GoToMeeting

Whitepaper

Die Sicherheit der GoTo Webconferencing-Lösungen

GoTo Webconferencing-Tools bieten stabile „End-to-End“-Datensicherheitsmechanismen, die bei der Nutzung von GoToMeeting, GoToWebinar und GoToTraining sowohl vor passiven als auch aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten schützen.

GoToMeeting, GoToWebinar und GoToTraining gehören zu den sichersten Webconferencing-Produkten, die derzeit auf dem Markt erhältlich 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 in GoToMeeting, GoToWebinar und GoToTraining integrierten Sicherheitsfunktionen. Es ist für technische Gutachter und Sicherheitsspezialisten vorgesehen, die für die Sicherheit eines Unternehmensnetzwerks, den Datenschutz und die Integrität der geschäftlichen Kommunikation verantwortlich sind.

GoToMeeting, GoToWebinar und GoToTraining sind Webconferencing-Lösungen, die mittels Bildschirmübertragung, Remote-Steuerung von Tastatur und Maus, Chat und anderer Funktionen die Interaktion mehrerer PC- und Mac-Benutzer ermöglichen. GoToMeeting ist ideal für Vertriebsdemos und kooperative Online-Meetings geeignet. GoToWebinar ist auf ein größeres Publikum zugeschnitten und eignet sich hervorragend für Marketing-präsentationen und Unternehmensveranstaltungen. Und GoToTraining bietet spezielle Funktionen für webbasierte Schulungen, wie z.B. einen Online-Zugang zu Tests und Schulungsmaterialien sowie einen gehosteten Kurskatalog.

Bei diesen Produkten handelt es sich um gehostete Dienste, die über Webbrowser, herunterladbare und ausführbare Client-Dateien und ein Netzwerk verschiedener Multicast-Kommunikationsserver bereitgestellt werden. Sitzungen werden über GoTo Webseiten oder über Client-Software geplant, einberufen und moderiert. Aus Gründen der Benutzerfreundlichkeit sind VoIP- und Telefonkonferenzfunktionen bereits in GoToMeeting, GoToWebinar und GoToTraining integriert.

Sichere Zusammenarbeit ist für jedes Unternehmen entscheidend

Einfach zu nutzende Online-Lösungen 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 Produkte unterscheiden sich jedoch 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 Webconferencing-Lösungen 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 Webconferencing-Lösungen wurden von Grund auf so entwickelt, dass die 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 Schulungssitzungen zu planen. Ein Organisator bereitet eine Sitzung vor, lädt andere Benutzer ein, initiiert und beendet die Sitzung und bestimmt, wer die Moderation übernimmt.
- Teilnehmer sind berechtigt, an einer Sitzung teilzunehmen. Die Teilnehmer sehen den Bildschirm des Moderators, können mit anderen Teilnehmern chatten und die Teilnehmerliste einsehen.
- Moderatoren sind Teilnehmer, die ihren Bildschirm für die anderen Teilnehmer übertragen können. Moderatoren entscheiden außerdem, welchem anderen Teilnehmer ggf. die Kontrolle über Tastatur und Maus des Moderatoren-Computers übergeben werden darf.
- Bei internen Administratoren handelt es sich um Mitarbeiter, 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. Externe Administratoren können Kontofunktionen konfigurieren, Organisatoren autorisieren und haben Zugang zu verschiedenen Berichterstattungsfunktionen.

Die Benutzeroberflächen von GoToMeeting, GoToWebinar und GoToTraining bieten intuitive Funktionen zur Sitzungsverwaltung und Statusanzeigen, um produktive und sichere Online-Sitzungen zu ermöglichen.

Welche Bedienfunktionen und Berechtigungen für die einzelnen Benutzer zur Verfügung stehen, hängt von der aktuell zugewiesenen Rolle ab: Organisator, aktiver Moderator oder allgemeiner Teilnehmer.

Berechtigungen des Organisators

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

Zu den speziellen Berechtigungen von Organisatoren zählen beispielsweise 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.
- Die Berechtigung, jeden beliebigen Teilnehmer zum aktiven Moderator hochzustufen und zu bestimmen, welcher Desktop jeweils angezeigt wird.
- Deaktivieren der Chatfunktion für einen oder mehrere Teilnehmer. Zulassen von Nebendiskussionen nur dann, wenn dies sinnvoll ist.
- Die Berechtigung, die Verbindung von Teilnehmern zu trennen.
- 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 des Moderators

Ein Moderator kann seinen Bildschirm für andere Teilnehmer freigeben. Innerhalb einer Sitzung kann immer nur einem Teilnehmer die aktive Moderatorrolle zugewiesen werden. Moderatoren verfügen über folgende Steuerungsmöglichkeiten:

- Aktivieren, Deaktivieren oder Pausieren der gemeinsamen Bildschirmnutzung, wobei Letzteres nützlich ist, um die Offenlegung vertraulicher Daten zu verhindern, die auf dem Desktop des Moderators 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 Moderatorrolle an einen anderen Teilnehmer, um während der Sitzung einen flexiblen und dynamischen Ablauf zu erreichen.

Sobald der Moderator seinen Bildschirm für die anderen Teilnehmer freigegeben hat, wird dies auf seinem Bedienpanel angezeigt. Um den Bildschirm freizugeben, muss der Moderator im Bedienpanel auf die Schaltfläche „Meinen Bildschirm übertragen“ klicken. Durch diese Funktionen wird sichergestellt, dass der Moderator immer weiß, wann die Bildschirmfreigabe aktiv ist, damit Desktop-Inhalte nicht unbeabsichtigt für andere Teilnehmer sichtbar gemacht werden.

Berechtigungen der Teilnehmer

Reguläre Teilnehmer verfügen über folgende Berechtigungen:

- Teilnehmen an einer Sitzung, zu der sie vor dem Start und während der Sitzung eingeladen wurden.
- Anzeigen des Moderatorbildschirms, sofern der Moderator die gemeinsame

Bildschirmnutzung nicht pausiert oder deaktiviert hat.
- Steuern der Tastatur und Maus des Moderators, sofern der Moderator dies zulässt. (Die Berechtigung zur Fernsteuerung wird automatisch entzogen, wenn die Rolle des aktiven Moderators weitergegeben wird.)
- Verwenden der Chatfunktion zum Senden von Textnachrichten an alle oder bestimmte Teilnehmer. (Die Chatfunktion 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 Moderator wechseln. Die Moderatoren behalten die vollständige Kontrolle über ihren Desktop, während die Organisatoren über alle erforderlichen Funktionen zur effektiven Verwaltung der Sitzung verfügen.

Funktionen zur Konto- und Sitzungsauthentifizierung

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

Kundenkonto-Anmeldung über die 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 denjenigen Benutzern angezeigt werden, die sich erfolgreich authentifiziert haben und außerdem zu deren Anzeige berechtigt sind, sind potenziell vertrauliche Informationen wie beispielsweise das Thema der Sitzung, der Name des Organisators und der Sitzungstermin nie für Hacker, neugierige Websurfer oder Mitbewerber sichtbar.

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 der Erstellung einer Sitzung erhält der Organisator eine eindeutige, 9-stellige Sitzungs-ID, die vom GoToMeeting, GoToWebinar oder GoToTraining Service Broker mittels eines Generators von Pseudozufallszahlen erstellt wird. Diese Sitzungs-ID kann dann allen eingeladenen Teilnehmern per E-Mail, Instant-Messaging, Telefon oder auf anderen Kommunikationswegen übermittelt werden.

Wenn ein Teilnehmer einer Sitzung beitreten möchte, muss er zunächst die Sitzungs-ID an den Service Broker übermitteln. Dies geschieht durch Klicken auf eine URL, die 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 Service Broker 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 wird 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 Zufalls-wert, der vom Service Broker 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 empfehlen wir nachdrücklich die Verwendung der Kennwortfunktion.

Es ist wichtig zu beachten, dass das optionale Kennwort nie an uns übertragen wird. Dies bietet die zusätzliche Gewissheit, dass keine unbefugten Personen (einschließlich unserer Mitarbeiter) 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 widersteht einer Vielzahl von Angriffen, darunter sowohl passives Abhören und als auch aktives Knacken von Kennwörtern.

(Weitere Informationen zu SRP finden Sie unter http://srp. stanford.edu)

GoToMeeting, GoToWebinar und GoToTraining bieten zwei Ebenen der Teilnehmerauthentifizierung. Dadurch wird sichergestellt, dass nur autorisierte Teilnehmer an Sitzungen teilnehmen können, zu denen sie eingeladen wurden, und dass jeder Benutzer diejenigen Berechtigungen erhält, die seiner jeweiligen Rolle entsprechen.

Sicherheit der Administrationswebsite

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 der Teilnehmer einer GoToMeeting, GoToWebinar oder GoToTraining Sitzung erfolgt über einen Overlay-Multicast-Netzwerkstapel, der logisch über dem konventionellen TCP/IP-Stapel auf den Computern der einzelnen Benutzer angeordnet ist. Dieses Netzwerk wird durch eine Gruppe von Multicast-Kommunikationsservern (Multicast Communications Servers, MCS) realisiert, die von uns betrieben werden.

Teilnehmer (Sitzungsendpunkte) kommunizieren über ausgehende TCP/IP-Verbindungen auf den Ports 8200, 443 und 80 mit Kommunikationsservern und Gateways der GoTo 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 nicht öffentlichen Geschäftskommunikation zu bewahren, verfügen diese Tools auch über robuste Sicherheitsfunktionen für die Kommunikation.

Vertraulichkeit und Integrität der Kommunikation

GoToMeeting, GoToWebinar und GoToTraining bieten stabile „End-to-End"-Datensicherheitsmechanismen, die sowohl vor passiven als auch aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten schützen. Alle Verbindungen sind End-to-End-verschlüsselt und nur für autorisierte Sitzungsteilnehmer zugänglich.

Die Daten, die bei der Bildschirmfreigabe, Tastatur- und Maussteuerung, Dateiübertragung, Remote-Diagnose und in Text-Chats anfallen, während sie temporär auf den Kommunikationsservern gespeichert sind oder über öffentliche oder private Netzwerke übertragen werden, sind niemals unverschlüsselt einsehbar.

Kommunikationssicherheitskontrollen basieren auf starker Kryptografie und sind auf zwei Schichten implementiert: der TCP-Schicht und der Multicast-Paket-Sicherheitsschicht (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.

Kunden wird empfohlen, zur eigenen Sicherheit die Browser so zu konfigurieren, dass standardmäßig und nach Möglichkeit immer sichere Verschlüsselung verwendet wird, und stets die aktuellen 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 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 die Kommunikation von Support-Sitzungen einzubinden.

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 uns selbst.

Die Schlüsselerstellung für die Multicast-Paket-Sicherheitsstufe erfolgt mittels eines zufällig generierten 128-Bit-Schlüssels, der vom Service Broker ausgewählt und über TLS an alle Endpunkte verteilt wird. Er wird als Eingabe für eine vom NIST bestätigte HMAC-SHA1-basierte Schlüsselableitungsfunktion verwendet. Bei Beendigung der Sitzung wird der Schlüsselwert aus dem Service Broker-Speicher gelöscht.

Des Weiteren schützt MPSL Multicast-Paketdaten vor Abhörversuchen mithilfe einer 128-Bit-AES-Verschlüsselung im Counter-Modus. Klartextdaten werden 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.

Trotz dieser wichtigen Kommunikationssicherheitsfunktionen entstehen keine zusätzlichen Kosten, Leistungsabfälle oder Beeinträchtigungen der Benutzerfreundlichkeit. Hohe Leistung und auf Standards basierende Datensicherheit sind Bestandteil jeder Sitzung.

Kompatibilität mit Firewalls und Proxyservern

GoToMeeting, GoToWebinar und GoToTraining enthalten eine integrierte Proxy-Erkennungs- und Verbindungsverwaltungslogik, die eine automatisierte

Softwareinstallation unterstützt, komplexe (Neu-)Konfigurationen vermeidet und gleichzeitig 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 Endpunktsoftware von GoToMeeting, GoToWebinar oder GoToTraining gestartet wird, wird über das Endpunkt-Gateway (EGW) eine Verbindung mit dem Service Broker hergestellt, indem eine oder mehrere ausgehende SSL-geschützte TCP-Verbindungen über die Ports 8200, 443 und/oder 80 initiiert werden. Die Verbindung, die zuerst antwortet, wird verwendet, die anderen werden verworfen. Diese Verbindung ist die Grundlage für die Teilnahme an allen zukünftigen Sitzungen und ermöglicht die Kommunikation zwischen den gehosteten Servern und dem Benutzer-Desktop.

Wenn der Benutzer an einer Sitzung teilnehmen möchte, stellt die Endpunkt-Software eine oder mehrere zusätzlichen Verbindungen mit den Kommunikations-servern 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 Sitzung.

Zur Optimierung der Konnektivität initiiert die Endpunkt-Software eine oder mehrere kurzlebige TCP-Verbindungen auf den Ports 8200, 443 und/oder 80, die nicht durch 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

GoToMeeting, GoToWebinar und GoToTraining bieten integrierte Audio-Konferenzen für Sitzungen über das Telefonnetz (PSTN) und über VoIP (Voice over Internet Protocol). PSTN gewährleistet bereits die Vertraulichkeit und Integrität der Sprachkommunikation. 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.

Sicherheit der Videoübertragung

GoToMeeting, GoToWebinar und GoToTraining bieten integrierte Videokonferenzen für Sitzungen über das Internet.
Um die Vertraulichkeit und Integrität der Videoverbindungen von den Endpunkten zu den Videoservern sicherzustellen, wird ein SRTP mit AES-128-HMAC-SHA1-basiertem Protokoll verwendet. Der Schlüsselaustausch zwischen Client und Server erfolgt über eine TLS-geschützte TCP-Verbindung.

Sicherheitsfunktionen für die Endpunkte

Webconferencing-Software muss mit einer Vielzahl von Desktop-Umgebungen kompatibel sein und dennoch auf dem jeweiligen Benutzer-Desktop einen sicheren Endpunkt erstellen. GoToMeeting, GoToWebinar und GoToTraining erreichen

dies durch ausführbare Dateien mit sicheren Verschlüsselungsmethoden, die aus dem Internet heruntergeladen werden.

Signierte Endpunkt-Software

Alle ausführbaren Dateien sind digital signiert, um die Integrität zu schützen. Während der Entwicklung und Bereitstellung werden strenge Qualitätskontrollen und Konfigurationsverwaltungsverfahren durchgeführt, 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. Hierdurch werden Desktops, die an Sitzungen teilnehmen, vor einer Infizierung durch einen von einem anderen Teilnehmer verwendeten, gefährdeten Host geschützt.

Implementierung des kryptografischen Subsystems

Alle von der Software für GoToMeeting, GoToWebinar und GoToTraining Client-Endpunkte verwendeten Verschlüsselungsfunktionen und Sicherheitsprotokolle werden mit Open Source-OpenSSL-Verschlüsselungsbibliotheken implementiert.

Die Verwendung der Verschlüsselungsbibliotheken ist auf die GoToMeeting, GoToWebinar und GoToTraining Endpunktanwendungen beschränkt. Es sind keine externen APIs vorhanden, auf die andere auf diesem Desktop ausgeführte Anwendungen möglicherweise zugreifen könnten. Alle Verschlüsselungs- und Integritätsalgorithmen, Schlüsselgrößen und anderen 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 beeinträchtigen. 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

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

Skalierbare und zuverlässige Infrastruktur

Unsere globale Service-Architektur ist für maximale Leistung, Zuverlässigkeit und Skalierbarkeit ausgelegt. GoToMeeting, GoToWebinar und GoToTraining werden auf industriestandardkonformen Hochleistungsservern betrieben, auf denen die neuesten Sicherheitspatches installiert sind. Redundante Switches und Router sind Teil der Architektur, damit es nie einen ‚Single Point of Failure' 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 Kommunikationsserver .

Physische Sicherheit

Alle Web-, Anwendungs-, Kommunikations- und Datenbankserver sind in sicheren Rechenzentren untergebracht. Der physische Zugang zu den Servern ist stark eingeschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante

Anhang: Kompatibilität mit Sicherheitsstandards

GoToMeeting, GoToWebinar und GoToTraining erfüllen die Anforderungen der folgenden Industriestandards 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 Nr. 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

Stromversorgungseinrichtungen und Umweltkontrollen.

Netzwerksicherheit

Firewalls, Router und eine VPN-basierte Zugangskontrolle sichern unsere privaten Netze und Backend-Server ab. Die Sicherheit der Infrastruktur wird ebenfalls kontinuierlich überwacht. Interne Mitarbeiter und externe Sicherheitsexperten führen regelmäßige Tests auf Schwachstellen durch.

Schutz der Kundendaten

Da das Vertrauen unserer Kunden höchste Priorität für uns hat, verpflichten wir uns, 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 transparent eine sichere und zuverlässige Umgebung für die Zusammenarbeit zwischen mehreren Endpunkten bereit. Wie in diesem Whitepaper aufgezeigt wird, bieten GoToMeeting, GoToWebinar und GoToTraining eine einfache Bedienung und große Flexibilität, ohne dabei die Integrität, den Datenschutz oder die administrative Kontrolle über die geschäftliche Kommunikation oder geschäftliche Güter zu gefährden.

Kontaktieren Sie uns

Gerne beraten wir Sie im persönlichen Gespräch oder stellen Ihnen ein kostenloses Testprodukt zur Verfügung. Rufen Sie einfach einen unserer Berater an, unter der gebührenfreien Telefonnummer 0800 182 0591. (Österreich: 0800 836 785; Schweiz: 0800 292 810).

545DE/WP/2017.07-01