GoToMeeting

Webkonferenz-Tools von Citrix: Whitepaper zu Sicherheits-aspekten

Citrix bietet bei der Nutzung von GoToMeeting, GoToWebinar und GoToTraining echte End-to-End-Datensicherheitsmechanismen, die vor passiven und aktiven Angriffen gegen die Vertraulichkeit, Integrität und Verfügbarkeit schützen.

www.gotomeeting.de

by CITRIX

Inhalt

Einleitung 3

Geschäftsanforderungen für sichere Zusammenarbeit 4

Rollenbasierte Sicherheitsfunktionen 5

Berechtigungen des Organisators 5

- Berechtigungen des Moderators 6
- Berechtigungen der Teilnehmer 6

Funktionen zur Konto- und Sitzungsauthentifizierung 7

- Kundenkonto-Log-In 7
- Offenlegung von Sitzungsinformationen 7
- Authentifizierung von Sitzungsteilnehmern 7
- Sicherheit der Administrationswebseite 8

Sicherheitsfunktionen für die Kommunikation 9

- Vertraulichkeit und Integrität der Kommunikation 10
- TCP-Sicherheitsstufe 10
- Multicast-Sicherheit 10
- Firewall- und Proxykompatibilität 11
- Sprachsicherheit 12

Sicherheitsfunktionen für Endpunktsysteme 12

- Signierte Endpunkt-Software 12
- Implementierung des Verschlüsselungssubsystems 12

Sicherheitsfunktionen für die gehostete Infrastruktur 13

- Skalierbare und zuverlässige Infrastruktur 13
- Physische Sicherheit 13
- Netzwerksicherheit 13
- Schutz der Kundendaten 14

Fazit 14

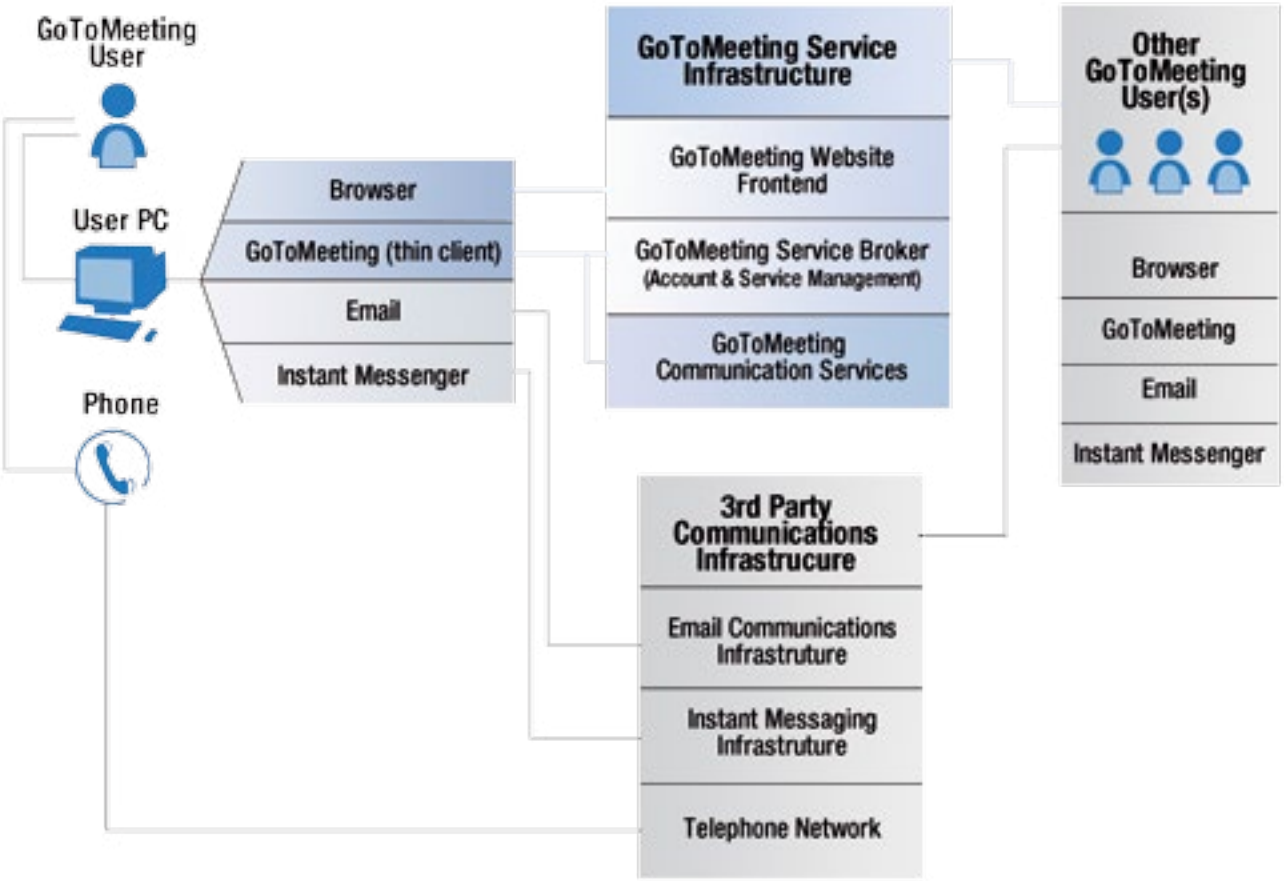
Anhang: Kompatibilität mit Sicherheitsstandards 14

Einführung

Die Tools GoToMeeting, GoToWebinar und GoToTraining von Citrix sind die sichersten Produkte für Webkonferenzen, die verfügbar sind. Bei allen Lösungen sorgt die Kombination aus standardkonformer Kryptografie mit echter End-to-End-Verschlüsselung, einer hochverfügbaren, gehosteten Service-Infrastruktur und einer intuitiven Benutzeroberfläche für maximale Vertraulichkeit, Integrität und Verfügbarkeit.

Dieses Dokument enthält eine technische Beschreibung der integrierten Sicherheitsfunktionen in GoToMeeting, GoToWebinar und GoToTraining. Es ist für technische Gutachter und Sicherheitsspezialisten vorgesehen, die für die Sicherheit eines Unternehmensnetzwerks, den Datenschutz und die Integrität der geschäftlichen Kommunikation verantwortlich sind.

Bild 1



GoToMeeting, GoToWebinar und GoToTraining sind Webkonferenz-Werkzeuge, mit deren Hilfe mehrere PC- und Mac-Benutzer mittels gemeinsamer Bildschirmnutzung, Fernbedienung von Tastatur und Maus, Text-Chats und anderer Funktionen zusammenarbeiten können. GoToMeeting ist ideal für Vertriebsdemos und kooperative Online-Meetings. GoToWebinar ist für eine größere Teilnehmerzahl vorgesehen, beispielsweise für Marketingpräsentationen und Firmen-Events. GoToTraining ist speziell auf webbasierte Trainings ausgerichtet und bietet Onlinezugriff auf Tests, Unterlagen und einen gehosteten Kurskatalog.

Diese Produkte sind gehostete Dienste, die über einen Webbrowser genutzt werden. Sie umfassen auch herunterladbare Client-Programme und ein Netzwerk von Multicast-Kommunikationsservern, die Citrix betreibt. Die Sitzungen werden über die Website von Citrix Online oder über Client-Software geplant, einberufen und moderiert. Aus Gründen der Benutzerfreundlichkeit bieten GoToMeeting, GoToWebinar und GoToTraining auch VoIP- und Telefonkonferenzfunktionen.

Sichere Zusammenarbeit ist für Unternehmen wichtig

Einfach zu nutzende Online-Tools zur Zusammenarbeit wie GoToMeeting, GoToWebinar und GoToTraining, die auf den geschäftlichen Einsatz ausgerichtet sind, können Unternehmen dabei helfen, durch eine effektivere Kommunikation und Interaktion mit Mitarbeitern, Geschäftspartnern und Kunden ihre Produktivität zu steigern. Derartige Tools unterscheiden sich erheblich, wenn man die integrierten Sicherheitsfunktionen näher betrachtet. Darüber hinaus ist es wichtig, die Auswirkungen der Online-Zusammenarbeit auf die Sicherheit zu verstehen und die Richtlinien zur sicheren Nutzung einzuhalten.

Die Nutzung jeglicher Art von Webkonferenzlösung erfordert eine sorgfältige Prüfung der möglichen Bedrohungen und der daraus resultierenden Geschäftsrisiken. Zu den geschäftlichen Sicherheitsanforderungen, die üblicherweise beim Einsatz eines Webkonferenzprodukts bedacht werden müssen, gehören folgende:

- Verhindern des unbefugten Zugriffs auf den Dienst und dessen Funktionen, sodass nur berechtigte Benutzer und eingeladene Teilnehmer Online-Sitzungen planen und daran teilnehmen können.
- Vermeiden jeglicher Gefährdung von Unternehmensgütern, einschließlich Client-Computern und daran angeschlossenen privaten Netzwerken.
- Schutz der Daten und der Integrität einer vertraulichen Kommunikation, einschließlich gemeinsamer Bildschirmnutzung, Chats, E-Mail und Sprachkommunikation.
- Sicherstellen der Verfügbarkeit und Zuverlässigkeit des Dienstes selbst, damit die geschäftliche Kommunikation jederzeit möglich ist und nicht unterbrochen wird.
- Nahtlose Integration in andere Netzwerk- und Computersicherheitsmaßnahmen, damit die Webkonferenzdienste von den Sicherheitsvorkehrungen eines Unternehmens profitieren und diese nicht unterlaufen.

Unsere Webkonferenz-Tools wurden von Grund auf so entwickelt, dass diese allgemeinen geschäftlichen Sicherheitsanforderungen eingehalten werden. Durch integrierte Sicherheitsfunktionen, die einfach zu nutzen und zu verwalten sind, ermöglichen GoToMeeting, GoToWebinar und GoToTraining eine effektive und sichere Online-Kommunikation im geschäftlichen Bereich.

Rollenbasierte Sicherheitsfunktionen

Damit die betreibenden Unternehmen ihre Richtlinien betreffend der Nutzung des Dienstes und einzelner Funktionen durchsetzen können, kann jedem Benutzer von GoToMeeting, GoToWebinar und GoToTraining eine von mehreren anwendungsdefinierten Rollen zugewiesen werden.

- Organisatoren sind berechtigt, Meetings, Webinare und/oder Trainingssitzungen zu planen. Ein Organisator bereitet eine Sitzung vor, lädt andere Benutzer ein, initiiert und beendet die Sitzung und bestimmt, wer als Präsentator fungiert.
- Teilnehmer sind berechtigt, an einer Sitzung teilzunehmen. Die Teilnehmer sehen den Bildschirm des Präsentators, können mit anderen Teilnehmern chatten und die Teilnehmerliste einsehen.
- Präsentatoren sind Teilnehmer, die den Inhalt ihres Computerbildschirms für andere Teilnehmer freigeben können. Präsentatoren entscheiden auch, welche anderen Teilnehmer die Tastatur und Maus des Präsentator-Computers bedienen dürfen, sofern dies sinnvoll ist.
- Bei internen Administratoren handelt es sich um Mitarbeiter von Citrix, die berechtigt sind, Dienste und Konten von GoToMeeting, GoToWebinar und GoToTraining zu verwalten.
- Externe Administratoren sind Mitarbeiter des Kunden, die zur Verwaltung von Mehrbenutzerkonten berechtigt sind. Die externen Administratoren können Funktionen des Kontos konfigurieren, Organisatoren autorisieren und verschiedene Berichts-Tools verwenden.

Die Benutzeroberflächen von GoToMeeting, GoToWebinar und GoToTraining bieten intuitive Sitzungssteuerungsfunktionen und Statusindikatoren, die produktive und sichere Online-Sitzungen ermöglichen.

Die für die einzelnen Benutzer verfügbaren Steuerelemente und Berechtigungen sind von der zugewiesenen Rolle abhängig: Organisator, aktiver Präsentator oder allgemeiner Teilnehmer.

Berechtigungen der Organisatoren

Organisatoren verfügen über die meisten Steuerungsmöglichkeiten in einer Sitzung. Sie können anderen Teilnehmern verschiedene Berechtigungen erteilen und entziehen.

Zu den spezifischen Berechtigungen für Organisatoren gehören folgende:

- Einladen von Teilnehmern vor und während der Sitzung, sodass nur autorisierte Teilnehmer an einer Sitzung teilnehmen können.
- Anzeigen der vollständigen Teilnehmerliste einschließlich aktueller Rollen und Berechtigungen, damit der Organisator jederzeit den Überblick über die anwesenden Personen behält.
- Starten und Beenden einer Sitzung. Dies verhindert, dass andere Teilnehmer versehentlich die Sitzung unterbrechen.
- Festlegen eines Teilnehmers als aktiven Präsentator. Steuern, welcher Desktop während der Sitzung angezeigt wird.
- Deaktivieren der Chat-Funktion für einen oder mehrere Teilnehmer. Zulassen von Diskussionen „am Rande“ nur dann, wenn dies sinnvoll ist.

- Trennen von Teilnehmern.
- Übertragen der Organisatorrolle an einen anderen Teilnehmer, damit die Sitzung fortgesetzt werden kann, falls der Organisator sie verlassen muss. (Nachdem ein anderer Teilnehmer als Organisator bestimmt wurde, kann diese Berechtigung nicht mehr zurückgenommen werden.)

Berechtigungen der Präsentatoren

Ein Präsentator ist der Benutzer, dessen Desktop-Bildschirm für alle anderen Teilnehmer sichtbar ist. In einer Sitzung kann es zur gleichen Zeit immer nur einen Teilnehmer geben, dem die Rolle des aktiven Präsentators zugewiesen ist. Den Präsentatoren stehen folgende Steuerelemente zur Verfügung:

- Aktivieren, Deaktivieren oder Pausieren der gemeinsamen Bildschirmnutzung, wobei Letzteres nützlich ist, um die Offenlegung vertraulicher Daten zu verhindern, die auf dem Desktop des Präsentators sichtbar sind (z. B. beim Suchen nach Dateien oder Ordnern).
- Einem anderen Teilnehmer die Berechtigung zum Steuern der Tastatur und Maus erteilen oder entziehen. Dies erleichtert die Kommunikation mithilfe von Interaktionen auf dem Desktop.
- Übergeben der Präsentatorrolle an einen anderen Teilnehmer, um während der Sitzung einen flexiblen und dynamischen Ablauf zu erreichen.

Wenn der Desktop eines Präsentators für andere Teilnehmer freigegeben ist, wird dem Präsentator ein „Auf Sendung“-Indikator angezeigt. Zur Freigabe des eigenen Desktops muss der Präsentator auf die Schaltfläche „Show My Screen“ (Meinen Bildschirm anzeigen) klicken. Durch diese Funktionen wird sichergestellt, dass der Präsentator immer weiß, wann die Bildschirmfreigabe aktiv ist, damit Desktop-Inhalte nicht unbeabsichtigt für andere Teilnehmer sichtbar gemacht werden.

Berechtigungen der Teilnehmer

Benutzer mit der Teilnehmerrolle verfügen über folgende Berechtigungen:

- Teilnehmen an einer Sitzung, zu der sie vor dem Start und während der Sitzung eingeladen wurden.
- Anzeigen des Präsentatorbildschirms, sofern der Präsentator die gemeinsame Bildschirmnutzung nicht pausiert oder deaktiviert hat.
- Steuern der Tastatur und Maus des Präsentators, sofern der Präsentator dies zulässt. (Die Berechtigung zur Fernsteuerung wird automatisch entzogen, wenn die Rolle des aktiven Präsentators weitergegeben wird.)
- Verwenden der Chat-Funktion zum Senden von Textnachrichten an alle oder bestimmte Teilnehmer. (Die Chat-Funktion kann von einem Organisator für einen oder mehrere Teilnehmer deaktiviert werden.)
- Verlassen der Sitzung zu einem beliebigen Zeitpunkt.

Da Zugriffsrechte und Berechtigungen auf zugewiesenen Rollen basieren, sind flexible Sitzungen mit einer sehr dynamischen Interaktion zwischen den Teilnehmern möglich, ohne dass dabei die Kontrolle oder Transparenz

gefährdet wird. Organisatoren können auf einfache Weise nach Bedarf Teilnehmer hinzufügen oder während der Sitzung den Präsentator wechseln. Die Präsentatoren behalten die vollständige Kontrolle über ihren Desktop, während die Organisatoren über alle erforderlichen Funktionen zur effektiven Verwaltung der Sitzung verfügen.

Funktionen zur Konto- und Sitzungs-Authentifizierung

Eine rollenbasierte Autorisierung erfordert die Möglichkeit, jeden Anwender korrekt zu identifizieren und zu authentifizieren. Damit sichergestellt ist, dass es sich bei jedem Organisator, Präsentator und Teilnehmer um die Person handelt, die diese vorgibt zu sein, verfügen GoToMeeting, GoToWebinar und GoToTraining über robuste Funktionen zur Konto- und Sitzungs-Authentifizierung.

Anmeldung beim Konto über eine Website

Für den Zugriff auf ein Benutzerkonto auf der Website von GoToMeeting, GoToWebinar und GoToTraining müssen die Benutzer eine gültige E-Mail-Adresse und das dazugehörige Kennwort eingeben. Damit diese Kennwörter schwer zu erraten sind, müssen sie mindestens acht Zeichen und sowohl Buchstaben als auch Ziffern enthalten. Bei zu vielen fehlgeschlagenen Anmeldeversuchen wird das Website-Konto vorübergehend gesperrt, um ein Erraten des Kennworts zu verhindern. Die Kennwörter werden in der Datenbank des Dienstes verschlüsselt gespeichert. Sie werden mithilfe einer kryptografisch gesicherten Verifizierungsfunktion geprüft, die sehr widerstandsfähig gegenüber Offline-Wörterbuchangriffen ist.

Offenlegung von Sitzungsinformationen

Im Gegensatz zu einigen Lösungen von Mitbewerbern sind Informationen, die geplante Sitzungen mit GoToMeeting, GoToWebinar und GoToTraining beschreiben, nur für den Organisator und eingeladene Teilnehmer verfügbar. Da Sitzungsbeschreibungen nur Benutzern angezeigt werden, die sich erfolgreich authentifiziert haben und außerdem zu deren Anzeige berechtigt sind, sind potenziell vertrauliche Informationen nie für Hacker, neugierige Websurfer oder Mitbewerber sichtbar. Dazu Zählen Informationen wie das Thema der Sitzung, der Name des Organisators oder der Sitzungstermin.

Authentifizierung der Sitzungsteilnehmer

Da die meisten Organisationen viele Sitzungen mit einem eingeschränkten Teilnehmerkreis abhalten, ist es nicht ausreichend, wenn jeder Benutzer, der einem Konto bei GoToMeeting, GoToWebinar oder GoToTraining zugeordnet ist, Sitzungsbeschreibungen sehen oder an Sitzungen teilnehmen darf. Daher basiert die Autorisierung zur Teilnahme an einer Sitzung auf einer eindeutigen Sitzungs-ID und einem optionalen Kennwort.

Während eine Sitzung geplant wird, generiert der Servicebroker von GoToMeeting, GoToWebinar oder GoToTraining auf Zufallsbasis eine neunstellige eindeutige Sitzungs-ID und übergibt sie an den Organisator. Die Sitzungs-ID wird anschließend an alle eingeladenen Teilnehmer übermittelt. Dies kann per E-Mail, Instant Messaging, Telefon oder einem anderen Kommunikationsmittel erfolgen.

Wenn ein Teilnehmer einer Sitzung beitreten möchte, muss er zunächst die Sitzungs-ID an den Servicebroker übermitteln. Dies geschieht durch Klicken auf eine URL, welche die Sitzungs-ID enthält, oder durch manuelle Eingabe der ID in ein Formular, das der heruntergeladene GoToMeeting-, GoToWebinar- oder GoToTraining-Client präsentiert.

Nachdem eine gültige Sitzungs-ID an den Servicebroker übermittelt wurde, gibt dieser einen Satz eindeutiger Sitzungsidentifikationsdaten an den GoToMeeting-, GoToWebinar- oder GoToTraining-Client zurück. Diese Sitzungsidentifikationsdaten sind für den Teilnehmer nie sichtbar, sondern werden von der Software für Verbindungen mit einem oder mehreren Kommunikations-Servern verwendet. Die Identifikationsdaten beinhalten eine 64 Bit lange Sitzungs-ID, eine kurze Rollen-ID und ein optionales Rollen-Token von 64 Bit. Anhand dieser Daten werden die entsprechende Sitzung identifiziert und der Benutzer transparent als Organisator oder Teilnehmer authentifiziert. Die gesamte vertrauliche Kommunikation erfolgt über SSL-geschützte Verbindungen, um eine Offenlegung der Sitzungsidentifikationsdaten zu verhindern.

Zusätzlich müssen die Teilnehmer eine „End-to-End-Authentifizierung“ beim Organisator der Sitzung durchführen. Diese basiert auf einem geheimen Zufallswert, der vom Servicebroker bereitgestellt wird, und einem optionalen Kennwort, welches der Organisator auswählt und den Teilnehmern mitteilt. Für maximalen Schutz vor unbefugtem Zugriff und zum Sicherstellen der Sitzungsvertraulichkeit empfiehlt Citrix nachdrücklich die Verwendung der Kennwortfunktion.

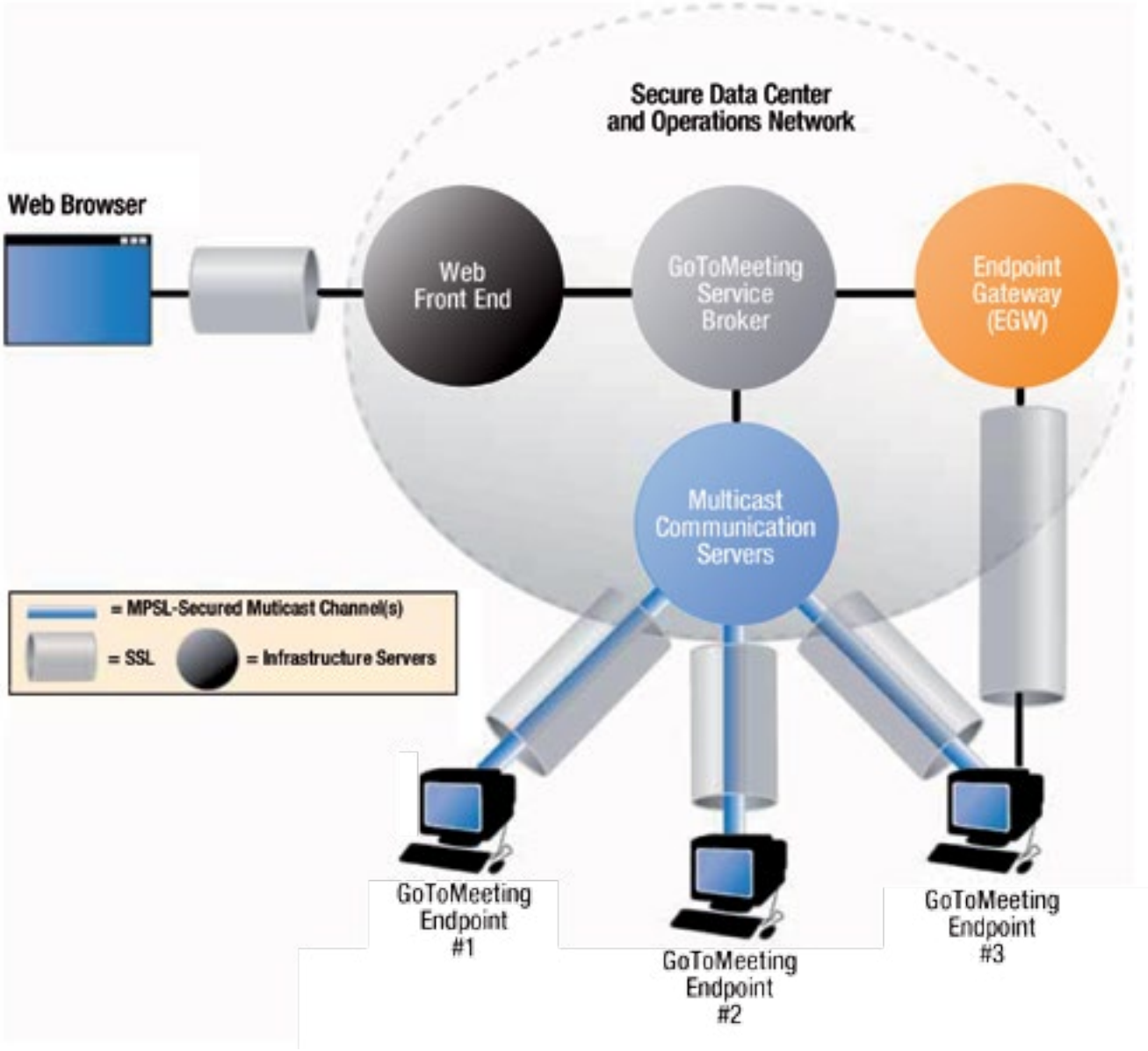
Es ist wichtig zu beachten, dass das optionale Kennwort nie an Citrix übertragen wird. Dies bietet die zusätzliche Gewissheit, dass keine unbefugten Personen (einschließlich Mitarbeiter von Citrix) an einer Sitzung teilnehmen können.

Die End-to-End-Authentifizierung erfolgt über das SRP-Protokoll (Secure Remote Password). SRP ist ein etabliertes, robustes und sicheres kennwortbasiertes Authentifizierungs- und Schlüsselaustauschverfahren. SRP ist widersteht einer Vielzahl von Angriffen, darunter passives Abhören und aktives Knacken von Kennwörtern. (Weitere Informationen zu SRP finden Sie unter http://srp.stanford.edu.)

Aufgrund der zweistufigen Teilnehmerauthentifizierung können GoToMeeting, GoToWebinar und GoToTraining sicherstellen, dass nur autorisierte Teilnehmer Sitzungen beitreten können, zu denen sie eingeladen wurden, und dass jedem Benutzer die Berechtigungen zugewiesen werden, die der zugewiesenen Rolle entsprechen.

Sicherheit der Administrations-Seite

Wie alle Verbindungen mit der Website von GoToMeeting, GoToWebinar und GoToTraining sind auch die Verbindungen zum Administrationsportal mittels SSL/TLS geschützt. Administrative Funktionen werden durch starke Kennwörter, Aktivitätsprotokollierung, regelmäßige Audits und eine Vielzahl von internen physischen und Netzwerksicherheitskontrollen geschützt.



Sicherheitsfunktionen für die Kommunikation

Die Kommunikation zwischen den Teilnehmern in einer GoToMeeting-, GoToWebinar- oder GoToTraining-Sitzung erfolgt über einen Overlay-Multicast-Netzwerkstapel, der logisch über dem konventionellen TCP/IP-Stapel auf den PCs der einzelnen Benutzer angeordnet ist. Dieses Netzwerk wird durch eine Gruppe von Multicast-Kommunikations-Servern (Multicast Communications Servers, MCS) realisiert, die von Citrix betrieben werden. Diese Kommunikationsarchitektur wird in der unten stehenden Abbildung dargestellt.

Teilnehmer (Sitzungsendpunkte) kommunizieren über ausgehende TCP/IP-Verbindungen auf den Ports 8200, 443 und 80 mit Kommunikations-Servern und Gateways der Citrix Infrastruktur. Da es sich bei GoToMeeting, GoToWebinar und GoToTraining um gehostete, webbasierte Dienste handelt, können sich die Teilnehmer überall im Internet befinden – in einem Büro an einem anderen Standort, zu Hause, in einem Business-Center oder im Netzwerk eines anderen Unternehmens. Der jederzeit und von jedem Ort aus mögliche Zugriff auf die Dienste von GoToMeeting, GoToWebinar und GoToTraining bietet ein Maximum an Flexibilität und Konnektivität.

Um jedoch auch die Vertraulichkeit und Integrität der nichtöffentlichen Geschäftskommunikation zu bewahren, verfügen diese Tools auch über robuste Sicherheitsfunktionen für die Kommunikation.

Vertraulichkeit und Integrität der Kommunikation

GoToMeeting, GoToWebinar und GoToTraining bieten echte End-to-End-Datensicherheitsmechanismen, die passive und aktive Angriffe gegen die Vertraulichkeit, Integrität und Verfügbarkeit abdecken. Alle Verbindungen sind End-to-End-verschlüsselt und nur für autorisierte Sitzungsteilnehmer zugänglich.

Die Daten, die bei der Bildschirmfreigabe, Tastatur- und Maussteuerung und in Text-Chats anfallen, sind nie unverschlüsselt, während sie sich vorübergehend auf den Kommunikationsservern von Citrix befinden oder über öffentliche oder private Netzwerke übertragen werden.

Kommunikationssicherheitskontrollen basieren auf starker Kryptografie und sind auf zwei Schichten implementiert: der „TCP-Schicht“ und der „Multicast-Paketsicherheitsschicht“ (MPSL).

Sicherheit der TCP-Schicht

Die in IETF-Standards definierten Protokolle SSL (Secure Sockets Layer) und TLS (Transport Layer Security) werden verwendet, um die gesamte Kommunikation zwischen Endpunkten zu schützen. Um ein Höchstmaß an Schutz vor Abhöraktionen, Modifikationen oder Replay-Attacken zu erreichen, wird als einzige SSL-Cipher-Suite für Nicht-Website-Verbindungen über TCP nur 1024-Bit-RSA mit 128-Bit-AES-CBC und HMAC-SHA1 unterstützt. Für maximale Kompatibilität mit nahezu jedem Desktop-Webbrowser unterstützt die Website von GoToMeeting, GoToWebinar und GoToTraining jedoch eingehende Verbindungen mit den meisten unterstützten SSL-Cipher-Suites.

Citrix empfiehlt den Kunden, zur eigenen Sicherheit die Browser so zu konfigurieren, dass standardmäßig und nach Möglichkeit immer starke Kryptografie verwendet wird, und immer die aktuellsten Patches für das Betriebssystem und den Browser zu installieren.

Wenn SSL/TLS-Verbindungen mit der Website und zwischen den Komponenten von GoToMeeting, GoToWebinar oder GoToTraining aufgebaut werden, authentifizieren sich die Citrix Server bei den Clients mit Zertifikaten für öffentliche Schlüssel von VeriSign/Thawte. Als weitere Sicherheitsvorkehrung gegen Infrastrukturangriffe erfolgt eine gegenseitige, zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z. B. MCS-zu-MCS, MCS-zu-Broker). Diese starken Authentifizierungsmaßnahmen hindern potenzielle Angreifer daran, sich als Infrastrukturserver zu tarnen oder sich in eine Sitzungsdatenübertragung einzuklinken.

Sicherheit der Multicast-Schicht

Zusätzliche Funktionen bieten eine vollständige End-to-End-Sicherheit für Multicast-Paketdaten, unabhängig von den von SSL/TLS gebotenen Funktionen. Insbesondere werden sämtliche Multicast-Sitzungsdaten durch End-to-End-Verschlüsselung und Integritätsmechanismen geschützt, die jeden mit Zugriff auf unsere Server – ganz gleich, ob Freund oder Feind – daran hindern, eine Sitzung abzuhören oder Daten unerkannt zu manipulieren. Diese zusätzliche Stufe in der Vertraulichkeit und Integrität der Kommunikation gibt es nur bei unseren Produkten. Die Kommunikation eines Unternehmens wird nie für Dritte sichtbar. Dies gilt auch für Benutzer, die zu einer bestimmten Sitzung nicht eingeladen sind, sowie für Citrix selbst.

Die Einrichtung des MPSL-Schlüssels erfolgt über eine Schlüsselvereinbarung, die auf öffentlichen Schlüsseln basiert und über SRP 6 authentifiziert wurde. Dabei wird zum Aufbau eines Wrapping-Schlüssels ein 1024-Bit-Modulus verwendet. Dieser Wrapping-Schlüssel wird anschließend zum symmetrischen Gruppenschlüsselaustausch über den 128-Bit-AES-CTR-Algorithmus verwendet (siehe http://srp.stanford.edu/design.html). Alle schlüsselrelevanten Materialien werden über einen FIPS-konformen Pseudozufallszahlengenerator generiert, der zur Laufzeit mit Entropiedaten gefüttert wird, die aus verschiedenen Stellen des Host-Computers stammen. Diese robusten und dynamischen Methoden zur Schlüsselgenerierung und zum Schlüsselaustausch bieten einen starken Schutz vor dem Erraten oder Knacken von Schlüsseln.

Des Weiteren schützt MPSL Multicast-Paketdaten vor Abhörversuchen mithilfe einer 128-Bit-AES-Verschlüsselung im Counter-Modus. Klartextdaten werden in der Regel vor der Verschlüsselung mit proprietären Hochleistungstechniken zur Optimierung der Bandbreite komprimiert. Der Schutz der Datenintegrität wird durch einen Integritätskontrollwert erreicht, der mit dem HMAC-SHA-1-Algorithmus generiert wird. Da GoToMeeting, GoToWebinar und GoToTraining sehr starke, auf Industriestandards basierende Verschlüsselungsverfahren einsetzen, können die Kunden darauf vertrauen, dass die Multicast-Sitzungsdaten vor unbefugter Offenlegung oder unentdeckter Modifikation geschützt sind.

Darüber hinaus gibt es keine zusätzlichen Kosten, keine Leistungseinbußen und keine Einschränkungen der Nutzbarkeit durch diese wichtigen Maßnahmen zur Kommunikationssicherheit. Hohe Leistung und auf Standards basierende Datensicherheit ist Bestandteil jeder Sitzung.

Kompatibilität mit Firewalls und Proxyservern

Wie andere Produkte von Citrix auch, verfügen GoToMeeting, GoToWebinar und GoToTraining über eine integrierte Erkennung von Proxyservern und eine Logik zur Verbindungsverwaltung, die eine automatisierte Softwareinstallation unterstützt, eine komplexe (Neu-)Konfiguration des Netzwerks vermeidet und so die Benutzerproduktivität maximiert. Firewalls und Proxyserver, die bereits Teil Ihres Netzwerks sind, müssen nicht speziell konfiguriert werden, um die Nutzung unserer Webkonferenz-Tools zu ermöglichen.

Wenn die Endpunkt-Software von GoToMeeting, GoToWebinar oder GoToTraining gestartet wird, versucht diese, den Servicebroker über das Endpunkt-Gateway (EGW) zu erreichen, indem eine oder mehrere ausgehende, SSL-geschützte TCP-Verbindungen auf den Ports 8200, 443 und/oder 80 aufgebaut werden. Die Verbindung, die zuerst antwortet, wird verwendet, die anderen verworfen. Diese Verbindung bietet die Grundlage zur Teilnahme an allen zukünftigen Sitzungen, indem die Kommunikation zwischen den gehosteten Servern und dem Desktop des Benutzers ermöglicht wird.

Wenn ein Benutzer versucht, einer Sitzung beizutreten, stellt die Endpunkt-Software eine oder mehrere zusätzliche Verbindungen zu den Kommunikations-Servern von Citrix her. Dazu werden wieder SSL-geschützte TCP-Verbindungen auf den Ports 8200, 443 und/oder 80 verwendet. Über diese Verbindungen werden während einer aktiven Sitzung die Daten übertragen.

Zur Optimierung der Konnektivität initiiert die Endpunkt-Software eine oder mehrere kurzlebige TCP-Verbindungen auf den Ports 8200, 443 und/oder 80, die nicht mit SSL geschützt sind. Diese „Netzwerkfühler“ enthalten keine vertraulichen oder verwertbaren Informationen, sodass keine Gefahr der Offenlegung vertraulicher Daten besteht.

GoToMeeting, GoToWebinar und GoToTraining bieten ein Höchstmaß an Kompatibilität mit bestehenden Netzwerksicherheitsvorkehrungen, da sie sich automatisch an die Gegebenheiten des lokalen Netzwerks anpassen, indem ausschließlich ausgehende Verbindungen über einen Port verwendet werden, der in den meisten Firewalls und Proxyservern bereits geöffnet ist. Im Gegensatz zu einigen anderen Produkten müssen die Unternehmen keine vorhandenen Sicherheitsmaßnahmen deaktivieren, um Webkonferenzen zu ermöglichen. Diese Eigenschaften maximieren sowohl die Kompatibilität als auch die Sicherheit des gesamten Netzwerks.

Sicherheit bei der Sprachübertragung

Citrix bietet integrierte Audiokonferenzen für GoToMeeting-, GoToWebinar- und GoToTraining-Sitzungen sowohl über normale Telefonverbindungen als auch über VoIP (Voice over Internet Protocol). Normale Telefonverbindungen sind von Haus aus auf die Vertraulichkeit und Integrität der Sprachverbindungen ausgerichtet. Zum Schutz der Vertraulichkeit und Integrität der VoIP-Verbindungen zwischen den Endpunkten und den Servern verwenden wir ein SRTP mit einem AES-128-HMAC-SHA1-basierten Protokoll über UDP und TLS-RSA-1024-AES-128-HMAC-SHA1 über TCP.

Sicherheitsfunktionen für die Endpunkte

Webkonferenz-Software muss mit einer Vielzahl von Desktop-Umgebungen kompatibel und selbst ein sicherer Endpunkt auf einem Benutzer-Desktop sein. GoToMeeting, GoToWebinar und GoToTraining erreichen dies über Programme, die aus dem Web heruntergeladen werden und starke Verschlüsselungsmechanismen bieten.

Signierte Endpunkt-Software

Bei unserer Client-Endpunkt-Software handelt es sich um eine Win32-Programmdatei, die auf die Computer der Endbenutzer heruntergeladen wird. Ein digital signiertes Java-Applet wird verwendet, um den Download von den Citrix Servern zu vermitteln und die Integrität der GoToMeeting-, GoToWebinar- und GoToTraining-Endpunkt-Software zu verifizieren. Dadurch werden die Benutzer vor einer versehentlichen Installation eines Trojaners oder einer anderen Malware, die sich als unsere Software ausgibt, geschützt.

Die Endpunkt-Software besteht aus mehreren Win32-Programm- und DLL-Dateien. Citrix führt während der Entwicklung und Bereitstellung strenge Qualitätskontrollen und Konfigurationsverwaltungsverfahren durch, um die Sicherheit der Software zu gewährleisten. Die Endpunkt-Software verfügt über keine extern zugänglichen Netzwerkschnittstellen und kann nicht von Malware oder Viren verwendet werden, um Remote-Systeme auszunutzen oder zu infizieren. Dadurch werden andere Desktops, die an einer Sitzung teilnehmen, vor der Infizierung durch einen infizierten Computer eines anderen Sitzungsteilnehmers geschützt.

Implementierung des kryptografischen Subsystems

Alle kryptografischen Funktionen und Sicherheitsprotokolle, die von der Client-Endpunkt-Software von GoToMeeting, GoToWebinar und GoToTraining eingesetzt werden, wurden mithilfe der modernen Bibliotheken von ® Crypto™ und Certicom Security Builder® SSL™ implementiert, um Sicherheit und Leistung zu gewährleisten.

Die kryptografischen Bibliotheken können nur von den Endpunktanwendungen von GoToMeeting, GoToWebinar und GoToTraining verwendet werden. Es sind keine externen APIs für den Zugriff durch andere Software, die auf dem jeweiligen Desktop ausgeführt wird, vorhanden. Alle Verschlüsse-

lungs- und Integritätsalgorithmen, Schlüsselgrößen und anderen Parameter der kryptografischen Richtlinien werden statisch kodiert, während die Anwendung kompiliert wird. Da keine vom Endbenutzer konfigurierbaren kryptografischen Einstellungen vorhanden sind, ist es unmöglich, dass unsere Sicherheitsmaßnahmen durch eine versehentliche oder absichtliche Fehlkonfiguration geschwächt werden. Ein Unternehmen, das GoToMeeting, GoToWebinar und/oder GoToTraining einsetzt, kann sicher sein, dass alle Webkonferenzen dieselben hohen Sicherheitsstandards einhalten, unabhängig davon, wem ein teilnehmender Desktop gehört oder wer ihn betreibt.

Sicherheitsfunktionen der gehosteten Infrastruktur

Citrix stellt GoToMeeting, GoToWebinar und GoToTraining über ein ASP-Modell bereit, das einen stabilen und sicheren Betrieb gewährleistet und sich dabei nahtlos in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt.

Skalierbare und zuverlässige Infrastruktur

Die Service-Architektur von Citrix ist für maximale Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt. GoToMeeting, GoToWebinar und GoToTraining werden auf industriestandardkonformen Hochleistungs-Servern betrieben, auf denen die neuesten Sicherheits-Patches installiert sind. Redundante Switches und Router sind Teil der Architektur, damit es nie eine alleinige Fehlerstelle gibt. Geclusterte Server und Backup-Systeme garantieren einen nahtlosen Fluss der Anwendungsprozesse, selbst bei einer hohen Auslastung oder einem Systemausfall. Um eine optimale Leistung zu erreichen, verteilen die Broker von GoToMeeting, GoToWebinar und GoToTraining die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikations-Server.

Physische Sicherheit

Alle Web-, Anwendungs-, Kommunikations- und Datenbank-Server von Citrix befinden sich in Rechenzentren an sicheren Kollokationsstandorten. Der physische Zugang zu den Servern ist stark eingeschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante Stromversorgungs- und Kühlungseinrichtungen.

Netzwerksicherheit

Citrix betreibt Firewalls, Router und eine VPN-basierte Zugangskontrolle, um seine privaten Netze und Backend-Server abzusichern. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und externe Sicherheitsexperten führen regelmäßige Tests auf Schwachstellen durch.

Kundenseitiger Datenschutz

Da das Vertrauen unserer Kunden höchste Priorität für uns hat, verpflichtet sich Citrix, Ihre Daten zu schützen. Einen Link zu unserer aktuellen Datenschutzerklärung finden Sie online unter www.gotomeeting.de.

Fazit

Mit GoToMeeting, GoToWebinar und GoToTraining ist es auf einfache Weise möglich, die geschäftliche Kommunikation zu verbessern und online Meetings abzuhalten, Informationen zu präsentieren und Produkte vorzuführen. Die intuitiven Benutzeroberflächen und die Funktionsvielfalt machen diese Tools zu äußerst effektiven Lösungen für Webkonferenzen.

Im Hintergrund stellt die gehostete Service-Architektur von Citrix transparent eine sichere und zuverlässige Umgebung für die verteilte Zusammenarbeit bereit. Wie in diesem Whitepaper aufgezeigt wird, bieten GoToMeeting, GoToWebinar und GoToTraining eine einfache Bedienung und Flexibilität, ohne dabei die Integrität, den Datenschutz oder die administrative Kontrolle über die geschäftliche Kommunikation oder geschäftliche Güter zu gefährden.

Anhang: Sicherheitsstandards

GoToMeeting, GoToWebinar und GoToTraining erfüllen die Anforderungen der folgenden Industriestandards und Standards der US-Regierung für kryptografische Algorithmen und Sicherheitsprotokolle:

- TLS/SSL-Protokoll, Version 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
- AES-Cipher-Suites für TLS, IETF RFC 3268
- RSA, PKCS #1
- SHA-1, FIPS 180-1
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Generierung von Pseudozufallszahlen, ANSI X9.62 und FIPS 140-2

Citrix Online

Die Online Services Division von Citrix stellt sichere und spielend einfach zu bedienende cloud-basierte Lösungen für orts- und zeitunabhängige Zusammenarbeit bereit. Unternehmen und Anwender steigern mit diesen ihre Produktivität, senken Reisekosten und optimieren ihre globalen Vertriebsaktivitäten sowie Schulungs- und Serviceangebote.
Unser Portfolio: GoToMeeting für Online-Meetings, GoToWebinar für Online-Events, GoToTraining für Mitarbeiter- und Kundenschulungen, GoToMyPC für den jederzeitigen Zugriff auf entfernte Macs® oder PCs, GoToAssist für IT-Support und -Management sowie ShareFile, um auf sichere Weise Dateien, Dokumente und Daten zu teilen.
Weitere Informationen erhalten Sie unter www.citrixonline.de

GoToMeeting kostenlos testen:

Deutschland: 0800 182 0591
Schweiz: 0800 836 785
Österreich: 0800 292 810
http://www.gotomeeting.de

CITRIX® | online

Citrix Online Division
7414 Hollister Avenue
Goleta, CA 93117
U.S.A.
T +1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe
Middle East & Africa
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific
Level 3, 1 Julius Ave
Riverside Corporate Park
North Ryde NSW 2113
Australia
T +61 2 8870 0870
asiapac@citrixonline.com

Über Citrix
Citrix Systems, Inc. verändert die Art und Weise, wie Personen, Unternehmen und IT in Zeiten von Cloud-Computing zusammenarbeiten. Das Portfolio der GoTo Cloud Services bietet Personen dafür einfach zu bedienende, cloud-basierte Lösungen für ortsunabhängige Zusammenarbeit sowie Remote-Zugriff und IT-Support, die sich in allen Geschäftsbereichen einsetzen lassen.
Erfahren Sie mehr unter www.citrix.de und www.citrixonline.de

©2012 Citrix Online, UK Ltd. Alle Rechte vorbehalten. Citrix® ist eine eingetragene Marke von Citrix Systems, Inc. GoToAssist, GoToMeeting, GoToMyPC, GoToTraining und GoToWebinar sind Marken von Citrix Systems, LLC, und können beim US-Patent und Markenamt sowie in anderen Ländern eingetragen sein. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. Mac und iPad sind Marken von Apple Inc., die in den USA und in anderen Ländern eingetragen sind. Android ist eine eingetragene Marke von Google, Inc.

058DE_WP/B-50216/2012-06-28