sikkerhed er dets tilladelsesbaserede adgangskontrolmodel til beskyttelse af adgang til kundens pc og de data, der findes på den.

For det første skal alle GoToAssist Corporate-sessioner igangsættes eksternt af kunden. GoToAssist Corporate er ikke designet til uovervågede supportscenarier.

For det andet bliver kunden altid bedt om tilladelse, før alle skærmdelinger, fjernkontrol eller overførsel af fejlfindingsdata, -filer eller andre oplysninger påbegyndes.

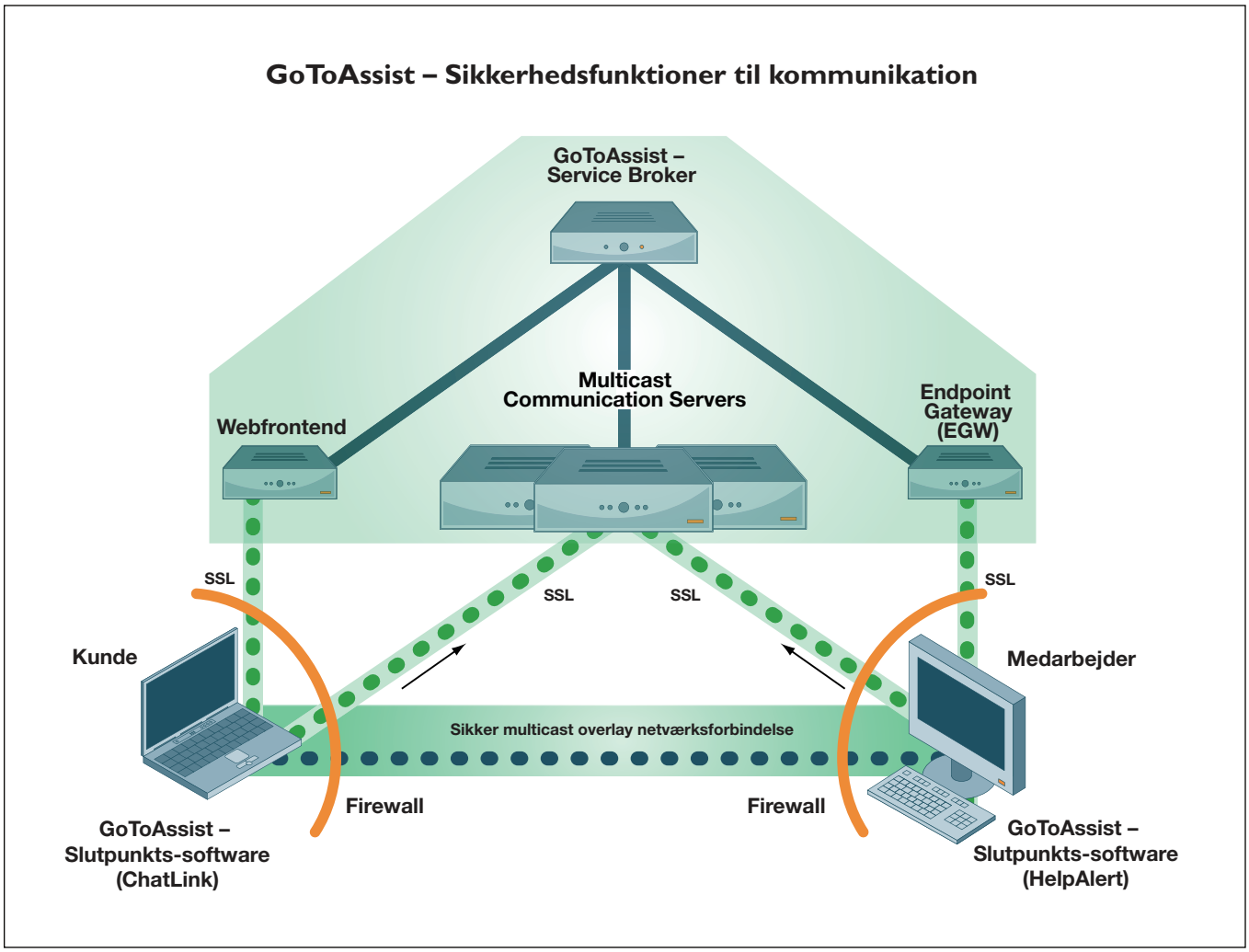
Hvis fjernkontrol og skærmdeling godkendes, kan kunden hele tiden overvåge, hvad medarbejderen gør. Desuden kan kunden nemt tage kontrollen tilbage eller afslutte sessionen når som helst.

Lokale sikkerhedsfunktioner på kundens pc tilsidesættes aldrig. Kunden eller medarbejderen skal stadigvæk angive alle legitimationsoplysninger til Windows eller applikationer.

Endelig logges alle forbindelsesaktiviteter, og skærmdelinger og chatsessionen kan evt. optages og afspilles til gennemsyn på et senere tidspunkt.

Funktioner til kommunikationssikkerhed

Kommunikationen mellem deltagere i en GoToAssist Corporate-session sker via en overlay multicast-netværksstak, der logisk ligger over en konventionel TCP/IP-stak i hver brugers pc. Dette netværk realiseres af en gruppe MCS'er (Multicast Communication Servers), der drives af Citrix Online. Arkitekturen for kommunikationen vises i nedenstående figur.



Deltagerne i en GoToAssist Corporate-session ("slutpunkter") kommunikerer med Citrix Online-infrastrukturens kommunikationsservere og -gateways via udgående TCP/IP-forbindelse på port 8200, 443 og 80. Da GoToAssist Corporate er en hostet webbaseret service, kan deltagerne befinde sig overalt på internettet – på et fjernkontor, i hjemmet, et virksomhedscenter eller tilsluttet via et andet firmas netværk.

Adgang når som helst/hvor som helst til GoToAssist Corporate-servicen giver maksimal fleksibilitet og tilslutning. GoToAssist Corporate indeholder imidlertid også robuste funktioner til kommunikationssikkerhed for at bevare fortroligheden og integriteten af privat virksomhedskommunikation.

Fortrolighed og integritet i kommunikation

GoToAssist Corporate leverer robuste end-to-end-datasikkerhedsmetoder, der forhindrer passive og aktive angreb mod fortrolighed, integritet og tilgængelighed. Alle GoToAssist Corporate-forbindelser er "end-to-end"-krypterede og kun tilgængelige for godkendte deltagere i supportsessionen.

Skærmdelingsdata, tastatur/musekontroldata og chat-oplysninger er altid krypterede, mens man bruger Citrix Online-kommunikationsserverne eller under transmissioner på tværs af offentlige eller private netværk.

Når optagelse er deaktiveret, beholdes GoToAssist Corporate-sessionsnøglen ikke på Citrix Online-servere i nogen form. Det betyder, at selv om der brydes ind på en server, kan nøglen ikke afsløres for krypterede optagelser, som den ubudne gæst måtte have hentet.

Når optagelse er aktiveret, gemmes chat-, skærmdelings- og skærmvisningsdata i krypteret form. Sessionsnøglen gemmes også, men er beskyttet med en offentlig/privat RSA-nøglekryptering på 1.024 bit. En portalspecifik offentlig nøgle bruges til at kryptere sessionsnøglen for lagring. Man skal bruge tre elementer for at afspille: Sessionsoptagelsen, den krypterede sessionsnøgle og portalens private nøgle.

Sikkerhedskontroller til kommunikationen er baseret på stærk kryptering og er implementeret i to lag: "TCP-laget" og "MPS-laget" (Multicast Packet Security).

TCP-lagsikkerhed

IETF-standard-SSL- (Secure Sockets Layer) og -TSL-protokoller (Transport Layer Security) bruges til at beskytte al kommunikation mellem slutpunkter. Den eneste SSL-ciffersuite, der understøttes for TCP-forbindelser til ikke-websteder, er 1.024 bit RSA med 128 bit AES-CBC og HMAC-SHA1, hvilket giver maksimal sikkerhed mod aflytnings-, ændrings- og afspilningsangreb. Imidlertid understøtter GoToAssist-webstedet indgående forbindelser vha. de fleste understøttede SSL-ciffersuiter for at opnå maksimal kompatibilitet med stort set alle webbrowsere på brugernes computer. Citrix Online anbefaler, at kunderne beskytter sig bedst muligt ved at konfigurere deres browsere til at bruge stærk kryptering som standard, når det er muligt, og at de altid installerer de nyeste sikkerhedsrettelser til operativsystemet og browseren.

Når SSL/TLS-forbindelser er etableret til GoToAssist-webstedet og mellem GoToAssist Corporate-komponenter, godkender Citrix Online-servere sig selv til klienter vha. offentlige VeriSign/Thawte-nøglecertifikater. Gensidig certifikatbaseret godkendelse bruges på alle server-til-server-links (f.eks. MCS-til-MCS, MCS-til-Broker) for at opnå øget sikkerhed mod infrastrukturangreb. Disse stærke godkendelsesmetoder forhindrer mulige angribere i at kunne maskere sig som infrastrukturservere eller indsætte sig selv midt i supportsessionskommunikationer.

Multicast-pakkesikkerhedslag

Andre funktioner giver komplet "end-to-end"-sikkerhed for multicast-pakkedata, uafhængigt af dem, der stilles til rådighed af SSL/TLS. Alle multicast-sessionsdata er beskyttet af "end-to-end"-krypterings- og integritetsmekanismer, der forhindrer nogen med adgang til vore kommunikationsserverer (uanset om de er venner eller fjender) i at aflytte en GoToAssist Corporate-session eller manipulere data, uden at det bliver opdaget. Dette ekstra niveau af kommunikationsfortrolighed og -integritet er enestående for GoToAssist Corporate. Virksomhedskommunikation er aldrig synlig for tredjepart, herunder brugere, som er inviteret til en given supportsession, og Citrix Online selv.

MPSL-nøgleetablering opnås ved at bruge en offentlig nøglebaseret SRP-6-godkendelsesnøgleaftale og en 1024 bit modulus til at etablere en primærnøgle til krypteringsnøgler. (Se http://srp.stanford.edu/design.html.) Denne primærnøgle bruges derefter til gruppesymmetrisk nøgledistribution vha. AES Key Wrap-algoritmen, IETF RFC 3394. Alt nøglemateriale genereres vha. en FIPS-kompatibel pseudo-tilfældig nummergenerator, der er forsynet med entropi-data, som er indsamlet under run-time fra flere kilder på værtsmaskinen. Disse robuste, dynamiske nøglegenererings- og udvekslingsmetoder giver høj beskyttelse mod nøglegæt og nøglebrydning.

MPSL beskytter yderlige multicast-pakkedata mod aflytning ved at bruge en 128 bit AES-kryptering i Counter Mode. Almindelig tekst-data komprimeres før kryptering vha. beskyttede højydelsesteknikker for at opnå optimeret båndbredde. Dataintegritetsbeskyttelse opnås ved at inkludere en integritetskontrolværdi, der genereres med HMAC-SHA-1-algoritmen. Da GoToAssist Corporate bruger meget stærke standardkrypteringsmetoder, kan kunderne være sikre på, at multicast-supportsessionsdata er beskyttede mod uautoriseret blotlæggelse eller uregistreret ændring.

Desuden er der ingen ekstra omkostninger, forringelse af ydelse eller i brugervenligheden tilknyttet disse vigtige kommunikationssikkerhedsfunktioner. Standarddatasikkerhed med høj ydelse er en indbygget funktion i alle GoToAssist Corporate-sessioner.

Nøglepunkter

- 128 bit AES-kryptering bruges til sessionsfortrolighed.
- Den første sessionsnøgle vælges tilfældigt af Broker, og videresendes til slutpunkter over godkendte og krypterede kanaler.
- Slutpunkterne finder derefter indbyrdes frem til den endelige sessionsnøgle.
- Den endelige sessionsnøgle er ikke kendt af Broker.
- Kommunikationsserverne sender kun krypterede pakker og har ikke sessionskrypteringsnøglen.
- GoToAssist Corporate-arkitekturen minimerer risikoen for dataafsløring, samtidig med at evnen til at koble medarbejdere sammen med dem, der har brug for hjælp, maksimeres.

Firewall- og proxy-kompatibilitet

Som alle andre Citrix Online-produkter indeholder GoToAssist Corporate indbygget proxy-registrering og forbindelsesstyringslogik, der hjælper med at automatisere softwareinstallation, undgå behov for kompleks netværks(gen)konfiguration og maksimere brugerproduktiviteten. Firewalls og proxyer, som allerede findes på dit netværk, behøver normalt ikke nogen specialkonfiguration til at aktivere brug af GoToAssist Corporate.

Når GoToAssist Corporate-slutpunkt-software er startet, forsøger det at kontakte GoToAssist Service Broker via EGW (Endpoint Gateway) ved at initiere en eller flere udgående SSL-beskyttede TCP-forbindelse på port 8200, 443 og/eller 80. Den forbindelse, der svarer først, bruges, og de andre droppes. Denne forbindelse danner grundlaget for at deltage i alle fremtidige supportsessioner ved at etablere kommunikation mellem hostede servere og brugerens desktop.

Når brugeren forsøger at deltage i en supportsession, etablerer GoToAssist Corporate-slutpunktsoftwaren en eller flere ekstra forbindelser til Citrix Online-kommunikationserverne igen vha. SSL-beskyttede TCP-forbindelser på port 8200, 443 og/eller 80. Disse forbindelser transporterer supportsessionsdata under en aktiv session.

Desuden igangsætter slutpunktsoftwaren en eller flere kortvarige TCP-forbindelser på port 8200, 443 og/eller 80, som ikke er SSL-beskyttede for at optimere forbindelsen. Disse netværks"sonder" indeholder ingen informationer, der er følsomme eller kan udnyttes, og udgør ingen risiko for, at følsomme informationer bliver afsløret.

Man kan se en komplet liste over de IP-adresser, der bruges af Citrix Online, på www.citrixonline.com/iprange.

Ved kun at bruge udgående forbindelser og vælge en port, som allerede er åben i de fleste firewalls og proxyer, under automatisk justering af de lokale netværksbetingelser, leverer GoToAssist Corporate en høj grad af kompatibilitet med eksisterende netværkssikkerhedsfunktioner. Modsat visse andre produkter kræver GoToAssist Corporate ikke, at virksomhederne deaktiverer eksisterende netværkssikkerhedsfunktioner i forbindelse med online supportsessionskommunikation. Disse funktioner maksimerer kompatibiliteten og den generelle netværkssikkerhed.

Slutpunktsystemets sikkerhedsfunktioner

Software til online supportsessioner skal være kompatibel med en lang række desktop-miljøer, og alligevel kunne oprette et sikkert slutpunkt på hver brugers desktop. GoToAssist Corporate opnår dette ved at bruge eksekverbare filer, der kan hentes på internettet, og som bruger stærke krypteringsmetoder.

Signeret slutpunktsoftware

GoToAssist Corporate-klientslutpunktsoftwaren er en Win32-eksekverbar fil, der overføres til brugernes pc'er. En digitalt signeret Java-applet bruges til at overføre programmet og kontrollere integriteten af GoToAssist Corporate-slutpunktsoftwaren fra Citrix Online-serverne. Det beskytter brugeren mod uforvarende at installere en trojansk hest eller anden malware, der udgiver sig for at være GoToAssist Corporate-software.

Slutpunktsoftwaren består af flere Win32-eksekverbare filer og DLL'er. Procedurer til streng kvalitetskontrol og konfigurationsstyring følges nøje af Citrix Online under udvikling og implementering for at sikre softwaresikkerhed. Slutpunktsoftwaren udsætter ingen eksternt tilgængelige netværksinterfaces for fare og kan ikke bruges af malware eller virusser til at udnytte eller inficere fjernsystemer. Derved beskyttes andre desktop-pc'er, der deltager i en supportsession, mod at blive inficeret af en kompromitteret vært, som bruges af en anden deltager.

Implementering af kryptografisk subsystem

Alle krypteringsfunktioner og sikkerhedsprotokoller, der anvendes af GoToAssist Corporate-klientslutpunktsoftwaren, implementeres vha. avanceret Certicom Security Builder® Crypto™-og Certicom Security Builder® SSL™-biblioteker for at sikre høj ydelse. (Se www.certicom.com for at få flere oplysninger.)

Det er kun GoToAssist Corporate-slutpunktapplikationen, der bruger krypteringsbibliotekerne. Ingen eksterne API'er udsættes for adgang fra anden software, der kører på denne desktop. Alle krypterings- og integritetsalgoritmer, nøglestørrelses- og andre krypteringsregelparametre er statisk kodede, når applikationen kompileres. Da der ikke findes nogen krypteringsindstillinger, som brugeren kan konfigurere, er det umuligt for brugerne at svække GoToAssist Corporate-sessionssikkerheden gennem tilfældig eller forsætlig miskonfiguration. Et firma, der bruger GoToAssist Corporate, kan være sikker på, at det samme niveau af sikkerhed i online supportsessioner er til stede for alle deltagende slutpunkter, uanset hvem der ejer eller bruger hver desktop.

Sikkerhedsfunktioner for værtsinfrastrukturen

Citrix Online leverer GoToAssist Corporate ved at bruge en ASP-model (Application Service Provider), der er designet specifikt til at sikre robust og sikker operation, samtidig med at det integreres problemfrit i et firmas eksisterende netværks- og sikkerhedsinfrastruktur.

Skalerbar og pålidelig infrastruktur

Citrix Onlines globale servicearkitektur er designet til maksimal ydelse, pålidelighed og skalerbarhed. GoToAssist Corporate-servicen drives af standardservere med høj kapacitet med de nyeste sikkerhedsrettelser installeret. Redundante switches og routere er indbygget i arkitekturen for at sikre, at der aldrig opstår et eneste fejlpunkt. Klyngeservere og backupsystemer hjælper med til at garantere en problemfri strøm af applikationsprocesser – selv under stor belastning eller systemfejl. GoToAssist Broker fordeler belastningen mellem klient/serversessioner jævnt på tværs af geografisk distribuerede kommunikationsservere for at få en optimal ydelse.

Fysisk sikkerhed

Alle GoToAssist Corporate-web-, -applikations-, -kommunikations- og -databaseservere har til huse i sikre, fælles datacentre. Fysisk adgang til servere er underlagt skarpe restriktioner og overvåges konstant. Alle anlæg har redundante strøm- og omgivelseskontrolfunktioner.

Netværkssikkerhed

Citrix Online anvender firewall-, router- og VPN-baseret adgangskontrol for at sikre vores privat-service-netværk og backend-servere. Infrastrukturens sikkerhed overvåges konstant, og der udføres regelmæssig sårbarhedstest af det interne sikkerhedspersonale og eksterne revisorer fra tredjepart.

Kundens privatliv

Da opretholdelse af vore brugeres tillid er af høj prioritet for os, er Citrix Online forpligtet til at respektere dit privatliv. Du kan finde et link til en kopi af de aktuelle Citrix GoToAssist Corporate-regler om beskyttelse af personlige oplysninger på service-webstedet på www.citrixonline.com.

Overholdelse af miljøvedtægter

Da GoToAssist Corporate indeholder et omfattende antal applikations- og kommunikationssikkerhedskontroller, herunder den kundegodkendte, tilladelsesbaserede sikkerhedsmodel, kan man med sindsro bruge det til at understøtte computere og applikationer i omgivelser, der er underlagt HIPAA-, Gramm-Leach-Bliley Act- eller Sarbanes-Oxley-vedtægterne, hvor robust datafortrolighed og integritetskontrol skal anvendes.

Citrix Online anbefaler, at organisationer nøje gennemgår alle standard- og konfigurerbare sikkerhedsfunktioner i GoToAssist Corporate, som gælder deres specifikke omgivelser, brugertal og regelkrav for at afgøre, hvilke funktioner der skal aktiveres, og hvordan man bedst konfigurerer dem. I visse tilfælde anbefales det, at man informerer brugerne om andre brugerretningslinjer, for at sikre at alle deltagerne overholder sikkerhedsmålene. Citrix Online Professional Service-teamet kan tilbyde mere materiale vedrørende de bedste metoder til at implementere og bruge GoToAssist Corporate.

Afslutning

GoToAssist Corporates intuitive og sikre grænseflade og funktionssæt gør det til den mest effektive løsning til afholdelse af online supportsessioner. Ved at bruge GoToAssist Corporate kan supportmedarbejdere, konsulenter og it-specialister hurtigt og nemt yde teknisk hjælp til kunder i hele verden.

Fra kulissen understøtter Citrix Onlines hostede servicearkitektur flerpunktssamarbejde ved at levere et sikkert, pålideligt miljø. Som denne whitepaper viser, promoverer GoToAssist Corporate brugervenlighed og fleksibilitet uden at kompromittere integriteten, privatlivet eller den administrative kontrol af virksomhedskommunikationen eller it-aktiverne.

Appendiks: Overholdelse af sikkerhedsstandarder

GoToAssist Corporate overholder følgende industri- og U.S. government-standarder for krypteringsalgoritmer og sikkerhedsprotokoller:

- TLS/SSL-protokollen, Version 1.0 IETF RFC 2246
- AES (Advanced Encryption Standard), FIPS 197
- (FIPS-valideret implementering, NIST-certifikat nr. 175)
- AES Cipher-suiter for TLS, IETF RFC 3268
- AES Key Wrap-algoritme, IETF RFC 3394
- RSA, PKCS nr. 1
- SHA-1, FIPS 180-1 (FIPS-valideret implementering, NIST-certifikat nr. 89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudo-tilfældig nummergenerering, ANSI X9.62 og FIPS 140-2

Citrix Online

Citrix Online division

Produktoplysninger:
www.citrixonline.com

Salgsforespørgsler:
Nordic@citrixonline.com
Telefon: (+45) 47334123

Henvendelser fra pressen:
pr@citrixonline.com
Telefon: +441 49 454 1715

www.citrixonline.com

Du kan få mere at vide om Citrix GoToAssist Corporate ved at besøge www.citrixonline.com

Om Citrix Online

Citrix Online leverer sikre, brugervenlige onlineløsninger, der gør det muligt at arbejde hvor som helst og med hvem som helst. Uanset om GoToMyPC® bruges til at få adgang til og arbejde på en fjern-pc, om GoToAssist® bruges til at supportere kunder, eller om GoToMeeting® bruges til at holde møder og webinarer, opnår vores kunder – mere end 35.000 virksomheder og mange tusind enkeltpersoner – en stadig større produktivitet, færre rejseomkostninger og øget salg, uddannelse og service globalt set. En afdeling af Citrix Systems, Inc. (Nasdaq: CTXS). Firmaet er baseret i Santa Barbara, Californien. Få flere oplysninger ved at besøge www.citrixonline.com eller ringe på 805-690-6400.

18191/11.17.08/PDF