ComConsult Research

# Der Netzwerk Insider

August 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

# SIP Trunking und SIPconnect

## bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

**von Dipl.-Inform. Petra Borowka**

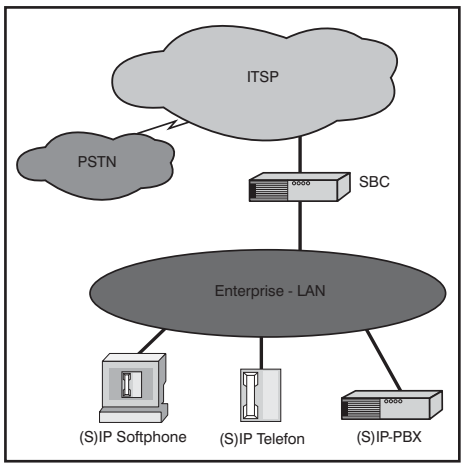
### 1. Die aktuelle Situation

Aktuell gibt es drei relevante Möglichkeiten, die Verbindung zwischen Enterprise-TK und öffentlich erreichbaren Teilnehmern zu fahren:

- Klassische PBX, hybride VoIP/ISDN Lösung
- proprietäres VoIP Trunking
- SIP Trunking

**Klassische PBX und hybride VoIP / ISDN-Lösung**

Aus der klassischen TK-Technik ist folgende Situation bekannt: zur Verbindung von zwei oder mehr TK-Anlagen wurden interne Trunks geschaltet und zur Verbindung einer Enterprise-Lösung mit dem weltweiten öffentlichen Telefonnetz wurden PSTN-Trunks geschaltet; beide Verbindungsarten wurden durch eine $S_{2M}$-Leitung oder Bündel von $S_{2M}$-Leitungen realisiert. Bei der Einführung von Voice over IP im Enterprise-Bereich werden mit so genannten hybriden Lösungen im Regelfall im ersten Migrationsschritt die vorhandenen $S_{2M}$-Leitungen auf PSTN-Gateways abgebildet, die Anzahl der angemieteten und monatlich bezahlten $S_{2M}$-Verbindungen bleibt gleich.




weiter auf Seite 21

Zweitthema

# Sicherheit in Unified Communications

## Integration und Sicherheit: Die Quadratur des Kreises?

**von David Ferrest, Dr. Simon Hoff und Dr. Michael Wallbaum**

**Es gibt heutzutage kaum ein Unternehmen, in dem nicht UM-, CTI- oder Alarmserver ihren Dienst verrichten. In der alten TK-Welt konnten diese TK-Applikationen unter dem Aspekt der Sicherheit noch als vergleichsweise harmlos gelten. Die Schnittstellen zu den IT-Systemen waren - soweit überhaupt vorhanden - klar durch dedizierte Gateways definiert, die nur einen eingeschränkten Durchgriff auf die jeweils andere Seite ermöglichten. Die IT- und die TK-Welt bildeten somit funktionale Inseln, die nur durch wenige Brücken verbunden waren.**

Im Kontext von Voice over IP (VoIP), d.h. mit einer gemeinsam durch IT- und TK-Komponenten genutzten Netzwerkinfrastruktur, stellt sich diese Situation jedoch drastisch anders dar. Per IP kann im Prinzip jede Komponente (Client oder Server) mit jeder anderen direkt kommunizieren.

Die Befürworter von VoIP und Unified Communications (UC) betrachten die bisherige Trennung von IT und TK durchaus zu recht als Produktivitätsbremse des Büroalltags.

weiter auf Seite 6

Neuer Kongress

## Rechenzentrum Infrastruktur-Redesign Forum 2008

Seite 5

Geleit

## Voice-over-IP-Forum 2008: der Markt am Wendepunkt?

ab Seite 2

Zum Geleit

# Voice-over-IP-Forum 2008: der Markt am Wendepunkt?

**Das ComConsult Voice-over-IP-Forum 2008 kommt zu einem kritischen Zeitpunkt. Der Markt ist an einem entscheidenden Wendepunkt angekommen:**

- Traditionelle TK-Hersteller befinden sich im Umbruch und repositionieren sich bzw. werden das in den nächsten Monaten machen. Speziell Alcatel und Siemens sorgen hier zur Zeit für Aufmerksamkeit
- Provider stabilisieren ihre Service-Modelle für IP-Telefonie. SIP-Trunking öffnet sich als neuer Markt und bietet den Unternehmen neue Optionen (siehe Schwerpunktartikel)
- Wichtige neue Produkte wie Microsoft OCS sind jetzt fast ein Jahr auf dem Markt, das nächste Release steht an und damit bei vielen Anwendern der Übergang aus dem Testbetrieb in den Operativbetrieb
- Die Sicherheitslage hat sich stabilisiert und etabliert, auch wenn mit Unified Communications neue Risiken entstehen (siehe Zweitthema)
- Unified Communications kommt langsam aus dem Nebel. Der Leistungsumfang wird klarer, die Produktrealität ist besser bewertbar und eine seriöse Planung somit möglich
- Cisco, Microsoft, Polycom, Siemens und Tandberg haben die Diskussion über die Videokonferenz als elementarer Teil moderner Kommunikations-Lösungen neu belebt

Was bedeutet das nun? Im Kern geht es um die Frage, ob der Mehrwert der neuen Produkte inzwischen ein Niveau erreicht hat, dass die Installation traditioneller TK-Anlagen, auch wenn sie auf Hybrid-Niveau erfolgen würde, eine Fehlentscheidung ist (Hybrid bedeutet an dieser Stelle, dass die Anlage IP-Telefonie unterstützt, aber noch die traditionelle Anlagen-Architektur hat). Konkreter formuliert: ist die Zeit einer HiPath 4000, einer OmniPCX oder ähnlicher Produkte zu Ende? Oder positiv formuliert: bieten die neueren Architekturen einen solchen Mehrwert, dass sich ein weiterhin bestehendes Stabilitäts-Risiko lohnt?

Die Frage ist nicht neu, wir stellen sie seit 2 Jahren. Aber aus den zu Beginn genannten Gründen haben wir jetzt einen möglichen Wendepunkt erreicht.

Im Rahmen dieses Geleitworts dazu drei zentrale Anmerkungen:

### 1. Unified Communications

Heutzutage telefonieren wir nicht mehr, sondern wir kommunizieren unified. Jeder Hersteller sucht sich dabei aus dem möglichen Funktions-Spektrum das raus, was am besten zu seinen Produkten passt. Naturgemäß entstehen dadurch Defizite. Unsere Sichtweise dazu ist ganz klar: UC bedeutet für uns Orientierung an Geschäftsprozessen. Wichtige Prozesse sollen vereinfacht werden, Kommunikation soll schneller und effizienter werden. Alle Hersteller, die dies mit ihren Produkten gar nicht können, reduzieren dies typischerweise auf die Präsenz-Anzeige. Dabei muss klar gesagt werden, dass eine Reduzierung von Geschäftsprozessen auf eine Präsenzanzeige grober Unfug ist. Zum einen bezweifle ich ganz eindeutig, dass die Idee der schnelleren Erreichbarkeit wirklich messbar umgesetzt werden kann. Der Aufwand der Regel-Konfiguration lohnt sich nur für wenige Gesprächspartner. Damit fällt dieser ganze Bereich für beliebig viele Geschäftsprozesse (zum Beispiel mit Zulieferern und Kunden) weg. Zum anderen garantiert schnelle Erreichbarkeit keine erhöhte Effizienz. Diese kommt in der Regel aus sauber aufbereiteter und gut zugreifbarer Information. An dieser Stelle unterscheiden sich zum Beispiel interne und externe Geschäftsprozesse deutlich. Intern wird man zu 90% die Informations-Bereitstellung über eine Web-basierte Kollaborations-Plattform als kostengünstiger und effizienter bevorzugen. Zudem sind hier mögliche Erweiterungen einfacher und schneller umsetzbar. Extern wird aus heutiger Sicht SIP der Träger aller Effizienz-Verbesserungen sein. Weitergehende Informationen wie Bilder, Diagramme oder Videos müssen in das laufende Gespräch eingebunden werden können.

Klares Statement: Unified Communications erfordert ein übergeordnetes und vollkommen Produkt-neutrales Design. Wir reden nicht über technische Basteleien, sondern über eine präzise Orientierung an Geschäftsprozessen. Diese kann nicht als Trivialrezept mit den Zutaten Präsenz und Sharepoint erreicht werden. Die ganze Diskussion muss weg von der Technik.

### 2. Offenheit

Wer Geschäftsprozesse und Effizienzverbesserungen wirklich ernst nimmt, der kann das nur mit offenen Lösungen erreichen. Die wirklichen Zugewinne liegen in der Kommunikation mit externen Partnern. Dies kann nur funktionieren, wenn sich alle Seiten an offene Standards halten. Jeder nicht genormte Codec, jedes nicht wirklich offene Gateway ist hier ein Hindernis. Wer von Offenheit redet und Kollaboration predigt, aber proprietäre Sprach- oder Video-Codecs einsetzt, der sagt nicht die Wahrheit.

### 3. Netzwerk-Eignung

Cisco und Microsoft haben die Diskussion über Quality of Service und die Eignung bestehender Netzwerke neu belebt. Dabei ist aus dem wirklichen Leben kommend folgendes festzustellen:

a) ja, es gibt die Projekte, in denen bestehende Netzwerke sich als Voice-ungeeignet herausgestellt haben. Das Problem liegt hier häufig an dem Phänomen, dass die Netzwerke die Anforderungen zu 100% der Zeit einhalten müssen. Die 3% Überlastung von WAN-Verbindungen, die bisher nicht aufgefallen ist, kann jedes VoIP-Projekt zum Platzen bringen.

b) hier wird auch viel Unfug verbreitet. Zum Teil wird VoIP als Vehikel eingesetzt, um unbegründet neue Netzwerke zu verkaufen. In vielen Fällen hat sich der Einsatz von QoS in Lokalen Netzwerken als völlig unnötig und sogar schädlich herausgestellt. Auch die Anforderungen an Latenzzeiten, die zum Teil genannt werden, lassen sich in der Praxis nicht bestätigen (ich telefoniere regelmäßig mit Zeiten von 350ms und erlebe immer wieder, dass die Leute mich fragen, ob ich gerade im Nachbarbüro bin, nach den Unterlagen einiger Hersteller dürfte die Kommunikation mit dieser Latenz kaum noch möglich sein). Allerdings ist Packet-Loss je nach eingesetztem Codec ein klares Geht-Nicht schon ab relativ niedrigen Verlusten.

Hier gilt:

a) die Eignung bestehender Netzwerke lässt sich ohne großen Aufwand messtechnisch feststellen (eigentlich sollte das bestehende Netzwerk-Management diese Daten hergeben, tut es das nicht, dann stimmt wohl was nicht mit der Management-Lösung)

b) Voice-Lösungen in Netzwerken ohne Service-Management sind Bastel-Lösungen auf Hobby-Niveau. Gerade weil Ende-zu-Ende Daten auch über WAN-Strecken gefordert sind und die vorgegebenen Qualitätskriterien zu über 99% einzuhalten sind, ist keine VoIP-Lösung ohne Service-Management denkbar.

Was ist jetzt die Antwort auf die zu Beginn gestellte Frage, ob die Zeit der HiPath´s und OmniPCX´s abgelaufen ist? Die Antwort ist, dass es darauf ankommt, ob das Projekt überhaupt ausreichend spezifiziert und vorbereitet ist. Viele der angebotenen UC-Lösungen sind mehr ein Marketing-Gag, einige Produkte lassen offene Lösungen vermissen, bestehende Infrastrukturen sind nicht immer auf dem notwendigen Stand. Ein nicht ausreichend vorbereiteter Einstieg in moderne Kommunikations-Lösungen ist riskant. Mit großer Besorgnis nehme ich zum Beispiel die vielen laufenden Microsoft OCS-Testinstallationen wahr. Gerade in der Microsoft-Welt ist die Schaffung einer wirksamen Effizienzsteigerung eine Herausforderung. Nicht weil OCS ein Problem hat, sondern weil das von Microsoft bereit gestellte Portfolio aus Exchange, OCS, Groove, Sharepoint, Office in seiner Gesamt-Komplexität jeden aktuellen Horror-Film locker an die Wand spielt.

Aber: ist ein solides Fundament gelegt, dann bringt die neue Welt einen solchen Mehrwert, dass die Zeit der alten Lösungen abgelaufen ist. Es gibt also kein klares Ja oder Nein als Antwort auf die Frage.

In diesem Sinne freue ich mich auf einen Diskussions-intensiven Kongress.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

# Voice-over-IP-Forum 2008

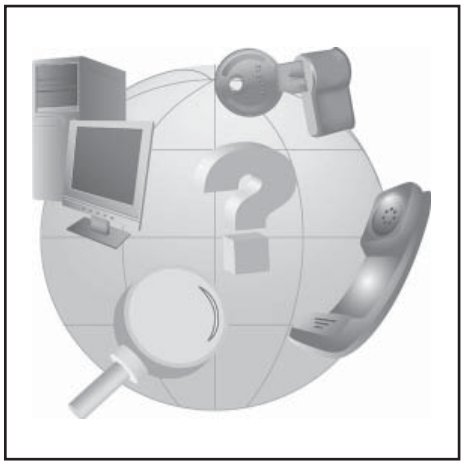
**Die ComConsult Akademie veranstaltet vom 10.11. - 13.11.08 ihr „Voice-over-IP-Forum 2008“ in Königswinter.**

Das ComConsult Voice-over-IP-Forum 2008 kommt zu einem kritischen Zeitpunkt.

Der Markt ist an einem entscheidenden Wendepunkt angekommen:

- Traditionelle TK-Hersteller repositionieren sich
- Provider erweitern ihre Service-Modelle für IP-Telephonie und SIP-Trunking
- Neue Produkte wie Microsoft OCS entwachsen den Kinderschuhen
- Die Sicherheitslage hat sich stabilisiert und etabliert
- Unified Communications kommt langsam aus dem Nebel. Der Leistungsumfang wird klarer, die Produktrealität ist besser bewertbar und eine seriöse Planung somit möglich

Was bedeutet das nun? Im Kern geht es um die Frage, ob die der traditionellen Anlagen-Architekturen abgelaufen ist? Oder positiv formuliert: bieten die neueren Architekturen einen solchen Mehrwert, dass



sich ein weiterhin bestehendes Stabilitäts-Risiko lohnt?

Hier setzt das ComConsult Voice-over-IP-Forum 2008 an.

Das Forum präsentiert

1) Neue und hochaktuelle Studien über Technologien und Produkte
2) Projekt- und Erfahrungsberichte
3) Kritische Detail-Analysen ausgewählter Technologien

a Wo steht Microsoft OCS ein Jahr nach Einführung?
b. Wie ist die Markt- und Produktsituation bei Siemens zu bewerten?
c. Unified Communications: zwischen Luftschloss und wirklicher Effizienzsteigerung
d. Telepresence: was bringt sie wirklich, sind 15 Mbit/s wirklich erforderlich, wo ist der messbare Mehrwert zu HD-Lösungen?
e. Anforderungen an Netzwerke: was ist wirklich schädlich, wo sind Projekte und warum gescheitert?
f. VoIP-Service-Management: Status-Quo
g. Wo stehen die Provider mit SIP-Trunking? Was leistet SIPconnect als Standard? Wie kann Multimedia-Interoperabilität erreicht werden?

Diese Aufstellung ist noch unvollständig. Details in den kommenden Wochen.

Das ComConsult Voice-over-IP-Forum wird auch in diesem Jahr der Treffpunkt der Branche. Versäumen Sie nicht, sich einen Platz in diesem herausragenden Forum zu sichern.

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung
# Voice-over-IP-Forum 2008

Ich buche den Kongress
**Voice-over-IP-Forum 2008**

☐ 10.11. - 13.11.08 in Königswinter
zum Preis von € 2.090,- * zzgl. MwSt.
*gültig bis 15.09.2008
(dann regulär € 2.290,- zzgl. MwSt.)

☐ mit Report „Analyse der Strategie und Marktposition von Siemens Enterprise Communications“
zum Preis von € 149,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Zimmer im Maritim Hotel Königswinter

vom_____ bis_____ 08

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.de**

| | |
|---|---|
| _____ Vorname | _____ Nachname |
| _____ Firma | _____ Telefon/Fax |
| _____ Straße | _____ PLZ,Ort |
| _____ eMail | _____ Unterschrift |

Neuer Kongress

# Rechenzentrum Infrastruktur-Redesign Forum 2008

**Die ComConsult Akademie veranstaltet vom 24.11. - 26.11.08 erstmalig ihren Kongress „Rechenzentrum Infrastruktur-Redesign Forum 2008“ in Königswinter.**

Unsere Rechenzentren befinden sich in Mitten einer der größten Redesign-Phasen der letzten 20 Jahre. Die wesentlichen Treiber dieses Redesigns sind: Server-Konsolidierung, Speicher-Konsolidierung, neue IT-Architekturen, mehr und mehr Web-basierte Applikationen.

Rechenzentren-Redesign bedeutet dabei vor allem ein Redesign der Infrastrukturen. Im Mittelpunkt stehen dabei: Netzwerke, Speicher-Systeme, Verkabelung, Strom und Klima.

**Zukunfts-fähige RZ-Netzwerke: was bedeutet das?**
Immer mehr Server auf immer weniger Raum. Die Kombination aus Blade-Server und Virtuellen Infrastrukturen führt zu immensen Anschlussdichten. Dies ist gepaart mit extrem hohen Bandbreiten-Bedürfnissen. Zu einfache Lösungen werden bereits an der notwendigen Ausfallsicherheit scheitern. Etablierte Verfahren wie Spanning-Tree sind hier fehl am Platz. RZ- und Server-Netzwerke bilden eine neue Generation von Netzwerk, mit neuen Switching-Produkten und neuen Netzwerk-Verfahren. Wir analysieren diese Technologien für Sie.

**Speicher-Konsolidierung: wohin fährt der Zug?**
Ethernet, Infiniband und Fibre Channel sind die Basis-Zutaten für ein explosives Technologie-Gemisch. Fibre Channel erweist sich immer mehr als zu teuer und zu langsam in der Weiterentwicklung. Die Integration in virtuelle Infrastrukturen wirft neue Anforderungen auf. Ethernet mit der Zuverlässigkeit des Fibre Channels: ist das die Quadratur des Kreises oder erreichbar. Kaum ein anderes Technologie-Feld wird so von Hersteller-Interessen dominiert wie dieses. Unsere große Analyse und der Technologie-Ausblick erwarten Sie auf dem Forum.

**RZ-Verkabelung 2008: wo stehen wir?**
Bandbreite + Anschlussdichte + Gewicht + neue Standards = Kupfer oder Glasfaser? Das ist die Kernfrage. Diese ist verbunden mit der Frage, wie wir aus der Altlastsituation im Doppelboden und in den Schränken sinnvoll in eine einfach zu handhabende und überschaubare Lösung kommen. Unsere Verkabelungs-Analyse wird die bestehenden Optionen analysieren und Empfehlungen auf dem Forum präsentieren.

**Infrastruktur-Sicherheit im RZ: eine echte Herausforderung**
Im Prinzip stehen die üblichen Verdächtigen auch im Rahmen der RZ-Konsolidierung zur Debatte. Aber extrem hohe Bandbreiten, kurze Signallaufzeiten und neue Netzwerk-Architekturen machen Firewalls, IPS, NAC, 802.1X und anderen Lösungsansätzen das Leben schwer. Was hat sich bewährt, was wird in diesem Umfeld nicht skalieren? Auch hier unsere Analyse auf dem Forum.

**Integration mobiler Mitarbeiter / Fixed-Mobile-Konvergenz**
Einbindung aller relevanten Mitarbeiter in die wichtigen Geschäftsprozesse, egal wo sich diese befinden. Das Thema ist nicht neu, aber die technischen Möglichkeiten verändern sich. Mehr Bandbreite, neue Gerätetechnologien, andere Applikations-Architekturen schaffen die Voraussetzung für mehr Effizienz und Erfolg mobiler Mitarbeiter. Wir analysieren die neuesten technischen Ansätze speziell aus dem Umfeld der Server- und Applikations-Konsolidierung für Sie auf dem Forum.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-phase bis 30.09.2008

# Anmeldung

## Rechenzentrum Infrastruktur-Redesign Forum 2008

Frühbucher-phase bis 30.09.2008

Ich buche den Kongress **Rechenzentrum Infrastruktur-Redesign Forum 2008**
☐ 24.11. - 26.11.08 in Königswinter
zum Preis von € 1.690,- * zzgl. MwSt.
*gültig bis 30.09.2008
(dann regulär € 1.890,- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich ein Hotelzimmer

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Zweitthema

# Sicherheit in Unified Communications

## Integration und Sicherheit: Die Quadratur des Kreises?

Fortsetzung von Seite 1

David Ferrest ist seit 2007 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der IT-Security. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Videokonferenz-Systeme befasst.

Dr. Simon Hoff ist technischer Direktor bei der ComConsult Beratung und Planung GmbH und unter anderem verantwortlich für den Bereich IT-Sicherheit. Dr. Hoff blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb in den Bereichen IT-Infrastrukturen, mobiler und drahtloser Kommunikationssysteme zurück.

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Betrachtet man allein die möglichen Verbesserungen der Arbeitsabläufe, die sich durch die Integration ergeben, so spricht in der Tat alles für eine zunehmende Verschmelzung der unterschiedlichen Systeme. Berücksichtigt man jedoch auch die Auswirkungen der Integration auf Vertraulichkeit, Integrität und Verfügbarkeit des Gesamtsystems, so kann die Beurteilung von UC nicht mehr ganz so eindeutig ausfallen.

Dieser Artikel beschreibt einige für UC wichtige TK-Applikationen und betrachtet insbesondere die durch sie entstehenden Gefährdungen der IT-Sicherheit und analysiert entsprechende Sicherheitsmaßnahmen. Grundlage ist die im Juli 2008 veröffentlichte Technische Leitlinie Sichere TK-Anlagen des Bundesamts für Sicherheit in der Informationstechnik (siehe [1]).

### 1. Bausteine von Unified Communications

Die Funktionen eines UC-Systems bzw. die Applikationen im Umfeld einer TK-Anlage sind äußerst vielfältig und reichen vom klassischen Sprachmailbox-System bis hin zur Steuerung von Gebäudetechnik über das Telefon. Solche Applikationen können sich der Vermittlungsfunktion einer TK-Anlage bedienen, die Anlage und Endgeräte steuern oder Informationen verwerten, die von der Anlage bzw. über die Anlage bereitgestellt werden. Abbildung 1 zeigt eine Auswahl weit verbreiteter Funktionen.

Auch wenn keine der dargestellten Funktionen wirklich neu ist, so erhalten sie doch mit der wachsenden Verbreitung von VoIP eine zunehmend größere Relevanz. Der Wegfall von kostspieligen proprietären Gateways und der Einsatz standardisierter Protokolle senkt die Kosten und erlaubt die Erschließung neuer Anwendungsfelder. Die Hersteller setzen verstärkt auf diesen Trend und bieten unter dem Stichwort Unified Communications Systeme an, die vielfältige Möglichkeiten zur Kommunikation bieten - aber auch zum potenziellen Missbrauch.

Im Folgenden werden die wichtigsten der in Abbildung 1 dargestellten und in der Praxis häufig vorzufindenden TK-Applikationen bzw. UC-Funktionen sowie die von Ihnen verwendeten Protokolle und Schnittstellen beschrieben.

#### 1.1 Unified Messaging

Unified Messaging (UM) integriert verschiedene Nachrichtenformate in einem einheitlichen System. Die Anwender entnehmen ihre Nachrichten (z. B. E-Mail, Fax, SMS und Sprachnachrichten) einer einzigen Datenbank bzw. können über eine einzige Nutzerschnittstelle Nachrichten unterschiedlichen Formats versenden. Viele UM-Systeme bieten zudem die Möglichkeit, auf diesen konsolidierten Nachrichteneingang über verschiedene Kanäle wie z. B. über eine Web-Oberfläche oder per Telefon zugreifen zu können.

Es muss betont werden, dass keine allgemein akzeptierte Definition des funktionalen Umfangs von UM existiert. So vertreiben einige Hersteller reine Sprachnachrichtensysteme unter dem Begriff UM, während Produkte anderer Hersteller nur den Empfang von Fax-Nachrichten im E-Mail-Postfach der Benutzer unterstützen. Im Folgenden wird der Begriff UM entsprechend der einleitenden Beschreibung sehr weit gefasst, um alle sicherheitsrelevanten Aspekte dieser Klasse von TK-Applikationen zu erfassen.

UM-Produkte mit einem umfassenden Funktionsspektrum benötigen naturgemäß

Sicherheit in Unified Communications - Integration und Sicherheit: Die Quadratur des Kreises?

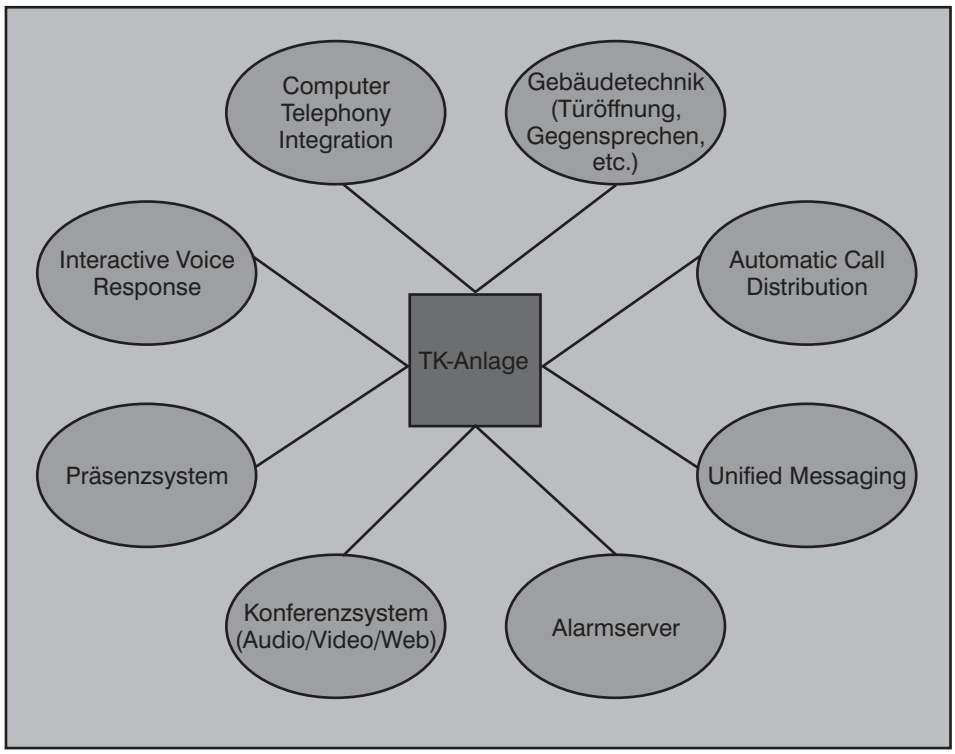



Abbildung 1: Applikationen und Mehrwertdienste mit Bezug zur Telekommunikation

eine Vielzahl von Schnittstellen für Benutzer sowie unterschiedliche Dienste und Anwendungen. Im Mittelpunkt stehen dabei die Schnittstellen zu TK-Anlagen und zu E-Mail-Systemen. Hinzu kommen noch Schnittstellen zur Kopplung mit anderen Kommunikationssystemen, Administrationsschnittstellen, Benutzerschnittstellen, Anbindungen an Verzeichnisdienste sowie Schnittstellen zu Geschäftsapplikationen (siehe Abbildung 2).

Für die Integration von UM-System und TK-Anlage werden (zumindest aus logischer Sicht) zwei Schnittstellen benötigt. Über eine Sprachschnittstelle werden von der TK-Anlage kommende Anrufe an das Sprachspeichersystem übergeben. Umgekehrt werden bei telefonischen Abfragen die Nachrichten über die Sprachschnittstelle ausgegeben. Die zweite Schnittstelle wird für Signalisierungsdaten benötigt, z. B. um Endgeräten zu signalisieren, dass neue Nachrichten auf den Benutzer warten, oder um die Ansage des Sprachspeichersystems an den jeweiligen Anrufer bzw. den Grund der Weiterleitung (besetzt, nicht verfügbar, etc.) anzupassen.

Die Integration mit klassischen TK-Anlagen und Hybrid-Systemen erfolgt in der Regel über eine in den UM-Server eingebaute Telefonie-Karte. Über diese Karte werden die Sprachdaten verarbeitet und bei einigen Produkten durch speziell kodierte Tonfolgen auch die Signalisierungsdaten.

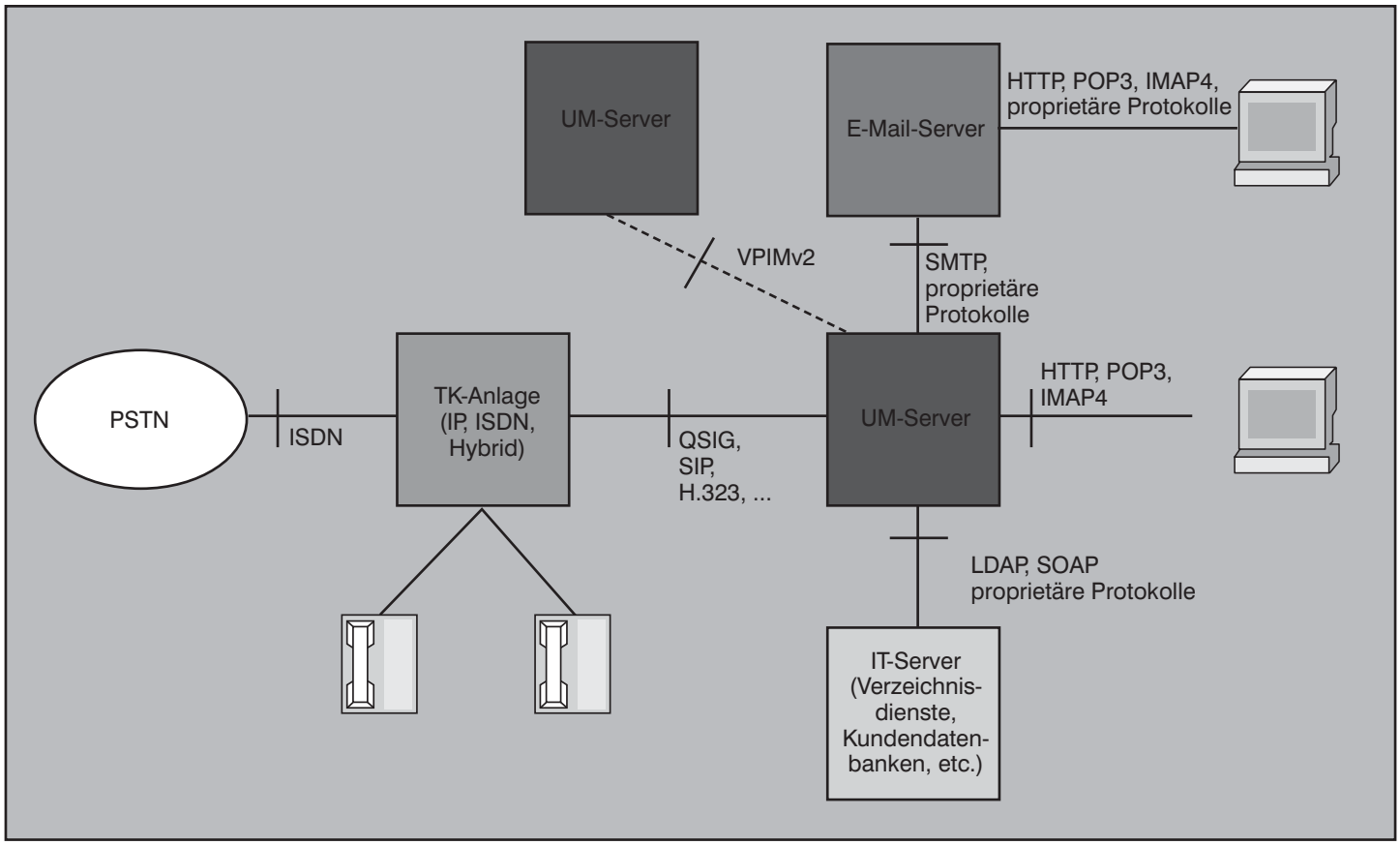



Abbildung 2: Typische Architektur eines Unified Messaging Systems mit Integration in ein IT-System

Alternativ wird die Signalisierungsschnittstelle durch ein serielles Verbindungskabel zwischen UM-Server und TK-Anlage bereitgestellt oder durch andere dedizierte und proprietäre Verbindungen. Bei modernen Anlagen erfolgt die Anbindung typischerweise durch ein VoIP-Protokoll (z. B. SIP oder H.323), wobei die IP-Verbindung sowohl für den Sprach- als auch den Signalisierungskanal verwendet wird und somit keine dedizierten Leitungen erforderlich sind.

Im Prinzip verhält sich der UM-Server aus Sicht der TK-Anlage zunächst wie ein Endgerät. Die Gefährdungssituation bezüglich der Sprachschnittstelle entspricht damit jener der Endgeräte einer entsprechenden TK-Anlage. Ein weiteres Gefährdungspotenzial ergibt sich aus der Signalisierungsschnittstelle, insbesondere dann, wenn diese mittels einer weiteren dedizierten Verbindung implementiert ist.

Bei der Integration mit E-Mail-Systemen muss zwischen zwei Szenarien unterschieden werden. Beim so genannten True Unified Messaging werden alle eingegangenen Nachrichten durch den UM-Server im E-Mail-Postfach eines Benutzers, d. h. auf dem E-Mail-Server, abgelegt. Für die Auslieferung der Nachrichten kann z. B. SMTP eingesetzt werden; weit verbreitet ist jedoch auch der Einsatz des proprietären MAPI-RPC Protokolls von Microsoft. Bei UM-Systemen, die kein True Unified Messaging unterstützen, werden die eingegangenen Nachrichten von einem auf dem UM-Server laufenden eigenen E-Mail-Server bereitgestellt. Die Nutzer müssen daher ihre E-Mail-Clients so einrichten, dass ihre Nachrichten z. B. über die bekannten Protokolle POP3 oder IMAP4, von diesem Server abgeholt werden.

Zusätzlich oder als Alternative zur Integration mit dem E-Mail-System bieten viele UM-Dienste eine Web-Schnittstelle, damit Benutzer auf ihre Nachrichten zugreifen können bzw. um Nachrichten zu versenden.

Zur Verbindung von UM- bzw. Sprachspeichersystemen untereinander, z. B. während Migrationsphasen, existieren zwei Protokolle. AMIS (Audio Messaging Interchange Specification) ist ein Protokoll zur Kopplung älterer Sprachspeichersysteme über eine analoge Telefonleitung. VPIM (Voice Profile for Internet Mail) wird von neueren digitalen Systemen eingesetzt und verwendet E-Mail zur Auslieferung von Sprach- und Faxnachrichten.

Es sollte beachtet werden, dass ein spezifisches UM-System noch eine Reihe weiterer Schnittstellen bieten kann, die hier nicht aufgeführt wurden. Beispiele hierfür sind Anbindungen an so genannten SMS Large Accounts zur massenhaften Versendung von Kurznachrichten und die Anbindung an Verzeichnisdienste und Fax-Server. Es ist daher im Einzelfall mit dem Hersteller eines Systems zu klären, welche Schnittstellen vorhanden sind, welche für den Betrieb unter den gegebenen Anforderungen benötigt werden und welche gegebenenfalls deaktiviert werden können.

| Abkürzung | Name | Beschreibung |
|---|---|---|
| TAPI | Telephony Application Programming Interface | Programmierschnittstelle für Windows-basierte Rechner; ermöglicht Einzel- und Mehrplatzlösungen |
| TSAPI | Telephony Server API | Programmierschnittstelle für Novell Netware; ermöglicht Mehrplatzlösungen |
| JTAPI | Java Telephony API | Java-basierte Programmierschnittstelle für Einzel- und Mehrplatzlösungen |
| CSTA | Computer Supported Telecommunications Applications | ISO-standardisiertes Anwendungsprotokoll für Einzel- und Mehrplatzlösungen |

Tabelle 1: Wichtige CTI-Programmierschnittstellen und -Protokolle

**1.2 Computer Telephony Integration**

Computer Telephony Integration (CTI) ermöglicht die Steuerung eines Telefons von einem PC aus. Dies umfasst insbesondere den automatischen Aufbau, die Annahme und Beendigung von Telefongesprächen, den Aufbau von Telefonkonferenzen, Anrufjournale, Telefonbuchdienste, sowie die Weitervermittlung von Gesprächen.

Es wird zwischen Einzelplatzlösungen (First Party Call Control) und Mehrplatzlösungen (Third Party Call Control) unterschieden. Bei Einzelplatzlösungen ist das Telefon entweder im Computer integriert oder direkt mit diesem verbunden. In diesem Fall kann eine CTI-Applikation lediglich das mit dem Computer verbundene Telefon steuern. Bei Mehrplatzlösungen ist in der Regel ein so genannter CTI-Server zwischen dem Computernetzwerk und dem Telefonnetz beziehungsweise der Telefonanlage geschaltet. Dies erlaubt zusätzlich zur Kontrolle des eigenen Telefons grundsätzlich auch die Steuerung anderer Apparate.

Zur Kopplung von Computer und Telefon bzw. von CTI-Server und TK-Anlage wurden eine Reihe von Protokollen und Programmierschnittstellen (APIs) entwickelt, deren bekannteste Vertreter in Tabelle 1 zusammengefasst sind.

TAPI bietet Entwicklern von Windows-basierten CTI-Anwendungen eine generische Schnittstelle zur Nutzung von Telefoniediensten in Einzel- und Mehrplatzszenarien. Die Spezifikation umfasst Funktionen zur Abfrage und Steuerung von Telefonen, Verbindungen und Konferenzschaltungen sowie zur Behandlung von Call-Center-spezifischen Aufgaben, wie zum Beispiel der Abfrage des Agentenstatus. Mithilfe dieses Funktionssatzes können von der einfachen Modemsteuerung bis hin zu komplexen Call Center Anwendungen eine Vielzahl von CTI-Applikationen implementiert werden.

Da TAPI nur eine Programmierschnittstelle darstellt, benötigt ein lauffähiges Programm einen so genannten Telephony Service Provider (TSP). Dies ist eine Art Treiberprogramm, das die Funktionsaufrufe der CTI-Anwendung in Kommandos für das zu steuernde Gerät umsetzt. Dieses Treiberprogramm wird in der Regel vom Hersteller der TK-Anlage bzw. des zu steuernden Geräts bereitgestellt, da praktisch jeder Hersteller sein eigenes Protokoll zur Verbindungskontrolle implementiert und diese proprietären Schnittstellen in der Regel auch nicht veröffentlicht werden. Ohne zusätzliche Maßnahmen ist die Vertraulichkeit und Integrität der Daten, die über eine solche CTI-Verbindung transportiert werden, damit abhängig vom Hersteller bzw. vom Produkt. Eine ungesicherte CTI-Verbindung erlaubt u.a. das Mitlesen von Anrufdaten und sogar die Steuerung eines fremden Telefons, z. B. zur Initiierung eines Anrufs.

Vergleichbar mit TAPI stellen TSAPI und JTAPI ebenfalls Programmierschnittstellen bereit, die über spezielle Treiberkomponenten Funktionsaufrufe auf herstellerspezifische Protokolle umsetzen. Unterschiede zu TAPI bestehen hauptsächlich im angebotenen Funktionsumfang sowie im Einsatzgebiet. So wurde TSAPI für den Einsatz in Novell Netware Umgebungen entwickelt. Zudem bietet es keine Unterstützung für First Party Call Control, da es primär für den Einsatz in Call Center Umgebungen entwickelt wurde. JTAPI hingegen unterstützt sowohl Einzel- als auch Mehrplatzlösungen, wobei für die CTI-Applikationen die Verwendung der Programmiersprache Java vorgesehen ist. Da diese Schnittstellen wie TAPI einen Treiber benötigen, der die Kommunikation mit der TK-Anlage übernimmt, ist die Sicherheit der CTI-Verbindung auch hier herstellerabhängig.

Im Gegensatz zu TAPI, TSAPI und JTAPI ist CSTA keine API sondern ein Protokoll der Anwendungsschicht. Der ISO-Standard CSTA spezifiziert die unterstützte Funktionalität sowie die zugehörigen Daten. Die Funktionalität umfasst dabei u.a. die Verbindungskontrolle, die Endgerätekontrolle, die Überwachung von Endgeräten und Verbindungen sowie die Abrechnung von Verbindungsdaten. CSTA unterstützt sowohl Einzel- als auch Mehrplatzlösungen. Die Spezifikation gibt keine Mechanismen für den Transport von CSTA-Nachrichten vor, d. h. insbesondere, dass die Vertraulichkeit und Integrität der Daten ähnlich wie bei den beschriebenen APIs von den jeweiligen Herstellern der CTI-Server und TK-Anlagen abhängt.

Abbildung 3 zeigt an einem typischen Aufbau einer Mehrplatzlösung den Einsatz der genannten Protokolle. Die in der Abbildung dargestellte Anbindung über eine CTI-Middleware ist nur dann erforderlich, wenn die TK-Anlage nicht über die verbreiteten CTI-Schnittstellen verfügt. Neben den genannten CTI-Protokollen werden in diesem Szenario zwei weitere Schnittstellen für die Anbindung an ein IT-System verwendet: LDAP (Lightweight Directory Access Protocol) und ODBC (Open Database Connectivity). Diese Art der Kopplung ist gerade bei CTI-Systemen sehr häufig vorzufinden, da z. B. Agentenarbeitsplätze in Call Centern mit Kundendatenbanken und anderen IT-Systemen ver-

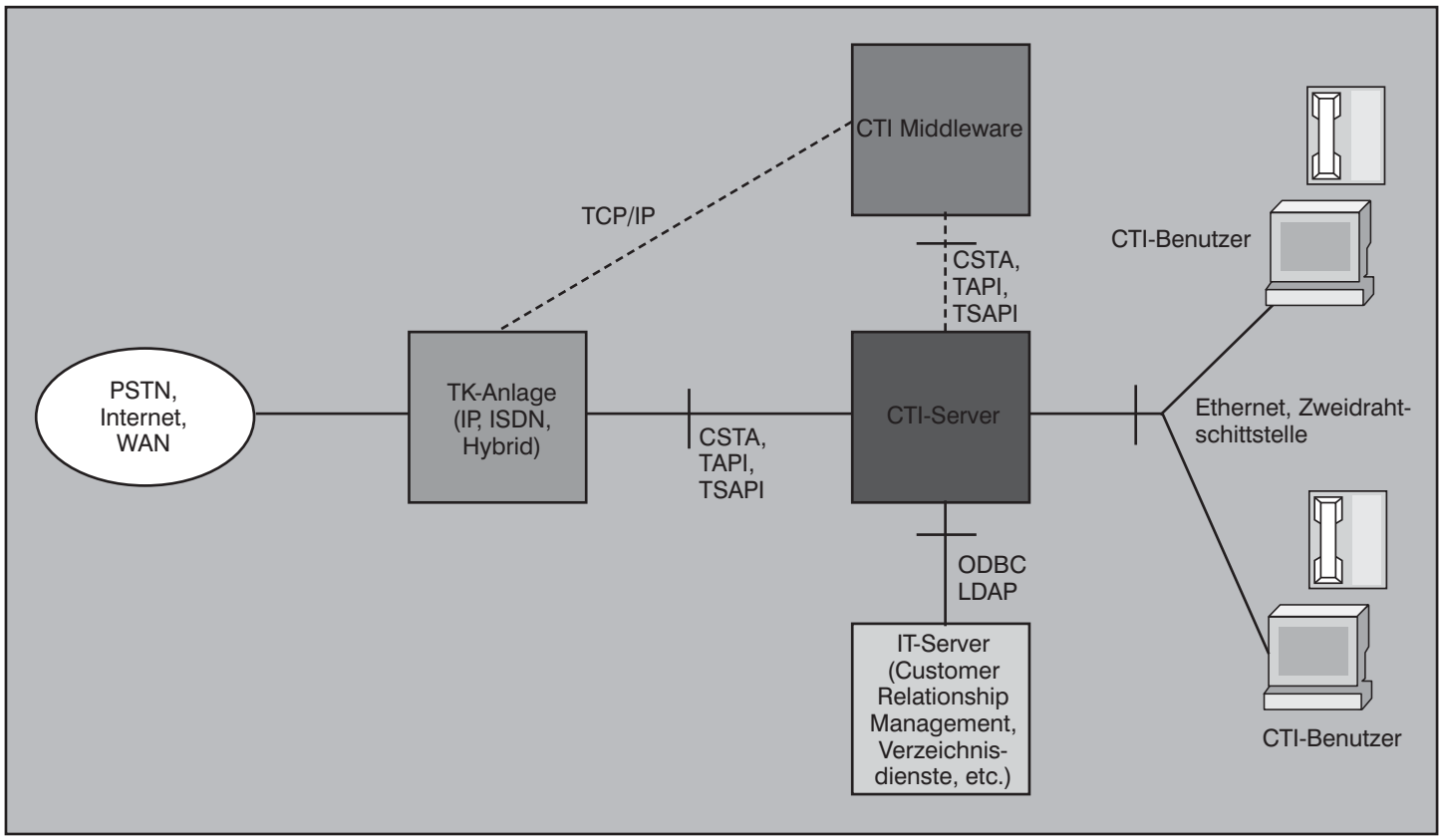



Abbildung 3: Typischer Aufbau einer CTI-Mehrplatzlösung mit Integration in ein IT-System

bunden werden. Beispielsweise kann über eine automatische Anruferidentifikation der passende Datensatz mit Kundendaten, Anrufhistorie, Vertragsdaten etc. aus einer Datenbank auf den Bildschirm gebracht werden. Die Anbindungen an solche Datenbanken erfolgt in der Regel über standardisierte Protokolle wie das bereits genannte LDAP bzw. über APIs wie ODBC. LDAP erlaubt die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes. ODBC ist eine standardisierte Datenbankschnittstelle, die SQL als Datenbanksprache verwendet. ODBC bietet also – vergleichbar mit TAPI – eine Programmierschnittstelle (API), die es einem Programmierer erlaubt, seine Anwendung relativ unabhängig vom verwendeten Datenbankmanagementsystem (DBMS) zu entwickeln, wenn dafür ein ODBC-Treiber existiert.

Ohne zusätzliche Maßnahmen ist die Vertraulichkeit und Integrität der Daten, die über eine ODBC-Verbindung transportiert werden, abhängig vom Hersteller des DBMS bzw. vom konkreten Produkt. LDAP hingegen sieht den Einsatz von TLS und SSL zur Authentisierung und Verschlüsselung vor.

In jüngster Zeit wird für die Anbindung an IT-Server zunehmend das SOAP-Protokoll eingesetzt. SOAP stand ursprünglich für Simple Object Access Protocol, jedoch wird der Begriff SOAP inzwischen als Eigenname verwendet und steht nicht mehr für eine Abkürzung. SOAP ist ein Protokoll zum Austausch XML-basierter Nachrichten über das insbesondere auch die Funktion eines Remote Procedure Call (RPC) realisiert werden kann (siehe [2]). Die Extensible Markup Language (XML) ist eine vom World Wide Web Consortium (W3C) spezifizierte Auszeichnungssprache, die zur formalen textuellen Beschreibung und Darstellung hierarchisch strukturierter Daten dient.

Es sollte beachtet werden, dass ein spezifisches CTI-System noch eine Reihe weiterer Schnittstellen bieten kann, die hier nicht aufgeführt wurden (beispielsweise Administrations-Schnittstellen). Es ist daher im Einzelfall mit dem Hersteller eines Systems zu klären, welche Schnittstellen vorhanden sind, welche für den Betrieb unter den gegebenen Anforderungen benötigt werden und welche gegebenenfalls deaktiviert werden können.

### 1.3 Interactive Voice Response

Interactive Voice Response (IVR) bietet die Möglichkeit, teil- oder vollautomatisierte Sprachdialoge zu führen. Dies umfasst sowohl einfache Sprachmenüs, durch die per Tastendruck navigiert wird („Für den Vertrieb drücken Sie bitte die ‚1', für Service die ‚2', ..."), als auch Systeme, die einen natürlichsprachlichen Dialog zur Abfrage von Informationen (z. B. Fahrplanauskünften) erlauben.

Bei frühen IVR-Systemen wurde nicht klar zwischen Applikationen (d. h. den konkreten Dialogabläufen) und der ausführenden Plattform getrennt. Die möglichen Dialoge waren bei solchen Systemen praktisch vorgegeben und nur schwer zu ändern bzw. anzupassen. Im Laufe der Zeit entwickelten die Hersteller von IVR-Systemen verschiedene proprietäre Dialogbeschreibungssprachen, die es den Administratoren und Anwendern erlauben eigene Sprachapplikationen zu entwickeln und anzupassen. Inzwischen existiert eine Reihe von Standards für Sprachen zur Beschreibung von Dialogabläufen. Einer der bekanntesten Standards ist die XML-basierte Empfehlung des World Wide Web Consortium (W3C) namens VoiceXML. Mithilfe von VoiceXML können Sprachapplikationen in ähnlicher Weise entwickelt und bereitgestellt werden wie visuelle Applikationen mittels HTML.

Aus dieser Ähnlichkeit ergeben sich Gefährdungen analog zu Web-Applikationen. Zum einen kann ein Sprachdialogsystem Zugriff auf schützenswerte Daten geben. Zu solchen Applikationen zählen beispielsweise das Telefon-Banking, der Anrufbeantworter im Netz oder die Abfrage des E-Mail-Postfachs per Telefon. Somit muss der Zugriff auf die gesamte Applikation bzw. auf schützenswerte Punkte gesichert sein. Bei Web-Applikationen erfolgt die Authentisierung in der Regel

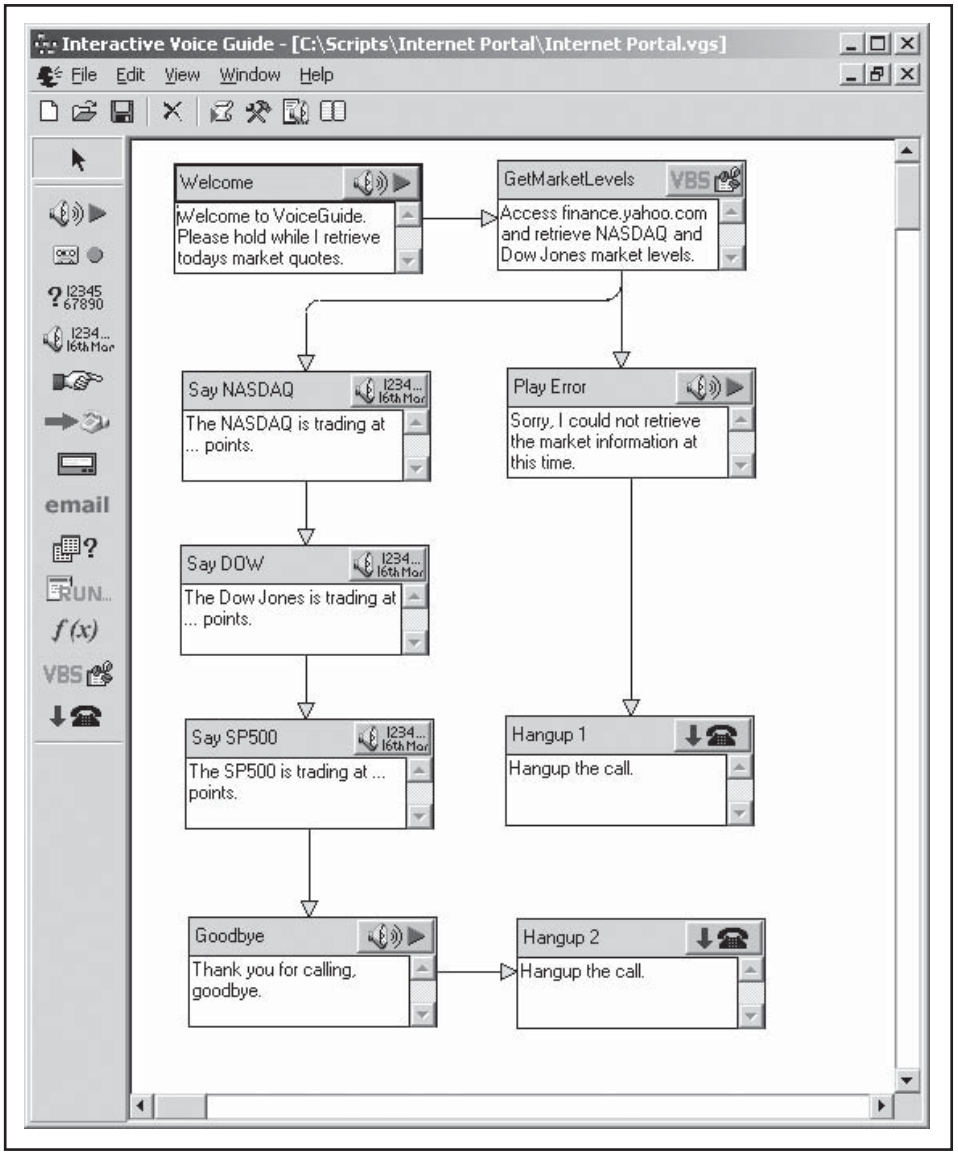



Abbildung 4: Struktur einer IVR-Anwendung zur Abfrage von Börsendaten (Quelle: VoiceCallCentral)

durch Benutzername und Passwort, während bei IVR-Systemen meist eine Personal Identification Number (PIN) verwendet wird. Vereinzelt werden auch Verfahren zur Sprechererkennung eingesetzt, jedoch sind diese z. Zt. selbst unter optimalen Bedingungen, d. h. ohne Hintergrundgeräusche und mit hochwertigem Sprachcodec, nicht zuverlässig. (siehe Abbildung 4)

Neben der Kopplung mit der TK-Anlage über einen Sprachkanal, ist ein IVR-System häufig auch mit anderen IT-Komponenten, z. B. mit Datenbanken, verbunden. Die spezifische IT-Komponente (und damit letztlich auch die spezifische Schnittstelle) hängt dabei von der implementierten IVR-Applikation ab. In der Regel werden für die Anbindung solcher externer Systeme jedoch die im vorangegangenen Abschnitt vorgestellten Schnittstellen, wie LDAP, ODBC und SOAP sowie weitere RPC-Mechanismen, verwendet. Es gelten die dort beschriebenen Gefährdungen.

Schließlich verfügen IVR-Systeme auch über Administrations- und Konfigurationsschnittstellen. Das Spektrum reicht von dedizierten Applikationen zur Erzeugung neuer Applikationen, die über proprietäre Protokolle oder Dateiformate mit dem IVR-System kommunizieren bis hin zu gewöhnlichen web-basierten Management-Schnittstellen. Es gilt auch hier, dass mit dem Hersteller eines Produkts die konkrete Zahl und Ausprägungen von Schnittstellen eines IVR-Systems geklärt werden sollte, um diese entsprechend abzusichern bzw. deaktivieren zu können.

### 1.4 Präsenzdienste

Präsenzinformation signalisiert die Möglichkeit und Bereitschaft der Nutzer eines Präsenzsystems zur Kommunikation. Ist das Präsenzsystem mit der Telefonanlage verbunden, so kann z. B. auch der Status „Im Gespräch“ angezeigt werden, wenn ein Benutzer gerade telefoniert. Entsprechende Clients bieten in der Regel auch CTI-Funktionalität, so dass sich z. B. durch einen Klick ein Anruf zu einem gesprächsbereiten Nutzer aufbauen lässt. Präsenzinformation wurde ursprünglich im Kontext von Instant Messaging, d. h. Systemen zum Austausch von kurzen Textnachrichten in Echtzeit, eingesetzt, gewinnt nun aber auch für (IP-basierte) TK-Anlagen eine zunehmende Bedeutung.

Die Präsenzinformation wird bei den meisten Systemen zentral durch einen Präsenzdienst bereitgestellt und verwaltet. Der Client eines Nutzers sendet die manuell oder automatisch ermittelte Verfügbarkeit des Nutzers an den Präsenzdienst, wo sie anderen Nutzern bzw. Clients zur Verfügung gestellt wird. Informationen zum Nutzerstatus können jedoch auch aus anderen Quellen stammen. In der Praxis verwenden Präsenzdienste üblicherweise noch den Kalender eines Nutzers sowie die Telefonanlage. In beiden Fällen ist die Umsetzung entsprechender Abfragen produktabhängig; mögliche Varianten reichen von einfachen Datenbankabfragen über proprietäre Protokolle bis hin zu standardisierten Mechanismen. Im Fall der Einbindung einer Telefonanlage können neben herstellerspezifischen Ansätzen u.a. die Protokolle CSTA oder auch SIP/SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) bzw. XMPP (eXtensible Messaging and Presence Protocol) eingesetzt werden.

SIP/SIMPLE dient wie das ebenfalls von der IETF spezifizierte Protokoll XMPP der Kommunikation zwischen Präsenzdienst und Clients. Die ersten Präsenz- und Instant-Messaging-Dienste waren auf Privatkonsumenten ausgerichtet und verwendeten proprietäre Protokolle. In der jüngsten Vergangenheit setzen sich insbesondere im Unternehmensbereich jedoch zunehmend Systeme auf Basis der beiden genannten Standards durch. SIP/SIMPLE ist eine Erweiterung des weit verbreiteten VoIP-Signalisierungsprotokolls SIP und bietet unter anderem die folgenden Funktionen:

- Registrierung für Präsenzinformation und Benachrichtigung, wenn sich der Status eines Nutzers ändert
- Senden und Empfangen von kurzen Textnachrichten
- Management von Sitzungen, in denen Nachrichten in Echtzeit ausgetauscht werden (so genannte „Chats“)

XMPP bietet im Kern dieselbe Funktionalität, ist jedoch nicht an SIP gebunden. Beide Protokolle bieten durch Registrierungen und Benachrichtigungen einen Ereignismechanismus, der für die Signalisierung des Telefoniestatus eines Nutzers an den Präsenzdienst geeignet ist. Damit können diese Protokolle nicht nur für die Kommunikation zwischen Präsenzdienst und Client, sondern auch für die Kommunikation zwischen Telefonanlage und Präsenzdienst eingesetzt werden.

Werden diese Schnittstellen nicht abgesichert, dann kann die Information, dass ein Nutzer telefoniert (und weiterer Nutzerkontext), abgehört werden. Da dieselben Protokolle auch dem Instant Messaging dienen, sind konsequenterweise auch Kurznachrichten gefährdet. Diese Gefährdung ist nicht zu unterschätzen, da die Inhalte eines Chats durchaus vergleichbar mit denen eines Telefonats sein können. Sowohl SIP/SIMPLE als auch XMPP bieten jedoch die Möglichkeit per TLS eine Authentisierung durchzuführen und den Nachrichtentransport zu verschlüsseln. Zudem erlauben einige Präsenzdienste

die Sichtbarkeit von Information für jeden einzelnen Teilnehmer detailliert festzulegen.

In Bezug auf die Schnittstellen und Gefährdungen, die aus der CTI-Funktionalität von Clients eines Präsenzsystems resultieren, wird auf den Abschnitt zum Thema CTI verwiesen. Des Weiteren sollte beachtet werden, dass ein spezifischer Präsenzdienst noch zusätzliche Schnittstellen bieten kann, die hier nicht aufgeführt wurden. Beispiele hierfür sind die als Alternative zum dedizierten Client häufig vorzufindenden Web-Schnittstellen für die Client-Kommunikation sowie Management-Schnittstellen. Es ist daher auch hier im Einzelfall mit dem Hersteller eines Systems zu klären, welche Schnittstellen vorhanden sind, welche für den Betrieb unter den gegebenen Anforderungen benötigt werden und welche gegebenenfalls deaktiviert werden können.

## 2. Gefährdungen

Im Folgenden wird die Gefährdungslage für TK-Applikationen und Mehrwertdienste genauer analysiert. Diese Systeme sind wie bereits erwähnt nicht nur Gefährdungen aus beiden Kommunikationswelten ausgeliefert, sondern über diese Systeme können auch Gefährdungen zwischen Tele- und Datenkommunikation überspringen. Zu beachten sind dabei insbesondere

- die erhöhte Gesamtwirkung einer Gefährdung durch die serverseitige Integration verschiedener IT- und TK-Systeme und
- die erhöhte Gesamtwirkung einer Gefährdung durch Nutzung gemeinsamer Endgeräte mit anderen Anwendungsformen, vor allem zur Datenverarbeitung.

Aufgrund der Komplexität von UC-Systemen können Gefährdungen bereits durch organisatorische Fehler bzw. durch fehlende Richtlinien zum Gebrauch und Betrieb eines UC-Systems entstehen. Hierbei bilden Verletzungen des Urheberschutzes noch das vermeintlich kleinste Risiko. Die Verwendung von Ansagen, Wartemusik oder Ruftönen, die nicht frei von Rechten bzw. nicht lizenziert sind, ist jedoch in vielen Unternehmen gang und gäbe, da diese Vergehen allgemein als Kavaliersdelikt betrachtet werden.

Abgesehen von solchen spezifischen Auswirkungen fehlender Vorgaben zum Gebrauch eines UC-Systems, können organisatorische Mängel ganz allgemein zu Gefährdungen führen. Im Folgenden werden einige dieser Mängel und mögliche Konsequenzen beschrieben (siehe [1] für eine umfassende Darstellung der Gefährdungslage in der modernen Telekommunikation).

**Organisatorische Mängel, unzureichende Konzepte, Regelungen und Prozesse**
Für den Betrieb einer TK-Applikation müssen häufig neben den TK-spezifischen Schnittstellen auch andere Schnittstellen z. B. zu Datenbanksystemen berücksichtigt werden. Der Betrieb der TK-Anlage, der IP-Infrastruktur und der Server für solche Anwendungen kann von unterschiedlichen Gruppen durchgeführt werden. Eine fehlende oder unzureichende Abstimmung der beteiligten Gruppen kann beispielsweise dazu führen, dass sich über eine CTI-Anwendung eine Gefährdung auf die TK-Anlage bzw. allgemein auf Telekommunikationsdienste fortpflanzt. Als besonders kritisch sind in allen Integrationsszenarien Versionswechsel eines Teilsystems zu bewerten. Hier kann unter ungünstigen Bedingungen die Verfügbarkeit des Gesamtsystems bedroht sein.

Konzepte, Regelungen und Prozesse, die eine TK-Anlage betreffen, müssen für die Integration mit TK-Applikationen entsprechend erweitert werden. Eine Gefährdung besteht darin, dass sich diese Erweiterung als unzureichend erweist. Kritisch sind dabei diejenigen Elemente, die einen übergreifenden Bezug zu TK-Anlage und TK-Applikation haben, z. B. die Änderung des Rufnummernplans.

Dieser Grundsatz gilt auch für die Konfigurationen und Sicherheitseinstellungen der Teilsysteme. Technologie- und produktbedingt werden für den TK- und den Applikationsbereich unterschiedliche Einstellungen vorgenommen, die geeignet abzustimmen sind, damit ein einheitliches Sicherheitsniveau gewährleistet ist. Dies beinhaltet sowohl die Einstellungen für einfache Nutzer als auch die Parameter für den administrativen Zugang. Werden diese Einstellungen nicht geeignet abgestimmt, kann es vorkommen, dass in einem Bereich (z. B. auf Seite der Applikation) ein zu geringes Sicherheitsniveau besteht.

Selbstverständlich schließt keine organisatorische Regelung und kein Konzept Gefährdungen durch technisches Versagen, Unachtsamkeit oder vorsätzliche Handlungen aus.

**Technisches Versagen und vorsätzliche Handlungen**
Aufgrund der Vielzahl der unter dem Begriff Unified Communications zusammengefassten TK-Applikationen kann hier keine umfassende Auflistung aller denkbaren konkreten Gefährdungen erfolgen. Es kann aber festgestellt werden, dass die Gefährdungslage sich auf die IP-basierten Komponenten eines Gesamtsystems konzentriert, da sich hier die größte Angriffsfläche bietet und auf eine Vielzahl bereits bekannter Angriffsmethoden zurückgegriffen werden kann. Dennoch kann nicht ausgeschlossen werden, dass Angriffe auch über andere Kommunikationswege, wie z. B. Fax oder SMS, erfolgen, wenn das Gesamtsystem diese Möglichkeiten bietet. Viele TK-Applikationen arbeiten mit personenbezogenen Daten und reichen diese unter Umständen an andere Anwendungen weiter. Durch die unterschiedlichen Schnittstellen zwischen den Systemen wird eine ausreichende Absicherung erschwert und die Auswirkungen eines Vertraulichkeitsverlustes aufgrund der zentralen Sammlung unterschiedlicher Nachrichtentypen können gravierend sein.

Folgende beispielhafte Szenarien verdeutlichen das Gefährdungspotenzial:

- Ein UM-System kann aufgrund einer absichtlich herbeigeführten Überlastung durch eingehende Sprachnachrichten nicht mehr in der Lage sein, Faxsendungen, E-Mails oder SMS-Nachrichten zu versenden und zu empfangen. Dies kann z.B. Auswirkungen auf einen Alarmserver haben, wenn dieser nicht mehr in der Lage ist, Benachrichtigungen zu versenden.
- Durch die unbefugte oder missbräuchliche Nutzung eines UM-Systems zum Versenden von Fax- und SMS-Nachrichten können nicht unerhebliche finanzielle Schäden entstehen.
- Eine weitere Bedrohung besteht im Vortäuschen einer scheinbar vertrauenswürdigen Identität. Dies ist besonders im Zusammenhang mit UM-Systemen problematisch, da die unbefugte Nutzung einen Angriff über viele Kanäle, z. B. E-Mail, Fax, SMS, erlaubt. Ein konkretes Beispiel für einen entsprechenden Angriff auf CTI-Nutzer wird in einem der folgenden Abschnitte beschrieben.
- Die unbefugte Nutzung eines Telefons oder einer TK-Applikation mit Türöffnungsfunktion kann unberechtigten Personen den Zutritt zu einem Gebäude verschaffen. Dabei muss sich der Einlass gewährende Nutzer unter bestimmten Bedingungen noch nicht einmal im betreffenden Gebäude aufhalten.

Neben solchen applikationsspezifischen Bedrohungen müssen auch Gefährdun-

gen berücksichtigt werden, die sich auf die einem System zugrundeliegenden Betriebssysteme, Verzeichnisdienste, Clients etc. beziehen, da sie selbstverständlich ebenfalls Auswirkungen auf TK-nahe Systeme haben können. Für jedes spezifische System müssen die relevanten Gefährdungen daher gesondert berücksichtigt werden.

### 3. Maßnahmen

Im Folgenden wird eine Auswahl an Sicherheitsmaßnahmen aufgeführt, die illustrieren, wie den oben aufgeführten Gefährdungen begegnet werden kann (siehe [1] für eine umfassende und detaillierte Beschreibung). Die Maßnahmen lassen sich grob in folgende Bereiche unterteilen:

- Endgeräte
- Server und Anwendungen
- Netzwerk
- Netz- und Systemmanagement
- übergreifende Aspekte

Allgemein gelten zusätzlich auch alle Sicherheitsmaßnahmen, die für die zugrundeliegende TK-Anlage (insbesondere für VoIP-Systeme) und für die Plattformen (Server Hardware und Betriebssystem) der TK-Applikation getroffen werden. Hierzu gehören unter anderem eine Produktauswahl unter Sicherheitsgesichtspunkten, physikalische Sicherung, gesicherte Administration, Härtung der Systeme und im Falle von VoIP insbesondere die Ende-zu-Ende-Verschlüsselung von Signalisierung und Medienstrom, die selbstverständlich auch im Kontext von TK-Applikationen und Mehrwertdiensten sinnvoll anwendbar sind.

### 3.1 Endgeräte

**Absicherung von TK-Applikationen auf Ebene der Endgeräte**

Viele TK-Applikationen und Mehrwertdienste basieren darauf, dass sie Dienste, die typischerweise über einen PC oder über eine spezielle Hardware bedient werden, auch sprachgesteuert über das Telefon anbieten. Als Beispiel sei hier der Zugriff auf das E-Mail-Postfach per Telefon genannt. Viele Systeme bieten hier die Möglichkeit sich E-Mails per Sprachsynthese vorlesen zu lassen. Umgekehrt lassen sich viele Dienste, die üblicherweise über das Telefon bzw. die TK-Anlage genutzt werden, auch per PC zugreifen. Anrufjournale und die Web-basierte Konfiguration von Telefonen sind Beispiele für solche Dienste. Eine dritte Kategorie wiederum verwendet die Browser-Funktion moderner Telefone, um beliebige Dienste (z. B. Zeiterfassung, Lagerverwaltung etc.) bereitzustellen.

Die Tatsache, dass solche Dienste auf mehreren Wegen erreicht und gesteuert werden können, hat für die Benutzer praktische Vorteile, stellt jedoch auch eine Gefährdung eines TK- und IT-Systems dar. Ein Dienst kann nur so sicher sein wie der am schwächsten geschützte Zugang.

Bei einem entsprechenden Schutzbedarf muss daher jedes Endgerät geeignet gesichert sein, um eine unbefugte Nutzung von TK-Applikationen und Mehrwertdiensten zu vermeiden. Für PC-Applikationen gelten hier für den normalen Schutzbedarf die Empfehlungen der IT-Grundschutz-Kataloge. Der Zugang zu Telefonen und anderen Endgeräten mit eingeschränkten Eingabemöglichkeiten und Rechenleistungen sollte zumindest über einen mehrstelligen Zahlencode abgesichert sein. Ein auf diese Weise gesichertes Endgerät sollte nach mehrfacher Falscheingabe des Codes ohne administrativen Eingriff nicht mehr zu verwenden sein. Sicherere Authentisierungsmechanismen wie Smartcards sind zu bevorzugen.

**Schulung der Nutzer**

Die Bedienung von TK-Applikationen und Mehrwertdiensten ist in den vergangenen Jahren bedeutend einfacher geworden. Andererseits ist die Zahl der in der Praxis eingesetzten Applikationen und Dienste erheblich gewachsen. Diese Situation kann dazu führen, dass Benutzer überfordert sind, Dienste nicht ihrer Bestimmung entsprechend nutzen oder fehlbedienen und sich möglicher Sicherheitsrisiken nicht bewusst sind. Hierdurch können die Vertraulichkeit und möglicherweise auch die Verfügbarkeit gefährdet sein.

Es ist daher erforderlich, die Nutzer von TK-Applikationen und Mehrwertdiensten zum richtigen Umgang mit den jeweiligen Diensten zu schulen und Hinweise auf mögliche Sicherheitsrisiken zu geben.

### 3.2 Server und Anwendungen

**Absicherung der E-Mail-Kommunikation einer TK-Applikation**

Der Austausch von E-Mails zwischen TK-Applikation und E-Mail-Clients oder anderen Diensten unterliegt den gängigen Gefährdungen der E-Mail-Kommunikation. Im Bereich der TK-Applikationen sind vor allem Unified Messaging Server betroffen. Abhängig davon, ob es sich um ein True Unified Messaging (TUM) System mit vereinheitlichtem Posteingang auf dem E-Mail-Server handelt oder nicht, sind unterschiedliche Schnittstellen zu schützen:

Im Falle von TUM ist die Verbindung zwischen E-Mail- und UM-Server zu schützen, welche zum Nachrichtenaustausch benötigt wird und in der Regel auf SMTP oder MAPI-RPC basiert. Bei einer direkten Verbindung der beiden Systeme (z. B. über ein einzelnes Netzwerkkabel) ist diese Verbindung meist nicht schutzbedürftig. Anders stellt sich die Situation bei räumlicher Entfernung, eventuell sogar über die Grenzen des Standortnetzwerks hinaus, oder erhöhtem Schutzbedarf dar. Bei der Kommunikation per SMTP kann auf SSL bzw. TLS zur Authentisierung und Verschlüsselung zurückgegriffen werden. Bei MAPI-RPC muss man sich auf proprietäre Mechanismen zur Absicherung verlassen.

Im Falle, dass UM-Server und E-Mail-Server dem Anwender separate Postfächer zur Verfügung stellen, muss der E-Mail-Client Verbindungen zu beiden Servern aufbauen. Wie die Verbindung zwischen Client und E-Mail-Server wird auch für die Verbindung von Client und UM-Server auf gängige Mailprotokolle zurückgegriffen. Das sind in der Hauptsache POP3 und SMTP sowie IMAP. Diese Protokolle sehen ursprünglich nur eine Übertragung der Authentisierungsdaten im Klartext vor. Im Falle von POP3 wurde nachträglich die Authentisierung mittels eines Hash-Verfahren spezifiziert, welches aber praktisch keine Relevanz hat. Effektiver ist die Absicherung der kompletten Datenübertragung mittels SSL bzw. TLS. Dieses Verfahren ist für alle drei Protokolle spezifiziert.

Die Absicherung von E-Mail-Kommunikation ist bereits in den IT-Grundschutz-Katalogen des BSI umfassend beschrieben. Diese Maßnahmen sind nicht nur auf UM-Systeme sondern auch auf andere TK-Applikationen mit E-Mail-Schnittstelle anzuwenden.

**Absicherung des Sprachkanals zwischen TK-Anlage und TK-Applikation**
Sprachverbindungen sind bei TK-Applikationen, sei es im Rahmen von Unified Messaging, IVR oder Alarmservern, naturgemäß von großer Bedeutung. Sowohl die Sprach- als auch die Signalisierungsdaten können sensible Inhalte haben und dementsprechend schützenswert sein.

Für die genutzten Übertragungswege muss geprüft werden, ob zusätzliche Schutzmaßnamen ergriffen werden müssen. Besteht ein erhöhter Schutzbedarf oder sind Strecken über unsichere Netze zu überbrücken, ist ein Schutz der Verbindungen notwendig. Unabhängig von der zugrundeliegenden Technik sollten in diesem Fall – sofern technisch möglich - folgende Maßnahmen ergriffen werden:

- Ende-zu-Ende-Verschlüsselung des Medienstroms
- Verschlüsselung der Signalisierung
- Authentisierung zwischen Endgeräten und Servern des VoIP-Systems
- Authentisierung zwischen Servern

Bei analoger oder digitaler Telefonie kann bei entsprechendem Schutzbedarf auf den Einsatz von Kryptoboxen zurückgegriffen werden.

Im Kontext IP-basierter Sprachübertragung können die genannten Maßnahmen wie folgt umgesetzt werden:

- Bei IP-basierter Sprachübertragung steht SRTP als verschlüsselte Variante des Real Time Protocol (RTP) zur Übertragung von Sprachdaten zur Verfügung. Alternativ können VPN-Techniken unter Verwendung von IPsec oder SSL genutzt werden.

- Zur Sicherung der Signalisierung per SIP kann auf TLS zurückgegriffen werden. In Ergänzung hierzu kann eine Verschlüsselung der SIP-Pakete nach S/MIME erfolgen, einem Verfahren das aber in der Praxis selten zur Anwendung kommt.

- Für H.323 gilt in Bezug auf Sicherheit der Standard H.235.

Die Endpunkte der Verschlüsselung bei Verwendung von SRTP sind in Abbildung 5 dargestellt.

**Absicherung von CTI-Verbindungen**
Bei Computer Telephony Integration (CTI) wird zwischen Einzelplatz- und Mehrplatzlösungen unterschieden. Während die direkte Verbindung zwischen Telefon und Rechner bei Einzelplatzlösungen in der Regel aufgrund der räumlichen Nähe und der proprietären, vom restlichen Netzwerk unabhängigen Anbindung keines zusätzlichen Schutzes bedarf, besteht bei Mehrplatzlösungen eine Verbindung zwischen jedem Endgerät und einem zentralen CTI-Server, der für die Steuerung der Endgeräte verantwortlich ist. Diese Verbindung wird oft auf Basis von CSTA realisiert. CSTA kann sowohl über ISDN als auch über TCP/IP-basierte Verbindungen transportiert werden. Je nach Anbindung des Endgerätes können verschiedene Verfahren Anwendung finden:

- Bei digitaler Anbindung können Kryptoboxen eingesetzt werden,

- IP-basiertes CSTA kann durch Verwendung von TLS oder IPsec gesichert werden

Neben CSTA finden im Bereich der CTI-Applikationen auch viele proprietäre Protokolle Verwendung, deren Umsetzungsdetails durch vom Hersteller an-

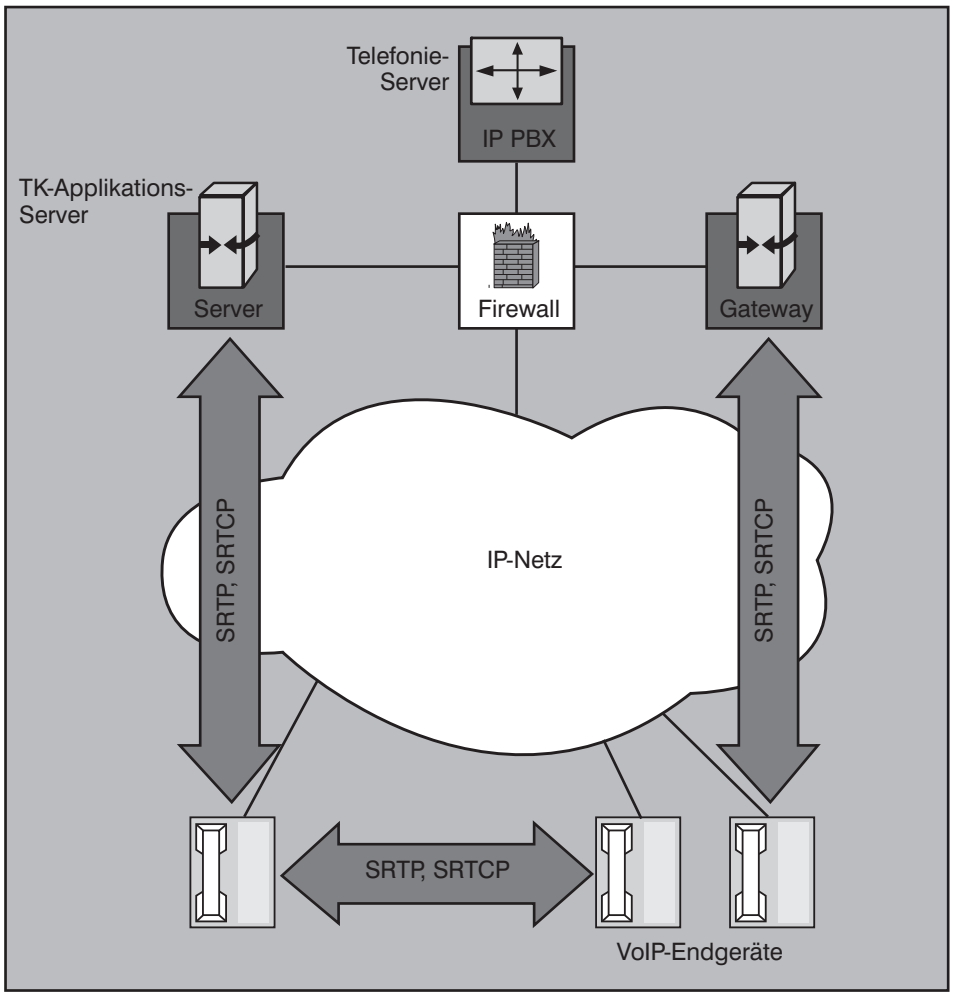



Abbildung 5: Endpunkte bei Verschlüsselung mit SRTP

gebotene Treiber für TAPI-, JTAPI- und TSAPI-Schnittstellen verborgen bleiben. Der Hersteller sollte in diesen Fällen zur grundsätzlichen Möglichkeit zur Authentisierung und Verschlüsselung sowie über die konkrete Konfiguration einer sicheren Verbindung befragt werden. Im Zweifel kann auch hier die Möglichkeit in Betracht gezogen werden, den gesamten Datenverkehrs zwischen Telefon und TK-Infrastruktur über ein geeignet gesichertes VPN zu tunneln.

**Absicherung der Kommunikation zwischen TK-Applikation und IT-System**
Die Kommunikation zwischen TK-Applikationen und IT-Systemen (d. h. Geschäftsanwendungen bzw. Verwaltungsverfahren) findet auf Basis von unterschiedlichsten Protokollen statt. Neben proprietären Schnittstellen und einer Vielzahl von Protokollen für Remote Procedure Calls (RPCs) kommen auch Standardprotokolle wie etwa HTTP zum Einsatz. Mit der zunehmenden Verbreitung von serviceorientierten Architekturen (SOA) und Web Services halten weitere Protokolle Einzug in die IT-Systeme (siehe [2]). Als Beispiele seien hier die XML-basierten Mechanismen zum Prozedur-Fernaufruf SOAP sowie XML Remote Procedure Call (XML-RPC) genannt. Darüber hinaus bieten weit verbreitete, herstellerabhängige Programmierschnittstellen wie Microsofts Component Object Model (COM, bzw. Distributed COM, DCOM) mit ihren intern verwendeten RPC-Protokollen weitere Angriffsflächen. Hier muss im Einzelnen geprüft werden, wie in der konkreten Implementierung mit den für die Protokolle spezifizierten Sicherheitsmechanismen umgegangen worden ist.

Eine pauschale Antwort, wie die Kommunikation zwischen TK- und Business-Applikationen abzusichern ist, kann also nicht gegeben werden. Erste Maßnahme sollte es daher sein, die verwendeten Protokolle durch Nachfrage bei den Herstellern und durch eigene Analysen zu ermitteln und sie auf verfügbare Sicherheitsmechanismen zu prüfen. Da Sicherheitsmechanismen bei weitem nicht für alle Protokolle zur Verfügung stehen, ist bei erhöhtem Schutzbedarf ein Tunnel z. B. auf Basis von IPsec die einfachste und umfassendste Lösung. Bei erhöhtem Schutzbedarf sollte jedoch im Zweifel auch in Betracht gezogen werden, von einer Integration von TK- und IT-Anwendungen Abstand zu nehmen.

**Absicherung der Kommunikation zwischen TK-Applikation und Datenbank**
Oftmals ist der Zugriff von TK-Applikationen auf Datenbanken notwendig, sei es, um Abfragen und Manipulationen am Unternehmensverzeichnis durchzuführen (z. B. mittels Lightweight Directory Access Protocol, LDAP) oder um Datenbestände wie Kundendaten oder die Lagerhaltung in die TK-Applikation einzubeziehen. Wichtig ist die umsichtige Vergabe von Zugriffsrechten auf Datenbanken und Verzeichnissen. Der TK-Applikation sollten nur solche Zugriffsrechte erteilt werden, wie sie für eine sinnvolle Nutzung notwendig sind. Darüber hinaus sollte der entstehende Datenverkehr bei einem erhöhten Schutzbedarf durch Verschlüsselung gesichert werden.

LDAP sieht zunächst keinerlei Verschlüsselungsmechanismen vor und überträgt sogar Authentisierungsdaten im Klartext. Die Verwendung von IPsec oder TLS zur Verschlüsselung der gesamten Kommunikation ist allerdings im aktuellen Standard LDAPv3 spezifiziert. Der Einsatz einer dieser Methoden ist in jedem Fall beim Einsatz von LDAP anzuraten.

Datenbankzugriffe unterliegen ähnlichen Gefährdungen wie Verzeichniszugriffe mittels LDAP. Die Kommunikation zwischen z. B. einem ODBC-Treiber und der Datenbank über ein Netzwerk findet oft anhand proprietärer Protokolle oder im Klartext statt. Bei erhöhtem Schutzbedarf sollte die Verbindung mittels IPsec oder TLS absichert werden.

Personenbezogene Daten und allgemein Daten mit erhöhtem Schutzbedarf sollten in der Datenbank verschlüsselt gespeichert werden.

**Absicherung der Kommunikation eines Präsenzsystems**
Präsenzinformationen sind, auch wenn Privatanwender oft sorglos mit ihnen umgehen, gerade im Geschäftsumfeld sensible Informationen. Neben der Verfügbarkeit eines Anwenders geben sie eventuell Informationen über aktuellen Aufenthaltsort und Betätigung preis. Daher ist es unumgänglich, auch Präsenz- und Instant Messaging-Systeme durch Verschlüsselung und Authentisierung zu sichern. Ein probates Mittel ist hier der Einsatz von TLS zwischen Client und Präsenzserver. Dieses Verfahren wird zumindest auch von den beiden wichtigsten Protokollstandards für diesen Zweck XMPP und SIP/SIMPLE vorgesehen.

**Einschränkung der Sichtbarkeit von Präsenzinformationen**
Auch wenn der unbefugte Zugriff durch Außenstehende auf Präsenzinformationen mithilfe von Verschlüsselung und Authentisierung unterbunden wird, ist innerhalb des authentisierten Nutzerstamms eine Einschränkung der grundlegenden Sichtbarkeit von Präsenzinformationen notwendig. Die Präsenzinformation eines Nutzers sollte daher vor Zugriff durch andere Nutzer des Präsenzsystems geschützt bleiben, sofern nicht eine individuelle Freigabe der Information erfolgt ist. (Nutzer, die eine solche individuelle Freigabe erhalten haben, werden üblicherweise „Buddy“, engl.: Kumpel, genannt.) Um dies zu ermöglichen, muss das verwendete Präsenzsystem über einen Mechanismus verfügen, der es zumindest den Administratoren oder besser noch den Nutzern erlaubt, die Sichtbarkeit von Präsenzinformationen einzuschränken.

Auch aus Datenschutzgründen muss es dem Benutzer möglich sein, die Sichtbarkeit der eigenen Präsenzinformationen nach außen steuern zu können.

**Differenzierung der Zugriffsrechte auf Präsenzinformationen**
Auch wenn ein Nutzer den Personenkreis, der grundsätzlich Zugriff auf die eigene Präsenzinformation besitzt, definieren kann, ist eine weitere Differenzierung der bereitgestellten Informationen notwendig. So ist es für bestimmte Personen, wie zum Beispiel Teamleiter, hilfreich, die Verfügbarkeit, die private Telefonnummer oder auch den Aufenthaltsort der Mitarbeiter einsehen zu können. Jedoch sollten nicht alle Nutzer des Präsenzsystems auf solch detaillierte Informationen zugreifen können. Um eine differenzierte Freigabe von Informationen zu ermöglichen, muss das verwendete Präsenzsystem über eine Rechtehierarchie verfügen, die es zumindest den Administratoren oder besser noch den Nutzern erlaubt, die Sichtbarkeit von Präsenzinformationen pro Benutzer oder Benutzergruppe einzuschränken. Auch aus Datenschutzgründen muss es dem Benutzer möglich sein, die Sichtbarkeit der eigenen Präsenzinformationen nach außen steuern zu können.

Eine konkrete Umsetzung zeigt Abbildung 6 am Beispiel des Clients des Microsoft Office Communications Server 2007.

**Absicherung des telefonischen Zugriffs auf TK-Applikationen durch eine PIN**
Falls aus technischen Gründen keine Authentisierung auf Basis von Zertifikaten oder Nutzerdaten realisierbar ist, muss jede sensible TK-Applikation zumindest durch eine PIN geschützt werden. Zu diesen Applikationen zählen zum Beispiel Uni-

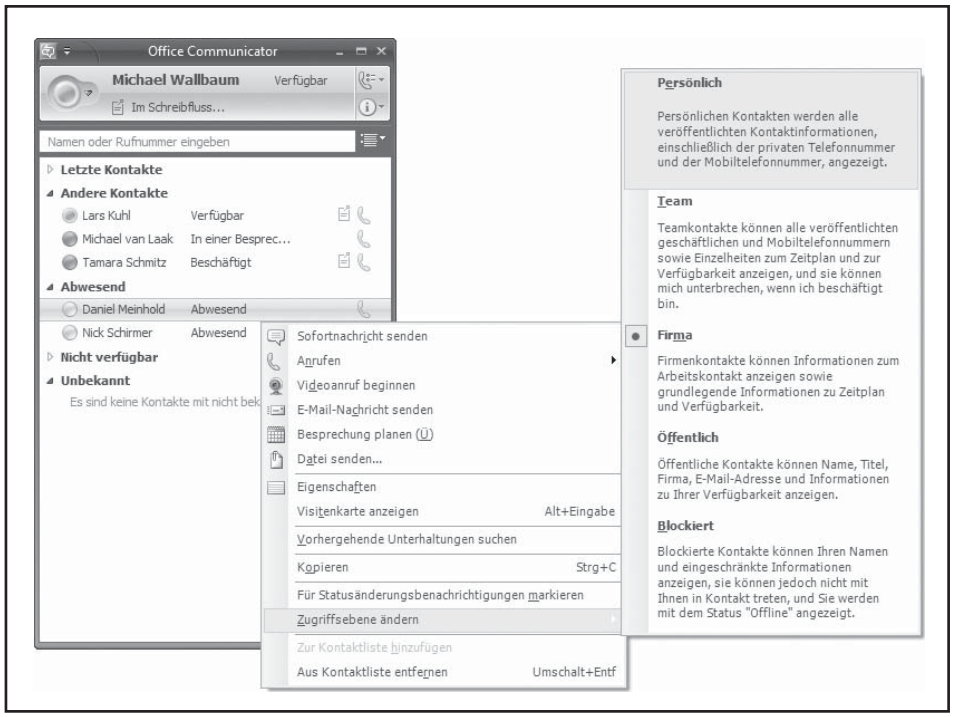



Abbildung 6: Zuweisung der Zugriffsebene eines Kontakts am Beispiel des Microsoft Office Communicators

fied Messaging Server mit telefonischem Zugriff auf den Posteingang, IVR-Applikationen mit Zugriff auf schützenswerte Daten oder Audiokonferenzsysteme.

Da eine PIN im Gegensatz zu Passwörtern nur aus Zahlen, und nicht aus alphanumerischen Zeichen besteht, ist es nicht möglich, den Grad der Komplexität durch das Hinzufügen von Buchstaben und Sonderzeichen zu erhöhen. Einzige Möglichkeit ist der Einsatz einer längeren PIN. Als absolutes Minimum gelten 4-stellige PIN, eine Länge von 6 oder mehr Stellen ist aber dringend empfehlenswert. (siehe IT-Grundschutz-Kataloge des BSI, M2.11 „Regelungen des Passwortgebrauchs“). Des Weiteren sind triviale PIN wie z. B. ‚0000’, ‚4321’ oder simple „Muster“ auf dem numerischen Tastaturblock zu vermeiden.

Um die fehlende Komplexität gegenüber alphanumerischen Passwörtern auszugleichen, ist es sinnvoll, bei wiederholter falscher Eingabe der PIN den Zugriff auf die TK-Applikation, zumindest temporär, zu sperren.

Es ist keine Selbstverständlichkeit, dass PINs oder Passworte verschlüsselt über ein Netzwerk übertragen werden. Ein Beispiel hierzu liefert Kapitel 4. In diesem Fall wäre also zumindest die Übertragung im Netzwerk entsprechend abzusichern.

**Einschränkung der Zugriffsrechte**
TK-Applikationen und Mehrwertdienste verbinden in vielen Fällen unterschiedliche Anwendungsdomänen wie z. B. Telefoniedienste mit Kundendatenbanken oder betriebswirtschaftlicher Software. Als konkretes Beispiel sei die Kopplung einer Telefonanlage mit einem Customer Relationship Management (CRM) System über einen CTI-Server genannt. Diese Brückenfunktion kann das Sicherheitsniveau der TK-Lösung, der TK-Applikation sowie darüber hinausgehend auch anderer IT-Systeme beeinträchtigen.

Abhängig vom geforderten Schutzbedarf sind daher die Zugriffsrechte der beteiligten Dienst- und Nutzerkonten geeignet einzuschränken, um einen unerlaubten bzw. unvorhergesehenen Durchgriff auf Informationen zu vermeiden. Die spezifischen Maßnahmen hängen dabei vom betrachteten Dienst bzw. auch vom Produkt ab. Folgende Aspekte sind bei erhöhtem Schutzbedarf zu beachten:

- Wenn Zugriffsrechte auf Basis von Benutzerkonten definiert werden, so ist die Verwendung eines zentralen oder zumindest synchronisierten Benutzerverzeichnisses einer getrennten Rechteverwaltung für unterschiedliche Anwendungsdomänen vorzuziehen. Auf diese Weise kann eine unkoordinierte bzw. unkontrollierte Rechtevergabe vermieden werden.

- Benötigen die betrachteten TK-Applikationen und Mehrwertdienste spezielle Dienstkonten, so sind deren Zugriffsrechte soweit einzuschränken, dass ausschließlich die für die Ausführung des Dienstes notwendigen Rechte zur Verfügung stehen. Auf diese Weise kann der Schaden, der durch eine unberechtigte Nutzung eines Dienstkontos (z. B. durch Schadsoftware) entstehen kann, minimiert werden.

### 3.3 Netzwerk

**Netztrennung zwischen TK-Applikationen und IT-Systemen**
Die Server für TK-Applikationen sollten in von anderen IT-Systemen getrennten IP-Subnetzen liegen. Der Zugang zu diesen Subnetzen sollte - sofern technisch möglich - durch ACLs kontrolliert werden. Für den erhöhten Schutzbedarf sollte eine Firewall zur Trennung der TK-Applikationen eingesetzt werden. Je nach geforderter Verfügbarkeit muss die Firewall redundant ausgelegt werden. Weiterhin muss die geforderte Leistung bei der Dimensionierung des Systems berücksichtigt werden. In Abhängigkeit von der Gefährdungslage ist der zusätzliche Einsatz eines IPS zu empfehlen. Das IPS kann dabei eine Komponente der Firewall oder eine separate Appliance sein.

TK-Applikationen stellen sowohl eine Verbindung zur TK-Anlage als auch zu IT-Systemen her. Bei einer IP-basierten Anbindung zwischen TK-Anlage und TK-Applikationen ist es daher sinnvoll, wie in Abbildung 7 exemplarisch für ein VoIP-System gezeigt, die Server für die TK-Applikationen in eine DMZ der Firewall, die TK-Systeme und IT-Systeme trennt, zu positionieren.

Da manche Protokolle (z. B. DCOM) dynamisch die für die Kommunikation verwendeten TCP- bzw. UDP-Ports aushandeln, kann eine ACL aber auch eine Firewall basierend auf einem einfachen dynamischen Paketfilter diese Protokolle nicht filtern und es müssten große Port-Bereiche permanent freigeschaltet werden. In diesem Fall muss eine Firewall mit entsprechender Applikationsintelligenz eingesetzt werden, die in der Lage ist, die entsprechenden Anwendungsprotokolle zu analysieren und Ports dynamisch freizuschalten und bei Beendigung der Kommunikation wieder zu schließen.

### 3.4 Netz- und Systemmanagement

**Sichere Administration der Server für TK-Applikationen und Mehrwertdienste**
Die Administration von Servern für TK-Applikationen und Mehrwertdienste muss durch Sicherheitsmechanismen angemessen geschützt werden. Hierzu sind allgemein folgende Maßnahmen umzusetzen:

- Härtung von Servern des Telekommunikationssystems
- Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems
- Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems
- Physikalische Sicherheit der Server
- Mehrstufiges Backup-Konzept

Für die sichere Administration von Anwendungs- und Management-Servern sind zusätzlich die folgenden Maßnahmen angemessen umzusetzen:

- Software-Sicherheit inkl. Patch-Management
- Sichere Konfiguration des Netzwerkmanagement-Protokolls

Bei Applikations-Servern mit VoIP-Mehrwertdiensten gilt meistens „Sicherheit vor Verfügbarkeit“. Beispiel: Eine vorübergehend nicht verfügbare Voice-Mail-Funktionalität ist oft besser als ein nicht sicherer (kompromittierbarer) Voice-Mail-Dienst. Anwendungs- und Management-Server müssen demnach vor schadenstiftender Software geschützt werden. Dies gilt insbesondere bei Verwendung von Standard-Betriebssystemen.

**Schulung der Administratoren**
TK-Systeme und integrierte Applikationen und Mehrwertdienste können nicht isoliert betrachtet werden. Änderungen an einem Teilsystem (z. B. die Einrichtung einer Fernwartungsmöglichkeit) können sicherheitsrelevante Auswirkungen auf andere Teilsysteme haben. Es ist daher erforderlich, die Administratoren der jeweiligen TK-Applikationen und Mehrwertdienste zu den Wechselwirkungen mit dem Gesamtsystem zu schulen und auf mögliche Sicherheitsrisiken hinzuweisen.

**Absicherung der Management-Schnittstellen einer TK-Applikation**
Um die Management-Schnittstelle von TK-Applikationen vor Manipulation und Ausspähen zu schützen, müssen eine Reihe von Maßnahmen ergriffen werden. Oftmals wird die administrative Bedienoberfläche einer Appliance als Web-Interface realisiert. Da unverschlüsselte HTTP-Verbindungen keinerlei Schutz bieten, ist hier unbedingt auf HTTPS zurückzugreifen. HTTPS bietet Verschlüsselung der übertragenen Daten und Authentifizierung nach dem SSL/TLS-Standard. Nicht geeignet gesicherte Administrationsschnittstellen sind unbedingt zu deaktivieren.

Eine zweite wichtige Administrationsschnittstelle ist das Simple Network Management Protocol (SNMP), welches die Fernwartung von Netzinfrastruktur und Serverapplikationen ermöglicht. SNMP liegt derzeit in drei verschiedenen Versionen vor, wobei die beiden älteren SNMP-Versionen keine starke Authentisierung und Verschlüsselung unterstützen. In der dritten Version des SNMP Protokolls wurden diese Schwächen beseitigt und ein ausreichender Schutz zur Wahrung der Vertraulichkeit und Integrität implementiert. Aus diesem Grund sollte, sofern es technisch möglich ist, die Version SNMPv3, die Sicherungsmechanismen zur Authentisierung und Verschlüsselung unterstützt, benutzt werden.

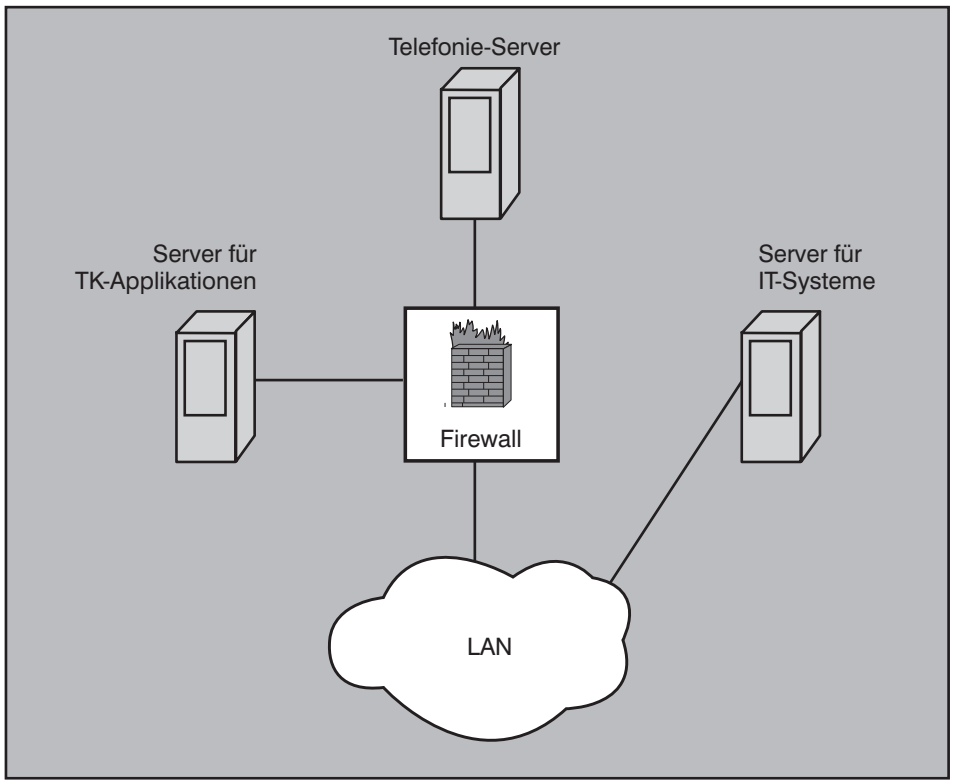



Abbildung 7: Trennung zwischen TK-Applikationen und IT-Systemen durch eine Firewall

### 3.5 Übergreifende Aspekte

**Koordination der Planung und Administration von TK-Anlage und TK-Applikation**
Um die möglichen Sicherheitsrisiken eines integrierten IT- und TK-Systems zu erkennen, ist eine Übersicht über das Gesamtsystem erforderlich. Die Risiken können nicht allein aufgrund der isolierten Betrachtung von Teilsystemen abgeschätzt werden; sie sind sozusagen mehr bzw. größer als die Summe der Einzelrisiken.

Vor diesem Hintergrund ist es erforderlich, sowohl die Planung als auch den Betrieb der Teilsysteme zu koordinieren. Die an diesen Prozessen beteiligten Personen und Organisationseinheiten müssen mittels geeigneter Maßnahmen über alle sicherheitsrelevanten Vorgänge informiert werden. Hierzu sind u.a. Vorgänge der folgenden Art zu zählen:

- Aufspielen von Patches bzw., Updates auf ein Teilsystem
- Einführung neuer Benutzergruppen
- Änderungen der Rechte von Benutzergruppen
- Änderungen der Zusammensetzung von Benutzergruppen
- Aktivierung neuer Funktionen der TK-Anlage und TK-Applikationen
- Konfigurationsänderungen, die über eine einfache Benutzerverwaltung hinausgehen

## 4. CTI-Sicherheit auf dem Prüfstand

Um die Angriffsmöglichkeiten auf ein ungeschütztes UC-System zu illustrieren, wird im Folgenden anhand einer konkreten Hersteller-Lösung gezeigt, wie ein CTI-Benutzer kompromittiert werden kann. Betrachtet wird die Telefonsteuerung über ein Mehrplatzsystem. Hierzu wird ein CTI-Server benötigt, der als Vermittler zwischen TK-Anlage, dem eigentlichen Benutzerarbeitsplatz und ggf. weiteren IT-Servern, mit Verzeichnis- oder CRM-Diensten dient.

Der Versuchsaufbau umfasst eine Siemens HiPath8000 als IP-PBX, den Siemens Hi-

Path CAP Server als CTI-Server bzw. Middleware, ein Siemens OptiPoint IP-Telefon mit CTI-Freigabe und einen Arbeitsplatz, der über einen Siemens TAPI-Treiber CTI-Funktionalität, d.h. insbesondere die Möglichkeit zur Steuerung des IP-Telefons, anbietet. In diesem Szenario besitzt der Angreifer Netzwerkzugang und hat die Möglichkeit, die CTI-Kommunikation, zwischen Arbeitsplatz und CTI-Server, mitzuhören. Dies kann im Vorfeld des eigentlichen Angriffs durch Switch Port Mirroring, ARP Poisioning, MAC Flooding oder sonstige Attacken zur Beeinflussung der Netzwerkkommunikation erfolgt sein, die hier nicht betrachtet werden. Der Versuchsaufbau ist in Abbildung 8 dargestellt.

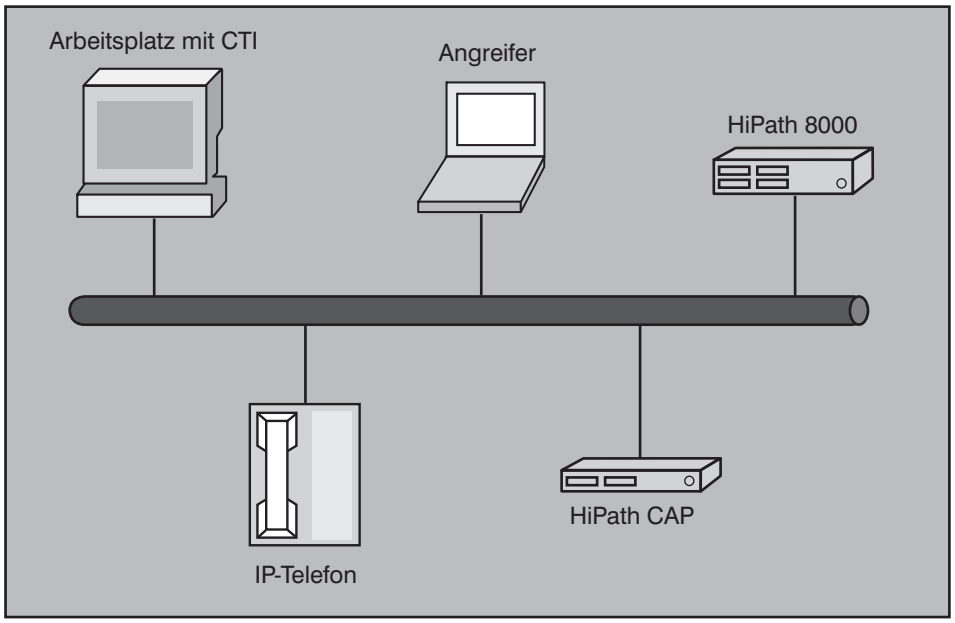



Abbildung 8: Versuchsaufbau

### 4.1 CTI-Verbindungsaufbau

Ein Anruf, der via CTI-Steuerung eingeleitet wird, durchläuft eine Reihe von Schritten, die die Beteiligung aller Komponenten des Versuchsaufbaus erfordert – den Angreifer mal ausgenommen. Zu Beginn meldet sich der Benutzer am CTI-Server an. Wählt der Benutzer im Folgenden einen Gesprächsteilnehmer aus, so wird der Vermittlungswunsch an den CTI-Server übermittelt. Im Anschluss übermittelt dieser der HiPath 8000 die Gesprächsdaten und initiiert damit den Verbindungsaufbau. Die HiPath 8000 leitet den Verbindungswunsch an das Telefon des Benutzers und baut eine Verbindung zum Gesprächspartner auf. Wird der Telefonhörer aufgelegt, signalisiert das Telefon der HiPath 8000 das Gesprächsende. Abbildung 9 zeigt diesen vereinfachten Verbindungsaufbau.

Ein Mitschnitt des Netzwerkverkehrs zwischen der Arbeitsstation und dem CTI-Server ermöglicht einen detaillierten Blick auf die ausgetauschten Informationen, die in diesem Szenario auch dem Angreifer zur Verfügung stehen, da er Zugriff auf das Kommunikationsnetzwerk besitzt. Die Analyse des Mitschnittes liefert den in Abbildung 10 skizzierten Verbindungsaufbau zwischen Arbeitsplatzrechner und HiPath CAP Server.

Für das angestrebte Ziel, d.h. die Kompromittierung eines CTI-Benutzers, werden im Folgenden nur die vom Arbeitsplatz gesendeten Pakete näher betrachtet, da diese ausreichen, um das Benutzertelefon unter die Kontrolle des Angreifers zu bringen.

Im ersten Schritt sendet der Arbeitsplatzrechner ein „Login-Paket“ an die HiPath CAP, welche mit einem „Login Reply“ antwortet. Das „Login-Paket“ enthält neben den Informationen über das verwendete Protokoll (NetTSPI in Version 2) auch den Benutzernamen und das zugehörige Passwort des Benutzers, sowie die verwendete Passwortkodierung, hier Base 64.

```
NetTSPI;version=2;login=49(2408)1436-192;passwd=MTIzNDU2;encoding=B64
```

Der Login entspricht hier der Telefonnummer des Benutzers und das Passwort muss für diesen Angriff eigentlich nicht im Klartext vorliegen. Eine Dekodierung stellt jedoch auch kein Hindernis dar, da der entscheidende Hinweis auf die Base64-Kodierung im Login-Paket freundlicherweise geliefert wird. Im Internet finden sich hinreichend viele Tools, um aus „MTIzNDU2“ das Passwort im Klartext „123456“ zu ermitteln.

Im zweiten Schritt werden die unterstützten Telefonie-Funktionen des Endgerätes abgefragt. In diesem Kontext ist es wichtig zu wissen, dass

- ein Benutzer über mehrere Endgeräte verfügen kann,

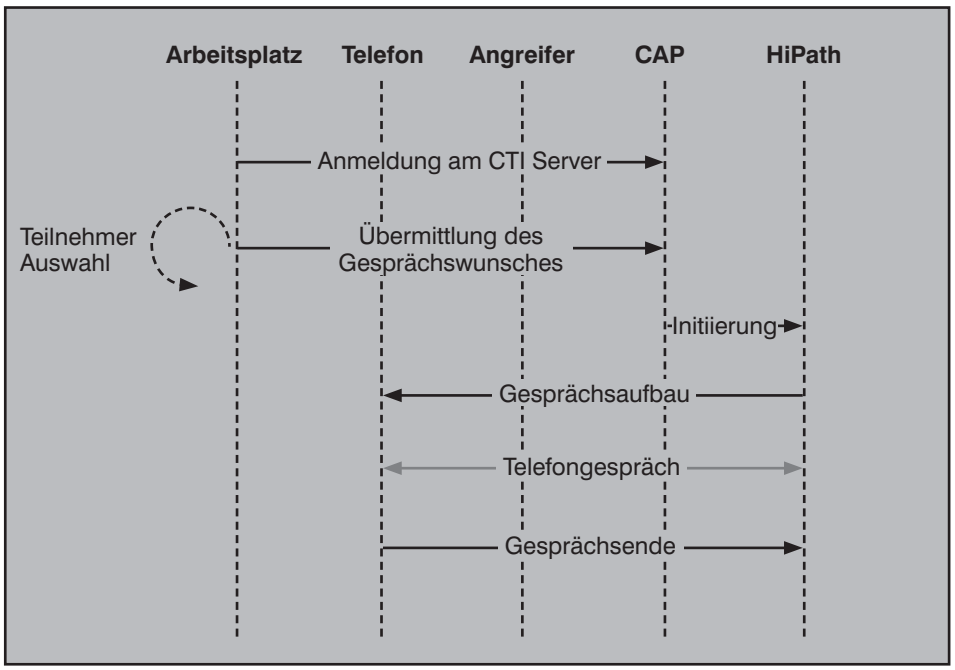



Abbildung 9: Vereinfachter Gesprächsaufbau

- jedes dieser Endgerät über mehrere Rufnummern besitzen kann,
- und das jeder Rufnummer verschiedene Funktionen, wie z.B. Rufübernahme, Konferenz, etc., zugeordnet werden können.

Aus diesem Grund muss sowohl die Rufnummern- als auch die Endgeräte-ID spe-

```
TSPI_lineGetAddressCaps 0 192
```

zifiziert werden.
Die Rufnummern-ID ist die 0 und das Endgerät wird mit der 192 adressiert.

Im dritten Schritt wird eine Leitung angefordert und dieser ein LineHandle zuge-

```
TSPI_lineOpen 5 5 9332056 15903128 131072 „49(2408)1436-192“
```

wiesen.
Das LineHandle ist hier 15903128. Die Bedeutung der anderen Parameter ist an dieser Stelle irrelevant.

Nun kann, im vierten Schritt, das eigentliche Telefongespräch eingeleitet werden. Dazu werden das zuvor definierte LineHandle und die Zielrufnummer angege-

```
TSPI_lineMakeCall 65672 15903128 9335352 1 „T0951192“ 0 1 0 0 4 8 1 0 0 0 0 0 „“
```

ben.
Das LineHandle 15903128, definiert in Schritt drei, muss wieder übereinstimmen. Die angegebene Zielrufnummer „T0951192“ kann beliebig abgeändert werden, wobei das Präfix „T“ bleibt und die nachfolgende Null die Amtsleitung belegt.

Die gesammelten Informationen ermöglichen dem Angreifer die Kontrolle über das Endgerät 192 zu erhalten. Neben den eigentlichen Paketdaten erlangt der Angreifer Kenntnis über die IP-Adresse und den verwendeten Port am HiPath CAP Server, (hier 26535) auf dem der CTI-Dienst Verbindungen entgegennimmt.

### 4.2 Angriff

Der einfachste Angriff besteht nun in der Reproduktion der vorher aufgezeichneten CTI-Pakete mit minimalen Änderungen, die sich nur auf die Zielrufnummer beziehen. Es genügt eine Telnet-Sitzung auf den Port 26535 zu starten und die Paketinhalte per Telnet an den CAP-Server zu senden.

Die in Abbildung 11 dargestellte Telnet-Verbindung zeigt die Interaktionen des Angreifers hellgrau eingerahmt. Es ist zu erkennen, dass nach dem Schritt 4, d.h. nach dem Aufruf von TSPI_lineMakeCall, ein Telefongespräch zustande gekommen ist. Demnach konnte der Angreifer das Benutzertelefon unter seine Kontrolle bringen.

Ohne zusätzliche Informationen über das verwendete Protokoll besteht für den Angreifer lediglich die Möglichkeit zur Initiierung eines Anrufs vom Benutzertelefon. Mit Insiderwissen oder Reverse Engineering sind weitergehende Möglichkeiten denkbar, die zu Identitätsdiebstahl, Gesprächsübernahme, Dreierkonferenz, Rufumleitung, Rufweiterleitung, etc. führen. Die einzige Bedingung ist, dass die (CTI-) Merkmale vom System für die Endgeräte und die jeweiligen Nutzer freigeschaltet sein müssen.

### 4.3 Schutzmaßnahmen

Der hier beschriebene Angriff auf den Siemens HiPath CAP Server in der Version 3.0 erfolgte auf ein System mit Default-Sicherheitseinstellungen. Das Resultat bestätigt eindeutig, dass diese ungenügend sind und dementsprechend angepasst werden müssen. In den Konfigurationseinstellungen im HiPath CAP Management besteht die Möglichkeit zwischen den folgenden Sicherheitsstufen auszuwählen:

- Stufe 0 (Default-Einstellung)
  keine Verschlüsselung, keine Authentisierung, keine Autorisierung
- Stufe 1
  Verschlüsselung, keine Authentisierung, keine Autorisierung

Es ist klar, das selbst die „hohe“ Sicherheitsstufe aufgrund der fehlenden Authentisierung keine ausreichende Sicherheit bietet. Gewisse Angriffe, wie z.B. der Zugriff durch nicht autorisierte Applikationen oder Man-In-The-Middle-Attacken sind trotzdem möglich.

Es muss angemerkt werden, dass auch bei anderen Herstellern von UC-Lösungen das Thema Sicherheit eher stiefmütterlich behandelt wird. So wurden im ComConsult-Labor als Nebenprodukt anderer Analysen beispielsweise folgende Mängel bei der Produktpalette von Cisco festgestellt:

- Bei Extension Mobility sind die PINs (bis Version 6.x des Cisco Unified Communications Manager, CUCM) während der Übertragung nicht verschlüsselt.
- Rufjournale sind auf den Telefonen ge-

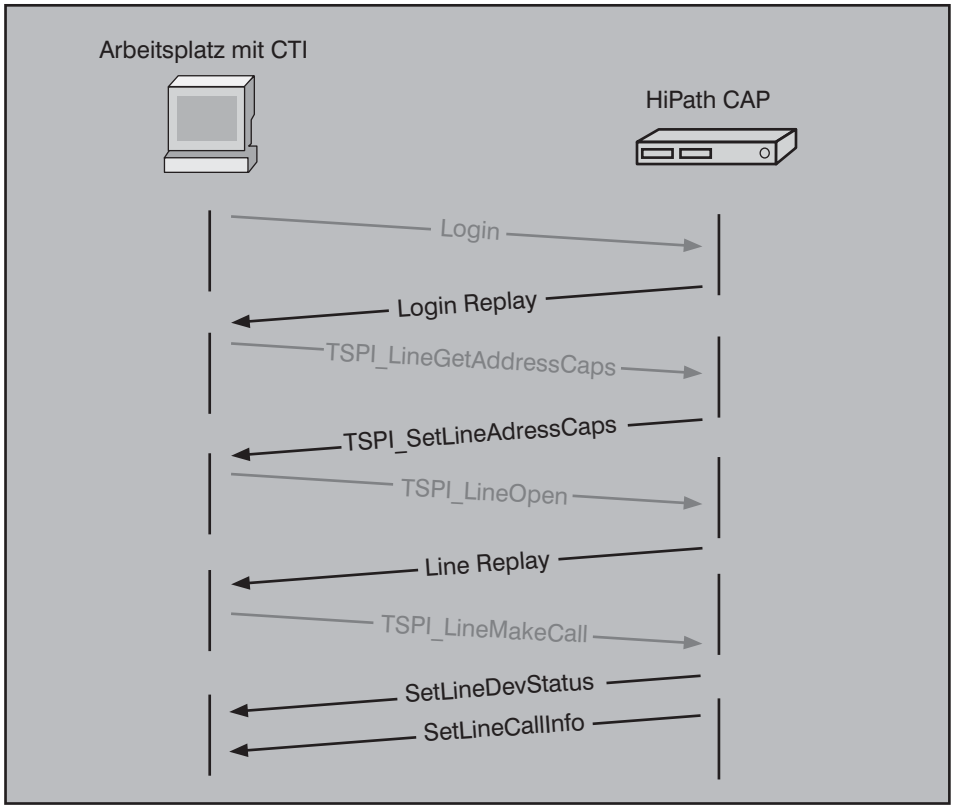



Abbildung 10: Verbindungsaufbau

speichert und für jeden mit Zugang zum Endgerät einsehbar.

- Der Zugang zu Sprachnachrichten über das Telefon wird zwar per PIN authentisiert - diese werden jedoch unverschlüsselt über das Netz übertragen.

Erfreulicherweise sticht Microsoft in punkto Sicherheit nach ersten Untersuchungen positiv heraus. Die UC-Produkte Office Communications Server 2007 (OCS) und Exchange 2007 verschlüsseln alle Kommunikation per Default. Die nicht standardkonforme Umsetzung von Protokollen sowie ein proprietärer Audio-Codec tun auch ihr übrigens, um Angreifern das Leben schwer zu machen (was allerdings durchaus ironisch zu verstehen ist).

### 5. Fazit

Für die Sicherheit von UC sind die zunehmende Zahl von Integrationspunkten (Schnittstellen), die wachsende Integrationstiefe und die Vielfalt unterschiedlicher Protokolle die kritischen Faktoren. Dabei ist eine wesentliche Bedrohung im Übergreifen von Gefährdungen zwischen den Schnittstellen bzw. Komponenten des Systems zu sehen. Die unzureichende Absicherung von TK-Applikationen kann prinzipiell die gesamte VoIP-Sicherheit aushebeln. Verschlüsselung und Authentisierung von Medienstrom und Signalisierung (z.B. per SRTP und TLS) können im schlimmsten Fall sogar wertlos werden, wenn durch eine Sicherheitslücke einer TK-Applikation ein Endgerät geeignet kompromittiert werden kann.

Stand heute bedeutet in Konsequenz die Absicherung von UC das „Durchdeklinieren“ aller Schnittstellen und der darüber transportierten Daten zur Festlegung der Sicherheitsmechanismen. Herstellerspezifische Lösungen liefern hier kaum einen Gewinn, und die Strategie mancher Hersteller in den Datenblättern eher schweigsam zu der Sicherheit der Anwendung oder der Schnittstelle zu sein ist kontraproduktiv. Der erste Schritt zum Aufräumen der Baustelle TK-Applikationen ist Offenheit. Einheitliche Standards sind dabei mehr als notwendig!

Die zunehmende Integration von IT- und TK-Komponenten in Einklang mit Sicherheitsanforderungen zu bringen, gleicht glücklicherweise trotzdem nicht dem Problem der Quadratur des Kreises. Jedoch kommt der umsichtigen Planung des Kommunikationssystems und der Umsetzung effektiver technischer Maßnahmen eine zunehmend größere Bedeutung zu. Bereits bei der Konzeptionierung und Beschaffung müssen Sicherheitsfunktionen stärker berücksichtigt werden, um ein böses Erwachen im Betrieb zu vermeiden.

### 6. Literatur

[1] BSI TL-02103, „Technische Leitlinie Sichere TK-Anlagen“, Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 1. Juli 2008, verfügbar unter http://www.bsi.de/literat/doc/tk-anlagen/TL02103.htm

[2] „SOA-Security-Kompendium - Sicherheit in Service-orientierten Architekturen“, Bundesamt für Sicherheit in der

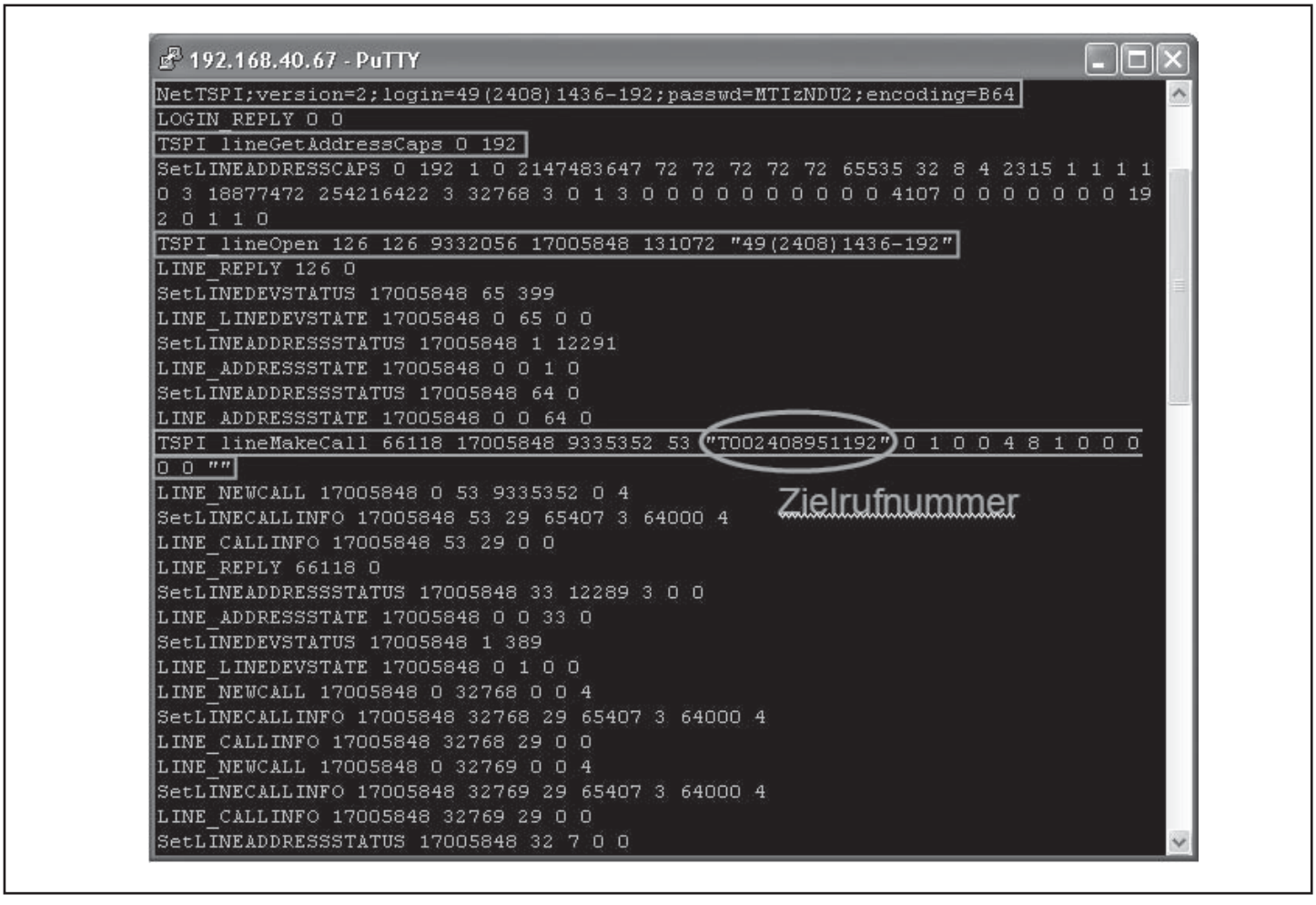



Abbildung 11: Telnet-Sitzung mit Interaktion zwischen Angreifer und CAP-Server

Schwerpunktthema

# SIP Trunking und SIPconnect

## bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Gespräche mit unternehmens-externen Teilnehmern werden weiterhin über zeittarifierte PSTN-Verbindungen gehandhabt (siehe Abbildung 1.1). Dies gilt insbesondere für Gespräche ins Ausland, die nach wie vor zu internationalen PSTN-Ferntarifen abgerechnet werden (siehe Abbildung 1.2).

### VoIP Trunking

Sofern das Corporate IP-Netz über freie Bandbreite für TK verfügt oder aber entsprechend hochgerüstet wird, können interne und externe $S_{2M}$-Trunks ganz oder teilweise durch unternehmensinterne IP-Verbindungen abgelöst werden. Hier setzen viele LCR-Lösungen von VoIP Implementierungen an: Ein Gespräch wird über das Corporate IP Netzwerk bis an den Standort weitergeleitet, der am nächsten d.h. tarifgünstigsten zu dem angewählten PSTN Teilnehmer liegt. Über das dortige PSTN-Gateway wird das Gespräch ins PSTN-Netz weitergeleitet. Dadurch entstehen nur noch PSTN-Kosten für lokale Tarife, PSTN-Kosten für Ferntarife werden optimiert oder ganz vermieden, wie in Abbildung 1.3 gezeigt. Soweit die Kapazität des Corporate-IP Netzwerks überschritten ist, kann durch Call Routing und CAC-Regeln konfiguriert werden, dass die überzähligen Gespräche wie bisher direkt ab Ausgangsstandort über das PSTN geroutet werden.

Bei Ende-zu-Ende Nutzung einer einheitlichen Enterprise Lösung stehen mit dem Einsatz proprietärer IP-Trunks (Alcatel ABC, Avaya DCS, Nortel MCDN, Siemens CorNet etc.) zwischen den TK-Knoten viele bis alle Leistungsmerkmale standortübergreifend zur Verfügung. Werden unterschiedliche Hersteller eingesetzt, so bietet H.323 im Regelfall lediglich die Möglichkeit, Basic Call Funktionalität über IP Trunks zu nutzen, da die allermeisten Hersteller die Zusatzfunktionen (H.450) nicht unterstützen. QSIG mit einem etwas höhern Funktionsumfang von ca. 10 bis 20 Leistungsmerkmalen steht hier nicht zur Debatte, weil die meisten Hersteller QSIG nicht über IP unterstützen. Die-

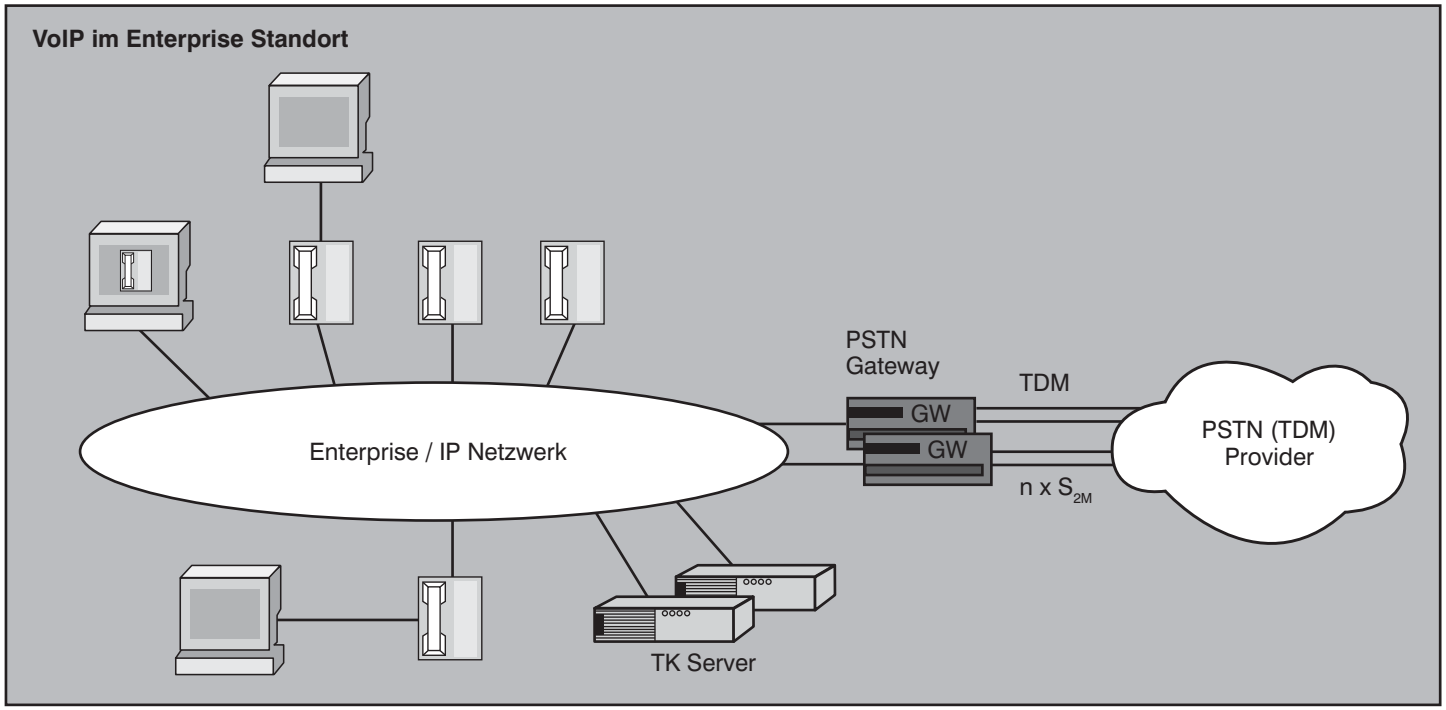



Abbildung 1.1: Hybride VoIP Lösung mit PSTN-Gateways

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

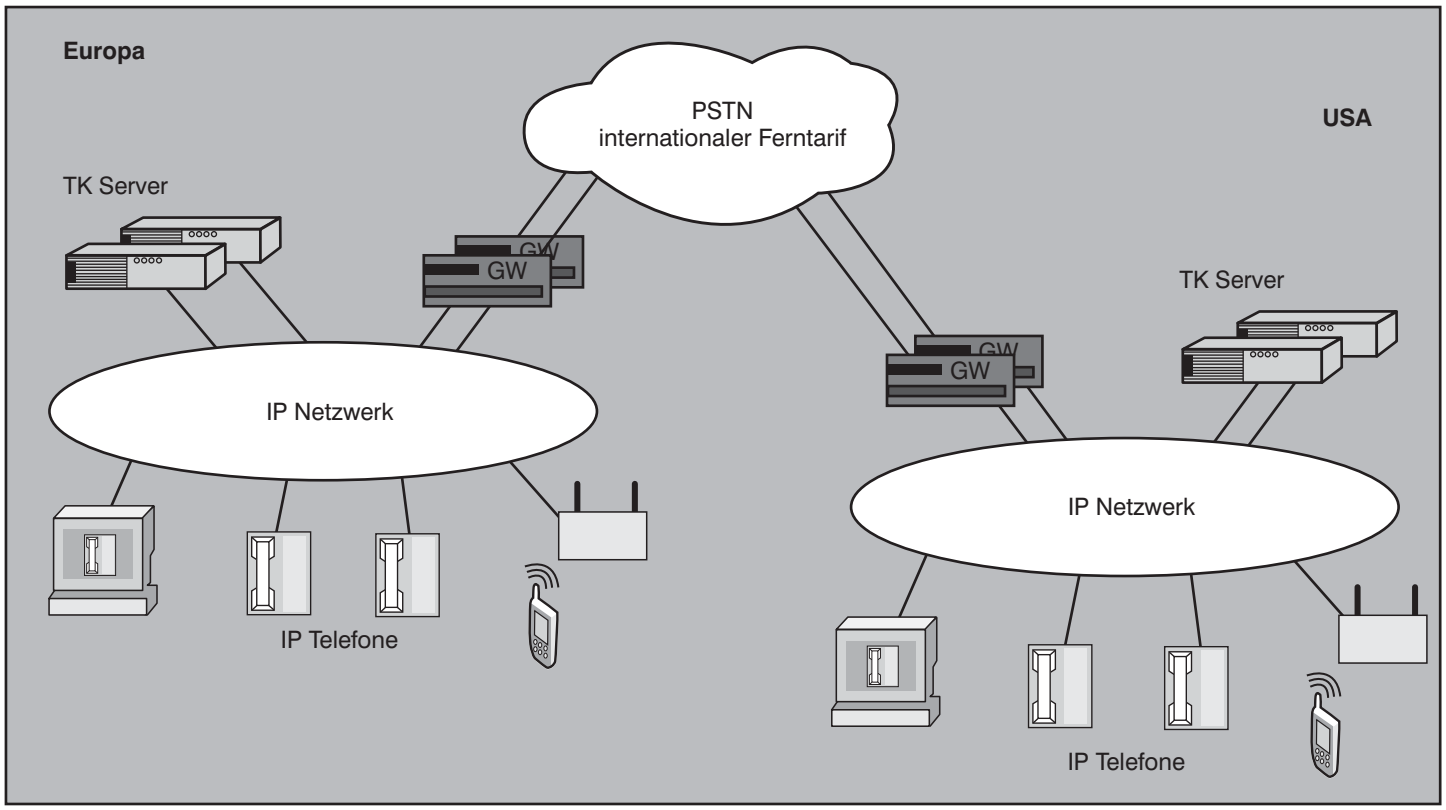



Abbildung 1.2: Hybride VoIP Lösung mit PSTN-Gateways je Standort

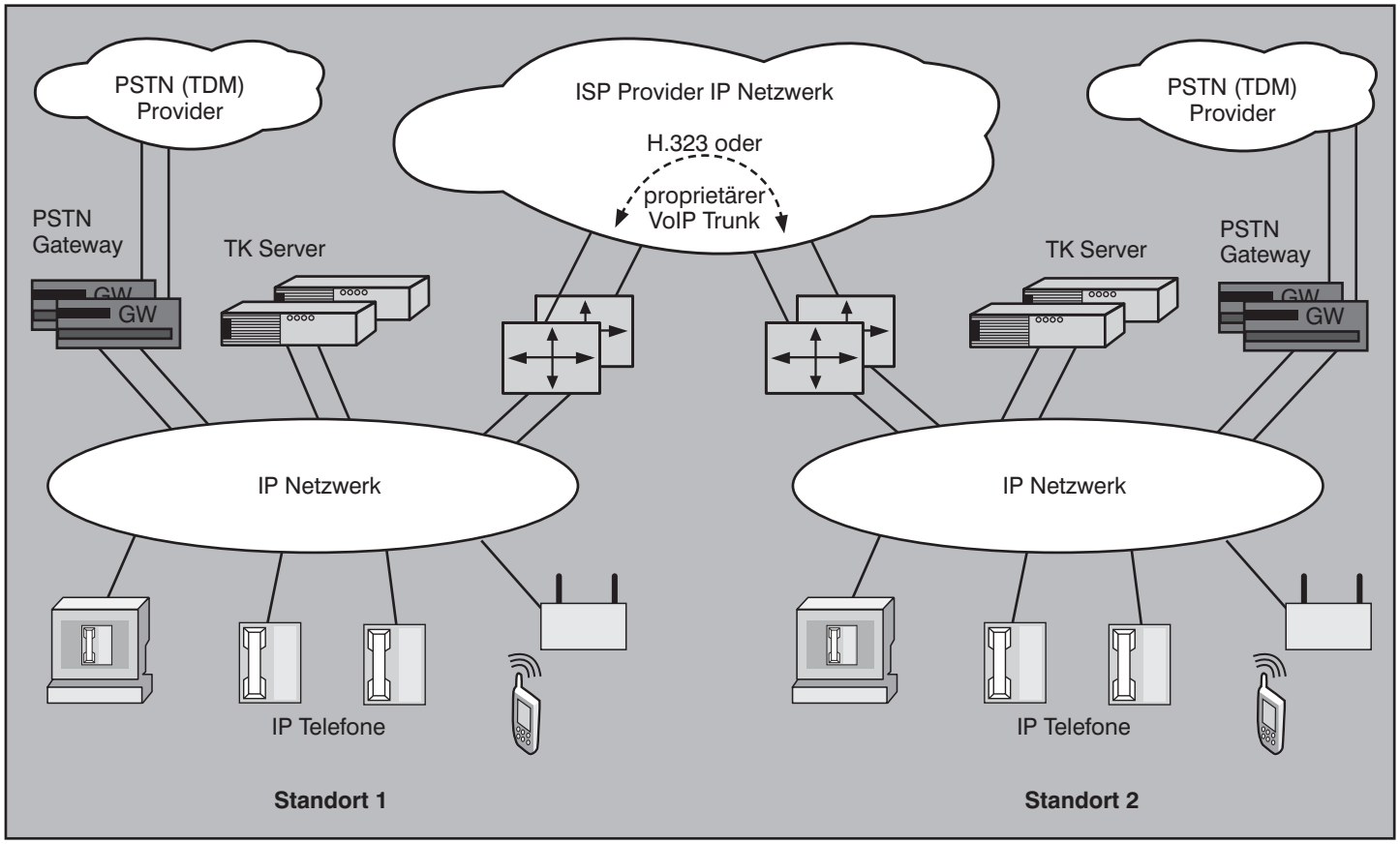



Abbildung 1.3: Nutzung des Corporate IP Netzwerks für Corporate VoIP Trunks

se Einschränkungen können sich mit SIP Trunking ändern.

**SIP Trunking**

Mit der Verbreitung von SIP Lösungen sowohl im Provider- als auch im Enterprise-Umfeld wachsen Bedarf und Möglichkeiten, Ende-zu-Ende Verbindungen zwischen Providern und Unternehmen mit SIP zu schalten. Die Enterprise und Provider-Seite werden im Regelfall als SIP Peers bezeichnet, das SIP Peering wird über einen Trunk-Dienst realisiert. Wird SIP Trunking zur Verbindung zweier ITSP-Provider eingesetzt, so sind die beiden Provider die SIP Peers. SIP Trunking verbindet VoIP/SIP Enterprise Lösungen mit VoIP/SIP Providern und hat die Zielsetzung, nicht nur IP-Verbindungen / ISP's für vordefinierte VoIP Trunks zu nutzen, sondern den PSTN-Dienst zur Verbindung aller Teilnehmer weltweit schrittweise auf SIP Verbindungen umzustellen und die Q.931/SS7 Signalisierung durch SIP Signalisierung zu ersetzen. (Grundkenntnisse über SIP werden an dieser Stelle vorausgesetzt, sie sind zu finden in den Insider Artikeln der Ausgaben Mai, Juni und August 2004 sowie in dem Technologie-Report „SIP - Session Initiation Protocol" von ComConsult Research.)

An die Stelle von Amtsbündeln treten SIP Trunking Dienste auf der Basis von IP-Netzzugängen zu SIP Providern. Die Amtskopf-Nummern eines Unternehmens lassen sich mittels ENUM auf SIP-Domänen mappen oder durch SIP Domänen mit alphanumerischen Domänennamen (FQDN) ersetzen. Dies ermöglicht eine weltweite Bekanntgabe / Erreichbarkeit von SIP Teilnehmern über den DNS-Dienst. Schlägt das SIP Lookup fehl, weil ein gesuchter Teilnehmer nicht SIP-fähig ist, wird er unter Zuhilfenahme von SIP/PSTN-Gateways wie bisher über seine PSTN-Amtsnummer angewählt.

**SIP Trunking ist der Ansatz, alle PSTN Verbindungen global durch SIP Verbindungen und E.164 Telefonnummern global durch SIP URI's zu ersetzen.**

Der Übergang ins PSTN-Netz zu Teilnehmern, die nicht IP/SIP-fähig sind, erfolgt nach dem LCR-Prinzip über das dem PSTN-Teilnehmer nächstgelegenen Gateway, das üblicherweise dann nicht mehr im Unternehmen sondern beim SIP-Provider steht. Einsatz-Beispiele für SIP Trunking zeigen Abbildung 1.4 und Abbildung 1.5. Insbesondere bei Nutzung von SIP Trunking in einem internationalen Szenario entstehen deutliche Kosteneinsparungen durch die Nutzung landesinterner PSTN-Gateways anstelle internationaler

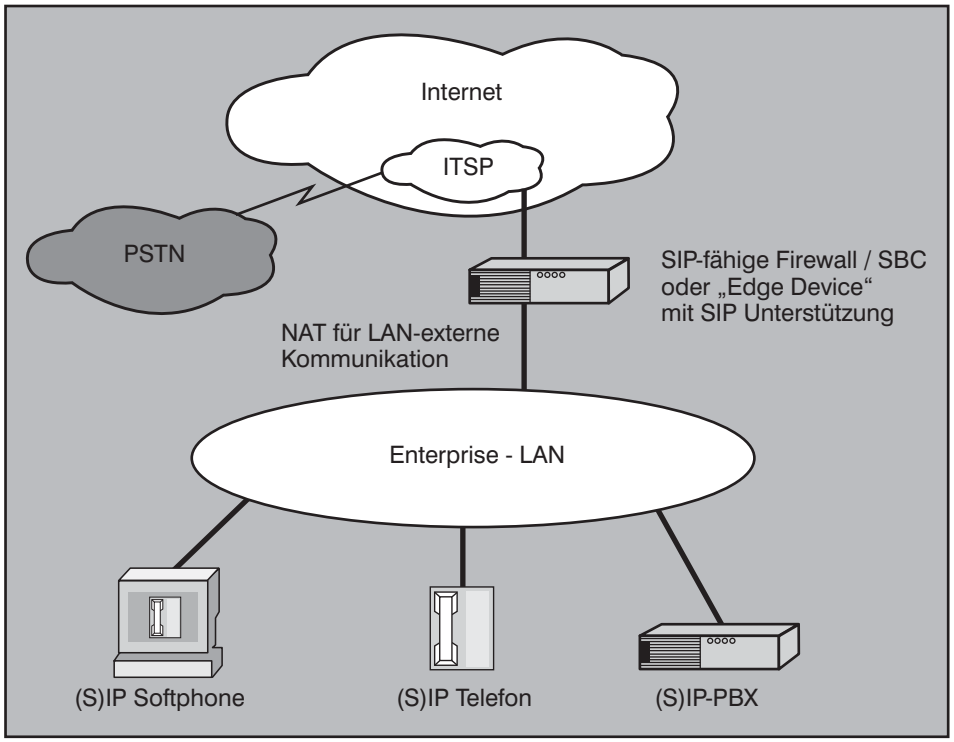



Abbildung 1.4: Einfaches SIP Trunking Szenario

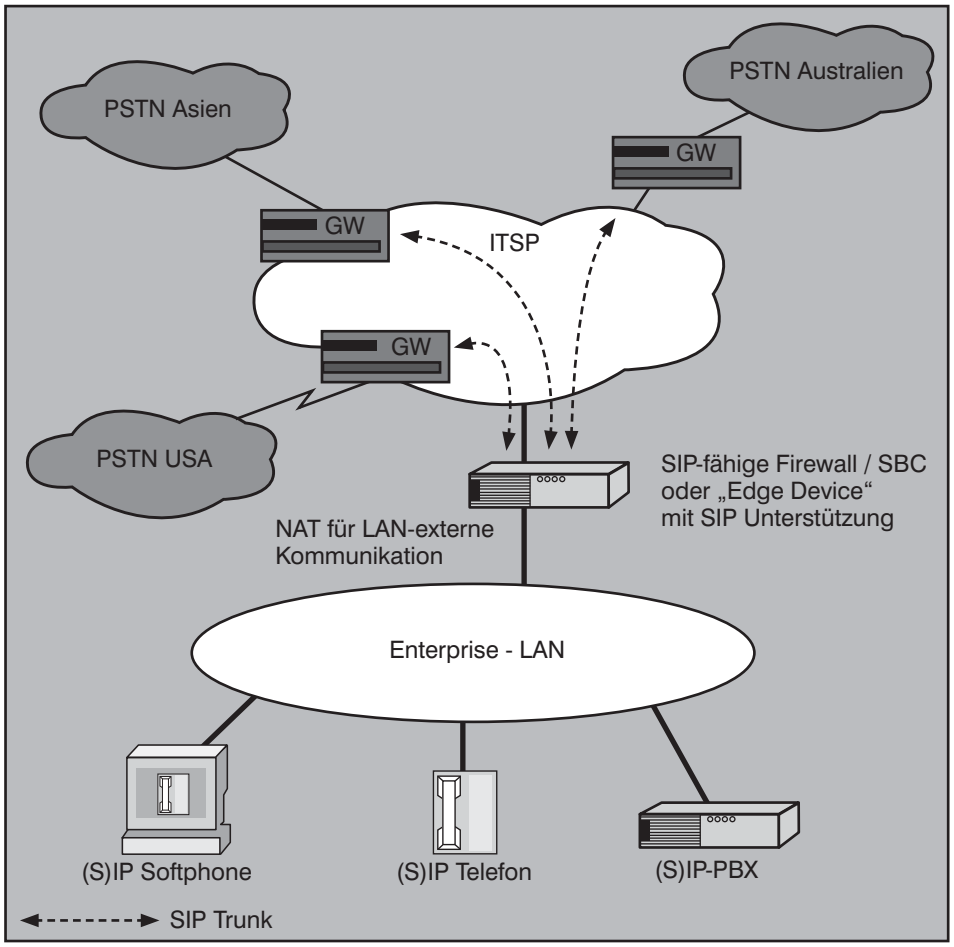



Abbildung 1.5: SIP Trunking Szenario mit internationalem LCR zu PSTN-Teilnehmern

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

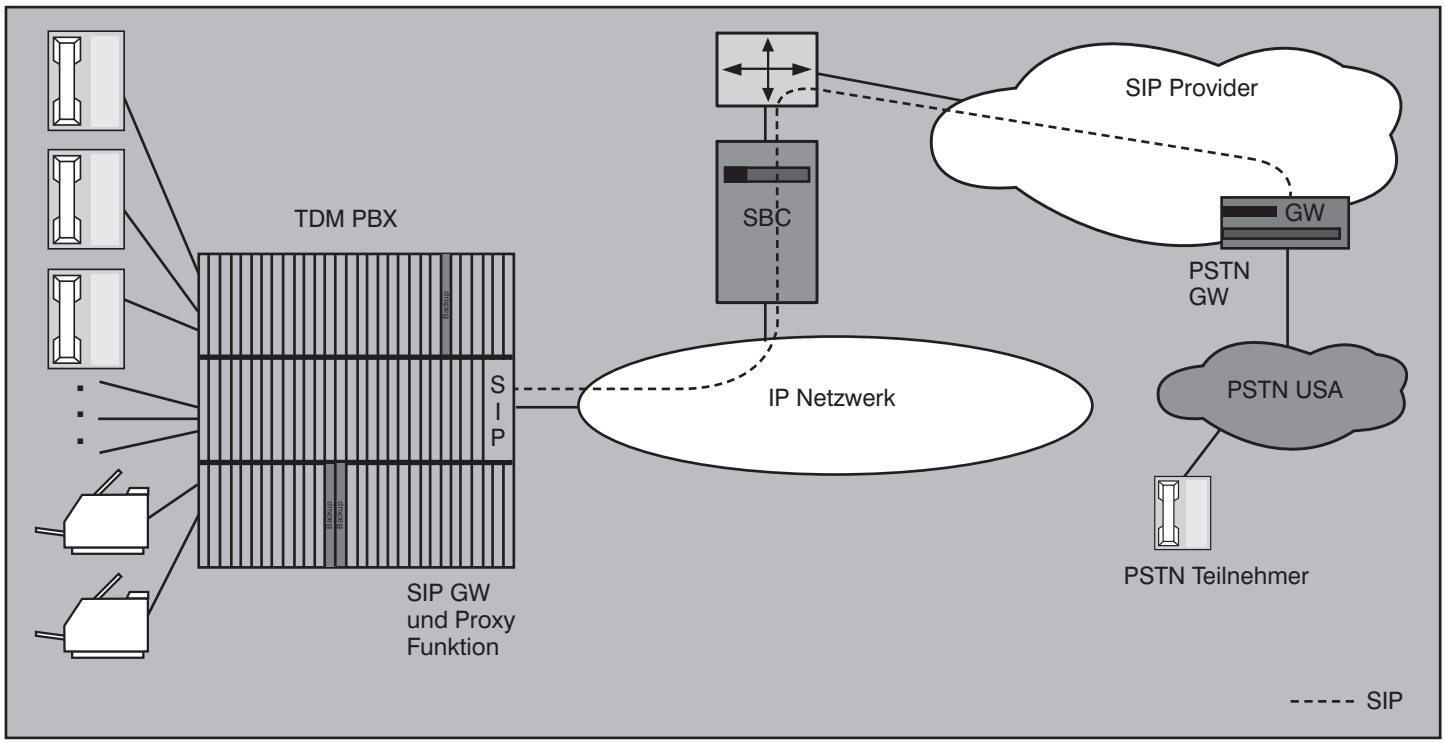



Abbildung 1.6: Einsatz von SIP Trunking und klassischer PBX

PSTN-Verbindungen. Ein Kriterium für die Auswahl eines SIP Providers kann daher auch die Anzahl und geografische Verteilung der PSTN-Gateways sein, über die er verfügt.

Voraussetzung auf Anwender-/Unternehmensseite ist eine SIP-fähige TK-Lösung, die auf der Enterprise-Seite eine von zwei Voraussetzungen benötigt:

- die Telefone und der TK-Server reden native SIP
- auf / im Zusammenspiel mit dem TK-Server läuft ein SIP-Gateway, das die proprietäre, meistens IP-basierte Signalisierung nach SIP konvertiert und so den Übergang in die SIP Welt ermöglicht.

Im Ausnahmefall kann SIP Trunking auch für klassische TDM PBX'en zum Einsatz kommen, wenn die TDM PBX über ein SIP Gateway / SIP Interface verfügt, das SIP Trunking unterstützt (siehe Abbildung 1.6).

Unterstützt der TK-Server SIP Trunking, so könnte er die Verbindung zum SIP Provider theoretisch alleine handhaben. Am Übergang zwischen Enterprise / Kunde und Provider steht jedoch aus mehreren technischen und Sicherheits-Gründen vielfach ein Session Border Controller, der die Verbindungen zwischen externen und internen Teilnehmern und / oder Diensten steuert.

Grundsätzlich lassen sich SIP Service Provider so wie früher PSTN Provider in „Endkunden-Provider" und „Backbone-Anbieter" unterscheiden. Erstere leisten die Schnittstelle zum Unternehmen, letztere implementieren die Backbone-Infrastrukturen, um Provider-Verbundnetzwerke zu betreiben. Sie funktionieren gleichsam als Aggregierungs-Ebene für Endkunden-Provider.

Ein SIP Provider muss nicht zwingend eine eigene IP Netzwerkinfrastruktur betreiben, sondern kann diese von einem ISP nutzen. Ein ISP kann seinerseits das Dienstangebot auf SIP Trunking und TK-Dienste erweitern. Natürlich ist das Dienstangebot im Zusammenhang mit SIP Trunking unterschiedlich, angefangen beim reinen Sprachdienst, den Sie eher bei den klassischen Sprachanbietern finden, bis hin zu den Unified Communications-Lösungen der neueren Anbieter im Markt.

## 2. Vorteile bei Einsatz von SIP Trunking

Die allgemeinen Vorteile von Sprachlösungen auf Basis IP (VoIP) setzen wir hier als bekannt voraus. Natürlich greifen die Vorteile einer VoIP-Lösung auch für SIP Lösungen. SIP Trunking bietet jedoch zusätzliche Vorteile.

### Einheitlichkeit

Der Einsatz von SIP-Lösungen bietet das Potenzial, sowohl unternehmensweit als auch bei der Verbindung über mehrere Provider hinweg dieselbe Signalisierung zu nutzen – SIP. Somit entfällt die aufwändige Konvertierung zwischen proprietärer Signalisierung und ISDN- / PSTN-Netzwerk, die sowohl Gateway-Ressourcen als auch Bearbeitungszeit und somit eine Erhöhung der Ende-zu-Ende Antwortzeit kostet. Zudem müssen Probleme in der Sicherheitstechnik wie NAT/FW-Traversal nur noch für ein einzelnes Protokoll gelöst werden: für SIP.

### Multivendor- / Multiprovider-Lösungen

Standardisiertes SIP und standardisiertes SIP Trunking sind die Voraussetzung für den Aufbau von Multivendor-Lösungen, bei denen Endgeräte / Telefone, TK-Server und TK-Applikationsserver von verschiedenen Herstellern im Mix und Match zum Einsatz kommen und sich Multiprovider-Lösungen mit der Nutzung mehrerer verschiedener Provider für die Vermittlung von externen Gesprächen durch ein einzelnes Unternehmen designen und betreiben lassen. In einer solchen Umgebung kann das Unternehmen sehr flexibel entscheiden, welchen ITSP/SIP Provider es in welchem Land nutzen will.

### Verfügbarkeit

Sowohl im Enterprise als auch beim Provider können SIP Server gedoppelt und als

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

fehlertolerante Lösungen (z.B. Cluster) betrieben werden. Dies soll hier nicht weiter vertieft werden.

Mit SIP Trunking kann ein Unternehmen an einem einzelnen Standort darüber hinausgehend mehrere ITSP/SIP Provider nutzen, um die Verfügbarkeit weiter zu erhöhen. Die Umschaltung von einem SIP Provider auf einen (vielleicht teureren, daher als Default weniger genutzten) Backup SIP Provider kann auf Basis eines Watchdog Timers (z.B. im Session Border Controller / SIP Edge Device) erfolgen, der zeitgesteuert die Erreichbarkeit des Default SIP Providers auch dann abfragt, wenn kein Verkehr anliegt und bei Nichterreichbarkeit des Default Providers auf den Backup Provider umschaltet. Diese Umschaltung funktioniert unabhängig davon, ob der Netzwerkzugang des Default SIP Providers oder seine SIP Server eine Störung haben.

Zusätzlich kann als Dritt-Absicherung ein eigener PSTN-Netzzugang betrieben werden, der bei Ausfall aller genutzten SIP Provider oder Providerzugänge als Fallback zur Verfügung steht, im Normalfall ungenutzt ist und somit auch keine Zeittarif-Kosten verursacht.

**Skalierbarkeit**

Ein Hochrüsten der Bandbreite des IP/Internetzugangs ist vielfach einfacher als das Hinzufügen weiterer S2M-Schnittstellenkarten, wenn z.B. anstelle der Beschaffung einer neuen ISDN-Karte sowie ggf. eines komplett neuen Gateways lediglich das Traffic Shaping des providerseitig sowieso vorhandenen Ethernet/IP-Zugangs softwaretechnisch auf eine höhere Bandbreite konfiguriert wird. Ebenso ist die vom IP-Provider benötigte Zeit für die Hochrüstung meistens niedriger als bei PSTN-Providern.

**Kosteneinsparung**

Hardware- und Software-/Lizenz-Investitionen in PSTN-Gateways und S0- (BRI) oder S2M- (PRI) Schnittstellen entfallen, der Zugang zum SIP Provider erfolgt über den bereits vorhandenen ISP-Zugang oder über ein weiteres Ethernet/IP Interface als SIP Providerzugang. Ebenso entfallen die Wartungs- und Betriebsgebühren für Gateway-Hardware und -Software. Natürlich entstehen bei SIP Trunking Investitionen und Wartungsgebühren für die SIP-Komponenten, die das Unternehmen mit dem Provider verbinden (SIP Edge Device). Diese kosten jedoch meist weniger als Media Gateways.

Mit SIP Trunking reduzieren sich die Kosten für externe Gespräche, da Bandbreite in Form von S2M-Bündeln mehr kostet als IP-Bandbreite und da die tatsächlich auftretende Last nicht zeittarifiert sondern im Regelfall als Flatrate abgerechnet wird.

Durch die Nutzung des Internet/ITSP Zugangs für Sprache und Daten kann die Bandbreitenausnutzung optimiert werden. Bei steigender Verkehrslast erfolgt eine einzelne Hochrüstung der gemeinsam genutzten Verbindung anstelle zweier Hochrüstungen für Daten und Voice. Die Hochrüstung von IP-Verbindungen ist bei Bedarf in kleineren Schritten möglich als S2M. Zudem sind die Mehrkosten pro 1-Mbit Hochrüstung für IP im Regelfall deutlich niedriger als pro 1-Mbit PSTN.

Least Cost Routing (LCR) erlaubt eine Kostenoptimierung auf nationaler und internationaler Ebene durch Nutzung derjenigen SIP Provider, die in verschiedenen Ländern jeweils das günstigste Preis/Leistungs-Verhältnis anbieten (siehe Abbildung 2.1). Soweit der Betreiber einer SIP Lösung dies möchte, kann er das Call Routing für verschiedene Tageszeiten unterschiedlich implementieren und hierdurch nochmals die Kosten optimieren.

Sofern der angewählte Teilnehmer ebenfalls SIP-fähige Telefonie unterstützt, kann die Kommunikation ausschließlich über IP-Verbindungen erfolgen und es fallen keinerlei Kosten für die Nutzung von PSTN-Gateways und PSTN-Wegen mehr an.

**Multimedia-Unterstützung**

SIP zeigt zwar mit Blick auf die aktuelle Standardisierung und Funktionalität eine gewisse Fokussierung auf Sprache (VoIP), es ist jedoch nicht auf Sprache beschränkt sondern per Definition auf globale Multimedia-Kommunikationsszenarien ausgelegt. Dies umfasst zusätzlich zu einem „einfachen Telefonat“ die Dienste

- Videokommunikation Peer-to-Peer
- Audio- / Videokonferenz
- Instant Messaging (IM)
- Erreichbarkeits-Dienste
- Verteilte Anwendung mit verteilter Dokumentenbearbeitung (Application Sharing), oder gemeinsamer Dokumenten-Einsicht (Document Viewing)
- Elektronisches Flipchart (Whiteboard wb)
- Alarmweiterleitung
- Dateitransfer
- u.a.m.

Diese Multimedia-Funktionalität wird vielfach auch als „Rich Communication“ oder „Rich Media Communication“ bezeichnet. Dabei öffnet die SIP Signalisierung für jede der oben genannten Funktionen einfach einen weiteren Media Stream. Natürlich kann eine SIP Session auch mehrere gleichartige Media Streams nutzen (z.B. zwei gleichzeitige Telefonate, die jeweils kurzzeitig auf Halten gesetzt werden).

In einem Umfeld mit SIP Trunking ist zusätzlich denkbar, dass die Applikationsserver für die beschriebenen Multimedia-Anwendungen ganz oder teilweise nicht mehr im Unternehmen selbst stehen und betrieben werden, sondern bei einem SIP Provider oder SIP Application Provider gehostet sind.

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

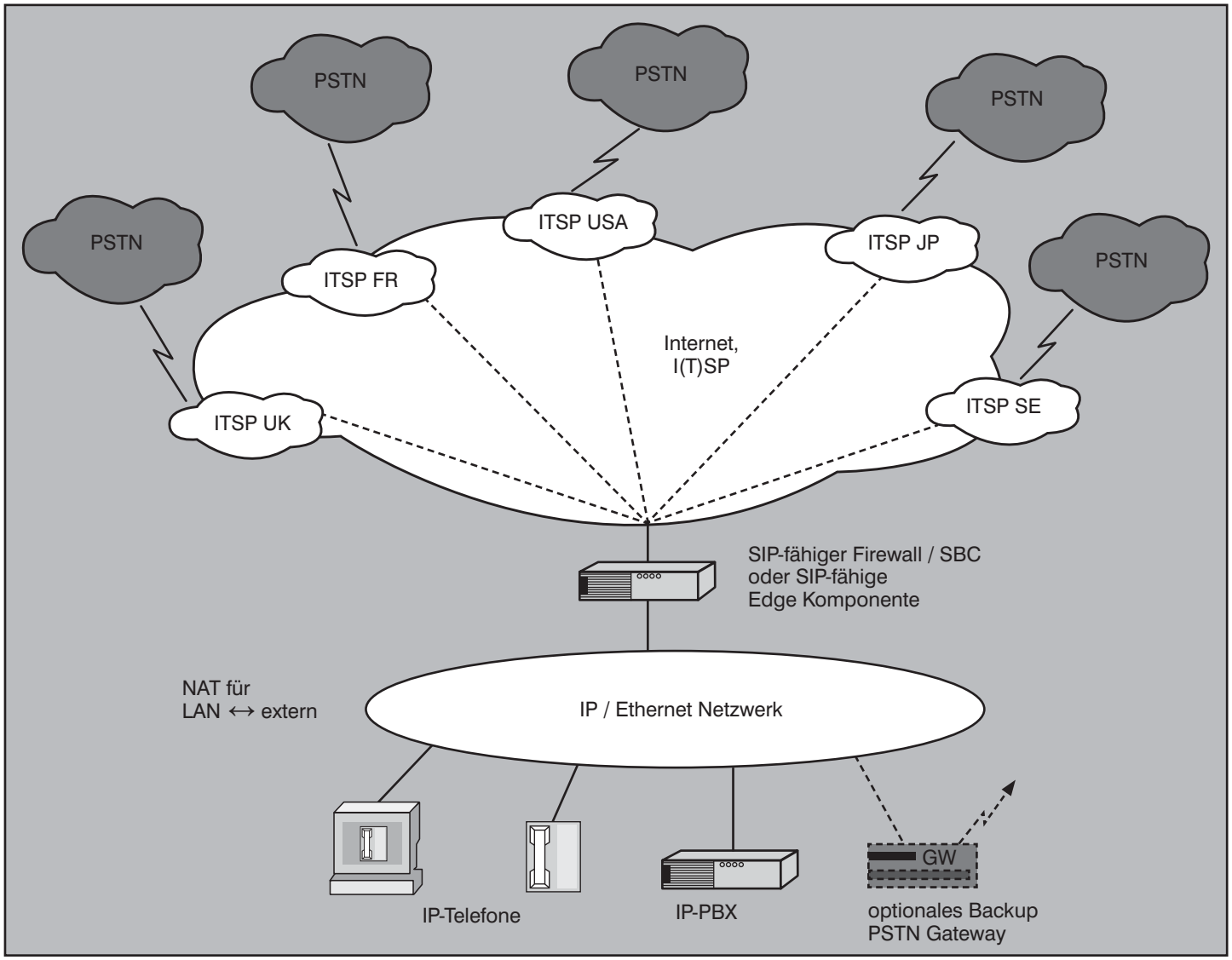



Abbildung 2.1: Kostenoptimierung durch Nutzung unterschiedlicher SIP Provider

**Produktivitäts-Steigerung durch UC und Erreichbarkeitsdienste**

Da SIP nicht nur für Sprache sondern auch Multimedia geeignet ist, bietet es die ideale Plattform für Unified Communication (UC) Lösungen. Dies sind integrierte Anwendungen / Anwendungsoberflächen, von der aus mittels Maus und Kontextmenüs viele oder alle Kommunikationsfunktionen (Voice, Video, IM, AS, A/V-Konferenz, Mail) bei gleichzeitigem Zugriff auf die nötigen Informationen durchgeführt werden können. Zusätzlich umfasst eine UC-Lösung Erreichbarkeitsfunktionen, die anzeigen, ob und wie ein gesuchter Teilnehmer erreichbar ist.

Erreichbarkeits-Dienste wurden unter dem Begriff „Presence“ in SIP/SIMPLE standardisiert (RFC‘s 3856, 3857, 3903, 4235, 4479 bis 4482, 4488, 4660 bis 4662, 4825 bis 4827, 4854, 4979, u.a.). Sie zeigen an, ob und mit welchem Dienst (z.B. Voice, Video, IM, Mail) / welcher Funktionalität / welchem Endgerät ein gesuchter Teilnehmer gerade erreichbar ist.

Alle etablierten VoIP-Lösungen setzen heute Erreichbarkeits-Dienste, Instant Messaging und Unified Communication auf Basis des SIP Protokolls ein. Nutzt eine Lösung für die Leistungsmerkmale noch eine proprietäre Signalisierung, so setzt der Hersteller zur Implementierung von Presence und UC ein SIP Gateway ein.

Genau wie für Multimedia-Anwendungen gilt auch für UC und Erreichbarkeitsdienste, dass die Anwendungsserver bzw. diese Dienste bei einem SIP Provider oder SIP Application Provider gehostet sein können und dann über SIP Trunking nutzbar werden.

**Einbindung mobiler Benutzer**

Werden SIP Signalisierung und SIP Trunking genutzt, so lassen sich mobile oder SOHO Benutzer auch für Telefonie leicht über bereits vorhandene Internet-Zugänge und im Unternehmen etablierte remote Zugangsverfahren einbinden. Ein Teilnehmer, z.B. Herr Müller-Lüdenscheid, kann sein SIP Softphone über einen beliebigen Internet Providerzugang als Browser Applet laden und sich über das SIP Webphone wie über eine lokale Nebenstelle in der im Hauptstandort betriebenen TK-Lösung einloggen. Ein Anrufer, z.B. Dr. Klöbner, wählt einfach die übliche Büronummer von Herr Müller-Lüdenscheid und merkt gar nicht, dass er mit ihm über SIP und SIP Trunking verbunden ist, weil Herr Müller-Lüdenscheid gerade in einem anderen Land über einen Hot Spot eingeloggt ist.

Mittels Personalisierung, Erreichbarkeits-

Diensten und einer zeitgesteuerten oder bedarfsgemäßen Einstellung „bevorzugter Endgeräte“ kann ein mobiler Benutzer über Single-Number-Funktionen, Wähl- und Umleitungsregeln automatisieren, wann er bevorzugt über welches Endgerät telefonieren bzw. angerufen werden will.

### 3. SIP Trunking mit SIPconnect

#### 3.1 Offene Punkte bei SIP Trunking und die Arbeit des SIP Forums

SIP ist ein text-basiertes Client-Server Protokoll, das mit dem Ziel designed wurde, interaktive Kommunikationsverbindungen über Sprache, Video, IM und andere Multimedia-Dienste aufzubauen, zu steuern / ändern und zu beenden. Es deckt also Registrierung, Basis-Signalisierung und das Auffinden eines Teilnehmers (User Location) ab. Darüber sind andere Protokolle leicht einbindbar (LDAPv3, RADIUS, MIME, DNS etc.). Die Implementierung von Leistungsmerkmalen bzw. Funktionen erfolgt mit so genannten Methoden (INVITE, OPTIONS, INFO, REFER, PRACK, FORK, SUBSCRIBE, NOTIFY…). Sowohl die Methoden als auch die Nutzung anderer Protokolle geben SIP eine sehr hohe Flexibilität in der Nutzung.

Aber gerade hier liegt auch das Problem hinsichtlich Kompatibilität: Eine bestimmte Funktion kann auf unterschiedliche Arten mit unterschiedlichen Methoden implementiert sein, und wenn zwei Komponenten jeweils unterschiedliche Implementierungen unterstützen, sind sie nicht oder nur teilweise kompatibel zueinander – wie zwei Verbindungsenden, die zwar beide korrekt zum Endgerät hin arbeiten, sich aber in der Mitte nicht treffen, sondern aneinander vorbei zeigen.

Zusätzlich haben die SIP Standards das Thema Trunking nicht lückenlos spezifiziert, insbesondere das Management hierarchischer logischer Strukturen ist der SIP Signalisierung ziemlich fremd. Gerade hierarchische Strukturen sind aber für ein effektives Peering von TK-Lösungen erforderlich, weil sie sowohl viele Einzelteilnehmer als auch optionale unternehmensweite Parameter wie Servicenummern oder Zugangscodes handhaben müssen.

Funktionierende Trunking Lösungen beruhen heute im Regelfall auf einer jeweiligen Anpassung spezieller SIP Clients / SIP Server auf der Enterprise Seite an den jeweils genutzten Provider – einige Anbieter liefern mit ihrer Enterprise-Lösung bis zu 30 Provider-Profile aus (die natürlich jeweils in der Release-Pflege mit gepflegt werden müssen!), die alle an irgendwelchen Stellen irgendwelche Bits verbiegen, damit‘s mit dem jeweiligen Provider klappt.

Daher ist eine de facto Standardisierung von SIP Trunking, die Lücken ausfüllt und von jeweils mehreren Optionen eine geeignete auswählt, für den Einsatz in der Breite dringend erforderlich. Regelungen sind insbesondere für folgende Bereiche erforderlich:

- Referenz-Architektur
- zu unterstützende Basis-RFC‘s
- zu unterstützende erweiterte RFC‘s
- zu unterstützende Methoden
- zu unterstützende Codecs, Paketierungs-Intervalle und Capability Negotiation
- Methode für DTMF
- Quality of Service
- Sicherheitsmodell (Authentifizierung, Verschlüsselung)
- Umgang mit NAT

Hier kommt das SIP Forum ins Spiel, das eine Arbeitsgruppe ins Leben gerufen hat, die seit 2005 unter dem Namen SIPconnect eine pragmatische Standardisierung für den Aufbau von SIP Peering Strukturen mit SIP Trunking erarbeitet. Die erste Version SIPconnect v1.0 wurde im Herbst 2007 inhaltlich fertiggestellt und am 23. Januar 2008 vom SIP Forum formal verabschiedet. Seit September 2007 gibt es das SIPconnect Compliant Programm, über das sich Hersteller für SIPconnect v1.0 zertifizieren können. Zertifizierte Produkte können dann in Multivendor-Lösungen für SIP Trunking eingesetzt werden. Die ersten Firmen, die eine Zertifizierung erhielten, waren Acme Packet, BroadSoft, Cbeyond, Digium, Ingate Systems und McLeodUSA. Was nicht sonderlich verwundert, da diese Firmen bei der Spezifikation von SIPconnect v1.0 mitgearbeitet haben.

#### 3.2 SIPconnect v1.0

**Referenz-Architektur, funktionale Komponenten, RFC‘s**

Die SIPconnect Referenz-Architektur aus Abbildung 3.1 definiert die einzelnen funktionalen Elemente, die ein Enterprise/Provider oder Provider/Provider Interface für SIP Peering mit SIP Trunking enthalten muss. Diese Elemente werden in der Spezifikation als separate Komponenten dargestellt. In der Praxis ist es jedoch möglich, mehrere funktionale Komponenten in einem konkreten Produkt zusammenzufassen. Ein typisches Beispiel hierfür ist eine IP PBX mit integriertem SIP Proxy Server und ggf. noch integrierten Firewall-Funktionen. Die Referenz-Architektur stützt sich auf die nachfolgend beschriebenen Komponenten ab.

Die **IP PBX** steht für die gesamte TK-Lösung eines Unternehmens und ist so definiert, dass sie Gespräche (Calls) aufbaut und terminiert. Dabei wird unterstellt, dass die Signalisierung SIP und der Media Stream RTP sind. Läuft die interne Signalisierung nicht über SIP, so muss zusätzlich ein Gateway zur Konvertierung der Signalisierung nach SIP unterstellt werden, das in die IP PBX integriert ist oder als separate Hardware betrieben wird.

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

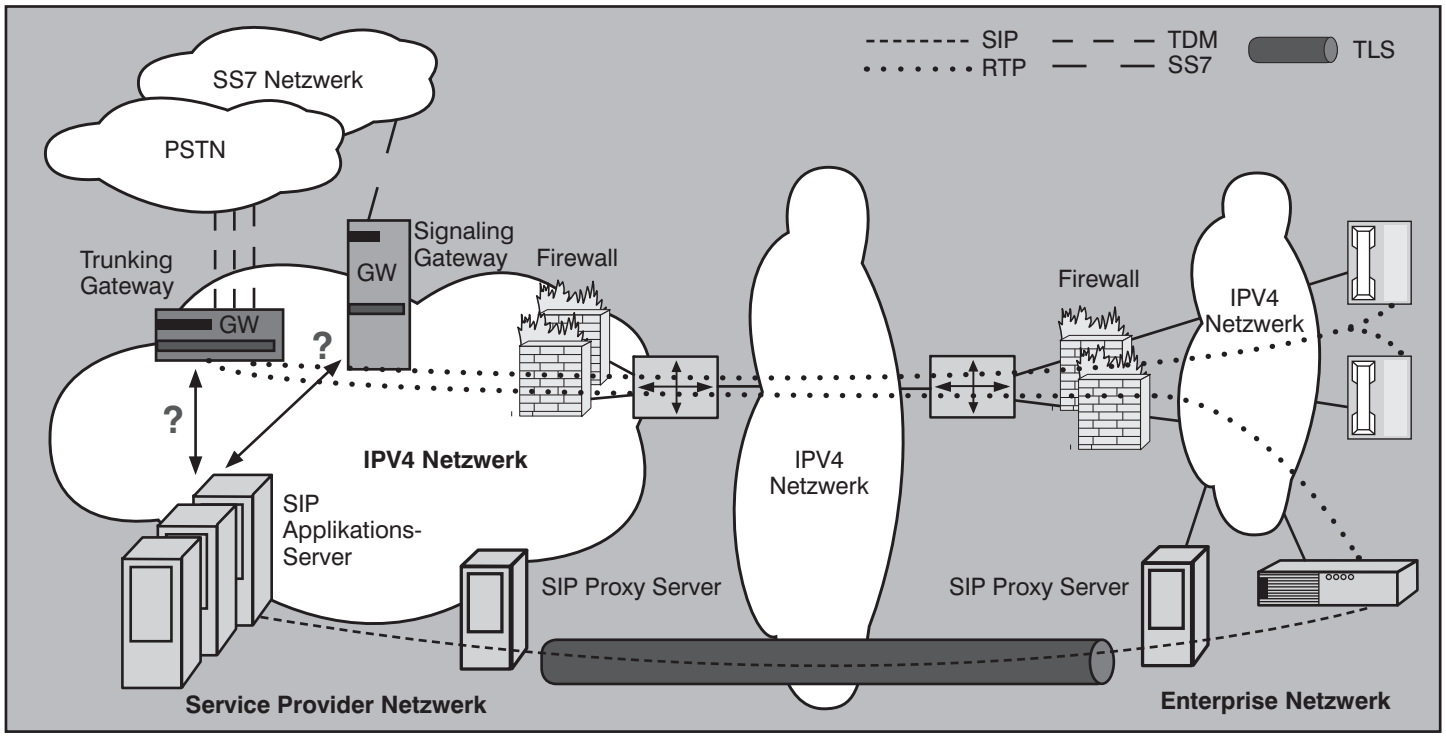



Abbildung 3.1: SIPconnect v1.0 Referenzarchitektur

**IP Telefone** sind VoIP-fähig und werden als Teil des PBX Systems betrachtet. Somit unterliegen sie den Anforderungen an die IP PBX, und die Anforderungen an IP Telefone benötigen keine weitergehende detaillierte Beschreibung. Theoretisch könnten auch ganz klassische TDM Telefone zusammen mit einer TDM PBX eingesetzt werden, wenn diese PBX ein SIP Gateway integriert hat. In der Praxis nutzen meist nur VoIP Lösungen SIP.

Der SIP Application Server **(SAS)** ist im Service Provider Netzwerk positioniert und leistet Aufbau / Terminierung von PSTN Gesprächen für Unternehmen, die SIP / SIP Trunking nutzen.

Der SIP Proxy Server **(SPS)** sorgt für das Routing von SIP Nachrichten und für TLS-Terminierung. Beide Seiten – Enterprise und Provider – benötigen einen eigenen SPS. Die funktionale Komponente „SPS“ kann durch einen oder mehrere physikalische Server im „Edge Bereich“ von Enterprise und Provider realisiert werden.

Das Signalisierungs Gateway **(SGW)** konvertiert SIP Signalisierung nach SS7.

Das Trunking Gateway **(TGW)** ist das eigentliche Media Gateway, stellt die physikalische Schnittstelle zum PSTN-Netzwerk und konvertiert paketvermittelte Sprachsamples in leitungsvermittelte TDM Sprachsamples.

Der Firewall **(FW)** handhabt Paketfilterfunktionen und allgemeine Sicherheitsdienste am jeweiligen Netzwerk-Übergang zwischen Provider und Enterprise.

Interactive Connectivity Establishment **(ICE)** stellt ein Verfahren für NAT Traversal bereit, das weitere Basisverfahren wie STUN und TURN nutzt, insbesondere um SIP-basierte Sprachverbindungen erfolgreich über die diversen NAT Typen hinweg übertragen zu können, die es zwischen einem remote Benutzer und einem zentralen (Provider-)Standort geben kann.

Simple Traversal of UDP over NATs (**STUN**, RFC 3489) ermöglicht es einem SIP Client hinter einem oder mehreren NAT-Komponenten, seine öffentlich genutzte Adresse, den genutzten NAT-Typ und die (anstelle seines lokalen Ports) internet-seitig genutzte Portnummer in Erfahrung zu bringen, um den eigenen SIP Header entsprechend zu manipulieren, so dass der Teilnehmer auf der Gegenseite die richtigen IP-Adresse und TCP/UDP-Portnummer(n) einträgt.

Traversal using Relay NAT **(TURN)** erlaubt einem Client hinter einem oder mehreren NATs, eingehende Daten über TCP oder UDP Verbindungen zu empfangen. TURN kommt meistens für Clients zum Einsatz, die hinter symmetrischen NATs oder FWs angebunden sind und die Empfängerseite einer Peer-Verbindung halten.

Application Layer Gateway **(ALG)** ändert IP Adressen und Portnummern innerhalb des „Datenteils“ (d.h. SIP Header) eines IP-Pakets – auch dann, wenn die IP Pakete nicht direkt an das ALG adressiert sind. SIP ALGs verhalten sich nicht unbedingt konform zu den in SIP beschriebenen Rollen; z.B. fügen die meisten SIP ALG‘s keinen ‚Via:‘ Header ein.

Das **IPv4 Netzwerk** besteht aus allen logischen und physikalischen Komponenten, die für Routing und Switching von IPv4 Paketen zwischen Enterprise und Service Provider Netzen erforderlich sind. Falls Ihnen jetzt etwas fehlt: Ja, SIPconnect v1.0 schweigt sich über IPv6 aus. Hier sind Nachbesserungen in SIPconnect v1.1 zu erwarten.

Die Festlegungen, welche RFC‘s zwingend und optional unterstützt werden sollen, zeigt Abbildung 3.2.

Die Liste der festgelegten RFC‘s ist zwar kurz, aber besser als nichts. Aus Sicherheitsgründen war die Entscheidung für eine verschlüsselte Verbindung zwischen Enterprise und Provider besonders wichtig. Der starke, um nicht zu sagen ausschließliche Bezug auf PSTN und E.164 Telefonnummern stellt dagegen eher eine Einschränkung dar. Ganz klar ist erkennbar, dass sämtliche PSTN-Übergänge ausschließlich auf Providerseite betrieben werden und der Provider somit für den Enterprise-Kunden den Amtskopf ersetzt. Um

| Standard ID | Beschreibung | SAS | PBX | SPS |
|---|---|---|---|---|
| Rec.E.164 | ITU-T Recommendation E.164: The international public telecommunication numbering plan | M | M | - |
| RFC 2246 | The TLS Protocol Version 1.0 | - | - | M |
| RFC 2833 | RTP Payload für DTMF Digits, Telephony Tones and Telephony Signals | - | M | - |
| RFC 2782 | A DNS RR for specifying the location of services (DNS SRV) | - | - | M |
| RFC 3261 | SIP: Session Initiation Protocol | M | M | M |
| RFC 3262 | Reliability of Provisional Responses in Session Initiation Protocol (SIP) | M | R | - |
| RFC 3263 | Session Initiation Protocol (SIP): Location SIP Servers | M | M | M |
| RFC 3264 | An Offer/Answer Model with Session Description Protocol (SDP) | M | M | - |
| RFC 3311 | The Session Initiation Protocol (SIP) UPDATE Method | M | R | - |
| RFC 3323 | A Privacy Mechanism for the Session Initiation Protocol (SIP) | M | R | M |
| RFC 3324 | Short Term Requirements for Network Asserted Identity | M | R | M |
| RFC 3325 | Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity with Trusted Networks | M | R | M |
| RFC 3489 | STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) | - | R | - |
| RFC 3581 | An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing | M | R | M |
| RFC 3725 | Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP) | M | R (RO) | - |
| RFC 4028 | Session Timers in the Session Initiation Protocol (SIP) | R | R | - |

**Legende**
M: MANDATORY (Senden und Empfangen)
R: RECOMMENDED (Senden und Empfangen)
R (RO): RECOMMENDED (mind. für Emfangen)
SAS: SIP Application Server
SPS: SIP Proxy Server
- nicht erforderlich / n/a

Abbildung 3.2: Standard-Unterstützung mit SIPconnect v1.0

die Spezifikation der Verbindung zwischen SAS und SGW sowie SAS und TGW (in Abbildung 3.1 mit Fragezeichen markiert) hat sich SIPconnect v1.0 herumgedrückt. Diese Verbindungen bleiben also Sache des Providers.

**Voraussetzungen und Abgrenzungen**

SIPconnect führt eine Reihe von IETF und ITU-T Spezifikationen an, die genutzt werden sollten, um die Anforderungen für die Verbindung zwischen der Enterprise IP PBX auf der einen Seite und dem Service Provider auf der anderen Seite zu erfüllen. Hierbei wird jedoch kein spezielles SIP Profil festgeschrieben: Im Rahmen der SIPconnect Empfehlung darf sich keine Seite darauf verlassen, dass die Gegenseite ein spezielles Feature oder eine Option unterstützt, selbst wenn dies in der Empfehlung als mandatory aufgeführt wird. Stattdessen muss sichergestellt werden, dass jede übliche SIP Erweiterung und alle Auswahlverfahren weiterhin von einer Gegenseite genutzt werden können.

Allerdings legt die SIPconnect Empfehlung einige Annahmen und Abgrenzungen fest:

1. Der hauptsächliche Dienst, der über die definierte Schnittstelle geleistet wird, ist Aufbau und Terminierung von Audio-Calls, insbesondere zu und von PSTN-Zielen.

2. Für alle mandatory Komponenten der Referenzarchitektur, die für die Enterprise und Provider Netzwerke spezifiziert werden, sind funktionierende Produkte im Markt verfügbar.

3. Die Signalisierung zwischen SIP Applikationsserver, Trunking Gateway und Signalisierungs-Gateway ist in dieser Empfehlung out of scope.

4. Die Signalisierung zwischen IP PBX und anderen Enterprise Geräten (z.B. IP Telefonen) ist in dieser Empfehlung out of scope.

5. Sowohl das Unternehmen als auch der Service Provider betreiben öffentlich zugreifbare DNS Server, die für eine oder mehrere Internet Domänen zuständig sind. Alternativ kann der Service Privider eine Subdomäne seiner eigenen Domäne an das Unternehmen delegieren und zur Nutzung zur Verfügung stellen.

6. Das Enterprise Netzwerk besitzt mindestens eine zugewiesene E.164 Adresse, die im PSTN-Netz zum Signalisierungs-Gateway des Service Providers geroutet wird.

7. Notruf-Aspekte in Verbindung mit mobilen SIP Endgeräten / Nutzern, z.B. das Routing zu nationalen Notrufnummern wie 110, 112, 911, 999, 000, sind in dieser Empfehlung out of scope.

8. Layer-3 Netzdesign, QoS-Überlegungen innerhalb eines Netzwerks und Voraussetzungen für QoS (wie RSVP) sind in dieser Empfehlung out of scope.

9. Element Management, Netzwerkmanagement, Netzwerksicherheit und OSS Überlegungen sind in dieser Empfehlung out of scope.

### 3.3 Empfehlungen zur Arbeitsweise der Komponenten

SIPconnect konzentriert die Empfehlungen auf einige wichtige Bereiche, die für Basisdienste und Basis-Kompatibilität unerlässlich sind:

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

- Lokalisierung
- Sicherheit
- Gestaltung des SIP URI
- QoS und Media Handhabung

In der nachfolgenden Darstellung verwenden wir die allgemeinen Standardisierung-Begriffe in deutscher Form: MUST = muss, SHOULD = sollte, SHALL = soll, MAY = kann, RECOMMENDED = empfohlen.

**Lokalisierung**

Die Sicherstellung des öffentlich zugreifbaren DNS-Dienstes ist für Enterprise und Provider zwingend erforderlich (MUST). Dabei müssen SRV Records und sollten NAPTR Records unterstützt werden.

Der Enterprise Betreiber MUSS sicherstellen, dass Gespräche, die zwecks Terminierung zum Provider geroutet werden sollen, auf jeden Fall an den SIP Proxy Server des Enterprise Kunden weitergeleitet werden. Umgekehrt MUSS der Provider sicherstellen, dass Gespräche, die beim Enterprise Kunden terminiert werden sollen, zum SIP Proxy Server des Providers weitergeleitet werden.

Damit diese Gespräche ordentlich funktionieren, muss folglich sichergestellt sein, dass der Enterprise SIP Proxy und der Provider SIP Proxy sich gegenseitig finden. Ein Enterprise SIP Proxy Server, der seinen Provider SIP Proxy Server sucht, muss dies mittels DNS SRV und NAPTR Queries tun, er darf sich nicht ausschließlich auf statische Konfigurationen abstützen. Gleiches gilt umgekehrt für den Provider SIP Proxy, der den Enterprise SIP Proxy sucht.

Optional darf die Enterprise PBX eine Kontaktadresse in Form eines oder mehrerer SIP URIs am SIP Application Server des Providers registrieren; sie ist aber nicht dazu verpflichtet. In jedem Fall gilt: Falls der Enterprise Kunde einen SIP URI am SAS registriert, muss diese URI mit der Domäne des Providers assoziiert sein – ansonsten würde das Routing nicht korrekt funktionieren oder entstünde ein wildes Gewirr von URI-Querverweisen der Provider untereinander. Der SIP Application Server eines Providers MUSS im Gegenzug in der Lage sein, Registrierungen für jede beliebige gültige SIP URI durchzuführen, die der Service Provider einem Enterprise-Kunden zugewiesen hat. Zwar schreibt SIPconnect an dieser Stelle keine Aktion vor, die mit einer erfolgreichen Registrierung getriggert wird, es wird aber explizit angemerkt, dass ein nützlicher Umgang mit Registrierungen das Update der eigenen DNS-Einträge ist, die mit der Enterprise IP PBX assoziiert sind.

**Der SIP URI - die neue Telefonnummer**

SIPconnect v1.0 mappt jede E.164 Adresse (d.h. internationale Telefonnummer) auf eine eigene „PSTN Identität“. Das bedeutet, eine IP PBX mit 100 Nebenstellen wird mit 100 PSTN Identities assoziiert. In diesem Sinne muss die IP PBX auf Einzelgesprächsbasis entscheiden, welche PSTN Identität sie nutzt. Erfolgt ein ausgehender Anruf von einem Benutzer, der keine eigene Telefonnummer (DID) hat, kann die PBX ihre „Haupt-Identität“ (im Regelfall die Amtskopf-Nummer) benutzen. Da die Verbindungen über SIP Trunking laufen, muss offensichtlich an irgendeiner Stelle eine Konvertierung von E.164 Adressen auf SIP URI‘s erfolgen. Diese Stelle ist üblicherweise der SIP Application Server, der eine Mapping Tabelle für jede Enterprise Domäne und die zugehörigen E.164 Adressen hält. Die Mapping Tabelle kann auch ausgelagert werden, beispielsweise auf eine externe ENUM Datenbank (RFC 3761).

Jede Komponente, die SIP Signalisierung handhabt, MUSS bei SIPconnect Adress-Schemata für geschlossene Nummernpläne (mit fixer Nummernlänge) und offene Nummernpläne (mit variabler Nummernlänge) unterstützen. Wie werden nun die PSTN Nummern (Identities) dem SAS des Providers mitgeteilt? Hier gibt es zwei Optionen. Option 1 ist (noch) die bevorzugte Option und sollte (SHOULD) von der IP PBX unterstützt werden, Option 2 wird als nachrangig eingestuft, aber sie MUSS von der IP PBX unterstützt werden (größter gemeinsamer Nenner). SIP Applikationsserver des Providers müssen beide Optionen unterstützen.

Option 1 nutzt die SIP Header ‚From:‘ in Verbindung mit ‚P-asserted-Identity:‘ (nach RFC 3325). So kann das Unternehmen dem SIP Provider je Gespräch eine „öffentliche“ und eine „private“ PSTN-Kennung übermitteln.

Die öffentliche Kennung ist diejenige, die der SIP Provider für das Gespräch ins PSTN bzw. zum Gegenteilnehmer signalisieren soll. Der Option 1 entsprechend enthält der ‚From:‘ Header die gewünschte öffentliche Kennung – üblicherweise ist dies die Amtskopf-Nummer – oder aber einen „anonymen URI“ nach RFC 3325.

Die private Kennung ist diejenige, die der Enterprise-Kunde ausschließlich dem Provider übermitteln will. In diesem Sinn wird der Enterprise SIP Proxy Server nach RFC 3325 als ein Teil der „Trust Domäne“ des SIP Providers betrachtet. Als besonders wichtig wird betont, dass der SAS Server des SIP Providers diese private Kennung ausschließlich für Abrechnungszwecke und/oder Priorisierungen, Bereitstellung von Diensten / Funktionen etc. nutzen darf, die der Enterprise Kunde vertraglich abgeschlossen hat. Routet der SAS das Gespräch zu irgendeiner Komponente im Providernetz, die den RFC 3325 nicht unterstützt, so MUSS diese Komponente als außerhalb der Trust Domäne betrachtet werden, d.h. der SAS darf dieser Komponente keinesfalls die private Kennung des Enterprise Kunden offenlegen oder irgendeine (Teil-)Information aus dem ‚P-Asserted-Identity:‘ Header zugänglich machen. Im Gegenteil, der SAS muss sogar alle ‚P-Asserted-Identity:‘ Headerfelder lö-

schen und ebenso die Headerfelder, die diese Privacy anfordern.

Wird Option 1 genutzt, so MÜSSEN alle INVITEs, die an den SIP Provider gesendet werden, nach folgenden drei Regeln formatiert werden:

1. Im ‚From:' Feld muss der URI stehen, der mit der gewünschten öffentlichen PSTN-Kennung assoziiert ist (möglich ist auch ein anonymer URI der Form <anonymous@[domain name]>. Dabei SOLLTE die IP PBX möglichst auch eine Namensanzeige für das Empfängerdisplay bereitstellen (z.B. Phantasialand Marketing) - diese Forderung ist jedoch nicht mandatory.

2. Die IP PBX muss ein ‚Privacy:' Headerfeld einfügen, das Vertraulichkeit der Kennung nach RFC 3325 anfragt.

3. Die IP PBX muss den ‚P-Asserted-Identity:' Header passend ausfüllen, in erster Präferenz nach ITU-T E.164 Format zuzüglich Enterprise Domänenname; in zweiter Präferenz nach RFC 3261 und einem URI Format, das zwischen Enterprise und Provider abgestimmt ist.

Zwei Beispiele für INVITEs, die der Option 1 entsprechen, sind nachfolgend aufgeführt. Eines nutzt das ITU-T E.164 Format, das andere ein RFC 3261-konformes URI Format

```
INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bKl54j1
From: „Acme Rockets Sales“ <sip:+16789901234@acmerockets.com;user=phone>;tag=1648468
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 502848105829482738
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
P-Asserted-Identity: „John Doe“ <sip:+16789902000@acmerockets.com;user=phone>
```

```
INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bK9kj2b
From: „Acme Rockets Sales“ <sip:sales@acmerockets.com>;tag=0323873
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 830284710729349284
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
P-Asserted-Identity: „John Doe“ <sip:johndoe@acmerockets.com>
```

Option 2 nutzt ausschließlich den ‚From:' Header, wie in RFC 3261 beschrieben. Diese Option ermöglicht natürlich insgesamt weniger Flexibilität, da für ein Gespräch nur eine einzige Kennung an den Service Provider übermittelt wird. Diese eine Kennung nutzt der Provider dann als öffentliche und ebenso als private Kennung. Der ‚From:' Header muss in diesem Fall eine SIP URI enthalten, in dem die gewünschte öffentliche PSTN-Kennung steht. Hat der Anrufer keine eigene Kennung, sollte die „Haupt-Kennung" (Amtskopfnummer) der IP PBX genutzt werden. Die Formate sind genau so wie bei Option 1, allerdings fehlen die Zeilen ‚Privacy' und ‚P-Asserted-Identity'.

Eine logische Betrachtungsweise legt nahe, dass Inhalt und Format des ‚To:' Headers ebenfalls mit SIP URIs und E.164 Nummern ausgefüllt werden. Beide Optionen sind aufgeführt; die Enterprise Seite muss mindestens eine Option unterstützen, die Provider Seite (d.h. der SAS) MUSS beide Optionen unterstützen.

Option 1:
To: <sip: + **[E.164 Adrese] @ [Service Provider Domänenname]** ; user=phone>

Option 2:
To: <tel: + **[E.164 Adrese]** >

Notruf-Format:
To: <sip: **[Landesspezifische Notrufnummer]**; phone-context= **[Vordefinierte Geografische E.164 Adresse] @ [Service Provider Domänenname]**; user=phone>

An diesem Punkt stellt sich die Frage, wie der ‚To:' Header eines Notrufs auszufüllen ist. SIPconnect empfiehlt hier, dass der SIP Service Provider die Terminierung von Notrufen für eine oder mehrere feste physikalische / geographische Lokationen (Standorte) unterstützt, die von der Enterprise IP PBX bedient werden. Für jede dieser Lokationen sollen Enterprise und Provider sich gegenseitig auf eine E.164 Nummer einigen, die bei Notrufen aus diesem Standort verwendet wird. Diese E.164 Nummern SOLLTEN dann genutzt werden, um sowohl den Notruf an eine geeignete Leitstelle (PSAP) zu routen als auch die für die Leitstelle notwendigen Ortsinformationen für die Leitstelle einzufügen. Dabei sollte (SHOULD) das nachfolgende Notruf-Format eingehalten werden.

**Sicherheit**

SIP Proxy Server müssen TLS nach RFC 2246 und TLS für SIP nach RFC 3261 unterstützen und die Signalisierung zwischen Enterprise und Provider SIP Proxy Servern zwingend mit TLS sichern. Jede Seite (Enterprise und Provider) muss in der Lage sein, eine TLS-gesicherte Verbindung aufzubauen. Dabei müssen sie für Einträge in die SIP Header Felder ‚Via:' und/oder ‚Route:' kanonische Hostnamen verwenden.

Sofern Zertifikate für die Einrichtung einer TLS-Session genutzt werden, MÜSSEN diese geprüft und KÖNNEN validiert werden. Die Überprüfung beinhaltet die Sicherstellung, dass

- das Zertifikat nicht abgelaufen ist,
- die sendende Zertifikatstelle eine ist, der der SIP Proxy Server vertraut und
- der Zertifikat-Inhalt mit dem Hostteil der Ziel-URI übereinstimmt.

Die Validierung beinhaltet einen Status Check des Zertifikats ebenso wie einen Status Check aller Zertifikate in der Zertifikat-Kette mittels CRLs oder mittels anderer Verfahren wie OCSP (RFC 2560).

Sofern der Service Provider eine lokale Sicherheitsregelung hat, dürfen optional auch Enterprise Zertifikate zum Einsatz kommen, die nicht durch eine vertrauenswürdige Zertifikatsstelle gegengezeichnet sondern eigengezeichnet sind. Dies gilt nicht für Service Provider Zertifikate, diese sollten stets durch eine 3rd Party Zertifikatsstelle gegengezeichnet sein.

SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen

Für NAT und FW Traversal gilt: Alle IP Adressen in SIP Headern und Message Bodies, die zwischen Enterprise und Service Provider weitergeleitet werden, MÜSSEN öffentlich routbare Adressen sein. Dies impliziert, dass jegliche für NAT Traversal etwa erforderliche „Behelfsfunktion“ sie STUN, TURN, ICE durchgeführt wurde, bevor die Nachricht den Enterprise / Provider Netzübergang passiert. Solche Behelfsfunktionen können von den beteiligten Endgeräten oder von anderen Netzkomponenten (SIP-aware Firewall, Session Border Controller etc.) ausgeführt werden. SIP Proxies hingegen dürfen definitiv in keinem Fall IP Adressen oder Portnummern im SIP Contact Header oder SIP Body ändern.

Für die Authentifizierung wurden zwei Alternativen zugelassen. Option 1 sind TLS Credentials; diese Option muss unterstützt werden und beruht auf der Überprüfung der Kennung, die in dem bei Einrichtung der TLS-Session geprüften Zertifikat eingefügt wurde. Sie erfordert, dass der SIP Proxy Server und SIP Application Server des Providers Autorisierungs-, Accounting- und Nutzungsinformationen auf Einzelgesprächs-Basis austauschen können, um sicherzustellen, dass sich die Abrechnungsinformationen durch das komplette Netzwerk hindurch tracen lassen.

Option 2 ist eine Digest Access Authentifizierung; diese Option KANN unterstützt werden. Sie nutzt eine Digest Authentifizierung wie in RFC 3261 beschrieben. Hier weist der Service Provider dem Enterprise Netzwerk Benutzernamen und Passwort zu, „Netzwerk Account“ genannt, der innerhalb der Service Provider Domäne gültig ist. An dieser Stelle sei nochmals angemerkt, dass die Nutzung eines Digest Authentifizierungsverfahrens nicht die Anforderung aufhebt, TLS zwischen Enterprise und Service Provider Netzwerk zu nutzen. Erfolgt von einer nicht-authentifizierten Enterprise IP PBX ein INVITE oder ein REGISTER, so muss der SAS diese Nachricht überprüfen, indem er gültige Authentifizierungs-Informationen von der IP PBX anfordert. Erhält die IP PBX auf ein INVITE oder REGISTER hin eine Überprüfung (Challenge), so muss sie mit den gültigen Authentifizierungs-Informationen antworten (d.h. mit dem Netzwerk Account, den der Service Provider zugewiesen hat). Um unnötigen Overhead zu vermeiden, wird empfohlen, dass die IP PBX diese Informationen schon vorab in jeden Request einfügt, den sie an den SIP Application Server sendet.

**Fortsetzung folgt!**

**Abkürzungen**

| | |
|---|---|
| A/V | Audio / Video |
| ABC | Alcatel Business Communication |
| ALG | Application Layer Gateway |
| AS | Application Sharing |
| BRI | Basic Rate Interface |
| CAC | Call Admission Control |
| CorNet | Corporate Network (Siemens, ISDN) |
| CRL | Certificate Revocation List |
| DCS | Distributed Communication System |
| DID | Direct Inward Dial |
| DNS | Domain Name Service |
| ENUM | Electonic NUMbering; E.164 Number and DNS (RFC 2916) |
| FQDN | Fully Qualified Domain Name |
| FW | Firewall |
| GW | Gateway |
| ICE | Interactive Connectivity Establishment |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| ITSP | Internet Telephony Service Provider |
| ITU-T | International Telecommunication Union-Telecommunication Standards |
| LCR | Least Cost Routing |
| MCDN | Meridian Customer Defined Network (Nortel) |
| NAT | Network Address Translation |
| OCSP | Online Certificate Status Protocol |
| OSS | Operations Support System |
| PBX | Private Branch eXchange |
| PRI | Primary Rate Interface |
| PSAP | Public Saftety Answering Point |
| PSTN | Public Switched Telephony Network |
| QoS | Quality of Service |
| QSIG | Q-interface SIGnalling protocol |
| RFC | Request for Comment |
| RSTP | Rapid Spanning Tree Protocol |
| RTC | Real Time Communications |
| RTCP | Real Time Control Protocol |
| SAS | SIP Application Server |
| SBC | Session Border Controller |
| SCCP | Skinny Client Control Protocol |
| SDP | Session Description Protocol |
| SGW | Signaling Gateway |
| SIMPLE | SIP for Instant Messaging and Presence Leveraging Extensions |
| SIP | Session Initiation Protocol |
| SPS | SIP Proxy Server |
| SRTP | Secure RTP |
| SS7 | Signaling System #7 / Signalisierungssystem Nummer 7 |
| STUN | Simple Traversal od UDP over NATs |
| TCP | Transmission Control Protocol |
| TDM | Time Division Multiplexing |
| TGW | Trunking Gateway |
| TLS | Transport Layer Security |
| TURN | Traversal Using Relay NAT |
| URI | Universal Resource Identificator |
| VLAN | Virtual LAN |
| VoIP | Voice over IP |
| WAN | Wide Area Network |

**Links**

**Mitglieder des SIP Forums**

www.3com.com
www.acmepacket.com
www.alcatel-lucent.com
www.aricent.com
www.aspect.com
www.audiocodes.com
www.avaya.com
www.bandwidth.com
www.bea.com
www.bluenotenetworks.com
www.broadsoft.com
www.cablelabs.com
www.cbeyond.com
www.cgi.com
www.cisco.com
www.covergence.com
www.coxbusiness.com
www.dataconnection.com
www.dialogic.com
www.digium.com
www.ericsson.com
www.hp.com
www.ibm.com
www.ietf.org
www.ingate.com
www.intertexdata.com
www.iol.unh.edu
www.ipunity-glenayre.com
www.mcleodusa.com
www.microsoft.com/uc
www.net.com
www.neustar.biz
www.nextpointnetworks.com
www.nokia.com
www.oracle.com
www.polycom.com
www.radvision.com
www.rfc-editor.org/rfcsearch.html
www.siemens.com
www.sipforum.org
www.snom.com
www.solinet.com
www.sonusnet.com
www.tandberg.com
www.tecnomen.com
www.tekelec.com
www.telsis.com
www.utstar.com
www.wipro.com

**Literatur**

Ingate Systems / Janne Magnusson:
SIP Trunking Benefits and Best Practices; 2006

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

### Sicherheit im LAN mit IEEE 802.1X, 08.09. - 09.09.08 in Bonn

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

### IP-Wissen für TK-Mitarbeiter, 08.09. - 09.09.08 in Bonn

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Preis: € 1.390,- zzgl. MwSt.

### Trouble Shooting in vernetzten Infrastrukturen, 09.09. - 12.09.08 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege. Preis: € 2.190,- zzgl. MwSt.

### Projekt-Erfahrungsbericht: Cisco CallManager Rollout und Migration CUCM Version 6, 15.09. - 16.09.08 in Aachen

Dieses 2-tägige Seminar beschreibt Planung, Installation und den Betrieb einer großen verteilten IP-Telefonie-Lösung auf der Basis des Cisco CallManagers. Es macht deutlich, in welchem Umfang die Standard-Installation angepasst und erweitert werden musste, um den Anforderungen der Teilnehmer zu entsprechen. Auch die Umstellung traditioneller Betriebsabläufe im Änderungs-Management und deren Auswirkung auf die Konfiguration des CallManagers wird beschrieben. In diesem Zusammenhang werden insbesondere auf die Akzeptanz der Benutzer und die damit notwendigen Änderungen in der Bedienung der Telefone eingegangen.

Preis: € 1.390,- zzgl. MwSt.

### SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 15.09. - 17.09.08 in Frankfurt a.M.

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Preis: € 1.690,- zzgl. MwSt.

### Lokale Netze für Einsteiger, 15.09. - 19.09.08 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt. Preis: € 2.290,- zzgl. MwSt.

### Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 22.09. - 26.09.08 in Bonn

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

### IP-Telefonie: Vorbereitung, Migration, Management, 13.10. - 15.10.08 in Bonn

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Diesem Ziel dient das Seminar.

Preis: € 1.690,- zzgl. MwSt.

### Internetworking: optimales Netzwerk-Design mit Switching und Routing, 13.10. - 17.10.08 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können. Preis: € 2.290,- zzgl. MwSt.

Zertifizierungen

## ComConsult Certified Network Engineer

**Lokale Netze**
15.09. - 19.09.08 in Aachen
24.11. - 28.11.08 in Aachen
02.03. - 06.03.09 in Aachen
11.05. - 15.05.09 in Aachen
31.08. - 04.09.09 in Frankfurt
23.11. - 27.11.09 in Hamburg

**TCP/IP und SNMP**
20.10. - 24.10.08 in Berlin
16.02. - 20.02.09 in Bonn
25.05. - 29.05.09 in Aachen
21.09. - 25.09.09 in Bonn

**Internetworking**
13.10. - 17.10.08 in Aachen
09.02. - 13.02.09 in Aachen
11.05. - 15.05.09 in Aachen
05.10. - 09.10.09 in Frankfurt

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

## ComConsult Certified Trouble Shooter

**Trouble Shooting in vernetzten Infrastrukturen**
09.09. - 12.09.08 in Aachen
03.02. - 06.02.09 in Aachen
05.05. - 08.05.09 in Aachen
06.10. - 09.10.09 in Aachen

**Trouble Shooting für Netzwerk-Anwendungen**
14.10. - 17.10.08 in Aachen
17.03. - 20.03.09 in Aachen
16.06. - 19.06.09 in Aachen
03.11. - 06.11.09 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt.
(Einzelpreise: je € 2.190.--)

## ComConsult Certified Security Expert

**Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit**
22.09. - 26.09.08 in Bonn
09.02. - 13.02.09 in Hamburg
14.09. - 18.09.09 in Köln

**Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten**
03.11. - 07.11.08 in Bonn
30.03. - 03.04.09 in Berlin
26.10. - 30.10.09 in Aachen

**Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs**
01.12. - 05.12.08 in Aachen
22.06. - 26.06.09 in Aachen
23.11. - 27.11.09 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

## ComConsult Certified Voice Engineer

**Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie**
15.09. - 17.09.08 in Frankfurt
17.11. - 19.11.08 in Frankfurt
30.03. - 01.04.09 in Berlin
15.06. - 17.06.09 in Stuttgart
28.09. - 30.09.09 in Bad Neuenahr
23.11. - 25.11.09 in Hamburg

**Basis-Seminar: Sicherheitsmechanismen für Voice over IP**
03.11. - 04.11.08 in Bonn
09.02. - 10.02.09 in Hamburg
14.05. - 15.05.09 in Bonn
05.10. - 06.10.09 in Frankfurt

**Alternative 1: IP-Telefonie evaluieren, planen, betreiben**
27.10. - 29.10.08 in Bonn
02.03. - 04.03.09 in Stuttgart
25.05. - 27.05.09 in Hamburg
14.09. - 16.09.09 in Köln
02.11. - 04.11.09 in Frankfurt

**Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management**
13.10. - 15.10.08 in Bonn
16.02. - 18.02.09 in Bonn
15.06. - 17.06.09 in Stuttgart
26.10. - 28.10.09 in Berlin

**Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter**
08.09. - 09.09.08 in Bonn
17.11. - 18.11.08 in Frankfurt
02.02. - 03.02.09 in Bonn
04.05. - 05.05.09 in Königswinter
07.09. - 08.09.09 in Aachen
09.11. - 10.11.09 in Königswinter

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie