ecos

Videokonferenzen im VS-NfD-Umfeld

ECOS **SecureConferenceCenter**

- **Sicherheitsaspekte**
- **Technische Herausforderungen**

Inhalt

Einführung 3
Sicherheitsaspekte 4
Bedrohungen und Risiken 4
Auflagen 5
Technische Herausforderungen 6
Endgeräte 6
Kommunikation im Netzwerk 7
Grundlagen 7
Netzwerkkommunikation 9
Topologie der Videokonferenzsysteme 12
Performance und Latenzen 14
ECOS SecureConferenceCenter 14

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Einführung

Videokonferenzen sind aus unserer heutigen Arbeitswelt nicht mehr wegzudenken. Sei es, um an Terminen, Workshops oder Schulungen von zu Hause oder unterwegs teilzunehmen oder um Informationen mit Kollegen weltweit auszutauschen.

Bei vielen Videokonferenzen müssen nicht nur die eigenen Mitarbeiter im Büro und im Homeoffice integriert werden, sondern es sollen auch Partnerunternehmen bzw. -organisationen, Dienstleister und Berater mit einbezogen werden. Durch externe Teilnehmer kommt so auch unbekannte Hardware ins Spiel, die nicht unter dem eigenen IT-Management steht.

Die Situation wird noch komplexer, wenn Geheimhaltung eine wichtige Rolle spielt und mit dem Geheimhaltungsgrad VS-NfD eingestufte Daten und Informationen in Videokonferenzen thematisiert werden.

Marktgängige Videokonferenzlösungen werden in öffentlichen Clouds betrieben, die den Sicherheitsauflagen für Verschlusssachen unter Umständen nicht gerecht werden. Die Auflagen und Gesetzgebungen, denen die Betreiberorganisationen unterliegen, unterscheiden sich oftmals von denen in Deutschland. Die Rechenzentren, in denen die Videokonferenzlösungen gehostet werden, können in den seltensten Fällen begutachtet werden, um die Sicherheitsauflagen zu prüfen. Der Schutzbedarf kann daher nicht sichergestellt werden.

Alternativen bieten fertige Black-Box- oder Open-Source-Lösungen, die aber einen Kompetenzaufbau seitens der betreuenden IT-Administration erfordern, was wiederum den Einsatz von Ressourcen in Form von Mitarbeitern, Zeit und Geld notwendig macht.

Die verschiedenen Bedrohungen und Risiken, die beim Einsatz von Videokonferenzlösungen zu berücksichtigen sind, erschweren die Auswahl einer geeigneten Lösung im VS-NfD-Umfeld.

VS-NfD bedeutet *Verschlusssache – Nur für den Dienstgebrauch* und ist die niedrigste der vier Geheimhaltungsstufen der deutschen Behörden. Verschlusssachen bedürfen besonderen Schutzes und werden aufgrund dessen in verschiedenen Geheimhaltungsstufen klassifiziert.
Sie dürfen nur autorisierten Personen zur Verfügung gestellt werden. Es müssen rechtliche Regelungen eingehalten werden.
Die IT-Sicherheit spielt bei der Verarbeitung von Verschlusssachen eine wichtige Rolle. Es müssen Schutzmaßnahmen ergriffen werden, um die Integrität, Vertraulichkeit und Verfügbarkeit der Verschlusssachen zu gewährleisten.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Sicherheitsaspekte

Videokonferenzen umfassen Ton- und Videoaufnahmen von Personen, es wird über als vertraulich eingestufte Inhalte gesprochen und Bildschirme mit schützenswerten Informationen werden geteilt. Schon die Teilnahme an einer Besprechung kann eine schützenswerte Information sein, die nur einem berechtigten Personenkreis zu Verfügung stehen soll.

Bedrohungen und Risiken

Eine große Bedrohung stellt die Kompromittierung des Endgeräts eines Teilnehmers durch Schadsoftware dar. Schützenswerte Inhalte können so durch Unbefugte abgegriffen werden. *Die Endgeräte aller Teilnehmer müssen sicher und frei von Schadsoftware sein.*

Auch kann die Kommunikation der Teilnehmergeräte einer Videokonferenz über ein unsicheres Netzwerk abgegriffen und entschlüsselt werden. *Die Netzwerkkommunikation bei einer Videokonferenz muss gesichert sein.*

Eine weitere Bedrohung kann die Manipulation der zentralen Serversysteme der Videokonferenzlösung sein, die bei einer cloudbasierten Software nicht durch die eigene IT-Administration gewartet werden und auf die kein Einfluss genommen werden kann. *Die Integrität der Serversysteme muss sichergestellt sein.*

Häufig ist es notwendig, dass Videokonferenzen aufgezeichnet werden. Hier besteht die Gefahr, dass die Aufzeichnungen auf unsicheren oder kompromittierten Fileservern oder Dateisystemen gespeichert werden. *Eine sichere Speicherung, Datensicherung und Archivierung der Aufzeichnungen muss gewährleistet sein.*

Ein hohes Risiko stellt die nicht autorisierte Teilnahme an einer Videokonferenz dar, die sehr leicht zustande kommen kann. Die E-Mails mit den Einwahldaten zur Konferenz werden versehentlich weitergeleitet oder Mitarbeiter haben Zugriff auf das entsprechende Postfach, z.B. aufgrund von Urlaubsvertretung. *Es muss sichergestellt sein, dass nur die Personen an einer Videokonferenz teilnehmen, die auch tatsächlich für die Teilnahme autorisiert sind.*

Ebenso besteht die Gefahr bei der Teilnahme an einer Videokonferenz im öffentlichen Raum, dass Unbefugte im Umfeld oder in den Räumlichkeiten unbemerkt schützenswerte Inhalte abgreifen und mitfilmen können. *Die Teilnehmer müssen entsprechend sensibilisiert sein.*

Im Videokonferenzsystem selbst können Hintertüren eingebaut sein, die fremdstaatlichen Nachrichtendiensten oder Ermittlungsbehörden Zugriff auf die schützenswerten Informationen ermöglichen. *Die Hintertüren müssen identifiziert und die Nutzung ausgeschlossen sein.*

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Auflagen

In Bezug auf Verschlusssachen gibt es bereits viele Vorgaben, Auflagen und Mindeststandards des BSI, die eine sichere Umsetzung und Nutzung von Videokonferenzsystemen erleichtern.

Vor der Einführung eines Videokonferenzsystems muss eine Sicherheitsrichtlinie erstellt werden, in der die Sicherheitsanforderungen identifiziert werden. Daraus resultiert ein ausführliches Sicherheitskonzept nach IT-Grundschutz[1], das eine umfassende Risikoanalyse beinhaltet.

Des Weiteren muss ein funktionales Konzept erstellt werden, um den Bedarf an Funktionen und die technischen Anforderungen zu ermitteln. Das BSI hat Mindeststandards für den Funktionsumfang festgelegt.[2] Sie enthalten u.a. Informationen zur Verschlüsselung, Signalisierung von Kamera- und Mikrofonaktivität und die Aufzeichnung von Videokonferenzen.

Ausführliche Informationen zu Videokonferenzsystemen wurden 2020 vom BSI im **Kompendium Videokonferenzsysteme**[3] zusammengefasst. Dort werden u.a. die Betriebsmodelle der verschiedenen Systeme, die Funktionsweise, die Gefährdungslage und die Sicherheitsanforderungen an ein Videokonferenzsystem behandelt.

Im Bereich VS-NfD sind weitere Auflagen zu beachten. Es müssen z.B. konkrete Anforderungen an das Netzwerk selbst, an bestimmte Hard- und Software eingehalten werden. Hersteller werden bei der Entwicklung geeigneter Lösungen durch VS-Anforderungsprofile[4] unterstützt.

Zusätzlich stellt das BSI auch eine Liste von Produkten[5] zur Verfügung, die für die Nutzung im VS-NfD-Umfeld zugelassen sind. Für die sichere Verwendung existieren für jedes Produkt ausführliche Einsatz- und Betriebsbedingungen (SecOPs). Einzelne Produkte, die innerhalb des gesicherten Netzes eingesetzt werden, müssen dabei nicht zwingend separat zugelassen werden. Dazu gehören z.B. Videokonferenzsysteme aber auch Terminalserverdienste oder Fileserver.

Wenn ein Unternehmen oder eine Organisation die hohen Sicherheitsanforderungen eines VS-NfD-Geheimhaltungsgrads nicht erfüllen muss, aber trotzdem einen erhöhten Schutzbedarf der Daten festgestellt hat, kann ein entsprechend entwickeltes Information Security Management System (ISMS) (gemäß ISO/IEC 27000 bzw. PCI-DSS) ebenfalls Auflagen definieren.

---

[1] Informationen zum IT-Grundschutz des BSI finden Sie hier (Stand 10/2022).
[2] Mindeststandard des BSI für Videokonferenzdienste (Version 1.0)
[3] Kompendium Videokonferenzsysteme (Version 1.0.1)
[4] Informationen zu bereits bestehenden VS-Anforderungsprofilen des BSI finden Sie hier (Stand 10/2022).
[5] Eine Übersicht der VS-NfD zugelassenen Produkte des BSI finden Sie hier (Stand 10/2022).

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Zu den technischen Auflagen kommen die Richtlinien in Bezug auf den Datenschutz und die DS-GVO hinzu.

Zum einen müssen die technischen und organisatorischen Maßnahmen überprüfbar sein, was sich bei Cloud-Anwendungen oft schwierig gestaltet.

Zum anderen wird in der Regel ein Auftragsverarbeitungsvertrag mit Drittanbietern abgeschlossen, die ihren Hauptsitz nicht in Deutschland oder der EU haben, weshalb eine abweichende nationale Gesetzgebung Anwendung findet.

Die Entscheidung über die Aufzeichnung von Ton und Bild liegen bei den einzelnen Teilnehmern und die Einwilligung muss vor dem Start der Aufzeichnung einer Videokonferenz eingeholt werden.

Viele Videokonferenzsysteme erfordern die Installation von Client-Software, die oft zusätzliche Hintergrundaktivitäten bedingt oder ermöglicht. Diese müssen überprüft und ggf. beschränkt oder abgestellt werden. Aus Datenschutzsicht ist die Nutzung eines Browsers von Vorteil, da keine zusätzliche Software installiert werden muss und die Browser Sandboxfunktionen besitzen, die einzelne Webseiten und/oder Prozesse isolieren.

Technische Herausforderungen

Bei Videokonferenzen im VS-NfD-Umfeld ist es wichtig, dass die herausgearbeiteten Sicherheitsaspekte auch technisch umgesetzt werden können. Neben der Unterstützung der verschiedenen Endgeräte bei den Teilnehmern ist auch die Kommunikation im Netzwerk zu sichern.

Endgeräte

Eine Herausforderung stellen die unterschiedlichen Geräte am Endpunkt der Teilnehmer dar, die von einem Videokonferenzsystem unterstützt werden müssen. Dazu zählen Mikrofone, Headsets und Webcams, die z.B. per USB angeschlossen sind. Dies kann bei hochsicher konfigurierten Endgeräten zu Konflikten führen, da diese oftmals einen USB-Port-Blocker aktiviert haben. Alternativ kann der Teilnehmer auf die integrierten Audiokomponenten im Endgerät selbst zurückgreifen, was allerdings zu Qualitätsverlusten führen kann, wenn der Teilnehmer sich bspw. in einem größeren Raum aufhält (Nachhall) oder mehrere Teilnehmer um dieses eine Gerät sitzen. Das unerwünschte Abhören aus der Umgebung oder Nebenräumen wird dadurch erleichtert.

Zusätzlich müssen das Endgerät, der VDI-Client und die Videokonferenzsoftware die angeschlossenen Geräte auch unterstützen und durch Updates der Treiber aktuell halten. Es ist Wartungsarbeit erforderlich, damit der Zugriff auf die Client-Komponenten auch erfolgt und zulässig ist.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Kommen VDI-Clients zum Einsatz, ist die Software-Kompatibilität zwischen Client und Terminalserverumgebung von besonderer Bedeutung. Häufig entscheidet ein komplexes Zusammenspiel zwischen VDI-Software, Komponenten für Hardwarebeschleunigung, Plugins für Kollaborationsdienste und dem Videokonferenzsystem über eine einsatzfähige Lösung.

Kommunikation im Netzwerk

Videokonferenzsysteme verwenden Echtzeitdaten wie Audio- und Videoübertragung oder auch Chats und Dateiübertragungen.

Bei der Kommunikation und der Übertragung dieser Echtzeitdaten im Netzwerk spielen neben den verschiedenen Protokollen auch der Aufbau des Netzwerks und seine Komponenten eine wichtige Rolle.

Grundlagen

Für die Nutzung von Videokonferenzsystemen gibt es spezielle Netzwerk- und Verschlüsselungsprotokolle, die eine sichere Kommunikation im Netzwerk auch für externe Teilnehmer ermöglichen.

User Datagram Protocol (UDP): UDP ist ein verbindungsloses Netzwerkprotokoll, das Datagramme in IP-basierten Netzwerken überträgt. Es findet häufig bei der Übertragung von Echtzeitdaten auf der Transportschicht Anwendung. Die Datenübertragung mit UDP wird nicht auf Vollständigkeit geprüft, d.h. nicht empfangene Datenpakete werden nicht erkannt und gehen verloren. Bei Echtzeitdaten wie einer Videoübertragung ist der Verlust nicht gravierend, da Menschen durch die Redundanz menschlicher Kommunikation Verluste einzelner Informationen in der Ton- und Bildübertragung gut kompensieren können.

Transmission Control Protokoll (TCP): Bei TCP handelt es sich um ein verbindungsorientiertes Netzwerktransportprotokoll. Es baut eine Verbindung zwischen zwei Endpunkten auf und überträgt auf dieser Verbindung die Pakete zwischen den Endpunkten. Paketverluste bei der Übertragung per TCP werden erkannt und die entsprechenden Pakete erneut verschickt. Für die Kommunikation zwischen Teilnehmern ist TCP eher ungeeignet, da bei Verlust und durch Nachsenden der Pakete spürbare Verzögerungen der Übertragung eintreten können.

Real-Time Transport Protocol (RTP): RTP überträgt in Echtzeit multimediale Daten, dazu gehören Audio- und Videodaten, über IP-basierte Netzwerke.

Secure RTP (SRTP): SRTP ist die AES-verschlüsselte Version des RTP.

Datagram Transport Layer Security (DTLS): Bei DTLS handelt es sich um ein von TLS abgeleitetes Netzwerkprotokoll, um gegenseitige Authentisierung und sicheren Austausch von Sitzungsschlüsseln (für SRTP) über UDP zu gewährleisten.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Web Real-Time Communication (WebRTC): WebRTC ist ein offener Standard für die Echtzeitkommunikation bei Peer-to-Peer-Verbindungen. Es wird genutzt, um mithilfe von SRTP und DTLS Webbrowsern das Übertragen von Echtzeitdaten von Servern und Webbrowsern anderer Anwender zu ermöglichen.

H.323-Standard: H.323 ist ein Protokollstandard, der oft von stationären Videokonferenzanlagen verwendet wird, ursprünglich mit einer Datenübertragung über Telefon- bzw. ISDN-Verbindungen. Mithilfe sogenannter Gatekeeper wird die Übertragung der Kommunikation über IP-Netze realisiert.

Session Initiation Protocol (SIP): Bei SIP handelt es sich um ein Netzwerkprotokoll, das die Kommunikation zwischen Teilnehmern aufbaut, steuert und wieder abbaut. Es wird überwiegend bei der IP-Telefonie verwendet. Bei Videokonferenzsystemen erlaubt es die telefonische Einwahl in eine Konferenz.

Network Address Translation (NAT): Mithilfe von NAT können verschiedene Geräte und Hosts die gleiche öffentliche IP-Adresse verwenden. Im IPv4-Header werden die Adressen und der Port durch die öffentliche IP-Adresse des NAT-Routers ausgetauscht. Je nach Art des NAT kann es sich um die Umschreibung der Quell- oder Zieladressen handeln. Damit kann die Knappheit der IPv4-Adressen gehandhabt werden. Ein NAT-Router dient auch als Firewall.

Session Traversal Utilities for NAT (STUN): STUN ist ein Netzwerkprotokoll, mit dessen Hilfe Geräte aus einem internen Netzwerkbereich ermitteln können, welche externe bzw. öffentliche Adresse sie durch ein NAT zugewiesen bekommen haben. Diese Adresse kann einem externen Kommunikationspartner zum Verbindungsaufbau mitgeteilt werden. Es findet unter anderem bei der SIP-Telefonie Anwendung.

Traversal using Relays around NAT (TURN): Bei TURN handelt es sich um ein Netzwerkprotokoll, das ähnlich wie STUN Verbindungen zwischen Geräten hinter NAT-Routern aufbaut. Es kommt vor allem zum Einsatz, wenn symmetrisches NAT eingesetzt wird, das den direkten Verbindungsaufbau zwischen Kommunikationspartnern verhindert. Um dennoch den Aufbau einer Verbindung zu ermöglichen, kann ein zwischengeschalteter TURN-Server als ein von beiden Seiten erreichbarer Vermittler (Relay) eingesetzt werden.

Interactive Connectivity Establishment (ICE): ICE ist eine Methode zur Aushandlung von Verbindungsparametern mithilfe von STUN und TURN und zur Übermittlung dieser Parameter über einen sogenannten Signaling Server (z.B. eine Telefonanlage) an die beteiligten Kommunikationspartner.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Netzwerkkommunikation

Der einfachste Aufbau eines Netzwerks für ein Videokonferenzsystem besteht aus zwei Teilnehmern und einem Server, die miteinander kommunizieren können. Teilnehmer A möchte mit Teilnehmer B sprechen. Beide geben ihre Informationen an den Signaling Server weiter, der sie an den jeweils anderen Teilnehmer weiterleitet. Teilnehmer A kann mit den Informationen eine Verbindung mit Teilnehmer B aufbauen und Daten austauschen.

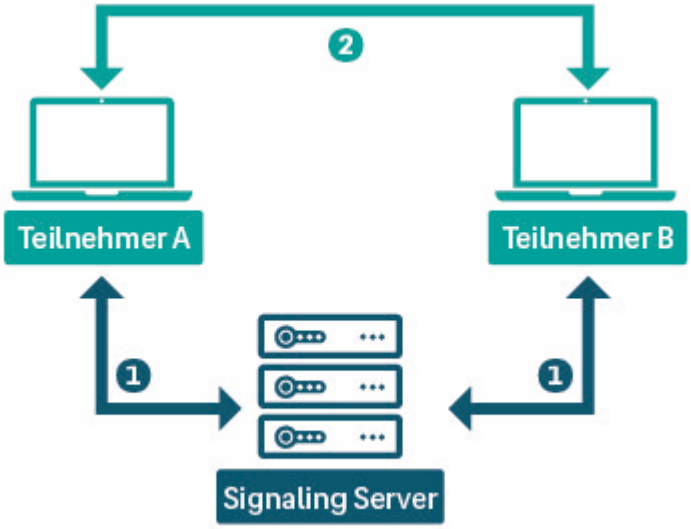

Abbildung 1: Kommunikation im Netzwerk - Basissetup

Kommt mindestens ein NAT-Router zum Einsatz, wird die Kommunikation zwischen Teilnehmern im Netzwerk komplexer. Teilnehmer A befindet sich hinter einem NAT-Router und möchte mit Teilnehmer B sprechen. Um dies zu ermöglichen, ermittelt Teilnehmer A seine Informationen, wie er öffentlich erreichbar ist, mithilfe des STUN-Server. Diese Informationen werden an den Signaling Server gegeben. Auch Teilnehmer B sendet seine Informationen an den Signaling Server. Dieser leitet die Informationen an den jeweils anderen Teilnehmer weiter. Teilnehmer A und B können eine Verbindung aufbauen und Daten austauschen.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

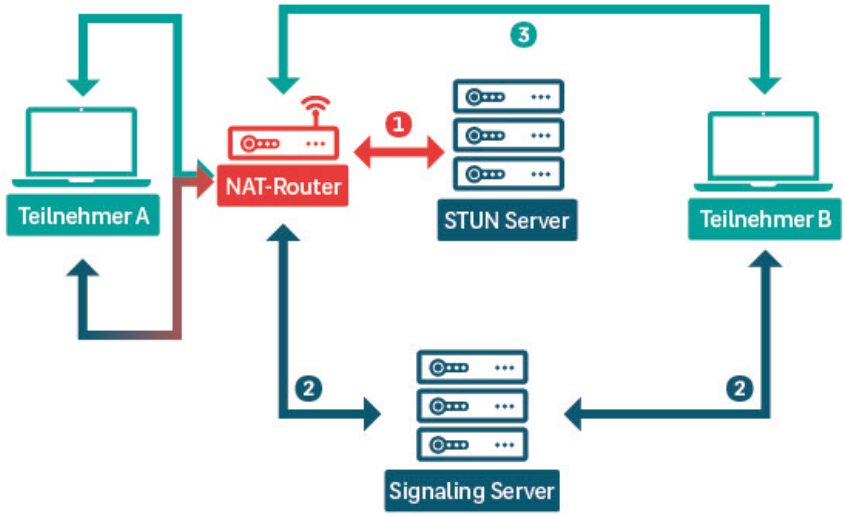

Abbildung 2: Kommunikation im Netzwerk mit NAT und STUN

In der Regel kommt ein symmetrisches NAT zum Einsatz. Dabei wird bei jeder einzelnen Verbindung nach außen ein anderer Quellport verwendet, um so den Zugriff von außen auf das interne Endgerät weiter einzuschränken. Nur das vom Teilnehmer angesprochene Ziel kann mit der Adresse und dem Port eine Verbindung aufbauen. Ein anderes Ziel kann mit den Informationen nichts anfangen. Um ein symmetrisches NAT zu identifizieren und trotzdem eine Verbindung aufbauen zu können, werden zwei separate STUN-Server und ein TURN-Server eingesetzt.

Teilnehmer A befindet sich hinter einem Router mit symmetrischem NAT und möchte mit Teilnehmer B kommunizieren. Teilnehmer A ermittelt seine öffentliche Erreichbarkeit über den STUN-Server. Der zweite STUN-Server prüft die ermittelte öffentliche Adresse (inkl. Portnummer) und stellt fest, dass er Teilnehmer A nicht erreichen kann, da dieser sich hinter einem symmetrischen NAT befindet. Daraufhin reserviert Teilnehmer A beim TURN-Server eine Adresse, die an den externen Teilnehmer B weitergegeben wird. Teilnehmer B nutzt diese Adresse, um mit dem TURN-Server zu kommunizieren, der wiederum als Relay die Kommunikation an Teilnehmer A weiterleitet. Der TURN-Server muss im Netzwerk von innen wie von außen erreichbar sein.

Anschließend geben Teilnehmer A und B dem Signaling Server zu verstehen, dass sie miteinander kommunizieren wollen. Die eigentliche Verbindung wird nicht direkt zwischen den Teilnehmern sondern über den TURN-Server als Vermittler aufgebaut. Der Datenaustausch erfolgt ebenfalls über den TURN-Server.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

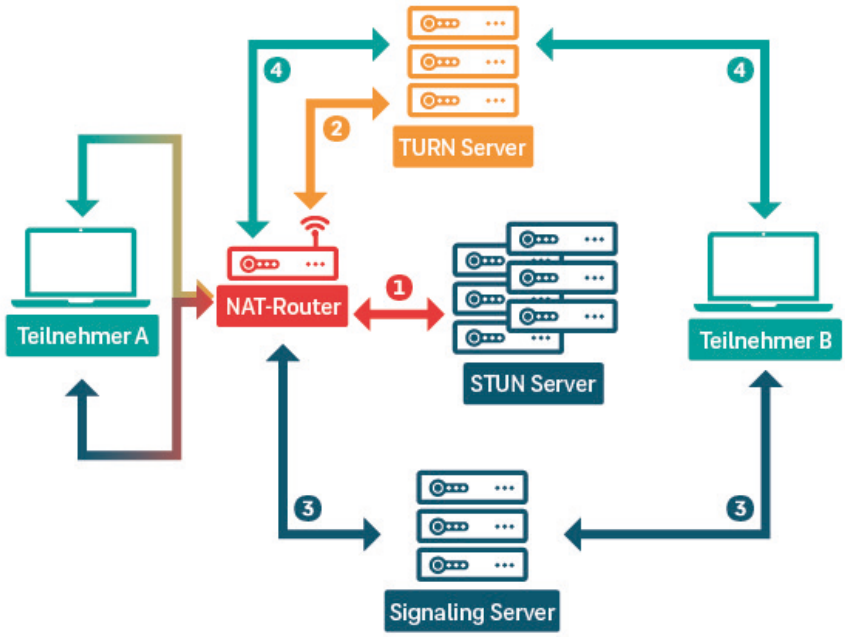

Abbildung 3: Kommunikation im Netzwerk mit symmetrischem NAT

Um den TURN-Server abzusichern, wird dieser in der Regel hinter einer Firewall betrieben. Die Firewall schränkt den Netzwerkverkehr ggf. stark ein und hat für die Kommunikation oftmals nur die Ports 80/443 (TCP) freigeschaltet. Der TURN-Server ermöglicht in diesem Fall auch die Kommunikation per TCP.

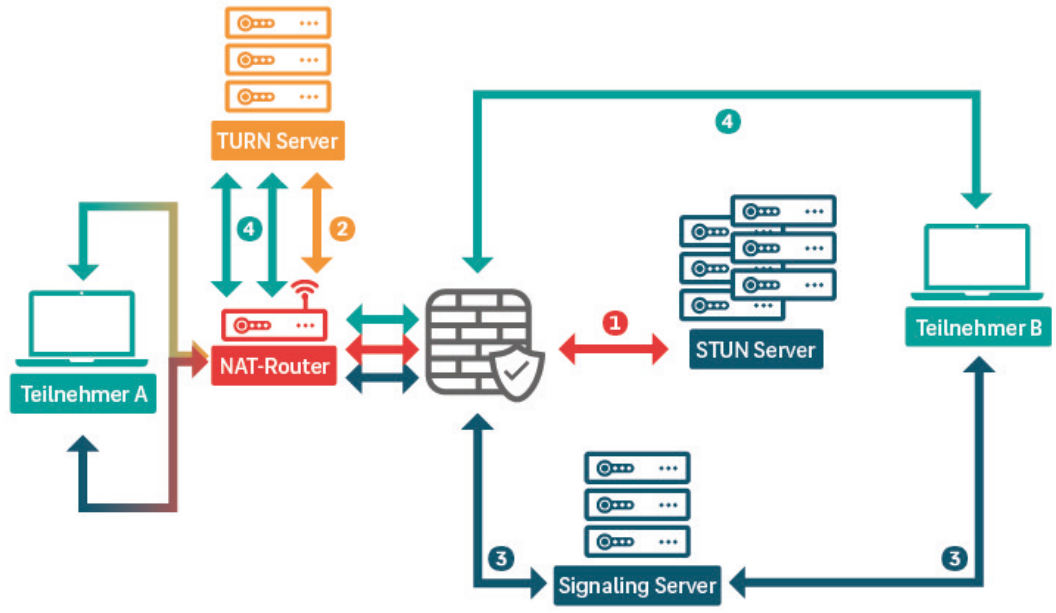

Abbildung 4: Kommunikation im Netzwerk – TURN via TCP

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Zusätzlich zu den Firewall-Restriktionen kommen weitere Aspekte bei der Kommunikation im Netzwerk hinzu.

In Netzwerken wird üblicherweise eine Segmentierung in unterschiedliche Sicherheitszonen vorgenommen, um Kontrolle über den Datenverkehr zu erhalten und ggf. zu limitieren. Um Zugang zu einzelnen hochgesicherten Zonen zu erhalten, wird der TURN-Server auch als Reverse Proxy eingesetzt. Er ermöglicht schrittweise den kontrollierten Zugriff von einer aus externen Bereichen zugänglichen Sicherheitszone in eine höher eingestufte Sicherheitszone. Diese kann wiederum über den TURN-Server mit der Außenwelt kommunizieren.

Topologie der Videokonferenzsysteme

Videokonferenzsysteme können in unterschiedlichen Topologien vorkommen.

Eine Variante ist das *Full Mesh*. Dabei sind alle Endpunkte miteinander verbunden und haben eine gegenseitige Vertrauensstellung aufgebaut. Man spricht von einer Ende-zu-Ende-Verschlüsselung. Bei vielen Teilnehmern resultieren daraus sehr viele Verbindungen. Nehmen drei Teilnehmer an der Videokonferenz teil, gibt es drei Verbindungen, sind es 4 Teilnehmer, steigt die Zahl auf 6 Verbindungen. Bei 5 Teilnehmern werden bereits 10 Verbindungen aufgebaut.

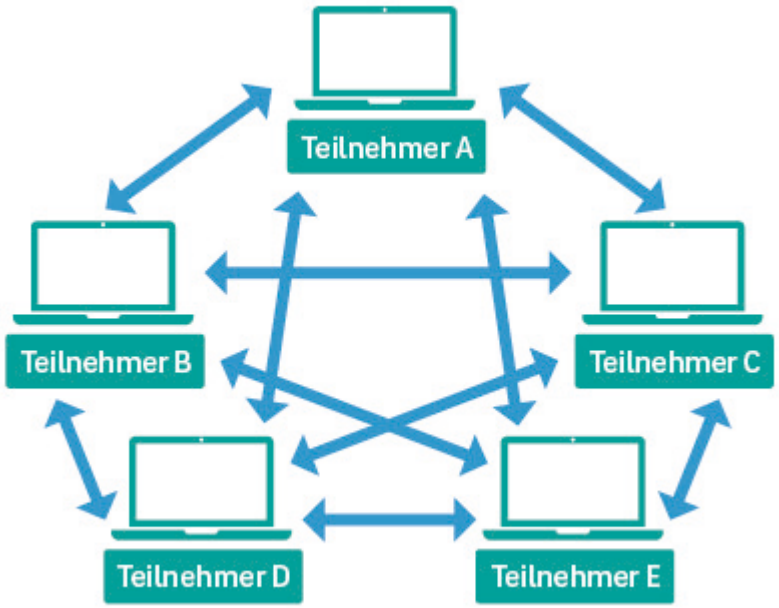

Abbildung 5: Topologie – Full Mesh

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Eine andere Variante ist eine Sterntopologie mit *Multipoint Control Unit (MCU)*. Dabei gibt es einen zentralen Punkt, der mit jedem Teilnehmer eine gesicherte Verbindung aufbaut. Die Teilnehmer untereinander sind nicht miteinander verbunden. Es gibt also immer nur so viele Verbindungen wie es Teilnehmer an der Konferenz gibt.

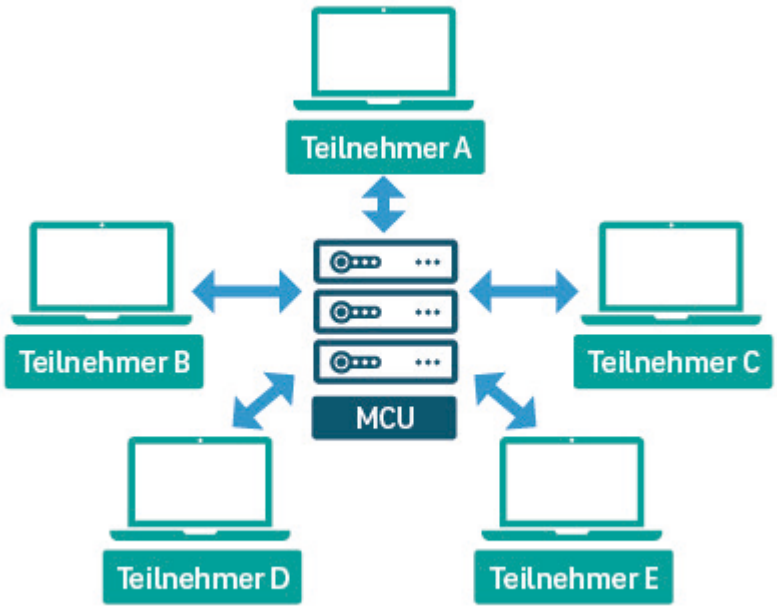

Abbildung 6: Topologie - MCU

Die MCU steuert den Datenverkehr zwischen den Teilnehmern. Sie empfängt den Datenstrom eines Teilnehmers und leitet ihn an die anderen Teilnehmer weiter. Sie entschlüsselt, verarbeitet und verschlüsselt die Daten. Dadurch kann zum Beispiel das Videosignal eines Teilnehmers, der aktuell nur zuhört und nicht selber spricht, herunterskaliert werden, um Bandbreite zu sparen oder einer geringeren Bandbreite eines Teilnehmers anzupassen.

Sollen oder müssen Videokonferenzen in einer gesicherten Umgebung aufgezeichnet werden, wird eine MCU benötigt. Auf der MCU als zentralem Punkt fließen alle Informationen der Videokonferenz zusammen und können sicher gespeichert werden.

Bei einer Verschlüsselung des Datenverkehrs einer Videokonferenz zählt auch die MCU als Verschlüsselungsendpunkt, da sie die Inhalte und Daten verarbeitet. Eine echte Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmern ist mit einer MCU nicht möglich. Es können nur die Datenströme im Sinne einer Transportverschlüsselung zwischen den Teilnehmern und der MCU gesichert werden.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Performance und Latenzen

Wie bei der Kommunikation im Netzwerk bereits festgestellt, sind durch Firewall-Restriktionen oft nur die TCP-Ports 80 und 443 (HTTP/HTTPS) nutzbar.

Die Datenübertragung über UDP – für Echtzeitdaten geeigneter – ist nicht möglich. Es muss TCP für die Übertragung genutzt werden. Das führt allerdings zu Performanceverlusten, da übermittelte TCP-Pakete geprüft und bestätigt sowie und bei einem Verlust erneut gesendet werden müssen.

Auch der Round Trip Delay (RTD) sollte bei Videokonferenzsystemen berücksichtigt werden. Je nach Lokation der Teilnehmer kann die Latenz sehr hoch sein. Bei Teilnehmern, die sich innerhalb der EU befinden, liegt der RTD in der Regel unter 25 ms. Gibt es zusätzliche Teilnehmer in den Vereinigten Staaten liegt die Latenzzeit zwischen 100-200 ms. Dieser Effekt wird bei der Nutzung von TCP durch das erneute Senden von nicht empfangenen Paketen verstärkt, so dass die Qualität der Videokonferenz spürbar leiden kann.

ECOS SecureConferenceCenter

Die Nutzung von Videokonferenzen im VS-NfD-Umfeld ist weiterhin auf ein Sicherheitskonzept angewiesen, das auf der Infrastruktur eines sicheren, umgebenden VS-NfD-Netzes basiert. Konzepte, um Daten unabhängig von einer sicheren, umgebenden Infrastruktur zu schützen, haben sich bisher nicht durchgesetzt. Die Daten müssen innerhalb der jeweiligen Infrastruktur sicher transportiert und gespeichert werden.

Die Konferenzinfrastruktur ist auf die einzelnen Serverkomponenten im sicheren Netzwerk angewiesen. Es müssen sichere und zulässige Zugangsmöglichkeiten geschaffen werden, die die Teilnehmer in das VS-NfD-Netz integrieren. Dies erfordert Lösungen, die sowohl einen sicheren Zugangsweg als auch einen zulässigen Endpunkt beim Teilnehmer gemäß VS-NfD-Anforderungen sicherstellen. Neben den im eigenen IT-Betrieb verwalteten Komponenten stellen vor allem Teilnehmer von externen Unternehmen oder Organisationen eine zusätzliche Herausforderung dar. In einem Videokonferenzsystem sind viele Parteien und Komponenten involviert, für die das System funktionieren muss.

Netzwerkinfrastrukturen bestehen vielfach aus dem sicheren VS-NfD-Netzwerk bzw. der Intranetzone, in der sich die verschiedenen Komponenten wie Terminalserver oder Verzeichnisdienste befinden. Davor ist häufig eine Demilitarisierte Zone (DMZ) geschaltet, die den Zugriff von außen auf das innere Netzwerk regelt und überwacht.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

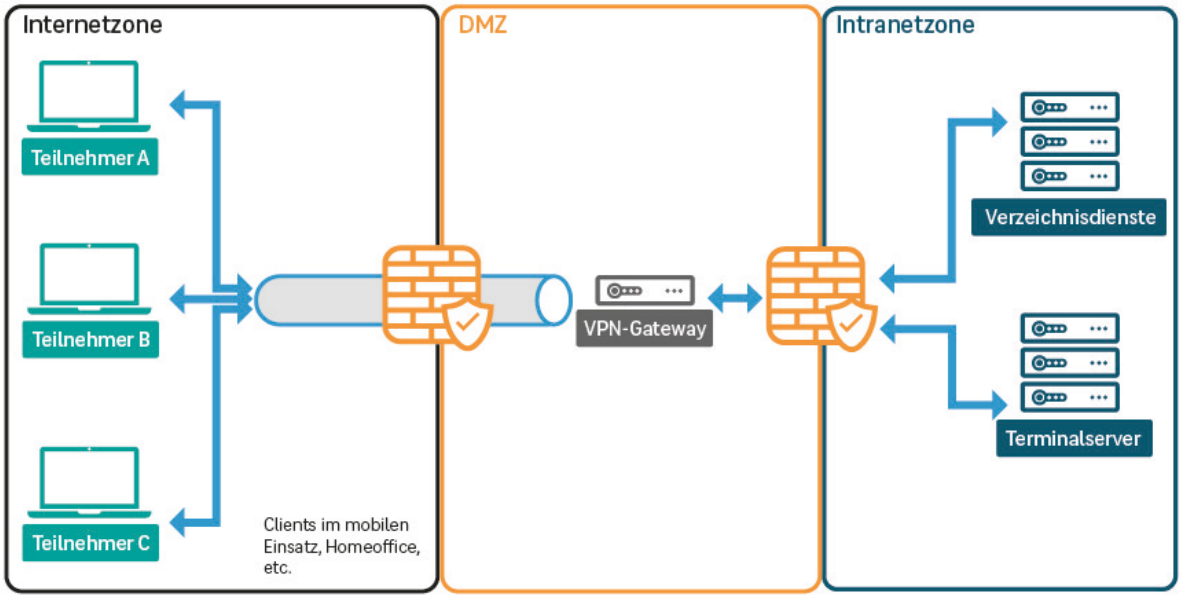

Abbildung 7: Vorhandene Netzwerkinfrastruktur

Externe Mitarbeiter im mobilen Einsatz oder Homeoffice greifen aus dem Internet durch Aufbau eines gesicherten Tunnels per IPsec-VPN auf das VPN-Gateway in der DMZ zu. Das Gateway leitet die Anfragen in die Intranetzone weiter und der Teilnehmer kann auf die dortigen Dienste und Daten zugreifen.

ECOS Technology stellt mit dem ECOS **SecureConferenceCenter,** in Verbindung mit dem ECOS **SecureBootStick®,** eine Lösung zur Verfügung, die die vorhandene Netzwerkinfrastruktur ergänzt und sichere Videokonferenzen VS-NfD-konform ermöglicht.

Das Secure Conference Center (SCC) basiert auf der Open-Source-Software BigBlueButton, die insbesondere unter Datenschutzgesichtspunkten empfohlen wird.

Das SCC ist im ECOS SecureLinux, ein von ECOS gehärtetes Betriebssystem, eingebettet, was den ungewollten Zugriff erschwert und auch bei VS-NfD-zugelassenen Produkten von ECOS zum Einsatz kommt.

Teilnehmer, egal ob extern oder intern, müssen keine Client-Software installieren, da die Einwahl über einen Webbrowser erfolgt.

Das SCC ist in die Entwicklungsinfrastruktur bei ECOS integriert und wird kontinuierlich gewartet. Beim Kunden wird dadurch der Aufwand eines Kompetenzaufbaus und der Einsatz der Ressourcen minimiert.

Das SCC bietet eine einfach einzusetzende und sicher gewartete Videokonferenzlösung auf der Basis einer empfohlenen Open-Source-Lösung.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333

Um einen sicheren Endpunkt des Teilnehmers zu gewährleisten, kommt der Secure Boot Stick (SBS) zum Einsatz. Der SBS transformiert auch private Hardware zu einem sicheren Endpunkt, indem er das private Betriebssystem ignoriert und ein von ECOS gehärtetes Betriebssystem bootet. Die vorhandenen Speichermedien werden isoliert und nicht in Betrieb genommen. Mögliche Schadsoftware wird dadurch nicht aktiviert, die privaten Daten gleichzeitig geschützt.

Die Administration des SBS erfolgt zentral und wird in die vorhandene Sicherheitsinfrastruktur integriert. Der Mitarbeiter baut mit dem SBS eine sichere Kommunikation per VPN mit dem VS-NfD-Netzwerk auf.

In den Varianten SX und ZX ist der SBS für VS-NfD zugelassen und gemäß der SecOPs explizit für den Einsatz von Videokonferenzen geeignet.

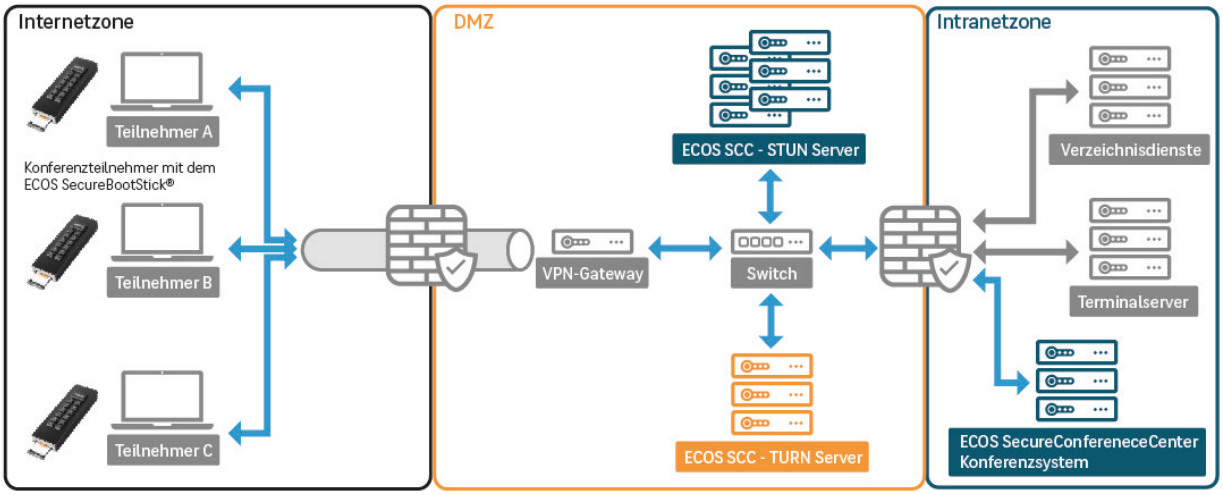

Abbildung 8: Netzwerkinfrastruktur mit dem ECOS SCC und SBS

Das SCC und der SBS ergänzen die bestehende Netzwerkinfrastruktur und ermöglichen VS-NfD-konforme Videokonferenzen – auch im Außenverhältnis mit externen Teilnehmern und Partnern.

ECOS Technology GmbH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939–0 | Fax: +49 6133 939–333