White Paper

GoToAssist® CORPORATE

Sicherheits-White Paper für Citrix GoToAssist Corporate

GoToAssist Corporate umfasst stabile End-to-End-Sicherheitseinstellungen, die sowohl vor passiven als auch aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten schützen.

CITRIX® | online

Inhaltsverzeichnis

Geltungsbereich und Zielgruppe 3
Einleitung 3
Architektur der GoToAssist-Leistungsbereitstellung 4
Definitionen 5
Anwendungssicherheit 6
Authentifizierung 7
Schutz des Kundencomputers und der Kundendaten 7
Sicherheitsfunktionen für die Kommunikation 8
Vertraulichkeit und Integrität der Kommunikation 9
TCP-Sicherheitsstufe 9
Multicast-Paket-Sicherheitsstufe 10
Firewall- und Proxykompatibilität 11
Sicherheitsfunktionen für Endpunktsysteme 12
Signierte Endpunktsoftware 12
Implementierung des Verschlüsselungssubsystems 12
Sicherheitsfunktionen für die gehostete Infrastruktur 13
Skalierbare und zuverlässige Infrastruktur 13
Physische Sicherheit 13
Netzwerksicherheit 13
Schutz der Kundendaten 13
Kompatibilität für Umgebungen unter behördlicher Aufsicht 14
Abschluss 14
Anhang: Kompatibilität mit Sicherheitsstandards 15

Geltungsbereich und Zielgruppe

Dieses Dokument richtet sich an Kunden und andere Interessengruppen von Citrix® GoToAssist® Corporate, die Informationen darüber benötigen, wie sich GoToAssist auf die Datensicherheit und Kompatibilität in ihrer Umgebung auswirkt.

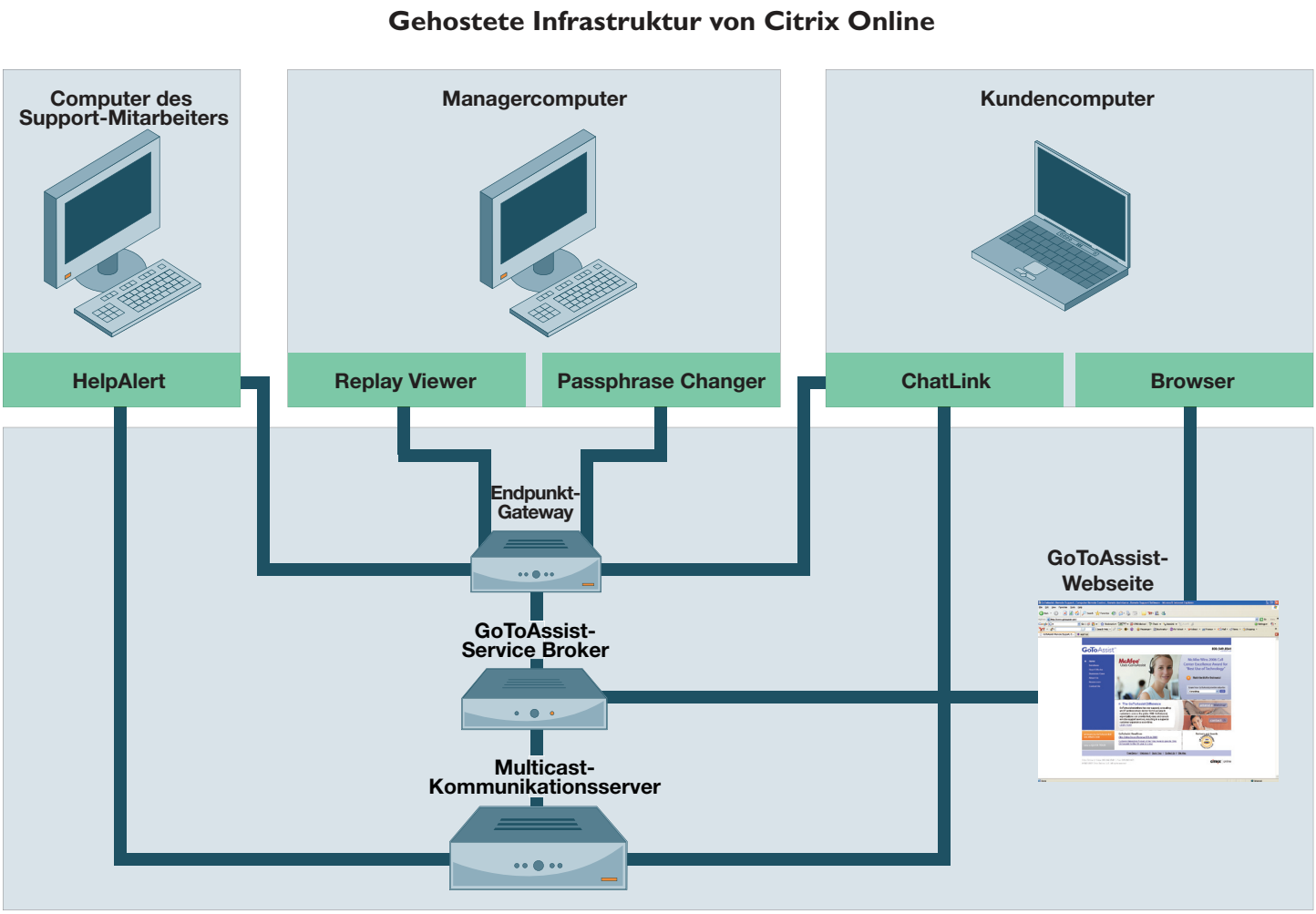
Einleitung

GoToAssist Corporate ist ein gehosteter Dienst, der die Bereitstellung eines Remote-Supports für Windows-basierte Computer ermöglicht. Mit GoToAssist Corporate können Benutzer eine Support-Anforderung an einen Support-Mitarbeiter senden, der dann über die Möglichkeit verfügt, den Computer des Endbenutzers remote anzuzeigen und optional auch zu steuern.

In diesem Dokument werden die GoToAssist Corporate-Sicherheitsfunktionen für Daten behandelt. Grundkenntnisse über das Produkt und seine Features werden hierbei vorausgesetzt. Zusätzliche Informationsmaterialien zu GoToAssist Corporate erhalten Sie online unter www.citrixonline.com oder von Ihrer Citrix Online Vertretung.

Architektur der GoToAssist Corporate-Leistungsbereitstellung

Das nachstehende Diagramm zeigt eine schematische Übersicht aller wichtigen Komponenten und Kommunikationspfade der Leistungsbereitstellung mit GoToAssist Corporate.



Definitionen

HelpAlert: Ausführbare Win32-Datei, die sich auf dem Mitarbeitercomputer befindet und diesem ermöglicht, eingehende Kundenanfragen zu empfangen und zu beantworten.

ChatLink: Endpunktanwendung, mit der die Text-basierte Kommunikation zwischen Kunde und Support-Mitarbeiter erleichtert wird.

Browser: Standard-Internet-Webbrowser, z. B. Firefox, Internet Explorer, etc.

Replay Viewer: Endpunktanwendung, mit der Unternehmensmanager, Teammanager und Personalmanager aufgezeichnete GoToAssist Corporate-Sitzungen wiedergeben können. Diese Anwendung ermöglicht die Wiedergabe von Remote-Bildschirmfreigaben, lokalen Bildschirmfreigaben, Chats und Remote-Diagnosen.

Passphrase Changer: Endpunktanwendung, mit der das Ändern des Zugriffskennworts zum Schutz von verschlüsselten Sitzungsaufzeichnungen erleichtert wird.

GoToAssist-Webseite: Webanwendung für den Zugriff auf die GoToAssist-Webseite und Web-basierte interne und externe Administrationsportale.

GoToAssist-Service Broker: Webanwendung zur Konto- und Dienstverwaltung, beständigen Speicherung und Berichterstattung von GoToAssist Corporate.

Multicast-Kommunikationsserver: Einer der vielen global verteilten Server, die zum Ausführen einer Vielzahl von Unicast- und Multicast-Kommunikationsdiensten mit hoher Verfügbarkeit verwendet werden.

Endpunkt-Gateway: Dieses spezielle Gateway wird von vielen Endpunktanwendungen verwendet, um aus verschiedenen Gründen über Remote-Prozeduraufruf sicher auf den GoToAssist-Service Broker zuzugreifen.

Anwendungssicherheit

GoToAssist Corporate ermöglicht den Zugriff auf eine Vielzahl von Ressourcen und Diensten. Hierzu wird ein Autoritäten-basiertes Zugriffssteuerungssystem verwendet, das von den verschiedenen Leistungsbereitstellungskomponenten ausgeführt wird. Die Autoritäten und zugehörigen Bestimmungen werden in der folgenden Tabelle definiert:

Autoritäten

Administrator (oder Admin)	Der Citrix Online Mitarbeiter, der Gruppen und Portale im GoToAssist Corporate Management Center eines Unternehmens erstellt. Administratoren können Konten, Portale, Unternehmens- und Teammanager für GoToAssist Corporate-Konten erstellen, Abonnement- und Preisinformationen ändern sowie andere administrative Aufgaben ausführen.
Unternehmen	GoToAssist Corporate-Kunde, für den Portale eingerichtet werden.
Unternehmensmanager	Ein Mitarbeiter des Kundenunternehmens, der über eine Zugriffsberechtigung auf das GoToAssist Corporate Management Center verfügt. Er kann die Konten, Portalteams und Mitarbeiter für sein Konto ändern.
Kunde	Die Person, die über GoToAssist Corporate eine Support-Anfrage an das Kundenunternehmen sendet.
Gruppe/Team	Eine Gruppe von Mitarbeitern, die einem bestimmten Portal zugewiesen sind. Jeder Mitarbeiter ist Mitglied von genau einer Gruppe oder einem Team. Jede Gruppe oder jedes Team ist jeweils nur einem Portal zugeordnet. Gruppen/Teams weisen einige Standardeinstellungen für Mitarbeiter auf.
Gruppenmanager/Teammanager	Ein Mitarbeiter, der von einem Unternehmensmanager die Berechtigung erhält, bestimmte Aspekte im Team sowie im zugehörigen Portal und bei den Mitarbeitern zu ändern.
Mitarbeiter	Der Support-Mitarbeiter, der über HelpAlert die Kundenanfragen beantwortet.

Authentifizierung

Administratoren, Manager und Mitarbeiter werden über einen Kontonamen und ein sicheres Kennwort für GoToAssist Corporate authentifiziert.

Die Kennwörter unterliegen den folgenden Richtlinien:

Sichere Kennwörter: Ein sicheres Kennwort ist zwischen 8 und 32 Zeichen lang und muss mindestens drei der folgenden Elemente enthalten: Großbuchstaben [A-Z], Kleinbuchstaben [a-z], Zahlen [0-9] und Sonderzeichen [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Sichere Kennwörter dürfen nicht dem Zugangsnamen oder dem Vornamen und Nachnamen des Mitarbeiterkontos entsprechen. Bei der Erstellung oder Änderung werden Kennwörter hinsichtlich ihrer Sicherheit überprüft.

Ablaufzeitraum für Kennwort: Der Ablaufzeitraum für Kennwörter ist konfigurierbar (min: 10 Tage, max: 120 Tage, Standard: 90 Tage). Wenn sich der Kontoinhaber anmeldet und das Kennwort abgelaufen ist, ist der Kontoinhaber gezwungen, das Kennwort zu ändern.

Kennwortverlauf: Für die Kennwörter wird eine Verlaufschronik erstellt. Ein Kennwort kann nicht zu einem Kennwort geändert werden, das bereits im Kennwortverlauf vorhanden ist. Die Verlaufstiefe für Kennwörter ist konfigurierbar (min: 1, max: 5, Standard: 3).

Kontosperrung: Nach 3 aufeinanderfolgenden fehlerhaften Anmeldeversuchen wird für das Konto eine obligatorische Kontosperrung (befristet) ausgeführt. Dies bedeutet, dass für den Kontoinhaber für einen konfigurierbaren Zeitraum (min: 5 Minuten, max: 30 Minuten, Standard: 5 Minuten) keine Kontoanmeldung möglich ist. Nach Ablauf dieser Sperrzeit kann der Kontoinhaber erneut versuchen, sich für das Konto anzumelden.

Eine weitere Konfigurationsoption ist die unbefristete Kontosperrung. Nach einer konfigurierbaren Anzahl von fehlerhaften Anmeldeversuchen wird das Konto vollständig gesperrt. Dies bedeutet, dass der Kontoinhaber sich erst dann wieder anmelden kann, wenn das Kontokennwort von einem anderen berechtigten Kontoinhaber neu eingerichtet wurde. Eine unbefristete Kontosperrung wird nach einer konfigurierbaren Anzahl von Anmeldeversuchen aktiviert (min: 10, max: 50, Standard: 10).

Schutz des Kundencomputers und der Kundendaten

Eine wichtige Komponente bei der Sicherheit von GoToAssist Corporate ist das Berechtigungs-basierte Steuerungsmodell zum Schutz vor unberechtigtem Zugriff auf den Computer des Kunden und die darin enthaltenen Daten.

Alle GoToAssist Corporate-Sitzungen müssen vom Remote-Kunden initiiert werden. GoToAssist Corporate ist nicht für unbeaufsichtigte Support-Szenarien ausgelegt.

Der Kunde wird außerdem immer zuerst um Erlaubnis gefragt, bevor eine Bildschirmfreigabe, Remote-Steuerung oder Übertragung von Diagnosedaten, Dateien oder Informationen gestartet wird.

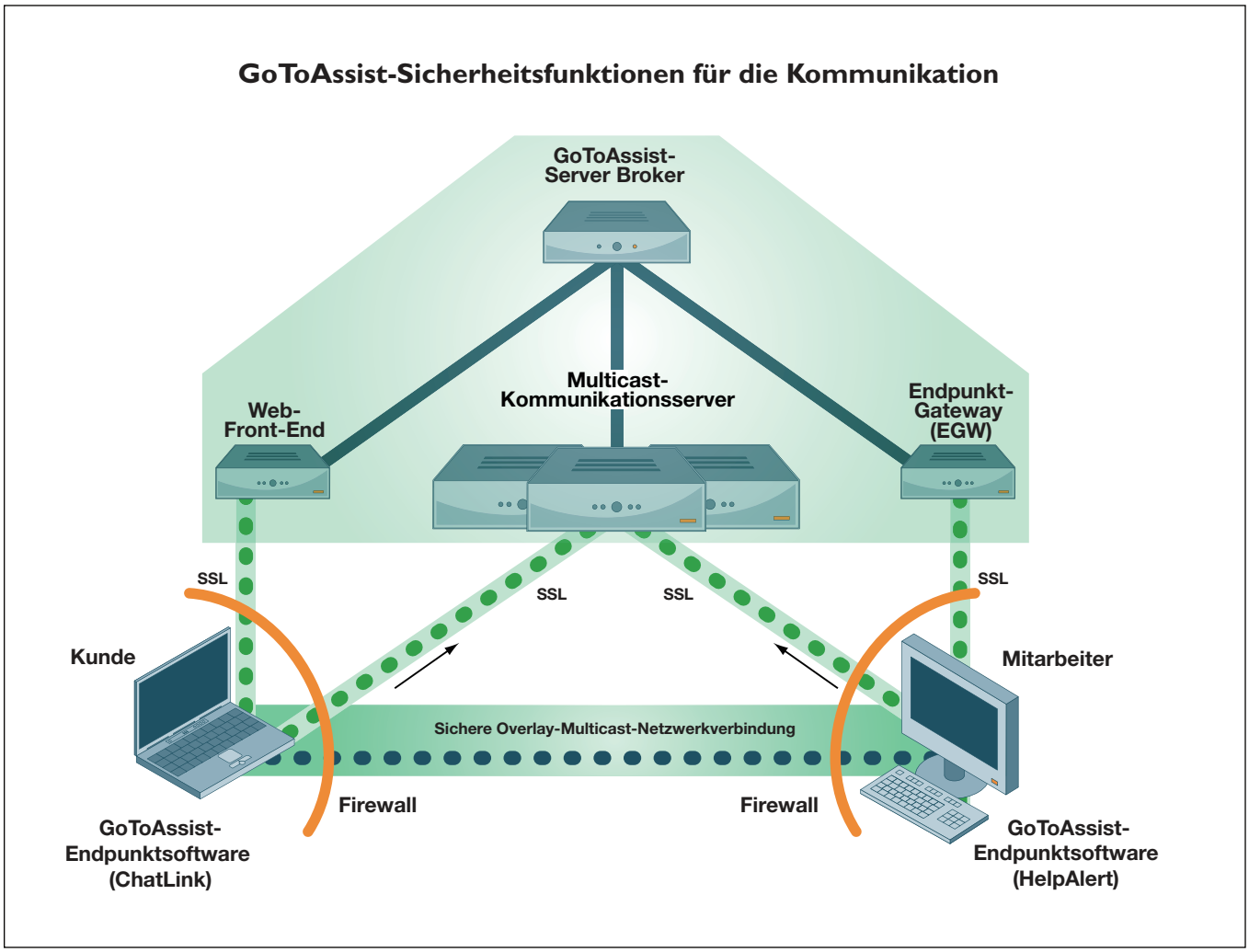
Im Fall einer autorisierten Remote-Steuerung oder Bildschirmfreigabe kann der Kunde stets mitverfolgen, welche Aktionen die Support-Mitarbeiter ausführen. Der Kunde kann zu jedem Zeitpunkt auch selbst wieder die Steuerung der Sitzung übernehmen oder die Sitzung beenden.

Die lokalen Sicherheitseinstellungen auf dem Kundencomputer werden zu keinem Zeitpunkt außer Kraft gesetzt. Der Kunde oder Mitarbeiter muss zudem weiterhin alle erforderlichen Anmeldeinformationen zur Authentifizierung bei Windows oder anderen Anwendungen bereitstellen.

Zusätzlich werden alle Verbindungsaktivitäten protokolliert und die Bildschirmfreigabe und Chat-Sitzungen können optional aufgezeichnet und zur Überprüfung später wiedergegeben werden.

Sicherheitsfunktionen für die Kommunikation

Die Kommunikation der Teilnehmer einer GoToAssist Corporate-Sitzung erfolgt über einen Overlay-Multicast-Netzwerkstapel, der sich auf jedem Benutzercomputer über dem normalen TCP/IP-Stapel befindet. Dieses Netzwerk besteht aus einer Sammlung von Multicast-Kommunikationsservern, die von Citrix Online ausgeführt werden. Die Kommunikationsarchitektur wird in der folgenden Abbildung zusammengefasst:



Die Teilnehmer an GoToAssist Corporate-Sitzungen ("Endpunkte") verwenden ausgehende TCP/IP-Verbindungen über die Ports 8200, 443 und 80, um mit den Kommunikationsservern und Gateways der Citrix Online Infrastruktur zu kommunizieren. GoToAssist Corporate ist ein Web-basierter gehosteter Dienst, daher können sich die Teilnehmer an einem beliebigen Ort mit Internet befinden (in einem Außenbüro, zu Hause, in einem Geschäftszentrum oder verbunden mit einem Netzwerk eines anderen Unternehmens).

Dieser Zugriff auf GoToAssist Corporate von einem beliebigen Standort und zu jeder Zeit bietet optimale Flexibilität und Verbindungsmöglichkeiten. Damit die Geheimhaltung und Integrität der vertraulichen Unternehmenskommunikation ebenfalls gewährleistet ist, enthält GoToAssist Corporate außerdem stabile Sicherheitsfunktionen für die Kommunikation.

Vertraulichkeit und Integrität der Kommunikation

GoToAssist Corporate umfasst stabile "End-to-End"-Sicherheitseinstellungen, die sowohl vor passiven als auch aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten schützen. Alle GoToAssist Corporate-Verbindungen sind durch eine "End-to-End"-Verschlüsselung gesichert und nur autorisierte Teilnehmer der Support-Sitzung können auf die Verbindung zugreifen.

Daten über die Bildschirmfreigabe, Steuerungsdaten von Tastatur/Maus und Chat-Informationen sind nie in unverschlüsselter Form verfügbar, während sie temporär auf den Citrix Online-Kommunikationsservern gespeichert sind oder über öffentliche oder private Netzwerke übertragen werden.

Wenn die Aufzeichnungsfunktion deaktiviert ist, wird der GoToAssist Corporate-Sitzungsschlüssel in keiner Form auf den Citrix Online-Servern gespeichert. Daher kann auch bei einem unberechtigten Zugriff auf einen Server kein Schlüssel für verschlüsselte Daten preisgegeben werden, die durch einen Angreifer möglicherweise erfasst wurden.

Bei aktivierter Aufzeichnungsfunktion werden die Daten aus Chat und Bildschirmfreigabe/-anzeige verschlüsselt gespeichert. Der Sitzungsschlüssel wird ebenfalls gespeichert, er wird jedoch durch eine 1024-Bit RSA-Verschlüsselung für öff./priv. Schlüssel gesichert. Vor der Speicherung wird ein Portal-spezifischer öffentlicher Schlüssel verwendet, um den Sitzungsschlüssel zu verschlüsseln. Für die Wiedergabe sind daher drei Elemente erforderlich: die Sitzungsaufnahme, der Schlüssel zum Entschlüsseln der Sitzung und der private Schlüssel für das Portal.

Die auf einer sicheren Verschlüsselung basierenden Sicherheitseinstellungen für die Kommunikation werden in zwei Stufen implementiert: "TCP-Stufe" und "Multicast-Packet-Sicherheitsstufe".

TCP-Sicherheitsstufe

Zum Schutz der Kommunikation zwischen den Endpunkten werden die IETF-Standards SSL-Protokoll (Secure Sockets Layer) und TLS-Protokoll (Transport Layer Security) verwendet. Für einen maximalen Schutz vor Abhöraktionen, Abänderungen und Angriffen auf die Wiedergabe wird 1024-Bit RSA mit 128-Bit AES-CBC und HMAC-SHA1 als einzige SSL-Verschlüsselungssammlung für TCP-Verbindungen außerhalb von Webseiten unterstützt. Da jedoch eine möglichst große Kompatibilität mit fast allen Webbrowsern auf allen Benutzer-Desktops erwünscht ist, unterstützt die GoToAssist-Webseite eingehende Verbindungen mit weithin üblichen SSL-Verschlüsselungssammlungen. Zum eigenen Schutz empfiehlt Citrix Online seinen Kunden, so oft wie möglich standardmäßig eine Browserkonfiguration mit sicherer Verschlüsselung zu verwenden und stets das aktuelle Betriebssystem und die neuesten Sicherheitspatches zu installieren.

Wenn eine SSL/TLS-Verbindung zur GoToAssist-Webseite und zwischen GoToAssist Corporate-Komponenten hergestellt ist, werden VeriSign/Thawte-Zertifikate für öffentliche Schlüssel verwendet, um die Citrix Online-Server für Clients zu authentifizieren. Für einen zusätzlichen Schutz gegen Angriffe auf die Infrastruktur wird für alle Server-zu-Server-Verknüpfungen eine beidseitige Zertifikat-basierte Authentifizierung verwendet (z. B. MCS-zu-MCS, MCS-zu-Broker). Durch diese sicheren Authentifizierungsmethoden wird verhindert, dass mögliche Angreifer als Infrastrukturserver getarnt sind oder sich in die Kommunikation von Support-Sitzungen einbinden.

Multicast-Paket-Sicherheitsstufe

Zusätzliche Funktionen, die unabhängig von SSL/TLS sind, bieten eine vollständige "End-to-End"-Sicherheit für Multicast-Paketdaten. Insbesondere alle Multicast-Sitzungsdaten werden durch "End-to-End"-Verschlüsselung und Integritätsmechanismen gesichert, die verhindern, dass Personen mit Zugriff auf unsere Kommunikationsserver (mit guten oder bösartigen Absichten) eine GoToAssist Corporate-Sitzung abhören oder Daten unbemerkt manipulieren können. Diese zusätzliche Stufe an Kommunikationsgeheimhaltung und -integrität ist eine einzigartige Komponente von GoToAssist Corporate. Die Unternehmenskommunikation ist zu keinem Zeitpunkt für Dritte sichtbar, ebenso wenig für Citrix Online selbst und für Benutzer, die kein Mitglied einer bestimmten Support-Sitzung sind.

Die Schlüsselerstellung für die Multicast-Paket-Sicherheitsstufe erfolgt mittels einer auf öffentlichen Schlüsseln basierenden authentifizierten SRP-6-Schlüsselvereinbarung, wobei für den Verpackungsschlüssel ein 1024-Bit-Modul verwendet wird. (Siehe http://srp.stanford.edu/design.html.) Dieser Schlüssel zum Verpacken des letzten Schlüssels wird dann für die gruppensymmetrische Schlüsselverteilung mit dem AES-Schlüsselverpackungsalgorithmus IETF RFC 3394 verwendet. Alle Schlüsselerstellungsmaterialien werden mit einer FIPS-kompatiblen Generierung von Pseudozufallszahlen erstellt. Hierzu werden Entropiedaten verwendet, die bei der Ausführung von mehren Quellen auf dem Hostcomputer erfasst wurden. Diese stabilen und dynamischen Schlüsselerstellungs- und Austauschmethoden bieten einen sicheren Schutz vor dem unberechtigten Versuch, den Schlüssel durch Zufall oder Cracking herauszufinden.

Die Multicast-Paket-Sicherheitsstufe schützt Multicast-Paketdaten außerdem auch im Zählermodus durch eine 128-Bit-AES-Verschlüsselung. Klartextdaten werden vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert, um die Bandbreite zu optimieren. Der Schutz der Datenintegrität erfolgt durch einen integrierten Integritätsprüfungswert, der vom HMAC-SHA-1-Algorithmus erstellt wird. Da GoToAssist Corporate besonders sichere Verschlüsselungsmethoden mit Industriestandard verwendet, können die Kunden darauf vertrauen, dass die Multicast-Informationen der Support-Sitzung gegen eine unberechtigte Offenlegung oder unbemerkte Änderung geschützt sind.

Außerdem entstehen durch diese wichtigen Kommunikationssicherheitsfunktionen keine zusätzlichen Kosten, Leistungsbeeinträchtigungen oder Benutzungsauflagen. Die leistungsfähige und auf Standards basierende Datensicherheit ist eine bereits "integrierte" Funktion jeder GoToAssist Corporate-Sitzung.

Wichtige Punkte

- Zur Geheimhaltung der Sitzung wird eine 128-Bit-AES-Verschlüsselung verwendet.
- Der erste Sitzungsschlüssel wird vom Broker zufällig ausgewählt und dann über authentifizierte und verschlüsselte Kanäle an die Endpunkte übermittelt.
- Nur die Endpunkte legen zusammen den letzten Sitzungsschlüssel fest.
- Der Broker kennt den letzten Sitzungsschlüssel nicht.
- Die Kommunikationsserver leiten verschlüsselte Pakete nur weiter und haben keinen Zugriff auf den Schlüssel zur Sitzungsverschlüsselung.
- Durch die GoToAssist Corporate-Architektur werden die Risiken einer Enthüllung der Sitzungsdaten minimiert und gleichzeitig die Verbindungsmöglichkeiten zwischen Support-Mitarbeiter und Kunden maximiert.

Firewall- und Proxykompatibilität

GoToAssist Corporate enthält wie auch alle anderen Citrix Online-Produkte eine integrierte Erkennungs- und Verbindungsverwaltungslogik, die eine automatisierte Softwareinstallation unterstützt, komplexe (Neu-)Konfigurationen vermeidet und gleichzeitig die Benutzerproduktivität maximiert. Firewalls und Proxies, die bereits im Netzwerk vorhanden sind, benötigen im Allgemeinen keine besondere Konfiguration, um die Verwendung von GoToAssist Corporate zu aktivieren.

Wenn die GoToAssist Corporate-Endpunktsoftware gestartet wird, wird über das Endpunkt-Gateway (EGW) eine Verbindung mit dem GoToAssist-Service Broker hergestellt, indem eine oder mehrere ausgehende SSL-geschützte TCP-Verbindungen über die Ports 8200, 443 und/oder 80 initiiert werden. Es wird die Verbindung verwendet, die zuerst eine Antwort sendet, die anderen werden verworfen. Diese Verbindung ist die Grundlage für die Teilnahme an allen zukünftigen Support-Sitzungen und ermöglicht die Kommunikation zwischen den gehosteten Servern und dem Benutzer-Desktop.

Wenn der Benutzer an einer Support-Sitzung teilnehmen möchte, stellt die GoToAssist Corporate-Endpunktsoftware eine oder mehrere zusätzlichen Verbindungen mit den Kommunikationsservern von Citrix Online her, und zwar erneut mit SSL-geschützten TCP-Verbindungen über die Ports 8200, 443 und/oder 80. Diese Verbindungen übertragen während einer aktiven Sitzung Informationen der Support-Sitzung.

Zur Verbindungsoptimierung initiiert die Endpunktsoftware zusätzlich eine oder mehrere TCP-Verbindungen von nur kurzer Dauer über die Ports 8200, 443 und/oder 80, die nicht SSL-geschützt sind. Diese "Netzwerktests" enthalten keine vertraulichen oder sensiblen Informationen und beinhalten nicht das Risiko der Offenlegung solcher Daten.

Eine vollständige Liste der von Citrix Online verwendeten IP-Adressbereiche finden Sie unter www.citrixonline.com/iprange.

Durch die automatische Anpassung der lokalen Netzwerkbedingungen, die Verwendung von ausschließlich ausgehenden Verbindungen und die Auswahl eines Ports, der bereits in den meisten Firewalls und Proxies geöffnet ist, verfügt GoToAssist Corporate über eine hohe Kompatibilität mit den bereits vorhandenen Netzwerksicherheitseinstellungen. Im Gegensatz zu einigen anderen Produkten ist es für GoToAssist Corporate nicht erforderlich, dass Unternehmen bestehende Sicherheitseinstellungen für das Umkreisnetzwerk deaktivieren, um die Online-Kommunikation für Support-Sitzungen zuzulassen. Diese Funktionen maximieren sowohl die Kompatibilität als auch die Sicherheit des gesamten Netzwerks.

Sicherheitsfunktionen für Endpunktsysteme

Die Software für Online-Support-Sitzungen muss mit einer Vielzahl von Desktop-Umgebungen kompatibel sein und dennoch auf dem jeweiligen Benutzer-Desktop einen sicheren Endpunkt erstellen. GoToAssist Corporate erreicht dieses Ziel durch ausführbare Dateien mit sicheren Verschlüsselungsmethoden, die aus dem Internet heruntergeladen werden können.

Signierte Endpunktsoftware

Die Software für GoToAssist Corporate-Clientendpunkte ist eine ausführbare Win32-Datei, die auf die Computer der Benutzer heruntergeladen wird. Mit einem digital signierten Java-Applet wird der Download ausgeführt und die Integrität der GoToAssist Corporate-Endpunktsoftware von den Citrix Online-Servern überprüft. Dies schützt den Benutzer vor der unbeabsichtigten Installation eines Trojaners oder anderer Malware, die sich als GoToAssist Corporate-Software tarnt.

Die Endpunktsoftware besteht aus mehreren ausführbaren Win32-Dateien und dynamisch verknüpften Bibliotheken. Damit die Sicherheit der Software gewährleistet ist, führt Citrix Online bei der Entwicklung und Bereitstellung strenge Qualitätskontrollen und Konfigurationsverwaltungsprozesse durch. Die Endpunktsoftware weist keine extern verfügbaren Netzwerkschnittstellen auf und kann nicht von Malware oder Viren als Sicherheitslücke und zur Infizierung von Remote-Systemen verwendet werden. Hierdurch werden Desktops, die an Support-Sitzungen teilnehmen, vor einer Infizierung durch einen von einem anderen Teilnehmer verwendeten, gefährdeten Host geschützt.

Implementierung des Verschlüsselungssubsystems

Alle von der Software für GoToAssist Corporate-Clientendpunkte verwendeten Verschlüsselungsfunktionen und Sicherheitsprotokolle werden mit der modernen Certicom Security Builder® Crypto™-Bibliothek und Certicom Security Builder® SSL™-Bibliothek implementiert, um die Sicherheit und Leistungsfähigkeit zu gewährleisten. (Weitere Informationen finden Sie unter www.certicom.com.)

Die Verwendung der Verschlüsselungsbibliotheken ist auf die GoToAssist Corporate-Endpunktanwendung beschränkt. Es sind keine externen APIs vorhanden, auf die andere auf diesem Desktop ausgeführte Anwendungen möglicherweise zugreifen könnten. Alle Verschlüsselungs- und Integritätsalgorithmen, Schlüsselgrößen und andere Parameter der Verschlüsselungsrichtlinie werden bei der Kompilierung der Anwendung statisch codiert. Da keine für den Endbenutzer konfigurierbaren Verschlüsselungseinstellungen vorhanden sind, besteht keinerlei Gefahr, dass die Benutzer durch unbeabsichtigte oder bewusste Fehlkonfigurationen die Sicherheit der GoToAssist Corporate-Sitzung beeinträchtigen. Ein Unternehmen, das GoToAssist Corporate verwendet, kann sicher sein, dass auf allen teilnehmenden Endpunkten die gleiche Sicherheitsstufe für Online-Support-Sitzungen vorhanden ist, unabhängig vom Besitzer oder Benutzer des jeweiligen Desktops.

Sicherheitsfunktionen für die gehostete Infrastruktur

Citrix Online stellt GoToAssist Corporate mit einem ASP-Modell (Application Service Provider) bereit, das speziell für eine stabile und sichere Ausführung entwickelt wurde. Gleichzeitig gewährleistet es eine nahtlose Integration in das bereits im Unternehmen vorhandene Netzwerk und in die bestehende Sicherheitsinfrastruktur.

Skalierbare und zuverlässige Infrastruktur

Die globale Servicearchitektur von Citrix Online wurde für eine maximale Leistung, Zuverlässigkeit und Skalierbarkeit entwickelt. GoToAssist Corporate wird von hochleistungsfähigen Servern und Netzwerkkomponenten mit Industriestandard ausgeführt, die über die aktuellen Sicherheitspatches verfügen. Redundante Switches und Router sind in die Architektur integriert, um zu gewährleisten, dass zu keinem Zeitpunkt eine einzelne Fehlerquelle auftritt. Servercluster und Sicherungssysteme garantieren eine problemfreie Ausführung der Anwendungsprozesse, auch bei starker Auslastung oder bei einem Systemfehler. Für eine optimale Leistung wird die Auslastung der Client/Server-Sitzungen durch den GoToAssist-Broker auf geografisch verteilte Kommunikationsserver aufgeteilt.

Physische Sicherheit

Alle Web-, Anwendungs-, Kommunikations- und Datenbankserver von GoToAssist Corporate sind in sicheren Rechenzentren untergebracht. Der physische Zutritt zu den Servern ist äußerst beschränkt und wird ununterbrochen überwacht. Alle Einrichtungen verfügen über eine redundante Stromversorgung und Umgebungsüberwachung.

Netzwerksicherheit

Citrix Online verwendet Firewall, Router und VPN-basierte Zugriffssteuerungen, um die privaten Servicenetzwerke und Back-End-Server zu schützen. Die Infrastruktursicherheit wird ununterbrochen überwacht und interne Sicherheitsmitarbeiter und Drittprüfer führen regelmäßige Überprüfungen des Sicherheitsrisikos durch.

Schutz der Kundendaten

Das uns von unseren Kunden entgegengebrachte Vertrauen hat für uns Priorität. Daher verpflichtet sich Citrix Online zum Schutz der Kundendaten. Ein Link zu einer Ausgabe der aktuellen Datenschutzrichtlinie für Citrix GoToAssist Corporate finden Sie auf der Support-Webseite unter www.citrixonline.com.

Kompatibilität für Umgebungen unter behördlicher Aufsicht

Aufgrund der umfangreichen Sicherheitseinstellungen für Anwendungen und Kommunikation (einschließlich des Berechtigungs-basierten Sicherheitsmodells der Kundenautorisierung) kann GoToAssist Corporate bedenkenlos für den Support von Computern verwendet werden, die gesetzlichen Bestimmungen unterliegen (z. B. Gesetz zur Vereinheitlichung des elektronischen Datenverkehrs im Gesundheitswesen sowie der Datensicherheit, Gramm-Leach-Bliley oder Sarbanes-Oxley) und eine stabile Datengeheimhaltung und Integritätssteuerung erfordern.

Citrix Online empfiehlt Unternehmen, alle standardmäßigen und konfigurierbaren Sicherheitsfunktionen von GoToAssist Corporate sorgfältig unter Berücksichtigung der jeweiligen Umgebungen, Benutzergruppen und Richtlinienanforderungen zu überprüfen, um zu bestimmen, welche Funktionen aktiviert werden sollen und wie diese optimal zu konfigurieren sind. In manchen Fällen ist die Übermittlung von zusätzlichen Benutzerrichtlinien ratsam, um zu gewährleisten, dass die Sicherheitsziele aller Beteiligten zur Zufriedenheit erfüllt werden. Das Service-Team für Unternehmen von Citrix Online verfügt über zusätzliche Materialien zu bewährten Methoden bei der Bereitstellung und Verwendung von GoToAssist Corporate.

Abschluss

Durch die intuitive und sichere Oberfläche sowie die integrierten Sicherheitsfunktionen ist GoToAssist Corporate eine äußerst effektive Lösung für Online-Support-Sitzungen. Mit GoToAssist Corporate können Support-Mitarbeiter, Berater und IT-Experten schnell und einfach Kunden rund um den Globus technische Unterstützung bereitstellen.

Durch die Gewährleistung einer sicheren und zuverlässigen Umgebung ermöglicht die gehostete Service-Architektur von Citrix Online, gleichsam aus dem Hintergrund, auf transparente Weise die Zusammenarbeit von mehreren Endpunkten. Wie in diesem Dokument dargelegt wurde, ist GoToAssist Corporate sowohl benutzerfreundlich als auch flexibel, ohne dabei die Integrität, den Datenschutz oder die Verwaltungsfunktionen der Geschäftskommunikation oder IT-Bestände zu gefährden.

Anhang: Kompatibilität mit Sicherheitsstandards

GoToAssist Corporate erfüllt die folgenden Industriestandards und Standards der US-Regierung für Verschlüsselungsalgorithmen und Sicherheitsprotokolle:

- TLS/SSL-Protokoll, Version 1.0 IETF RFC 2246
- AES (Advanced Encryption Standard, Erweiterter Verschlüsselungsstandard), FIPS 197
- (FIPS-validierte Implementierung, NIST-Zertifikat Nr. 175)
- AES-Verschlüsselungssammlungen für TLS, IETF RFC 3268
- AES-Schlüsselverpackungsalgorithmus, IETF RFC 3394
- RSA, PKCS Nr. 1
- SHA-1, FIPS 180-1 (FIPS-validierte Implementierung, NIST-Zertifikat Nr. 89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Generierung von Pseudozufallszahlen, ANSI X9.62 und FIPS 140-2

Citrix Online

Unternehmensgruppe Citrix Online

Produktinformationen:
www.citrixonline.com

Verkaufsanfragen:
Germany@citrixonline.com
Telefon: 0049 891 2140 0859

Medienanfragen:
pr@citrixonline.com
Telefon: +441 49 454 1715

www.citrixonline.com

Weitere Informationen über Citrix GoToAssist Corporate erhalten Sie unter www.citrixonline.com

Informationen über Citrix Online

CITRIX® | online

Citrix Online bietet sichere und benutzerfreundliche Online-Lösungen, die eine weltweite Zusammenarbeit über das Internet ermöglichen. Durch die Verwendung von GoToMyPC® für den Zugriff und das Arbeiten auf einem Remote-PC, GoToAssist® für den Kunden-Support und GoToMeeting® für Online-Meetings und Web-Seminare können unsere Kunden (mehr als 35.000 Unternehmen und Hunderttausende Einzelpersonen) ihre Produktivität steigern, die Reisekosten senken sowie Vertrieb, Schulung und Service weltweit verbessern. Citrix Online, eine Unternehmensgruppe von Citrix Systems, Inc. (Nasdaq: CTXS), hat ihren Sitz in Santa Barbara, Kalifornien. Weitere Informationen erhalten Sie unter www.citrixonline.com oder +1-805-690-6400.

18191/17.11.08/PDF