

Whitepaper

Sicherheit bei Telefon- und Webkonferenzen.

Gemeinsam mehr erleben.



Vorwort

Telefon- und Webkonferenzen sind für viele Unternehmen zu einem unverzichtbaren Bestandteil des Arbeitsalltags geworden. Geschäftspartner und Projektteams können auf diese Weise an unterschiedlichen Orten und dennoch gemeinsam arbeiten. Zum Beispiel können Dokumente diskutiert und bearbeitet werden.

Die Sicherheit der Daten ist hierbei von höchster Priorität. Sämtliche Konferenzprodukte der Telekom werden daher grundsätzlich durch höchste technische und organisatorische Sicherheitsmaßnahmen geschützt, wodurch ein Datendiebstahl oder -missbrauch verhindert wird. Je nach Konferenzlösung kommen unterschiedliche Methoden zum Einsatz, die einen optimalen und perfekt abgestimmten Schutz gewährleisten.

Im Portfolio der Telekom stehen Konferenzen sowohl per Telefon als auch mit einem PC (Webkonferenzen) oder eine Kombination aus Telefon- und Webkonferenz zur Verfügung. Hierbei unterscheiden sich die einzelnen Angebote zusätzlich durch verschiedene Leistungsmerkmale, auf die in den folgenden Kapiteln ausführlicher eingegangen wird.

Zeitaufwendige Terminabsprachen und kostenintensive Anreisen fallen dank der modernen Kommunikationskanäle nicht mehr an. Vielmehr ermöglichen sie spontane Entscheidungen sowie schnelle Ergebnisse und steigern die Effizienz des Unternehmens. Diese innovative Art, Konferenzen und Meetings durchzuführen, schont die Umwelt, da die Telefon- und Webkonferenzen der Telekom CO₂-neutral angeboten werden.

Inhalt

Telefonkonferenz

4	1 Anwahlart
4	1.1 Dial-In
4	1.1.1 Einzelauftrag
4	1.1.2 Dauerauftrag
5	1.1.3 Anytime
5	1.2 Dial-Out
5	2 Erweitere Sicherheitsmaßnahmen
5	2.1 Rollcall
6	2.2 Entry/Exit Tone
6	2.3 Moderatoren- und Teilnehmer-Code
6	2.4 Sicherheits-Code
7	2.5 DTMF-Kommandos
8	3 Konferenzraumabschließen
8	4 Blacklisting für webgebuchte Konferenzen
8	5 Bereitstellung aufgezeichneter Konferenzen

Webportal

9	6 Portalseite
9	7 Konferenzportal
10	7.1 Software
10	7.2 Hardware
10	7.3 Best Practices
11	8 Benachrichtigungsdienst
11	9 Conference Control Panel

Webkonferenz

12	10 WebMeeting
-----------	----------------------

Weitere Sicherheitsmaßnahmen

15	11 Physikalische Sicherung
15	12 Conferencing Personal
16	13 Lieferantenbeziehungen
16	14 Resümee

Telefonkonferenz

Die Telefonkonferenz ist eine schnelle und sichere Möglichkeit, orts- und zeitunabhängig mit Geschäftspartnern und Mitarbeitern zu konferieren. Der Zugang ist sowohl über das Public Switched Telephone Network (einen klassischen ISDN- oder Analog-Telefonanschluss) oder alternativ über das Next Generation Network (IP-Telefonie) möglich.

1 Anwahlart

Grundsätzlich wird bei Telefonkonferenzen zwischen einer aktiven Einwahl der Teilnehmer (Dial-In, Onetime, Anytime) und der Anwahl durch eine Konferenzbrücke (Dial-Out) unterschieden.

1.1 Dial-In

Das Dial-In-Verfahren ist eine von mehreren Möglichkeiten, sich einer Telefonkonferenz anzuschließen. Die Teilnehmer wählen sich aktiv mittels eines gültigen Zugangs-Codes in die Konferenz ein. Der benötigte Code wird vor Beginn der Sitzung entweder durch einen Benachrichtigungsdienst, zum Beispiel in Form einer E-Mail-Einladung, oder durch den Veranstalter der Konferenz selbst zugestellt.

Des Weiteren wird prinzipiell zwischen dem Moderatoren-Code und dem Teilnehmer-Code unterschieden, die verschiedene Berechtigungen beinhalten. Somit ist es nur einem authentifizierten Moderator möglich, Steuerbefehle zum Beispiel mittels DTMF-Kommandos (Dual-Tone Multi-Frequency) abzusetzen.

Um sicherzustellen, dass sich kein Teilnehmer versehentlich in eine falsche Konferenz einwählt, werden die fünf- bis achtstelligen Einwahl-Codes nach Beendigung der Konferenz von der Wiedervergabe ausgenommen.

1.1.1 Einzelauftrag

Bei einer Onetime Konferenz handelt es sich um eine einmalige Konferenz zu einem vereinbarten Zeitpunkt. Die Zugangs-Codes für den Moderator und für die Teilnehmer sind nur dann gültig. Zudem sind die Codes nach Ende der Konferenz noch für einige Zeit reserviert, danach sind sie nicht mehr verwendbar.

1.1.2 Dauerauftrag

Als weitere Kommunikationslösung bekommen Interessenten auch einen Dauerauftrag angeboten. Hier wird eine bestimmte Anzahl von Konferenzen gebucht. Die Zugangs-Codes für den Moderator und die Teilnehmer bleiben in diesem Fall für alle Termine identisch – für einfache und bequeme Besprechungen. Der grundlegende Unterschied zur Anytime Konferenz besteht darin, dass die Zeiten der Meetings bereits im Vorfeld (bei Buchung) festgelegt werden und die Codes nur dann gültig sind.

1.1.3 Anytime

Kennzeichnend für eine Anytime Konferenz ist, dass die zugeteilten Moderatoren- und Teilnehmer-Codes nicht nur für einen einzelnen Termin gültig sind. Vielmehr können diese spontan und ohne erneute Buchung genutzt werden, zum Beispiel für den Jour fixe. Analog zur Onetime Konferenz bleiben die zugeteilten Codes nach dem Ende der virtuellen Besprechung noch für einige Zeit reserviert.

1.2 Dial-Out

Im Gegensatz zum Dial-In-Verfahren wählen sich die Teilnehmer bei einer Dial-Out Konferenz nicht aktiv in eine virtuelle Besprechung ein, sie werden bei diesem Verfahren mittels eines Triggers über eine Konferenzbrücke angewählt. Das geschieht entweder zeitgesteuert oder über ein webbasiertes Conference Control Panel. Alternativ kann diese Aufgabe auch an einen Operator des Callcenters übertragen werden.

Bei diesem Verfahren ist es notwendig, vor der Besprechung die Liste der anzurufenden Teilnehmer im System zu hinterlegen. Für noch mehr Sicherheit ist es möglich, nach erfolgreicher Einwahl einen weiteren Berechtigungs-Code als zusätzliche Schutzmaßnahme abzufragen. Nur authentifizierten Personen wird es ermöglicht, an der Konferenz teilzunehmen.

Optional kann der Moderator die Teilnehmer darüber hinaus bei nicht webbasierten Konferenzen vor Zuschaltung in die Konferenz mit einem Operator sprechen lassen, um den Anrufer zu identifizieren. Bei webbasierten Konferenzen hat der Moderator jederzeit die Möglichkeit, den aktuellen Status der Dial-Out-Teilnehmer zu kontrollieren, beispielsweise ob der Anruf schon angenommen wurde oder gerade die Begrüßungsansage eingespielt wird.

2 Erweiterte Sicherheitsmaßnahmen

Zum optimalen Schutz einer Telefonkonferenz stehen zusätzlich nachstehende Sicherheits-Features zur Verfügung.

2.1 Rollcall

Der Rollcall ist eine weitere effektive Schutzmaßnahme. Nach erfolgreicher Eingabe des Zugangs-Codes werden die Konferenzteilnehmer aufgefordert, ihren Namen aufzusprechen. Diese Aufzeichnung wird den anwesenden Konferenzteilnehmern in Form einer Ansage vorgespielt.

Der Moderator hat mehrere Optionen, den Rollcall einzusetzen. So kann er ihn zum Beispiel nur für das Betreten der Konferenz aktivieren. Alternativ ist es möglich, die Stimmprobe sowohl beim Betreten als auch beim Verlassen der Konferenz abzufragen. Darüber hinaus ist der Moderator berechtigt, mittels eines DTMF-Kommandos das Abspielen aller Aufzeichnungen der anwesenden Teilnehmer während einer Konferenz zu veranlassen.

2.2 Entry/Exit Tone

Bei jeder Telefonkonferenz ist ein standardisierter Entry Tone als Kontrollfunktion aktiviert. Der Entry Tone löst bei jeder Zuschaltung eines Teilnehmers in die Konferenz einen Signalton aus. Auf diese Weise wird jeder neue Teilnehmer bemerkt und unberechtigte Zuhörer werden erkannt.

Optional wird auch ein Exit Tone angeboten. Dieser erklingt als Ergänzung zum Entry Tone, sobald ein Teilnehmer auflegt oder die Verbindung getrennt wird.

2.3 Moderatoren- und Teilnehmer-Code

Mit der bereits erwähnten getrennten Verwendung von Moderatoren- und Teilnehmer-Codes ist es möglich, bestimmte Berechtigungen auf ausgewählte Personen zu verteilen. So ist beispielsweise nur der Moderator autorisiert, steuernde DTMF-Kommandos in einem Konferenzraum auszuführen. Darüber hinaus wird sichergestellt, dass erst die Einwahl des Moderators den Konferenzraum eröffnet. So können vor dem wirklichen Beginn der Konferenz keine Kosten für den Account-Inhaber entstehen.

2.4 Sicherheits-Code

Der Sicherheits-Code ist eine ergänzende Sicherheitsabfrage zum Zugangs-Code. Nach erfolgreicher Eingabe des Zugangs-Codes müssen die Teilnehmer einen weiteren Code eingeben, um sich in die Konferenz einzuwählen. Diese Maßnahme ermöglicht zusätzliche Datensicherheit für Besprechungen. Der Zusatz-Code kann vom Auftraggeber frei gewählt werden und ist normalerweise vierstellig.

2.5 DTMF-Kommandos

In unten stehender Tabelle findet sich eine Auflistung verfügbarer DTMF-Kommandos.

*1	Wortmeldung anzeigen ¹
*3	Wortmeldung löschen ¹
*6	Eigene Leitung stumm schalten bzw. wieder freischalten
*5	Alle Teilnehmerleitungen stumm schalten bzw. wieder freischalten (nur Moderator)
*7	Konferenzraum schließen/öffnen (nur Moderator) ²
*2	Anzahl Teilnehmer anhören (nur Moderator)
*4	Konferenzaufnahme starten/beenden (nur Moderator)
#5	Musikeinspielung starten/stoppen ³ (nur Moderator)
*8	Konferenz beenden und alle Teilnehmer trennen (nur Moderator)
*0	Operator rufen
#2	Namen aller Konferenzteilnehmer einspielen (nur Moderator) ⁴
#3	Namen aller Konferenzteilnehmer anhören (nur Moderator) ⁴
0	Anhören (von Namensansagen/Hilfe/...) abbrechen

¹ Wortmeldungen von Konferenzteilnehmern können im Conference Control Panel optisch angezeigt werden.

² Das Schließen des Konferenzraumes verhindert das Betreten von weiteren Konferenzteilnehmern

³ Sind noch keine Teilnehmer in der Konferenz, so kann der Moderator die Wartemusik an- oder ausschalten.

⁴ Für Konferenzen, die mit Namensansage/Rollcall gebucht werden.

3 Konferenzraum abschließen

Jeder virtuelle Konferenzraum kann jederzeit abgeschlossen werden. Dies kann nur durch den Moderator vorgenommen werden, und zwar entweder über ein DTMF-Kommando oder über die webbasierte Konferenzsteuerung. Weitere Teilnehmer oder ein Operator können sich danach nicht mehr in den virtuellen Konferenzraum zuschalten.

4 Blacklisting für webgebuchte Konferenzen

Als weitere effektive Schutzmaßnahme vergleicht die Konferenzbrücke der Telekom jede Rufnummer, die sich in eine Konferenz einzuwählen versucht, mit einer Blacklist. Nummern, die auf dieser Liste verzeichnet sind, werden sofort abgeblockt. Dies ist eine sichere Methode, um automatische Wahlmaschinen, die die gesamte Code-Range überprüfen (Brute Force Attack), abzuwehren. Angriffe dieser Art werden sofort identifiziert und unterbunden.

Um die Aktualität der Blacklist zu gewährleisten, wird diese durch Mitarbeiter der Telekom stets aktualisiert. Die verdächtigen Rufnummern werden sowohl manuell ermittelt (Abuse Management) als auch durch einen speziellen Prüfalgorithmus, der sämtliche Code-Eingabeversuche analysiert und Auffälligkeiten meldet.

5 Bereitstellung aufgezeichneter Konferenzen

Dem Auftraggeber steht eine Aufzeichnung der Telefonkonferenz per Download zur Verfügung. Diese wird zehn Tage nach stattgefundener Konferenz von allen Systemen gelöscht.

Webportal

Das Webportal der Telekom bietet zum einen unter www.telekom.de/konferenzen wichtige und interessante Informationen zu den einzelnen Produkten sowie ein Anmelde-Tool für die unterschiedlichen Konferenzangebote. Zum anderen ist hier über www.telekom.de/konferenzportal die webbasierte Steueroberfläche für die Nutzer der Konferenzbrücke zu erreichen.

6 Portalseite

Über die Portalseite www.deutsche-telekom.de/konferenzportal erhalten Interessenten Formulare sowie verschiedene nützliche Informationen zum Start und für die Nutzung von Telefon- und Webkonferenzen.

Betreiber der Internet-Seite ist ausschließlich die Telekom, die auch für das Hosting verantwortlich ist. Sämtliche Informationen werden einzig durch deren Mitarbeiter eingesehen und weiterverarbeitet. Das Login zum Konferenzportal erfolgt über eine gesicherte HTTPS-Verbindung.

7 Konferenzportal

Das Konferenzportal www.deutsche-telekom.de/konferenzportal stellt dem Nutzer eine Oberfläche zum Bestellen, Administrieren und Steuern der gebuchten Telefon- und Webkonferenzen sowie zu den zugehörigen Services zur Verfügung.

Der Zugang ist nur über eine HTTPS-Verbindung zu erreichen, wodurch sämtlicher Datenverkehr mit einer starken SSL-Verschlüsselung (2.048 bit) gesichert ist.

Das Einloggen in einen Account ist ausschließlich mit der richtigen Kombination aus Benutzernamen und Passwort möglich. Es werden hierbei Richtlinien angewandt, die nur sichere Zugangsdaten zulassen. Für Benutzernamen ist eine Mindestlänge vorgeschrieben und für Passwörter sind darüber hinaus Groß- und Kleinbuchstaben sowie mindestens ein Sonderzeichen gefordert. Auf diese Weise wird dem Erraten eines gültigen Logins mittels Brute Force Attack effektiv entgegengewirkt.

Des Weiteren ist eine gültige Session zur Sicherheit mit einem Time-out versehen. Verlässt ein Nutzer zum Beispiel seinen Arbeitsplatz, wird er nach einer gewissen Zeit automatisch ausgeloggt. So wird verhindert, dass eine unberechtigte dritte Person in einem unbeobachteten Moment die Kontrolle über den Account erlangt.

Zusätzlich hat die Telekom Sicherheitsmaßnahmen bei der Implementierung getroffen, die unter anderem XSS-, XSRF- und MITM-Attacken vorbeugen sollen. Serverseitig kommen effektive Methoden gegen Session Hijacking, Buffer Overflows, SQL-Injections sowie andere bekannte Angriffe auf die Datensicherheit zum Einsatz.

7.1 Software

Bei der Software wird ausnahmslos eine eigens entwickelte Lösung verwendet. Regelmäßig durchgeführte Tests und Updates gewährleisten Funktionalität und höchste Sicherheit.

Im Rahmen der hohen Ansprüche an die Datensicherheit dienen die aktuellen Sicherheitsrichtlinien als Maßstab für das Einsetzen, Konfigurieren und Patchen der Server-Software. Hierfür überwacht ein Emergency Response Team verschiedene bekannte Security-Advisory-Listen.

Updates finden zuverlässig stets zum frühestmöglichen Termin statt. Ergänzend werden etwas weniger kritische Patches in regelmäßigen Wartungsfenstern durchgeführt, und zwar zeitlich kurz hintereinander.

7.2 Hardware

Sämtliche Konferenz-Software wird auf dedizierter Hardware betrieben. Diese ist in Liegenschaften untergebracht, die ausschließlich von der Telekom genutzt werden. Sowohl der virtuelle als auch der physikalische Zugriff von unberechtigten Personen auf die Betriebs-Software oder Datenhaltung ist somit ausgeschlossen.

Der regelmäßige Austausch von beanspruchten Verschleißteilen wie Magnetspeichern (Festplatten) schließt einen Datenverlust durch Hardware-Ausfälle nahezu aus. Zusätzlich sorgt ein Back-up-Konzept dafür, dass sämtliche Daten gesichert sind.

7.3 Best Practices

Sogenannte Best Practices, das sind Leistungsmerkmale, die sich im Bereich der Sicherung sensibler Daten bewährt haben, dienen als Basis für die ständige Weiterentwicklung und Verbesserung der Systeme.

Zur Verdeutlichung hier einige Beispiele:

- Innerhalb des Telekom Konzerns wurden für alle IT-Systeme Standards erarbeitet, die die Daten- und Ausfallsicherheit des Betriebs gewährleisten. Die Telefon- und Webkonferenzsysteme werden gemäß diesen Standards betrieben auf gebaut.
- Die Systemlandschaft wird in einer eigenen Umgebung nach N-Tier-Architekturprinzipien betrieben. Darin eingeschlossen ist die Aufteilung in demilitarisierte und militarisierte Zonen. Jede Zone ist nach außen mit Firewalls abgesichert, wodurch ein Einbruch beispielsweise aus dem Internet in das Systemnetzwerk der Telekom verhindert wird.
- Sämtliche sensiblen Daten werden ausnahmslos über sichere Protokolle übertragen. Hierbei wird immer eine möglichst hohe Schlüsselstärke (zum Beispiel für SSL und Blowfish) gewählt.

- Die administrativen Systemzugänge, unter anderem für den technischen Betrieb, die Entstörung oder das Operating, unterliegen einem ausgearbeiteten Rollenkonzept. Hier findet das „Need to know“-Prinzip volle Anwendung. Allen Personen wird nur die Berechtigung erteilt, die zur Erfüllung der jeweiligen Tätigkeit tatsächlich notwendig ist.
- Wartungsfenster werden jedes Mal im Voraus auf dem Konferenzportal angekündigt und liegen stets in wenig frequentierten Zeiten.

8 Benachrichtigungsdienst

Nach Buchung einer Konferenz im Konferenzportal besteht für den Nutzer die Möglichkeit, Moderatoren und Teilnehmer per E-Mail über Details der Konferenz zu informieren und zu dieser einzuladen. Es werden hierfür vorgefertigte Templates verwendet, die der Nutzer individuell an seine Bedürfnisse anpassen kann.

Die E-Mail mit den Konferenzdetails kann entweder direkt aus dem Browser heraus (per Browser-E-Mail) oder über ein Standard-E-Mail-Programm des Nutzers (z. B. Outlook) versandt werden. Dabei unterscheiden sich die Einladungen für Moderatoren und Teilnehmer anhand verschiedener Templates mit den gewünschten Informationen. Auf diese Weise wird gewährleistet, dass kein Teilnehmer einen Moderatoren-Konferenz-Code mit den dazugehörigen Legitimationen erhält.

9 Conference Control Panel

Über das Konferenzportal (siehe auch Punkt 7) hat der Moderator die Möglichkeit, eine laufende Konferenz mittels eines Conference Control Panel zu steuern. Um eine laufende Konferenz handelt es sich, sobald ein Teilnehmer in die Telefon- oder Webkonferenz eingewählt ist.

Gesichert ist das Conference Control Panel über das Login (Benutzername und Passwort) in den Web-Account sowie die verschlüsselte Übertragung via SSL. Unbefugte können nicht auf das Panel zugreifen.

Im Panel selbst stehen dem Moderator alle wichtigen Informationen zur Konferenz zur Verfügung, wie zum Beispiel das Thema und die Dauer der aktuellen virtuellen Sitzung, der Zugangs-Code für die Teilnehmer, die Aktivierung der Aufzeichnung sowie eine Liste aller aktuellen Teilnehmer inklusive Einwahlzeit und Status.

Zusätzlich sind unter anderem folgende erweiterte Steuerungs-Tools verfügbar:

- Starten einer Aufzeichnung
- Abschließen oder Beenden einer Konferenz
- Ändern des Status einzelner oder mehrerer Teilnehmer (So können ein oder mehrere Teilnehmer auf laut, stumm oder parkend geschaltet werden, wobei „parkend“ bedeutet, dass der oder die Teilnehmer in diesem Moment nicht an der Konferenz teilnehmen. Er oder sie befinden sich in einem Warteraum und können jederzeit wieder zur Konferenz zugeschaltet werden.)

Webkonferenz

Mit einer Webkonferenz können mehrere Personen unabhängig von Ort und Zeit über das Internet gemeinsam und in Echtzeit zusammenarbeiten. Dabei ermöglicht ein vollwertiges Desktop-Sharing, dass Teilnehmer im View-Modus Anwendungen auf dem Bildschirm des Moderators bzw. Präsentators sehen können, sobald er diese zur Übertragung freigibt.

10 WebMeeting

Das WebMeeting ist eine von mehreren webbasierten Konferenzlösungen der Telekom. Über das eingangs erwähnte Desktop-Sharing können die Teilnehmer interaktiv und gesichert über das Internet Daten austauschen, diese gemeinsam einsehen und bearbeiten.

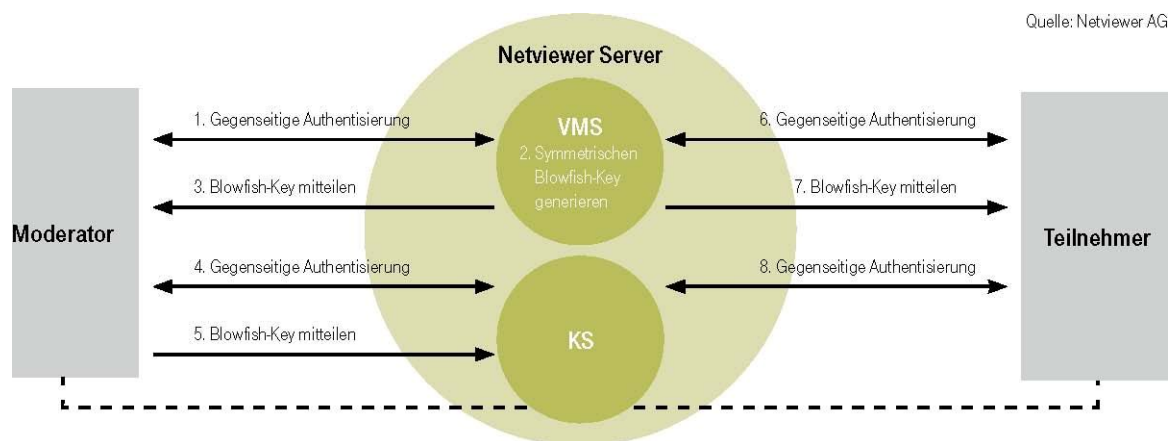
Als Basis für WebMeetings dient eine angepasste Version des Produkts one2meet der Netviewer AG. Hierbei implementiert eine serverseitige Kommunikationsschnittstelle die Integration von one2meet in die Telefonkonferenzbrückenlandschaft der Telekom.

Der für WebMeetings verwendete one2meet-Client wurde lediglich um ein integriertes Steuer-Panel für die Telefonkonferenz erweitert. Die bekannten Leistungsmerkmale und Sicherheitsmechanismen des Clients blieben hiervon völlig unberührt. Wie gewohnt ist ein Client jeweils nur für eine Konferenz verwendbar.

Sobald sich der Moderator der Sitzung über das Webportal mit seinem Benutzernamen und seinem Passwort eingeloggt hat, erhält er seinen Moderatoren-Client (Moderatorenprogramm). Für die weiteren Teilnehmer des WebMeetings steht ein gesondertes Login auf dem Webportal bereit. Die Anwender authentisieren sich mit dem Teilnehmer-Code, der auch für die in WebMeetings integrierte Telefonkonferenz gültig ist, und erhalten einen Teilnehmer-Client.

Darüber hinaus wird jeder WebMeeting-Client mit einem einzigartigen Token ausgeliefert, das serverseitig mit der jeweiligen Sitzung verknüpft ist. Auf diese Weise ist gewährleistet, dass ein Client-Programm nicht für andere Sitzungen verwendet werden kann.

Das Login und der Download des Clients erfolgen wie bereits erwähnt über das Webportal. Um ein Maximum an Sicherheit zu gewährleisten, erfolgt der Datenverkehr über das Webportal ausschließlich mit einer verschlüsselten Kommunikation via HTTPS-Verbindung (Port 443).



Der genaue Aufbau eines WebMeetings ist in der oben stehenden Abbildung grafisch dargestellt und wird im kommenden Abschnitt detailliert erläutert:

In einem ersten Schritt startet der Moderator das Moderatorenprogramm. Dieses kontaktiert daraufhin den Vermittlungs-Server (VMS) mit der Sitzungsanforderung. Als Nächstes erfolgt nun die Authentifizierung des Clients mittels eines Matching-Codes. Der Code erscheint am Bildschirm und muss über die Telefontastatur eingegeben werden. Auf diese Weise wird eine Telefonleitung eindeutig mit einem Moderatoren- oder Teilnehmer-Client verknüpft. Ist der Vorgang erfolgreich abgeschlossen, sendet der Vermittlungs-Server eine Sitzungsnummer und die Adresse eines Kommunikations-Servers (KS) an den Client zurück. Der Client kontaktiert jetzt einen der vorhandenen Kommunikations-Server und wartet, bis weitere Teilnehmer in die Sitzung eintreten.

Clients und Vermittlungs-Server authentifizieren sich gegenseitig über die asymmetrischen ECC-Schlüssel und das Client-Token, welches beim Download mitgeliefert wurde. Der Vermittlungs-Server generiert daraufhin einen symmetrischen Blowfish-Key und sendet ihn an den Client. Von nun an sind alle Signalisierungsdaten über den Blowfish-Key verschlüsselt. Daraufhin generiert der Vermittlungs-Server einen zweiten Blowfish-Key, der über einen sicheren Kanal an den Client gesandt wird. Der zweite Blowfish-Key sorgt nun für die zuverlässige Verschlüsselung des Sitzungsdatenstroms zwischen Client-Programm und Kommunikations-Server.

Jedes weitere Client-Programm muss sich, analog zu den eben beschriebenen Abläufen, am Kommunikations-Server authentisieren, um einen sicheren Kanal aufzubauen.

Der zweite Blowfish-Key wird vom Moderatorenprogramm auf dem Kommunikations-Server hinterlegt. Der Kommunikations-Server kann nun aufgrund der Kenntnis des zweiten Blowfish-Keys die übertragenen Sitzungsdaten individuell an die technischen Voraussetzungen (z. B. verfügbare Bandbreite) jedes einzelnen Clients anpassen. Mit dieser Methode ist es problemlos möglich, die hohen Performance-Anforderungen, die an die Online-Kollaboration gestellt werden, zu erfüllen. Während des WebMeetings gewährleistet letztendlich eine 128-bit-Blowfish-Verschlüsselung die Integrität der Daten.

Des Weiteren sind der Vermittlungs- und der Kommunikations-Server unabhängige Instanzen. Der Signalisierungsdatenstrom (z. B. Authentifizierung, Schlüsselaustausch) und der Sitzungsdatenstrom sind daher logisch voneinander getrennt. Zudem wurden die eingebetteten Übertragungsprotokolle proprietär von der Netviewer AG entwickelt.

Aktuell stehen folgende Ports für einen Verbindungsaufbau der WebMeetings mit dem Internet zur Verfügung:

- Port 2000: proprietäres Protokoll
- Port 443: proprietäres Protokoll über HTTPS-Tunnel
- Port 80: proprietäres Protokoll über HTTP-Tunnel

Zusätzlich ist die Kommunikation über Port 80 auch über die vorhergehend aufgeführten Maßnahmen geschützt, somit ist für alle drei Verbindungsvarianten eine vergleichbare Übertragungssicherheit gewährleistet.

Weitere Sicherheitsmaßnahmen

Neben den weiteren im Dokument genannten speziellen Sicherheitsmaßnahmen wurden nachstehende Methoden bei der Realisierung der Services beachtet.

13 Physikalische Sicherung

Sämtliche Systeme sind in den Gebäuden der Telekom untergebracht. Sowohl die betreffenden Grundstücke als auch die einzelnen Räume, die sich in den betreffenden Liegenschaften befinden, werden gegen unberechtigten Zugriff zuverlässig gesichert.

Die Zutrittssicherung wird unter anderem durch die folgenden Maßnahmen erreicht:

- rund um die Uhr besetzte Eingangspforte mit Zuganglisten und Zutrittskontrolle
- einbruchssichere Räume
- Türsysteme mit Zutrittskontrolle einzig für autorisierte Mitarbeiter
- Zutritt für Zulieferer nur in Begleitung von berechtigten Angestellten der Telekom
- einzeln verschließbare Server-Schränke
- keine offen zugänglichen Kabelzuführungen

Darüber hinaus wurden unter anderem nachstehende betriebliche Sicherheitsmaßnahmen ergriffen:

- redundante Klimatisierung der Technikräume
- eigener Brandabschnitt
- Brandfrüherkennung mit Feuermelderanbindung an die Leitstelle der Feuerwehr
- redundante Netzersatzanlage
- redundante Stromversorgung über öffentliches Stromnetz
- redundante Anbindung an mehrere Vermittlungsstellen des PSTN
- redundante Hardware für Processing, Storage, Firewalling und Routing

14 Conferencing Personal

Die Daten sind bei der Telekom in sicheren Händen. Um den höchstmöglichen Schutz zu gewährleisten, wird nicht nur auf modernste Technik zurückgegriffen, vielmehr wird auch das Personal mit Bedacht ausgewählt. In diesem Zusammenhang werden sämtliche Mitarbeiter jährlich mehrfach in Belangen des Datenschutzes geschult.

Die Aufgaben und Leistungen des Callcenters sowie des technischen Betriebs der Anlagen werden ohne Ausnahme von Angestellten der Telekom durchgeführt. Unter keinen Umständen werden in diesen Bereichen Aufträge an Fremdfirmen weitergegeben.

Alle Mitarbeiter sind sich ihrer Pflicht im Umgang mit sensiblen Daten bewusst und gehen stets vertraulich mit diesen um. Daher ist gewährleistet, dass keinerlei Informationen – weder offizielle noch inoffizielle – auf irgendeine Weise missbräuchlich genutzt werden. Des Weiteren werden alle Ausdrucke sicher als Datenmüll entsorgt.

Ihr Kontakt bei der Deutsche Telekom Value Added Services Austria GmbH
Mag. Katrin Maurer, Rennweg 97 -99, A-1030 Wien
+43 (0)1 798 4590 - 2914 (Tel.) +43 (0) 676 83 883 - 720 (Mob.)
+43 (0)1 798 4590 - 2920 (Fax)
E-Mail: katrin.maurer@deutschetelekom.at

15 Lieferantenbeziehungen

Im Rahmen der Datensicherheit bestehen zwischen der Telekom und allen Lieferanten besonders vertrauliche Geschäftsbeziehungen sowie zusätzliche Nondisclosure-Agreements (Vertraulichkeitserklärungen).

Zulieferern ist der Zugang zu den Systemen im Last-Level-Support, zum Beispiel bei der Entstörung der Systeme, ausschließlich in Begleitung eines Angestellten der Telekom möglich.

Sämtliche Zugriffe auf das System erfordern eine vorherige Authentisierung. Dementsprechend können administrative Aufgaben, insbesondere kundenbezogene Daten, im System nur von ausdrücklich berechtigten Personen durchgeführt bzw. eingesehen werden. Darüber hinaus findet eine Aufzeichnung aller durchgeführten Arbeiten statt.

Des Weiteren erfolgen der technische Betrieb und die Administration der Systeme ausschließlich durch das Technische Operating der Telekom.

16 Resümee

Alle von der Telekom angebotenen Konferenzlösungen basieren auf modernster Technik mit höchsten Sicherheitsstandards. Auf diese Weise können Daten schnell und unabhängig von Ort und Zeit präsentiert, bearbeitet und besprochen werden, und zwar geschützt vor Zugriffen unberechtigter Personen.