VAF REPORT

Informationen für **mittelständische Systemhäuser**

Mitgliedermagazin 1/2016

Pflicht oder Kür?

Sicherheit im SIP-Trunk, TK-Anlagen und E-SBC

Seite 12

Foto: © www.shutterstock.com

Fax-over-IP

Update zur Standort-bestimmung Seite 20

USV und VoIP

Telefonieren bei Stromausfall Seite 22

Installationskabel

Neue Anforderungen aus der BauPVo Seite 24

Unified Communications by innovaphone

Verbessern Sie ihre Erreichbarkeit, steigern Sie ihre Effizienz und beschleunigen Sie Geschäftsprozesse! All dies ist nur durch eine vereinheitlichte und integrierte Kommunikationsstruktur möglich. Unified Communications by innovaphone bietet genau dies. Die Unified Communications Lösung wird perfekt in die innovaphone PBX, eine leistungsstarke und durchdachte VoIP Telefonanlage, integriert. Verschiedene Unified Communications Bausteine machen aus der innovaphone PBX eine ausgereifte und dabei immer noch schlanke Kommunikationskomplettlösung.

myPBX

Einfach, übersichtlich und intuitiv– das ist der Unified Communications Client myPBX

- Steuerung aller denkbaren Endgeräte
- Vereint verschiedene Unified Communications Elemente wie Audiokonferenzen, Firmenverzeichnisse, Presence-Angaben, Instant Messaging, Application Sharing, Videotelefonie oder -konferenzen – egal ob vom Büro, Homeoffice oder von unterwegs

Video

Einfache und schlanke Video-Lösung

- Unkomplizierte Ad-hoc Videotelefonie
- 3er Videokonferenzen und Multi-User Videokonferenzen ohne seperate MCU
- Niedrige Implementierungskosten und geringer Bandbreitenbedarf

Fax

Schnelles und unkompliziertes Faxen

- Schnell und unkompliziert vom eigenen PC versenden, auch mobil von unterwegs
- Mail Client fungiert dabei als Faxgerät und macht Mail-to-Fax oder aber Fax-to-Mail möglich

Office Integration

Die Verfügbarkeit von Kollegen oder Geschäftspartnern stets im Blick haben

- Verbessert und beschleunigt Kommunikation
- Verschiedene Presence-Informationen werden zu einer einzigen Presence-Information gebündelt
- Übersichtliche und verständliche Darstellung

Mobile Integration

Immer und überall unter nur einer Rufnummer erreichbar sein

- Von unterwegs aus alle Leistungsmerkmale der Telefonanlage nutzbar
- Integriert Mobiltelefone als interne Teilnehmer und macht sie somit zur vollwertigen Nebenstelle

Voicemail

Immer ansprechbar und erreichbar sein

- Kein Anruf geht mehr verloren
- Professionelle, integrierte, serverunabhängige und netzwerkweit verfügbare VoiceMail-Lösung
- Für alle Teilnehmer der innovaphone PBX anwendbar

Application Sharing

Macht das Zusammenarbeiten so effizient und einfach wie noch nie

- Keine Installation, Anwahl und Authentifizierung notwendig
- Ausgewählten Inhalt des Bildschirms an Kollegen freigeben
- Funktioniert auch in Konferenzen

WebRTC

Einfachste Kundenansprache mit dem „Call Me Button"

- Ein Klick auf den Anrufbutton genügt und der Kunde ist mit dem Ansprechpartner seiner Wahl verbunden
- Mit wenig Aufwand lässt sich der „Call Me Button" in jede Website integrieren und dank Java Script perfekt an das firmeneigene Corporate Design anpassen
- Der Präsenzstatus der Mitarbeiter, die im „Call Me Button" hinterlegt sind, ist in Echtzeit auf der Website zu sehen.

Weitere Infos:
www.innovaphone.com

innovaphone
PURE IP COMMUNICATIONS

EDITORIAL

Hans A. Becker
1. Vorsitzender,
VAF Bundesverband
Telekommunikation

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

der Wechsel von der ISDN-Welt hin zu einer IP-basierten Technologiewelt ist in vollem Gange. Dies bringt für unsere Kunden und auch für uns zahlreiche neue Herausforderungen. Ich bin aber der festen Überzeugung, dass die Chancen für uns als ITK-Systemhausbranche die von manchen in den Vordergrund gestellten Risiken deutlich überwiegen. Schätzungen zufolge müssen noch rund eine Million Anschlussgeräte für die Alarmübertragung getauscht werden. Dies zeigt lediglich als Schlaglicht, an wie vielen Stellen unsere Leistungen gefragt sind.

Noch viel mehr gilt das für unser angestammtes Kerngeschäft, die professionelle Telekommunikation. Der Bericht zum aktuellen VAF-Programm im Fachbereich ITK-Technik und weitere Beiträge in diesem Heft zeigen, dass der VAF und seine Mitglieder »nah dran« sind, und dass wir die Herausforderungen annehmen.

Jetzt presst die Telekom mit ihrem Marketingmantra »Ende ISDN 2018« das Thema im Markt massiv voran. Bisher sind es allerdings die Wettbewerber des Ex-Monopolisten, die mit ihren SIP-Trunks die neuen Anschlussprodukte bereitstellen. Der Beratungsbedarf ist groß, manches steckt auch noch in den Kinderschuhen. Ein Beispiel ist die derzeit höchst kontroverse Diskussion zu den Sicherheitsanforderungen an SIP-Trunks sowie zur Rolle von SBCs. Mit dem entsprechenden Themenschwerpunkt dieses Heftes möchten wir einen Beitrag zur Versachlichung der Diskussion leisten.

VERBANDSNACHRICHTEN

AUS DEM MITGLIEDERKREIS

FACHBEITRÄGE

PRODUKTE & LÖSUNGEN

SERVICE

Fachausschuss ITK-Technik

Programmplanung im Zeichen der IP-Transformation

Am 25. Februar tagte der Fachausschuss ITK-Technik mit Vertretern aus Mitgliedsunternehmen in der VAF-Geschäftsstelle in Hilden. Auf der Sitzung wurden die Schwerpunkte für die aktuelle Arbeit des VAF im Fachbereich geplant. Zu den Ergebnissen wird hier kurz berichtet. Das derzeit vorherrschende Thema ist die All-IP-Transformation.

Schnittstellenbeschreibungen: Als gravierender Missstand wurde die oftmals unzureichende Bereitstellung technischer Spezifikationen von SIP-Trunk-Schnittstellen durch die Provider gesehen. Fehlende, veraltete oder unvollständige Spezifikationen erschweren die stark zunehmenden SIP-Anschaltvorgänge erheblich. Darum sollte – so ein Ergebnis im VAF-Ausschuss – insbesondere bei der Bundesnetzagentur für geeignete Maßnahmen zur Verbesserung der Auskunftslage durch die Provider geworben werden.

Neutrales SIP-Trunking-Know-how: Die sehr heterogene Ausprägung von SIP-Trunks erfordert ein solides Verständnis der providerunabhängigen SIP-Grundlagen. Erst auf einer neutralen Wissensgrundlage lassen sich Angebote vergleichen und technisch verlässlich bewerten. Der VAF ist darum aufgefordert, sein Schulungsprogramm umfassend und strukturiert auszubauen. Dazu gehören insbesondere auch Fragen rund um das Testen, Überwachen und Troubleshooting von VoIP-Strecken (Ende-zu-Ende).

Messprojekt wird fortgesetzt: Die unter Leitung von Prof. Dr. Gerd Siegmund und mit Unterstützung von Mitgliedern stattfindenden Netzwerkmessungen sollen voraussichtlich ab Sommer dieses Jahres fortgesetzt werden. Der Zweck der Analysen ist die Ermittlung typischer Verkehrsprofile (VoIP/Video/Daten) in realen Netzen. Aufgrund der aktuellen Weiterentwicklung der bisherigen Testmittel kann zudem mit einer deutlichen Effizienzsteigerung in der Durchführung der Feldmessungen gerechnet werden. Interessierte Mitglieder können an dem Projekt mitwirken, und Informationen werden vorab an alle Mitglieder versandt.

ITK-Sicherheit: Des Weiteren wurde auf der Sitzung diskutiert, wie der immer stärkeren Relevanz von Fragen der ITK-Sicherheit durch ganzheitliche Lösungskonzepte Rechnung getragen werden kann. In der praktisch orientierten Konzeptausarbeitung soll darum ein weiterer Schwerpunkt der Facharbeit liegen.

PacketRaptor: Einen weiteren Punkt der Agenda bildete die Vorstellung des seinerzeit vom VAF mitentwickelten Test- und Aufzeichnungsgeräts »PacketRaptor«. Das Gerät wird von der Nextragen GmbH hergestellt und jetzt in einer zweiten Version mit leistungsfähigerer Hardware herausgebracht. ■

Weitere Informationen

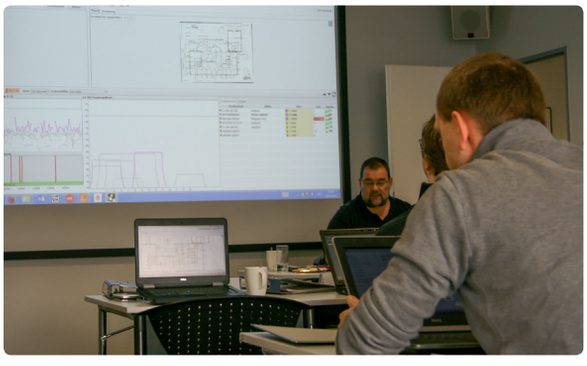
VAF-Mitglieder, die an weiteren Auskünften oder an Möglichkeiten der Mitwirkung interessiert sind, können sich an die VAF-Geschäftsstelle wenden: **info@vaf-ev.de, Tel.: 02103 700-250**

VAF-Wissenswerkstatt

Technische Schulungen **stark nachgefragt**

Das Jahr 2016 hat mit einer deutlichen Nachfragesteigerung im Bereich der technischen Schulungen begonnen. Besonders gefragt waren im ersten Quartal der sechstägige Grundlagenkurs zur Netzwerktechnik und der zweitägige Fortgeschrittenenkurs zur Planung und Dokumentation von WLANs mit der Profisoftware von ekahau.

Wichtiger Bestandteil des Kurses zur WLAN-Praxis: Im Sinne der Abarbeitung eines kompletten Kundenauftrags analysieren die Schulungsteilnehmer das vorhandene Funknetz im Schulungsgebäude. ■



Fotos: VAF

ATRT-Informationsveranstaltung Ende ISDN

Sicherheitstechnische Anwendungen

Foto: ATRT

Der große Sitzungssaal der Bundesnetzagentur in Mainz war bis auf den letzten Platz gefüllt.

ATRT
Der Ausschuss für technische Regulierung in der Telekommunikation ist ein unabhängiger, beratender Ausschuss für die Bundesnetzagentur.
www.bundesnetzagentur.de

Am 02. Februar 2016 veranstaltete der Ausschuss ATRT zusammen mit der Bundesnetzagentur in Mainz die öffentliche Informationsveranstaltung »Sicherheitstechnische Anwendungen – Migration spezifischer Sonderdienste und IP-Migra-tion bei den Teilnehmeranschlüssen im Festnetz«. Die Tagung wurde von Dr. Wilhelm Eschweiler, Vizepräsident der Bundesnetzagentur, eröffnet. Branchen- und Anwendervertreter informierten zu den Perspektiven sowie Anforderungen der IP-Migration und diskutierten mit dem Publikum.

Wichtige Ergebnisse der Tagung können aus Sicht des VAF thesenartig zusammengefasst werden: In technischer und normativer Hinsicht sind die Möglichkeiten für den Wechsel der Alarmübertragung von ISDN auf All-IP gegeben; Umrüstungen im Bereich der Anschlusstechnik werden noch in vielen Bestandsinstallationen erforderlich sein; die sichere Stromversorgung von NGN-Übertragungsgeräten wird noch nicht von allen Experten als befriedigend eingestuft; geschäftliche und behördliche Anwender reklamieren insbesondere einen längeren Planungsvorlauf und Planungssicherheit.

Die Tagung wurde vom VAF mitorganisiert und in der Durchführung unterstützt. Auch VAF-Mitglieder nutzten die Veranstaltung, um sich einen kompakten Überblick zum Stand der Fachdiskussion zu verschaffen. Die Präsentationen stehen auf der Website der Bundesnetzagentur zur Verfügung. ■

ATRT-Personalie

Lenkungskreis wählt neuen Vorsitzenden

Seit Beginn des Jahres 2016 liegt der Vorsitz des ATRT-Lenkungskreises in den Händen des VAF-Geschäftsführers Martin Bürstenbinder.

Die Wahl erfolgte einstimmig auf der regulären Ausschusssitzung am 2. November 2015 in Bonn. Der Lenkungskreis besteht aus derzeit 16 Vertretern der Anwender- und Anbieterseite des TK-Markts. Darüber hinaus nehmen Spitzenvertreter der Bundesnetzagentur als ständige Gäste des Ausschusses sowie weitere Vertreter gemäß fachlicher Erfordernisse an den Sitzungen teil. Der Lenkungskreis formuliert Mandate für die Einrichtung von Arbeits- und Projektgruppen im Aufgabengebiet des ATRT, führt Aussprachen zu den erarbeiteten Berichten durch und beschließt darauf basierende Empfehlungen an die Bundesnetzagentur. ■

ATRT-Projektgruppe eingerichtet

Schnittstellenbeschreibungen gem. § 5 FTEG

Die technischen Beschreibungen von TK-Schnittstellen der öffentlichen Netzbetreiber müssen von diesen veröffentlicht werden. So verlangt es das Funk- und TK-Endgeräte Gesetz (FTEG) im § 5. Die Beschreibungen müssen den gesetzlichen Vorgaben zufolge sowohl umfassend und detailliert als auch aktuell sein. Nach Auffassung des VAF reicht die im Markt beobachtbare Veröffentlichungspraxis zu SIP-Trunk-Spezifikationen überwiegend nicht an das mit den gesetzlichen Anforderungen verbundene Mindestniveau heran. Der VAF hat sich darum an der Formulierung eines Projektvorschlags beteiligt, durch den nun Verbesserungen erreicht werden könnten. Im Zentrum des Projektvorhabens steht die Erstellung eines Leitfadens, der Netzbetreibern praxisnah darlegen soll, wie Schnittstellen im Sinne des Gesetzes geeignet veröffentlicht werden sollten. Das Mandat zur Erarbeitung des Leitfadens wurde am 15. Februar auf der Sitzung des ATRT-Lenkungskreises im Bonner Sitz der Behörde beschlossen und im Anschluss auf der Website der Bundesnetzagentur veröffentlicht. Die Projektgruppe befindet sich derzeit in der konstituierenden Phase. Der VAF hat seine Mitwirkung bereits erklärt. ■

Leistungswettbewerb 2015 des Deutschen Handwerks

Wir gratulieren den **Bundessiegern!**

▲ 1. Bundessieger: **Tobias Vancura,** Ausbildungsbetrieb NTA Systemhaus GmbH & Co. KG

▲ 2. Bundessieger: **Andreas Riesch,** Ausbildungsbetrieb MTG Kommunikations-Technik GmbH

An den bundesweiten Ausscheidungswettbewerben der Innungen, Handwerkskammern und Fachverbände zum Leistungswettbewerb beteiligen sich jährlich mehrere Tausend Gesellen. Wer sich auf der Landesebene behauptet hat, kann im Bundesleistungswettbewerb des Deutschen Handwerks erneut zum Wettstreit unter den Landessiegern seines jeweiligen Ausbildungsberufs antreten. Im Berufsfeld »Elektroniker, Fachrichtung Informations- und Telekommunikationstechnik« sicherten sich die beiden ersten Plätze zwei Nachwuchstalente, die ihre Ausbildung bei den VAF-Mitgliedsunternehmen NTA Systemhaus GmbH & Co. KG und MTG Kommunikations-Technik absolvierten. Unter der Schirmherrschaft des Bundespräsidenten Joachim Gauck erfolgte am 5. Dezember 2015 die Ehrung der ersten Bundessieger in Frankfurt. ■

BFE und VAF im Dialog

Führungskräftenachwuchs im Handwerk

Für TK-Fachunternehmen ist die Entwicklung des Führungskräftenachwuchses aus den eigenen Reihen ein wichtiges Instrument, gerade in Zeiten des Fachkräftemangels. Unverändert hat hier die Meisterausbildung einen hohen Stellenwert, auch wenn andere Qualifizierungswege heute in Konkurrenz dazu getreten sind, wie z. B. die Weiterbildung zum Techniker oder das (duale) Hochschulstudium. Meisterklassen mit dem Schwerpunkt Kommunikations- und Sicherheitstechnik kommen allerdings kaum noch zustande. Dies wissend, raten oftmals Kammern den Interessenten, auf einen anderen Zweig der elektrotechnischen Meisterausbildung zu wechseln. Ein Teufelskreis.

Thorsten Janßen ist Direktor des Bundestechnologiezentrums für Elektro- und Informationstechnik (BFE) in Oldenburg, einer der führenden Meisterschulen in Deutschland. Janßen nahm auf Einladung des VAF-Vorsitzenden Hans A. Becker an der Vorstandssitzung des VAF im Dezember 2015 teil. Gemeinsames Thema: Wie könnten künftig flexible Lösungen im Rahmen der Meisterausbildung für TK-Fachunternehmen gestaltet werden? Die bisher entwickelten Ansätze werden auf der diesjährigen Frühjahrstagung den Mitgliedern präsentiert und zur Diskussion gestellt. ■

▲ **Thorsten Janßen** (BFE) sucht nach neuen Wegen in der Meisterausbildung.

Korrektur

In der Ausgabe Nr. 2/2015 des VAF-Reports war auf Seite 16 die Aufschlüsselung der ISDN-PMx-Bestandszahlen falsch wiedergegeben. Wir bitten um Entschuldigung und drucken hier die korrekten Zahlen ab.

PMx-Anschlüsse, 2014 in Deutschland

Telekom:	**57.000**
Wettbewerber:	**30.000**

Quelle: Jahresbericht 2014 Bundesnetzagentur, Seite 76. Veröffentlicht 2015 ohne Datum. **www.bundesnetzagentur.de**

Vortrag im Rahmen der GFT-/VAF-Frühjahrstagung in Trier

Meisterausbildung am Scheideweg

Thorsten Janßen, Direktor BFE

Freitag, 29. April 2016, 12:00 Uhr

OpenScape Business

UNIFY Partner

ALSO

NTplus
Die Telekommunikationsmarke.

OPENSCAPE BUSINESS V2

Flexibel, skalierbar und leistungsstark

Setzen Sie sich mit uns in Verbindung, es berät Sie gerne:

René Hittmeyer
Field Sales Manager
+49 541 91 43 594
rene.hittmeyer@also.com

OpenScape Business ist die „All-In-One“-Lösung für Sprache und UC, speziell entwickelt für den Mittelstand. Die OpenScape-Business-Lösungsarchitektur ermöglicht den Einsatz unabhängig von der vorhandenen Telefonie-Infrastruktur, egal ob klassische Telefonie, IP oder DECT.

- **OpenScape Business Vorteile und Highlights**
- Umfassende „All-In-One“-Telefonie & UC-Lösung für den Mittelstand (inkl. Faxlösung, Multimedia Contact Center u.v.m.)
- Flexibel skalierbar von 2 – 1.500 Teilnehmern, in Netzwerken bis zu 2.000 Teilnehmern
- Rein softwarebasiert, für Server oder voll virtualisierbar
- OpenScape Business ist „ALL-IP Ready“
- 3 Jahre Service Support inkludiert (Software Upgrades & Services)
- Desktop & Groupware Integration (myPortal for Outlook)
- Mobility Clients (myPortal to go App for Android & iOS mit VoIP)
- Drag & Drop-Konferenzen und Web Collaboration

channel trends+visions

ALSO

ACTIVE AREA

15.04.2016 Bochum

Channel Trends+Visions

We activate your business.

Sehen Sie die Neuigkeiten der OpenScape Business V2.1 auf der Channel Trends+Visions

OpenScape Business

ALSO Deutschland GmbH | Lange Wende 43, 59494 Soest, Tel. +49 2921 99 0 | Ernst-Heinkel-Straße 4, 94315 Straubing, Tel. +49 9421 93 3000
NT plus – Die Telekommunikationsmarke. | Leyer Straße 24, 49076 Osnabrück, Tel. +49 541 9143 01

Fotos: VAF

Tagungsrückblick

Jahrestagung Technik und Service

Volles Haus, gute Stimmung und ein zukunftweisendes Programm zu Fragen der ITK-Sicherheit sowie der System- und Netztechnik. Die 34. Jahrestagung des Fachbereichs Technik und Service war wieder ein voller Erfolg.

Der SIP-Trunk wird in der Anschlusstechnik der Next Generation Networks eine wesentliche Rolle spielen. Das Marktangebot ist allerdings noch in der Entwicklung, und insbesondere die drängenden Fragen zur Sicherheit IP-basierter Anschlussszenarien und Bereitstellungsmodelle stehen derzeit im Fokus des professionellen Lösungsgeschäfts. Das Programm stand darum unter dem Motto »Der sichere Betrieb am SIP-Trunk« und widmete sich der umfassenden, fachkundigen Orientierung zu den relevanten Aspekten. Das Themenspektrum reichte von den technischen Anforderungen an SIP-Anschlüsse und IP-Kommunikationssysteme über die Rolle des Session Border Controllers bis hin zu VoIP-Hacking und Sicherheitsrichtlinien. Vorträge und Diskussionen zu Voice-over-WLAN und zur Messtechnik sowie Berichte zu aktuellen Themen der technisch-regulatorischen Rahmenbedingungen (z. B. Notruf, Messkonzept der Bundesnetzagentur) rundeten das Fachprogramm ab.

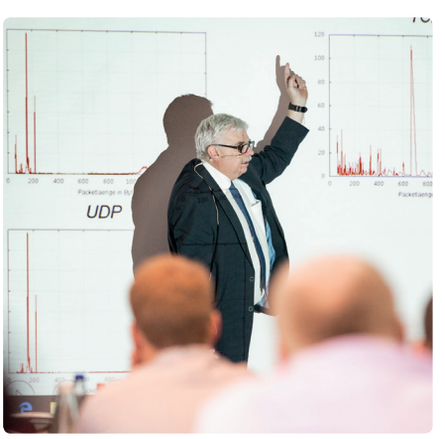
Herzliche Verabschiedung

Michael Kopp wurde auf der Tagung als langjähriger Sprecher des Fachbereichs in den Ruhestand verbschiedet. Die launige Laudatio hielt der ehemalige Serviceleiter der Telba AG, Klaus Rehklau, der als Weggefährte von Michael Kopp einige Anekdoten aus dem Schatzkästchen holte. Kopp nahm bereits als damals junger Serviceleiter der MTG Kommunikationstechnik an der ersten Jahrestagung teil, die seinerzeit noch als »Montage- und Revisionsleitertreffen« firmierte. Er prägte die Tagungen als Sprecher, der stets die Bedeutung des fachkollegialen Erfahrungsaustausches in den Vordergrund stellte. Als kleine Überraschung für den Vollblut-Münchner Kopp gab es am Abend noch ein Böllerschießen vor dem Festsaal des Augustiner Schützengartens.

Wir danken allen Teilnehmern, Referenten und Ausstellern für eine erkenntnisreiche und gelungene Tagung.

Nächster Termin

35. Jahrestagung Technik und Service
11. – 12. November 2016 in Erfurt



Fotos: VAF

Gespräch mit Dagmar Geer, Vorstandsvorsitzende der innovaphone AG

»Endlich sind wir im Markt angekommen«

Der schwäbische Hersteller innovaphone AG trat Ende der 1990er Jahre als Pionier in der IP-Telefonie an. VAF Report sprach mit der Vorstandsvorsitzenden Dagmar Geer über die Entwicklung seitdem und darüber, wie es weitergehen könnte.

VAF Report: Innovaphone ging im Jahr 1997 an den Start – damals war IP-Telefonie noch ein exotisches Thema. Haben Sie damit gerechnet, dass die IP-Telefonie mehr als ein Jahrzehnt benötigen würde, um sich zu etablieren?

Dagmar Geer: Eigentlich nicht. Aber wir haben auch nicht geglaubt, dass der Markt plötzlich explodiert, obwohl dies einige Marktforscher damals so prognostiziert hatten. Zum Glück waren wir zu keinem Zeitpunkt darauf angewiesen, dass die IP-Telefonie schnell zum Durchbruch kommt, denn wir hatten auch Gateways, PBX-Lösungen und Endgeräte im Portfolio, die alle im ISDN-Netz funktionierten.

VAF Report: Freut es Sie, dass durch den Abschied der Telekom von der ISDN-Technik die IP-Telefonie nun endlich in aller Munde ist?

Geer: Diese Entwicklung hätte ruhig etwas schneller kommen dürfen. Andererseits haben wir unser Wachstum immer dem Markt angepasst, was als positive Folge hat, dass wir bis heute eigenfinanziert sind und auf einer soliden Basis stehen. Auch technisch war dieser langsame Prozess wahrscheinlich positiv. Wenn der Markt für IP-Telefonie schon vor 15 Jahren durchgestartet wäre, hätten wir nicht die gleichen, ausgereiften Lösungen, die wir heute anbieten. So haben

Foto: innovaphone

wir anfangs beispielsweise auf H.323 und nicht auf SIP gesetzt, weil dieses Protokoll viel näher an ISDN war. Allerdings war H.323 auch viel schwerer zu implementieren, weshalb die Marktakzeptanz schwächer war und sich SIP auf längere Sicht durchgesetzt hat.

VAF Report: Welche Erfahrung haben Sie zuletzt mit Ihren Systemhauspartnern gemacht: Ist All-IP jetzt ein Routinethema, mit dem alle Partner souverän umgehen?

Geer: Manche unserer Partner sind da sehr weit, manche bessern derzeit ihr Fachwissen noch nach. Dafür ist es aber auch noch nicht zu spät, denn meiner Einschätzung nach wird die IP-Telefonie von jetzt an für einen langen Zeitraum ein echter Dauerbrenner sein. Ich freue mich allerdings, dass wir nun endlich in der gesamten Branche hoffähig sind. Heute bekommen wir von vielen Systemhäusern das Feedback, dass unsere Produkte für nahezu alle angefragten Telefonielösungen sehr gut geeignet sind.

VAF Report: Wie wichtig ist es aus Ihrer Sicht, »hungrig« zu bleiben und kontinuierlich auf technische sowie vertriebliche Fortbildung zu setzen?

Geer: Es ist wahrscheinlich eine Grundeigenschaft des Menschen, sich erst dann zu bewegen, wenn es wirklich notwendig ist. Die Telekommunikationsbranche hat sich lange nicht bewegt. Jetzt ist der Dornröschenschlaf aber definitiv zu Ende. Wir stehen vor gravierenden Änderungen, die Gepflogenheiten der Kunden ändern sich massiv. Die reine Telefonie ist nur noch selten ein Türöffner beim Anwender. UC-Lösungen sind heute vielen Kunden sehr wichtig und auch längst vertraut. Wer hier nicht »hungrig« ist, der verliert seine Kunden an die Mitbewerber.

VAF Report: Auf Ihrer Website heben Sie hervor, dass die NSA-Affäre das Vertrauen in die Informationstechnologie nachhaltig erschüttert hat.

Geer: Jahrelang haben selbst öffentliche Auftraggeber völlig bedenkenlos auf US-Hersteller gesetzt. Jetzt machen sich endlich einige Leute Gedanken, ob diese Entscheidung richtig war. Ich kann dazu sagen: Backdoors haben unsere Lösungen nicht. Wir spüren geradezu täglich, dass heute der Hinweis auf »Security – made in Germany« richtig zieht. Vielerorts wird wieder danach gefragt, ob der Hersteller aus Deutschland kommt. Da befinden wir uns natürlich in einer guten Ausgangslage.

> *Der Branche werden die Innovationen nicht ausgehen*
>
> *Dagmar Geer*

VAF Report: Auch innovaphone bietet neben klassischen Kommunikationsplattformen inzwischen die PBX und UC aus der Cloud an. Sprechen wir hier noch von einem Nischenmarkt, den Sie frühzeitig abdecken möchten, oder erwarten Sie, dass Cloud-Telefonie bald Standard ist?

Geer: Letzten Endes ist die Entscheidung für oder gegen eine Cloud-Lösung eine reine Glaubensfrage. Wichtig ist, dass man als Hersteller die Systemhäuser in die Lage versetzt, beides anbieten zu können – sowohl eine Cloud als auch eine On-Premise-Lösung. Manchmal ist es auch so, dass sich jemand für eine Cloud-Lösung aus Gründen entscheidet, die mit der Cloud als solcher eigentlich nichts zu tun haben. So steht die Cloud vermeintlich für Flexibilität. Dieselbe Flexibilität ist jedoch auch mit einem variablen Mietmodell erreichbar. Wenn Kunden nach einer Cloud-Lösung fragen, empfehle ich unseren Partnern immer, diese auch anzubieten. Allerdings sollte man genauestens nach den Beweggründen für diese Entscheidung fragen. Unser Cloud-Modell ist simpel und erhält die Kundenbindung. Wir setzen auf das Fachwissen und die Kundenbindung des Systemhauses als Schlüssel zum Erfolg.

VAF Report: Manche Lösungsanbieter machen sich schon jetzt Sorgen, welche »großen« Themen nach All-IP auf der Agenda stehen werden. Gehen der Branche allmählich die Innovationen aus?

Geer: Ich glaube nicht, dass der Branche die Innovationen ausgehen. Denken Sie einmal an Application Sharing, an die Vielzahl der Social-Media-Tools, an Videotelefonie. WebRTC ist im Moment ein großes Thema. Es wird durch eine Anwendung wie den »Call me«-Button auf der Webpage noch weiter getrieben. Das ist alles Kommunikation. Wir bei innovaphone finden das sehr spannend. Wir müssen allerdings akzeptieren, dass die reine Telefonie nur noch ein Thema zwischen vielen anderen Themen ist.

VAF Report: Frau Geer, wir danken Ihnen für dieses Gespräch.

Das Gespräch führte Folker Lück, freier Mitarbeiter des VAF Reports, im Januar 2016.

innovaphone
PURE IP-COMMUNICATIONS

innovaphone AG

Firmengründung: 1997
Mitarbeiter: 90
Firmensitz: Sindelfingen

Die Entwicklung findet in Sindelfingen und Berlin statt. Weitere Stützpunkte (Vertrieb/Technik) gibt es in Hannover, Hagen, Wien, Verona und Varekil (Schweden).
Produktportfolio: IP-Telefonie und Unified Communications, Komplettlösungen für Unternehmen unterschiedlicher Größen

Foto: innovaphone

Angemessene Lösungen erfordern Differenzierung der Szenarien

Sicherheitsbetrachtungen zum SIP-Trunking

Der Artikel liefert einen Überblick zu den Fragen und Maßnahmen des Risikomanagements, die ein Unternehmen beim Wechsel seines Sprachanschlusses auf einen SIP-Trunk berücksichtigen sollte.

Autor: Dipl.-Ing. Andreas Steinkopf

Einführung

Unternehmen und Organisationen haben heute viele Compliance-Regeln und -Normen zu beachten. Beim Thema Sicherheit kommt im Allgemeinen Fall die ISO 31000 als Antwort daher und gibt ein Regelwerk zum Risikomanagement vor. Telefonie gehört insbesondere durch die Computer-Telefonie-Integration (CTI) längst in die Welt der Informationstechnologie, genauso wie das IP-Protokoll und somit auch ein darauf aufbauender SIP-Trunk, der im Zuge des All-IP-Wandels den klassischen ISDN-Anlagenanschluss ablöst. Dies führt zum spezielleren Fall der Informationssicherheit und somit zur ISO-27000-Normenreihe, die ein Informationssicherheits-Managementsystem (ISMS) anbietet, sowie zum BSI-»IT-Grundschutzkatalog«, der kompatibel zur ISO 27001 ganz ähnliche Anforderungen beschreibt. Die ISO 31000 besagt, dass die Geschäftsleitung in einem Top-Down-Verfahren die Risiken identifizieren, analysieren und bewerten (lassen) muss. Ist die Kombination aus Eintrittswahrscheinlichkeit und potenziellem Auswirkungsschaden eines Risikos – wie insbesondere einer Sicherheitslücke – hinreichend groß, muss geplant werden, wie die Eintrittswahrscheinlichkeit und/oder der Schaden zu reduzieren ist, um ein vertretbares Restrisiko zu erreichen.

Wegen fehlender, verlässlicher Statistikinformationen zur Eintrittswahrscheinlichkeit oder Schadenshöhe tun sich viele Unternehmen und Organisationen jedoch schwer, eine eigenständige Risikoanalyse zu erstellen. Daher wird diese beim BSI-Grundschutz pauschaliert und der Grundschutzkatalog nennt Standardgefährdungen und Standardsicherheitsmaßnahmen für typische und verbreitete IT-Systeme und Netze. Allerdings soll auch hier eine IT-Strukturanalyse erfolgen, deren Ausgangsbasis im Kommunikationsumfeld der Netztopologie-Plan sein sollte. Pauschaliert wird auch der Schutzbedarf, der in die drei Schutzbedarfskategorien »normal«, »hoch« und »sehr hoch« unterteilt wurde.

Die hier zu erreichende Informations- bzw. Kommunikationssicherheit ist durch zwei englische Wörter besser aufgeschlüsselt: »Safety« steht für »Betriebssicherheit« im Sinne von Verfügbarkeit und Vermeidung von finanziellem Schaden. »Security« steht für die eigentliche, sichere Kommunikation, die wiederum auf Integrität, Authentizität und Vertraulichkeit beruht.

Dies aufgezeigt, erschließen sich Aufbau, Inhalt und Fachbegriffe der folgenden Abschnitte.

Inhalt

Kostensicherheit

Die mit Abstand höchste Kombination aus Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe ist nach der Erfahrung des Autors bzw. eines Internet-Telephony-Service Providers (ITSP) ein **Fraud-Fall** (engl. für Betrug), weil im Umfeld der TK-Anlage bzw. des SIP-Trunks ein Passwort nicht gut ausgewählt oder ein voreingestelltes oder leeres Passwort nicht geändert wurde (siehe auch M2.11 in **[BSI01]**). Eine derartige Unterlassung ermöglicht es Betrügern, über die TK-Anlagen-Administrations- oder Anwenderkonsole inkl. Fernwartungszugang, über ein Endgeräte-Login, über Voice-Mailboxen und auch über die SIP-Trunk-Registrierung die TK-Anlage bzw. den Sprachanschluss zu hacken und teure Verbindungen – meist zu Servicerufnummern im Ausland – zu generieren.

Aber auch mit sicheren TK-Passwörtern können Hacker moderne TK-Anlagen hacken, wenn diese Softwaresicherheitslücken – namentlich in ihrem Betriebssystem – aufweisen. Hier gilt es also zuvorderst, alle »normalen« Sicherheitsmaßnahmen für einen Server mit IP-Verbindungen zu ergreifen, wie z. B. regelmäßige Updates und natürlich sichere Administratoren-Passwörter.

Telefoniespezifisch sind sowohl auf der ITSP- als auch zusätzlich auf der Kundenseite weitere Maßnahmen ratsam:

Auf der Seite des Next Generation Networks (NGN) kann der SIP-Trunk vom ITSP für ausgehende Verbindungen zu Service- und Auslandsrufnummern gesperrt werden.

Und der ITSP kann eine allgemeingültige Fraud Prevention und Detection implementieren, die neben verschiedenen Anomalie-Screenings vielfach darauf beruht, dass er pro gefährdeter Rufnummerngasse Schwellwerte für das Verbindungsvolumen definiert und überwacht und im Alarmfall mit geringer Verzögerung geeignete Gegenmaßnahmen – wie eine SIP-Trunk-Abschaltung – ergreift. Auf der Kundenseite können zusätzlich Kundenindividuellere bzw. -spezifischere Gefahrenmuster und Schwellwerte implementiert, überwacht und Ereignisse sofort reportet werden. Dies entweder in der TK-Anlage selbst oder in einem vorgeschalteten Enterprise Session Border Controller (E-SBC), da sich nur diese beiden Komponenten hinreichend auf der SIP-Protokoll-Applikationsebene auskennen.

Betriebssicherheit

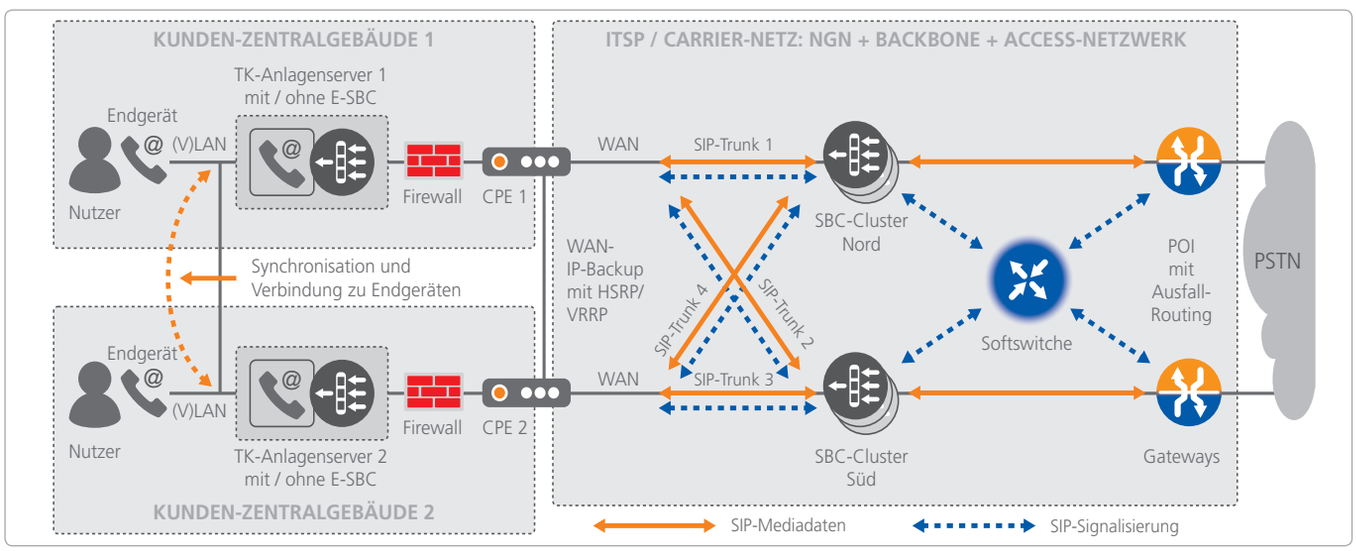
Wie Ausfälle der letzten Monate im noch »jungen« NGN der Deutschen Telekom gezeigt haben, hängt die Betriebssicherheit auf der ITSP-Seite stark davon ab, dass unter Einbeziehung der Systemlieferanten alle Systemkomponenten auch im Detail aufeinander abgestimmt sind, dass das NGN durchgängig mit stabilen und redundanten Komponenten aufgebaut ist und dass ein umfassendes System- und Change Management etabliert ist und optimiert wurde. Dies braucht Zeit, sprich das Beschreiten einer »Lernkurve«. Ganz ähnlich auf der Kundenseite: Auch hier muss gelernt werden, wie die Ausfallwahrscheinlichkeit des oder der neuen TK-Anlagenserver(s) und des IP-Netzwerks mit geeigneten Managementmaßnahmen – z. B. des BSI-Grundschutzkataloges – hinreichend gesenkt werden kann.

Ist eine **hohe bis sehr hohe Verfügbarkeit** gefordert, kann das Ausfallrisiko der IP-Telefonie weiter gesenkt werden, indem der SIP-Trunk, die IP-Standortanbindung und die TK-Anlage bzw. die Anlagenserver redundant ausgelegt werden. Dies wird in **Bild 1** im Detail dargestellt.

Verfügbarkeitsstufe 1 mit einem TK-Anlagenserver (im Bild TK-Anlagenserver 1) und einer Standortanbindung (im Bild CPE 1): Meist ohne Aufpreis für den Kunden kann der ITSP eine erhöhte SIP-Trunk-Verfügbarkeit liefern, indem er ortsredundante Session Border Controller (SBC) installiert. Der SIP-Trunk wird dann im »Dual Homing«-Modus betrieben: Im Normalfall baut die TK-Anlage den SIP-Trunk zum ersten SBC des ITSP auf (im Bild SIP-Trunk 1 zu SBC-Cluster Nord). Fällt dieser SBC aus, baut die TK-Anlage den SIP-Trunk zum redundanten SBC auf (im Bild SIP-Trunk 2 zu SBC-Cluster Süd). Schon etwas teurer, aber die Ausfallwahrscheinlichkeit gemäß SLA (Service Level Agreement) des Zuführungsproviders ein weiteres Stück senkend, ist die **Verfügbarkeitsstufe 2**, weiterhin mit einem TK-Anlagenserver an einem Standort, aber nun mit zwei Standortanbindungen (im Bild CPE 1 und CPE 2): Fällt hier die primäre Standortanbindung (an CPE 1) aus, übernimmt der sekundäre Router (CPE 2) automatisch die Kommunikation, indem er über eine VRRP- oder HSRP-Verbindung (VRRP = Virtual Router Redundancy Protocol gemäß RFC 5798, HSRP = Hot Standby Router Protocol von Cisco) mit dem primären Router kommuniziert. Dies wird meist einfach »IP-Backup« genannt.

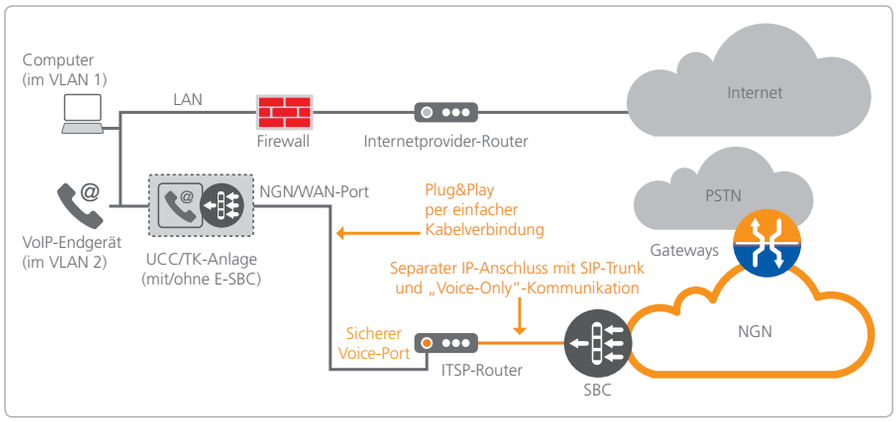
Verschiedene TK-Anlagenhersteller bieten eine optionale Redundanz für ihre TK-Anlagenserver an: In dieser **Verfügbarkeitsstufe 3** melden sich zwei – oder mehr – Anlagenserver der gleichen TK-Anlageninstanz für den gleichen logischen SIP-Trunk beim ITSP an (im Bild Anlagenserver 1 und 2) und können so beide abgehende Verbindungen aufbauen. Eingehende Verbindungen werden den Servern gleichverteilt zugestellt, die aus Sicht der ITSP-SBC »online« sind, also antworten. Die Server können sogar an verschiedenen Standorten stehen (im Bild Zentralgebäude 1 und 2), müssen sich aber auch dann permanent synchronisieren.

Mit dieser Stufe hat man alle »Single Points of Failure« ausgemerzt und eine Ortsredundanz auf ITSP- und Kundenseite geschaffen. Dies geht deutlich weiter als das ISDN-Leistungsmerkmal »Mehrfachabstützung«, mithilfe dessen bei Ausfall einer Vermittlungsstelle nur ein Teil der ankommenden Gespräche über die zweite Vermittlungsstelle abgewickelt werden konnte. Zudem unterstützten viele TK-Anlagen dieses Merkmal nicht. Und wenn man es schaffte, die Beschränkung auf ein Ortsnetz hinter sich zu lassen, konnten Taktprobleme zu Störungen führen.



Grafik: VAF/QSC

▲ **Bild 1:** Mit einem SIP-Trunk kann eine durchgängige Redundanz der Sprachanbindung realisiert werden.



▲ **Bild 2:** Eine klare Trennung der Daten- und VoIP-Netze sowie mehr Redundanz ergeben sich mit einem separaten »Voice-only«-Anschluss.

Internetsicherheit

Alle über IP angebundenen Geräte, die direkt oder indirekt mit dem Internet verbunden sind, unterliegen dem Risiko kaum überschaubarer, diverser Angriffsszenarien, sodass auf der anderen Seite diverse Gegenmaßnahmen, wie der Einsatz einer Firewall, dieses Risiko senken sollten. Im VoIP-Umfeld wird zusätzlich empfohlen, **Daten- und VoIP-Netz zu trennen.** Im Kunden-LAN erfolgt dies am besten auf Layer 2 mittels VLAN-Technologie (Virtual Local Area Networks) im Ethernet-Switch. Bei erhöhten Sicherheitsanforderungen wird sogar empfohlen, diese Netze physikalisch zu trennen (siehe auch M2.376 in **[BSI01]**), was den Aufwand im LAN mindestens verdoppelt.

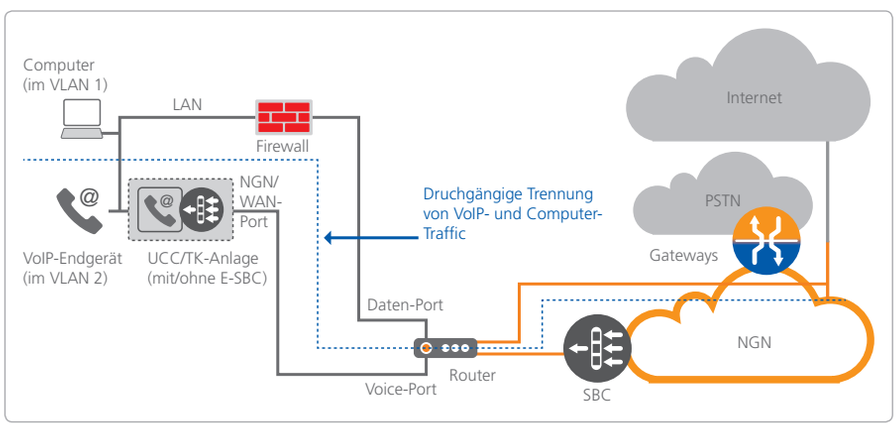
Viele Hersteller haben gelernt, ihren IP-basierten TK-Anlagen einen separaten **NGN- bzw. WAN-Ethernet-Port** zu spendieren. Dieser kann entweder in die »Haupt-Appliance«, einen separierten Mediation-Server oder einen vorgeschalteten E-SBC integriert sein. Auf der ITSP-Seite wurde ganz Ähnliches gelernt: Auch hier können einige Anbieter schon einen separaten **Voice-Ethernet-Port am Access-Router** liefern. Dieser wird – z. B. mittels Access-Control-Liste (ACL) – auf dem Router so konfiguriert, dass er ausschließlich mit den Voice-Komponenten des ITSP-NGN, also namentlich seinen SBC, kommunizieren kann. Da diese nur bereinigte SIP-Kommunikation passieren lassen, erreicht auch den Voice-Port des Access-Routers ausschließlich diese – nicht jedoch die gefährliche Internetkommunikation.

Beides zusammen ergibt nun die Möglichkeit, auch auf der SIP-Trunk-Seite die Netze zu trennen: Wie in **Bild 2** ersichtlich, kann ein vom Internetanschluss völlig getrennter **»Voice-only«-SIP-Sprachanschluss** direkt mit einem einfachen Kabel wie bei ISDN mit der IP-TK-Anlage verbunden werden, was den Installationsaufwand deutlich reduziert. Somit werden nicht nur die Netze höchst sichtbar getrennt, sondern auch die Verantwortungsbereiche: Das TK-Anlagen-Fachunternehmen braucht sich wegen des SIP-Trunks weder mit dem Firewall-Verantwortlichen abzustimmen, noch beim Internetprovider um eine Sprachdatenpriorisierung zu ersuchen.

Bei diesem »Single Play«-Anschluss wird also im Vergleich zum »Dual Play«-Anschluss der Internetdienst abgeschaltet, was der ITSP zum Anlass nehmen kann, ihn günstiger als einen Dual-Play-Anschluss – mindestens jedoch nicht teurer als einen ISDN-Anschluss – anzubieten.

Gleichwohl müssen zwei IP-Standortanbindungen bezahlt werden. Dies spricht aus Gründen der Anbindungskosten für die im **Bild 3** dargestellte **ITK-konvergentere Sprach/Datenanbindung**. Durch die Verbindung zum Internet steigt zwar das Risiko eines Router-Angriffs bzw. -Ausfalls ein wenig, aber durch die Trennung von Daten- und Voice-Port und die Separierung des VoIP-Traffics über die SBC des ITSP bleibt eine logische Trennung der Traffic-Arten erhalten. Und der Schutz vor Internetangriffen über den Voice-Port.

Ob bei den Szenarien der Bilder 2 und 3 vor bzw. mit der TK-Anlage ein E-SBC zu installieren ist, sei der Diskussion des TK-Anlagenherstellers und -Systemintegrators mit seinem Kunden bzw. den Betrachtungen des Fachbeitrags von Mathias Hein inklusive Plädoyers auf S.16 dieser Ausgabe überlassen.



▲ **Bild 3:** Auch die ITK-konvergente Standortanbindung separiert Internet- und VoIP-Traffic.

Kommunikationssicherheit

Welche technischen Protokolle verwendet werden sollten, um die Kommunikationssicherheit für einen SIP-Trunk zu erhöhen, ist weder von der Empfehlungs- noch der Hersteller/ITSP-Seite strittig: Wie in **Bild 4** (siehe grüne 1) gezeigt, kann die Vertraulichkeit, Integrität und Authentizität der Mediendaten auf dem Layer 5 des ISO/OSI-Schichtenmodells mit dem **Secure Real Time Protokoll** (SRTP) deutlich erhöht werden. Es ist sinnvoll, SRTP mit dem **Transport Layer Security Protocoll** (TLS) auf dem Layer 4 zu kombinieren (siehe grüne 2), das zusätzlich die Integrität und Authentizität der SIP-Signalisierung erhöht. Diese beiden optionalen SIP-Trunk-Protokolle erhöhen nur die Kommunikationssicherheit des SIP-

Trunks. Gerade wenn eine Organisation mehrere Standorte mit IP vernetzen will, empfiehlt es sich, dies mit einem IP-VPN zu tun, bei dem die IP-Kommunikation aller Anwendungen über private, nicht aus dem Internet zu erreichende IP-Adressen erfolgt. Ein IP-VPN kann komfortabel – weil Netz-basiert – vom ITSP gebaut und geliefert werden, indem dieser ein **Multi-Protocol-Label-Switching-VPN** (MPLS-VPN, siehe grüne 3 auf Layer 2) für den Kunden aufbaut. Auch der SIP-Trunk kann mit dem IP-VPN abgesichert werden, indem der ITSP eine direkte und private Verbindung zwischen dem Kunden-IP-VPN und seinen SBC herstellt.

Alternativ oder sogar auch zusätzlich kann ein **IPsec-VPN** (siehe grüne 4) aufgebaut werden, um alle Daten zwischen den Kundenstandorten und dem SIP-Trunk nicht nur »abzuschotten«, sondern auf Layer 3 auch zu verschlüsseln. Diese Verschlüsselung erfolgt für jeden Kundenstandort im Access-Router, was mit der Standortanzahl schnell ansteigend zu einem hohen Provisionierungs- und Managementaufwand führt. Der Aufwand lässt sich zwar mit geeigneten Provisionierungs/Managementsystemen wie z. B. dem Cisco-propietären Group-Encrypted-Transport-VPN (getVPN) drücken. Ein IPsec-VPN sollte aber erst zusätzlich zum Einsatz kommen, wenn selbst die Kombination aus TLS/SRTP und MPLS-VPN speziellen Compliance-Vorgaben nicht mehr gerecht wird.

	Schutzbedarf *		
SIP-Trunk/IP-Anbindung	Normal	Hoch	Sehr hoch
Fremd-Internetanschluss	mit TLS/SRTP und Firewall/E-SBC-Schutz	nicht empfehlenswert	nicht empfehlenswert
Internet/Dual-Play-Anschluss des ITSP, ohne Voice-Port	mit Firewall/E-SBC-Schutz	mit TLS/SRTP und Firewall/E-SBC-Schutz	nicht empfehlenswert
Internet/Dual-Play-Anschluss des ITSP mit Voice-Port (gemäß Bild 3)	so nutzbar	mit TLS/SRTP und E-SBC-Schutz	nicht empfehlenswert
Voice-only/Single-Play-Anschluss des ITSP (gemäß Bild 2)	so nutzbar	mit TLS/SRTP und E-SBC-Schutz	mit TLS/SRTP und E-SBC-Schutz
MPLS-IP-VPN-Anbindung des ITSP	so nutzbar	mit E-SBC-Schutz	mit TLS/SRTP und E-SBC-Schutz.

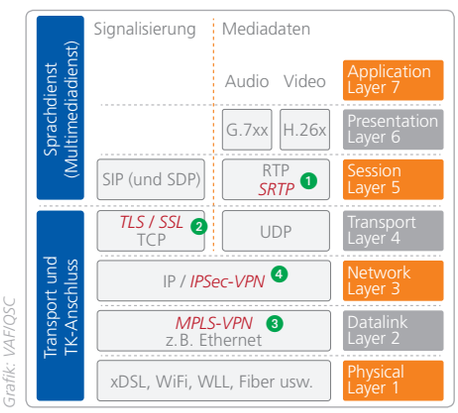
** Schutzbedarfskategorie gemäß BSI-Grundschutz*

▲ **Tabelle 1:** Empfehlungen für Sicherungsmaßnahmen

Bleibt die Frage, wann welches Sicherungsprotokoll genutzt werden sollte. Die Antwort hängt vor allem von diesen beiden kundenindividuellen Vorgaben ab: Wie sieht die Netztopologie für die komplette Übertragungsstrecke des SIP-Trunks aus und in welche Schutzbedarfskategorie (normal, hoch, sehr hoch) will sich der Kunde eingereiht sehen? Basierend auf diesen Angaben empfiehlt der Autor die in **Tabelle 1** genannten Sicherungsmaßnahmen.

Schlussbemerkung

Der Gedanke, Internet-Telefonie sei unsicherer als ISDN-Telefonie, lässt sicher noch einige Kunden so lange wie möglich auf ihrem bisherigen ISDN-Sprachanschluss beharren. Schaut man sich SIP-Trunking jedoch im Detail an, sieht man u. a., dass die Sprache hier ja meist gar nicht durch das offene Internet zum Kunden kommt, sondern über IP-Verbindungen, die vom Internet abgeschottet sind. Auch konnten die Daten eines ISDN-Anschlusses nicht verschlüsselt werden – die eines SIP-Trunks jedoch schon. Und auch bezüglich der Diensteverfügbarkeit beim Kunden kann beim SIP-Trunking eine Zuführungs- und Plattformredundanz geschaffen werden, wie sie bei ISDN nicht möglich war. Aus der Sicht des Autors sollte sich jetzt jeder Anwender für einen in absehbarer Zeit anstehenden Wechsel in der Anschlusstechnologie beispielsweise durch sein betreuendes TK-Fachunternehmen kundig beraten lassen. Die Topologie des Kommunikationsnetzwerks muss aufgenommen und der Schutzbedarf des Kunden ermittelt werden beziehungsweise geklärt sein. Daraufhin können die individuell passenden Empfehlungen ausgesprochen werden. ■



Grafik: VAF/QSC

▲ **Bild 4:** In vier Layern des ISO/OSI-Schichtenmodells können Sicherheitsprotokolle für die Kommunikationssicherheit des SIP-Trunks genutzt werden.

Quellen:
[BSI01]: *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, Maßnahmen zur Organisation. www.bsi.bund.de*

Autor:

Dipl.-Ing. Andreas Steinkopf ist Produktmanager für VoIP bei der Kölner QSC AG, die eines der größten deutschen NGNs betreibt und u. a. SIP-Trunks, Internet- und IP-VPN-Anschlüsse im indirekten Kanal vermarktet. **www.qsc.de**

E-SBC: Enterprise Session Border Controller

Welche Aufgaben übernimmt der E-SBC im SIP-Trunk?

Benötigt man in Verbindung mit einem SIP-Trunk auch einen E-SBC im eigenen Unternehmen? Diese Frage wird derzeit im Markt höchst kontrovers diskutiert. Der Artikel beschreibt die vielfältigen Aufgaben eines E-SBCs. Jedoch lassen sich erst anhand der Anforderungen eines Unternehmens die individuell passenden Antworten finden.

Autor: Mathias Hein

Ein Session Border Controller (SBC) ist eine Netzkomponente zur sicheren Kopplung von verschiedenen Rechnernetzen bzw. Netzwerkperimetern mit unterschiedlichen Sicherheitsfunktionen. SBC werden hauptsächlich in VoIP-Umgebungen eingesetzt, um externe (unsichere) Datennetze mit internen (sicheren) IT-Strukturen zu koppeln. Der SBC analysiert die verschiedenen Datenströme (Sessions) und greift, je nach Konfiguration, in die verschiedenen Datenströme ein.

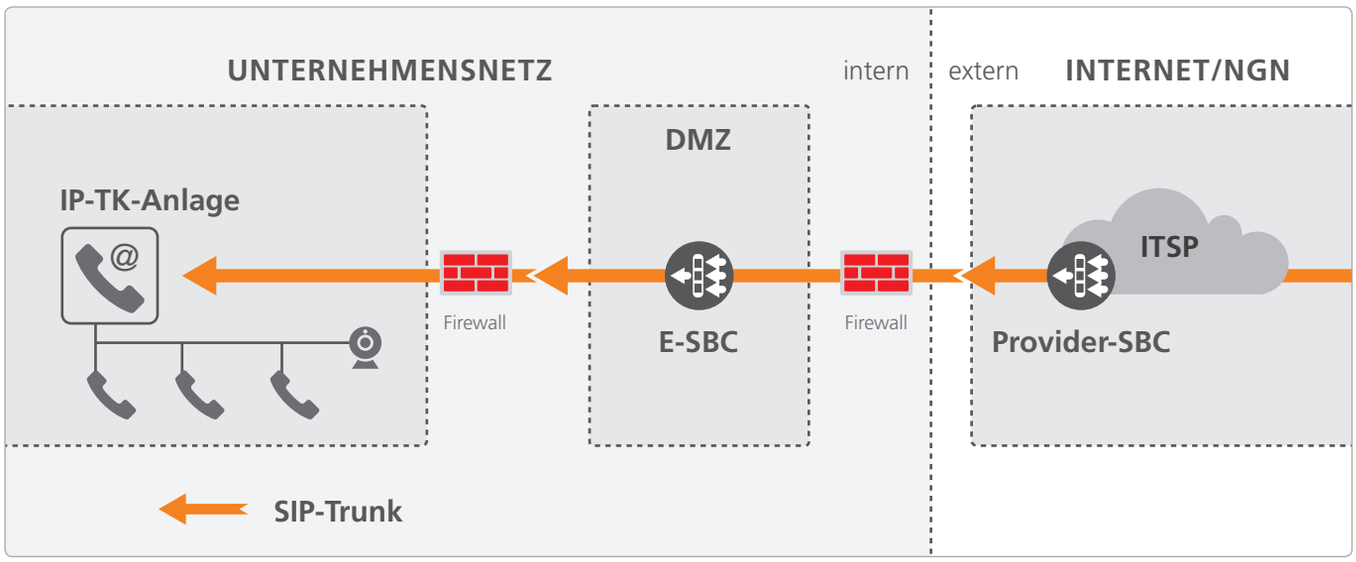
Aus Sicht der meisten Internet-Telephony-Service-Provider (ITSP) gehört der SBC zu deren umfassenden Dienstangebot, dient aber auch dem Schutz des eigenen NGN (Next Generation Networks). Der SBC agiert in dieser Konstellation meist als Back-to-Back-User-Agent (B2BUA), was dazu führt, dass er die SIP-Sessions der Kunden-TK-Anlagen terminiert und zum NGN des ITSP jeweils eine neue, normgerechte SIP-Session aufbaut. Somit filtert er alles aus, was nicht »saubere« VoIP-Pakete sind. In seinem Kern ist ein SBC eine Art spezieller SIP-Firewall. Diese führt eine Deep Packet Inspection durch und stellt sicher, dass nur ordnungsgemäße SIP-Nachrichten in das Netzwerk des ITSP bzw. in Richtung des SIP-Trunk-Kundens gelangen. In vielen Fällen wird auch der SIP-Trunk beim Kunden über einen Router des ITSP mit einem dedizierten Voice-Ethernet-Port (inklusive aller Access-Control-Listen) geleitet. Über diesen Port wird die Telefonanlage des Kunden angeschlossen. In die andere Richtung ist über diesen Port nur der SBC des ITSP zu erreichen.

Dadurch entsteht auch über die IP-basierte Standortanbindung ein quasi exklusiver VoIP-Kanal zwischen dem ITSP und der Telefonanlage des Kunden. Darüber hinaus wird durch dieses Verfahren eine durchgängige Trennung von VoIP- und Computerdaten gewährleistet und somit die BSI-Empfehlung, Computer- und VoIP-Netz zu trennen, auch im WAN-Bereich eingehalten. Als Nebeneffekt ist eine robuste Priorisierung (QoS) für alle VoIP-Daten (Signalisierungs- und Sprachpakete) gegenüber dem regulären Internetverkehr zum Provider möglich. Eine weiter differenzierende Darstellung möglicher Anschlussszenarien wird hier nicht vorgenommen, findet sich aber im Fachbeitrag von Andreas Steinkopf auf Seite 12 dieser Ausgabe.

STATEMENT

»In Zeiten von ALL-IP führt kein Weg mehr daran vorbei, sich den damit einhergehenden Herausforderungen in den Bereichen Sicherheit, Interoperabilität, QoS und Remote Access zu stellen. Der Einsatz von E-SBC gewinnt in der Planung moderner Multimedianetze große Bedeutung und ist heute eine unverzichtbare Komponente, die in unterschiedlichen Ausprägungen angeboten wird. Das Preisspektrum beginnt bei unter tausend Euro im KMU-Segment und reicht bis zu höheren sechsstelligen Beträgen für SBC, wie sie in großen und typischerweise in den öffentlichen Netzen eingesetzt werden. SBC erfüllen komplexe Aufgaben, dementsprechend erfordert die Konfiguration spezifisches Know-how. ITK-Systemhäuser müssen darauf vorbereitet sein, und Hersteller müssen hier unterstützen.«

René Princz-Schelter,
Director Presales DACH, Alcatel-Lucent Enterprise Deutschland GmbH (ALE)



Grafik: VAF

▲ **Bild 1:** Einbettung des E-SBC in die Netzarchitektur

Enterprise Session Border Controller (E-SBC)

Mit der Bereitstellung von SBC-Funktionen durch den ITSP sind je nach TK-Anlagen-Typ jedoch noch nicht alle technischen und logischen Probleme sowie Sicherheitsrisiken beseitigt. Aus diesem Grund wird oftmals noch ein Enterprise Session Border Controller (E-SBC) in die Verbindung zur VoIP-Telefonanlage zwischengeschaltet **(Bild 1).** Der E-SBC sorgt für Funktionen, die einige IP-TK-Anlagen nicht oder noch nicht beherrschen. So wird beispielsweise bei einigen Anlagen nur das UDP-Protokoll statt des meist vorgeschriebenen TCP-Protokolls für die Signalisierung genutzt. Auch das E.164-Format der Telefonnummern wird bei einigen Telefonanlagen noch nicht genutzt, und nicht alle PBX-Anlagen beherrschen schon die Anbindung mehrerer Standorte pro SIP-Trunk. Diesen Funktionsmangel gleicht ein E-SBC auf der Kundenseite bei adäquater Konfiguration aus.

Bereitstellung individueller Funktionen

Auch sind die ITSP kaum in der Lage, bestimmte Aufgaben, die ihre zentralen Carrier-SBC zu stark belasten würden, zu erfüllen. Hierzu gehört beispielsweise ein kundenindividuelles VoIP-Monitoring. Ein ordentlicher ITSP überwacht natürlich alle NGN-Komponenten inklusive seiner internen Backbone-Komponenten, aber kann (und will aus Kostengründen) diese Funktionen nicht auf den kundenseitigen Teil des SIP-Trunks ausweiten. In der Regel wird ein ITSP zumindest für Projektkunden mithilfe der üblichen SNMP- und MIB-basierenden Werkzeuge (Delay, Jitter, Paketverluste) den CPE-Router monitoren, aber weiter als bis zum Übergangs-Router geht die Überwachung nicht. Dies ist jedoch nicht zu verwechseln mit einem umfassenden VoIP-Monitoring beim Kunden. Dafür sind Zusatzmessungen erforderlich, die nur über einen E-SBC zu realisieren sind.

Dazu gehören:

- die Anzahl der möglichen und tatsächlichen parallelen Verbindungen,
- deren MOS-, Delay-, Jitter- und Paketverlustwerte,
- die Rate erfolgreicher Verbindungsaufbauten pro Anrufversuch (Answer Seizure Ratio, ASR),
- die Abbruchraten und
- die Rufaufbauzeiten.

Ergänzende Sicherheitsfunktionen

Auch im Bereich der Sicherheit ergänzt ein E-SBC die Funktionen des Vorleistungsprodukts des ITSP. Bei den VoIP-Sicherheitsproblemen handelt es sich um Angriffe auf der Session/Anwendungsschicht (TDOS-Attacken, IVR-Loops Detection, Rogue RTP), die über einen E-SBC beim Empfänger zielgerichtet abgefangen werden können. Auch ein SIP-Logging in Sende- und Empfangsrichtung sowie das gezielte Aufsplitten zur Aufzeichnung (Mitschnitt) von Sprachströmen ist mit einem E-SBC umsetzbar.

Ein E-SBC kann auch für die Beseitigung von SIP-Inkompatibilitäten zwischen unterschiedlichen Kommunikationssystemen, Softwareversionen und VoIP-Anwendungen sorgen. Ist beispielsweise eine TK-Anlage noch nicht mit dem SIP-Trunk eines bestimmten ITSP freigegeben, kann ein E-SBC dazu genutzt werden, eine entsprechende SIP-Protokollanpassung durchzuführen. Dies erfordert allerdings Expertenwissen.

Anpassung unterschiedlicher Codecs, SIP-Dialekte und Protokolle

Auch das Transcoding (die Umwandlung einer Audio- oder Videodatei in ein anderes Format) wird selten von einem ITSP erbracht. Soll beispielsweise ein G.722-Sprachstrom übermittelt werden und unterstützt das Empfängersystem diesen Codec nicht, so kann eine Codec-Anpassung (beispielsweise in G.711 oder G.729) vorgenommen werden. Da diese Funktion erhebliche Kosten (Lizenzen und Lasten) mit sich bringt, wird sie in der Regel nicht vom SBC des ITSP bereitgestellt, und der E-SBC muss diese übernehmen. Alternativ und üblich ist hier jedoch mittlerweile der Codec-Fallback: Die

anrufende TK-Anlage einigt sich mit dem Empfänger mittels Session-Description-Protokoll (SDP) auf den G.711-Codec, wenn das Empfängersystem kein G.722 unterstützt. Durch den Wegfall von typischerweise zwei Transcodings vermeidet man auch, dass die Sprachdatenpakete weiter verzögert werden.

Darüber hinaus stellen die meisten E-SBC eine Übersetzung zwischen den IP-Versionen IPv6 und IPv4 bereit, was eine eventuell notwendige Migration zwischen den unterschiedlichen Protokollwelten vereinfacht.

Network Address Translation

Die verfügbaren IPv4-Adressen sind vielen Internet-Providern und Unternehmen bereits vor Jahren ausgegangen. Aus diesem Grund liefern Internet-Serviceprovider (ISP) und VoIP-Provider, also die ITSP, standardmäßig ihren Kunden nur noch private IP-Adressen über ihre Zugangsrouter. Hierbei übersetzt der Router die kundenseitigen, privaten IP-Adressen auf eine oder mehrere öffentliche IP-Adressen des ISP oder ITSP, indem er eine Network Address Translation (NAT) durchführt. Diese NAT kann von SIP-Trunks nur überwunden werden, wenn sich die TK-Anlage mit einer SIP-Registrierung beim ITSP authentifiziert: Die zuerst ablaufende SIP-Registrierung baut eine SIP-Session zum SBC des Providers auf und öffnet damit den VoIP-Weg von innen nach außen. Die Rückroute können moderne SBC der ITSP dann selbst ermitteln. Alternativ kann diese Rückroute über einen STUN-Server ermittelt werden.

Wird vom – meist amerikanischen – Hersteller der TK-Anlage jedoch ein SIP-Trunk mit Fix-IP-Authentifizierung (auch Peering-Modus genannt) gefordert, so muss der Provider entweder tatsächlich eine oder mehrere fixe, öffentliche IP-Adressen ohne NAT an seinem Router und einen SIP-Trunk mit Fix-IP-Authentifizierung liefern. Auf dem weiteren Übertragungsweg bis zur Kunden-TK-Anlage darf keine Komponente eine NAT hinzufügen. Sind dem Endkunden fixe, öffentliche IP-Adressen nicht geheuer oder liefert der Provider keine öffentlichen IP-Adressen, so kann wieder ein E-SBC helfen: Dieser baut zum Provider einen SIP-Trunk mit Registrierung und NAT und zur TK-Anlage den geforderten Fix-IP-SIP-Trunk auf.

STATEMENT

»QSC liefert seit 2006 SIP-Trunks für TK-Anlagen mit oder ohne vorgeschalteten E-SBC. Aus ITSP-Sicht ist ein bestimmter E-SBC jeweils als Bestandteil der TK-Anlage zu sehen. Daher wird dieser im QSC-Freigabeprozess auch mitgetestet und freigegeben. Besonders um KMU beim All-IP-Übergang budgetgerechte Lösungen zu bieten, liefert QSC dedizierte Voice-Ports mit Access Control List (ACL) an seinen Internetanschlüssen und alternativ MPLS-basierte IP-VPNs. So kann auf einen E-SBC verzichtet werden, wenn der Kunde keinen erhöhten, individuellen Monitoring- oder Fraud-Control-Bedarf hat und dieser nicht durch die TK-Anlage gedeckt werden kann.«

Andreas Steinkopf,
Produktmanager VoIP, QSC AG

Individuelle Fraud Control und Abrechnungsdaten

Eine Binsenweisheit lautet: Jedes Unternehmen kann zum Angriffsziel werden. Ein wichtiges Angriffsszenario bei Telefonanlagen zielt mittels Hacking auf den Gebührenbetrug ab. Eine feingranulierte, kundenindividuelle Toll Fraud Control (Überwachung auf Gebührenbetrug) ist für den ITSP so gut wie nicht zu erbringen. Allenfalls Sperren für abgehende Rufe zu grob definierten Rufnummerngassen, zu bestimmten und beispielsweise als betrügerisch bekannten Servicerufnummern oder zu Auslandsvorwahlen und dergleichen sind als allgemeingültige Regel vom Provider umsetzbar. Ebenso muss die Definition und Überwachung von verdächtigen Verkehrsprofilen und den zugehörigen Schwellenwerten beim ITSP notwendigerweise grobmaschiger ausfallen, als es im einzelnen Unternehmen möglich ist. Daher sollte jedes Unternehmen eine individuell optimierte Sperrung nicht benötigter Zielrufnummern und Rufnummerngassen – z. B. durch Black- und Whitelists – im E-SBC erwägen. Die Einrichtung kann bzw. muss ggfs. an sich ändernde Verhältnisse angepasst werden. Des Weiteren lassen sich mithilfe eines E-SBC auch Passwortattacken auf SIP-Registrierungs-/Login-Passwörter erkennen.

E-SBC unterstützen zunehmend auch die Abrechnung bestimmter Leistungen. In Hotels, Krankenhäusern etc. ist es notwendig, an die Einzelverbindungsnachweise (EVN) für die Telefonrechnungen in Echtzeit zu gelangen. Ein E-SBC kann dafür genutzt werden, die Verbindungen individuell aufzuzeichnen und die gesammelten Informationen über eine entsprechende Schnittstelle zur Verarbeitung an nachgelagerte Systeme weiterzureichen, um so für den Gast oder Patienten exakte Nutzungsdaten bereitstellen zu können.

Hochverfügbarkeit besser als bei ISDN

E-SBC sind nicht nur für die oben genannten Sicherheitsfunktionen einsetzbar, denn diese Geräte agieren ja grundsätzlich als Koppelpunkte zwischen dem ITSP und dem Unternehmen. Der E-SBC sollte daher so ausfallsicher wie möglich aufgebaut sein. Manche Anbieter empfehlen, den E-SBC immer in seiner hochverfügbaren Konfiguration – also als Gerätedoppel – zu betreiben. Eine solche E-SBC-Konfiguration besteht aus einem aktiven E-SBC, gepaart mit einem Stand-by-E-SBC. Im Regelfall kümmert sich der aktive E-SBC um den gesamten SIP-Datenverkehr und der Stand-by-E-SBC wird nur aktiv, wenn das primäre Gerät ausfällt. Da eine direkte Verbindung zwischen den beiden E-SBCs besteht, verfügt der Stand-by-E-SBC über alle notwendigen Informationen zu den aktiven Verbindun-

gen, und der Ausfall des primären E-SBCs kann jederzeit nahtlos abgefangen werden.

Wo wird der E-SBC installiert?

Ein E-SBC gehört an den Netzwerkrand und wird in der Regel innerhalb der DMZ installiert. Da es sich bei diesem Gerät ja um eine Art spezieller SIP-Firewall handelt, wird immer wieder darüber diskutiert, ob ein E-SBC die klassische Firewall ersetzt. Klassische Datenfirewalls sind bisher nicht in der Lage, die VoIP-Ströme (SIP/TLS und RTP) zu kontrollieren. Aus diesem Grund blockieren klassische Firewalls die VoIP/Video-Ströme oder lassen diese ungeprüft durch. In der Regel werden alle VoIP-Ströme von der Firewall in der DMZ unkontrolliert über einen offenen Port an den E-SBC weitergeleitet. Dieser nimmt als anwendungsspezifische Prüfkomponente eine Deep Packet Inspection vor und stellt sicher, dass nur ordnungsgemäße SIP-Nachrichten an die VoIP-/Videokomponenten des eigenen Unternehmens gelangen. Da der E-SBC als Proxy agiert, können auch VoIP/Video-Interception durchgeführt und verschlüsselte Verbindungen überprüft werden. Nach der Prüfung werden die Daten wieder verschlüsselt und an den eigentlichen Empfänger weitergeleitet.

Darüber hinaus verhindert ein E-SBC auch Denial-of-Service-(DoS-)Attacken auf die Telefonanlage. Man kann beispielsweise Positiv- bzw. Negativlisten von IP-Adressen bekannter Angreifer anlegen. Dabei werden fehlgeschlagene Anmeldeversuche registriert und anschließend der potenzielle Hacker blockiert. Dies verhindert das Überfluten des Callservers mit Registrierungsnachrichten. Da ein E-SBC in der DMZ des Unternehmens installiert wird, muss dieser im Hoheitsbereich der Unternehmens-IT untergebracht werden.

Um die anwendungsspezifischen Funktionen wirksam umsetzen zu können, müssen die beiden Fachbereiche IT und TK bei der Administration eines E-SBCs nahtlos zusammenarbeiten.

Sind E-SBCs austauschbar?

Bei der Auswahl eines E-SBCs ist darauf zu achten, dass die meisten Funktions- und Kompatibilitätstests der Telefonanlagen an den im Markt angebotenen SIP-Trunks mit dem vom TK-Anlagenhersteller freigegebenen E-SBC auf der Kundenseite und einem SBC auf der Seite des ITSP erfolgen. Aus diesem Grund kann nicht jeder beliebige E-SBC in den SIP-Trunk eingefügt werden. Jede nicht abgestimmte Änderung zerstört im Prinzip die SIP-Trunk-Freigabe zwischen ITSP und dem TK-Anlagenhersteller.

Fazit

Erst anhand der individuellen Anforderungen des Unternehmens und der Vorleistungen bzw. Anschlussszenarien des ITSP lässt sich entscheiden, ob und mit welchem Funktionsumfang ein E-SBC benötigt wird. Die pauschale Ja/Nein-Frage zur Notwendigkeit eines E-SBCs ist darum nicht sachgerecht. Hier ist die Beratungskompetenz des ITK-Systemhauses gefragt. Bis sich Marktüblichkeiten etabliert haben, wird allerdings noch einige Zeit vergehen. ■

Autor:

Mathias Hein betreut im VAF den Fachbereich Netzwerktechnik und schult im Rahmen der VAF-Wissenswerkstatt insbesondere zu Netzwerkprotokollen.
E-Mail: hein@vaf-ev.de
www.vaf-ev.de

Update zum Sachstand

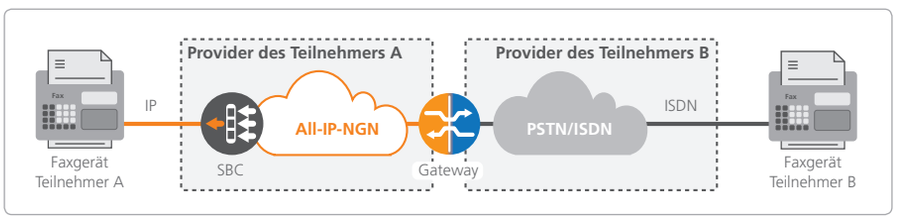
Fax-over-IP in den neuen Netzen

Die Autoren beschreiben, wie weit das Thema »Fax und NGN« gediehen ist und erläutern, was in Bezug auf Fax insbesondere bei der Einrichtung eines SIP-Trunks auf Kundenseite beachtet werden sollte.

Fax Gruppe 3 zählt im Umfeld der Next Generation Networks (NGN) sicherlich zu den Sonderdiensten oder neudeutsch »Legacy Devices«, also zu einem Technologieerbe, das im All-IP-Zeitalter längst einen technologischen Nachfolger hätte haben sollen. Doch mit welcher Technik kann man noch schnell und einfach verbindliche Dokumente wie Verträge oder Gerichtseingaben versenden? Mit De-Mail und der eID-Funktion des neuen, elektronischen Personalausweises? Sicherlich, aber hinsichtlich der Verbreitung, der Akzeptanz und der einfachen Nutzung hakt es noch erheblich, und die unerreichte Verbreitung sowie die Akzeptanz von Fax dürften zwei der Gründe sein, warum in praktisch allen größeren TK-Ausschreibungen nach Fax gefragt wird und warum in nahezu jeder Unified-Communications-Lösung Fax weiterhin ein zentraler Kommunikationsbaustein geblieben ist.

Fax mit T.38 oder mit G.711-Pass-Through?

Wie schon in Artikeln früherer Ausgaben des VAF Reports genauer aufgezeigt (siehe **[Deu01]** und **[Ste01]**) lässt sich Fax über IP-Strecken entweder mit dem Fax-over-IP-Protokoll T.38 oder mit G.711-Pass-Through übertragen. Bei den Autoren dieses Artikels herrscht die Meinung vor, dass T.38 besser geeignet ist, u. a. da es deutlich unempfindlicher gegenüber Paketverlusten ist und T.38-fähige Endgeräte – insbesondere Faxserver – es direkt erzeugen und interpretieren können, ohne sich mit leistungshungrigen DSP-Algorithmen um Modem-Codecs, z. B. für V.29, kümmern zu müssen.



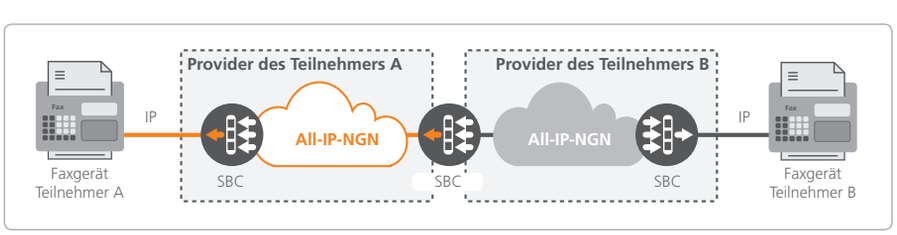
Grafik: VAF/Autoren

▲ **Bild 1:** Beim Übergang von einem NGN zum klassischen PSTN kann T.38 oder G.711-Pass-Through fest vorgegeben werden.

In zunehmendem Maße muss ein Fax-Device am NGN jedoch sowohl T.38 als auch G.711-Pass-Through unterstützen. Zum einen deshalb, weil die Deutsche Telekom in ihrer SIP-Trunk-Spezifikation 1TR118 **[DeT01]** dies zu Fax so spezifiziert (Auszug): »SIP-PBXs used for SIP-trunk must support fax based on G.711a at least. The NGN supports the transmission of T.38 fax, in a passive, transparent way, if the user entities agree to use it (offer-answer).« Und weiter: »The NGN supports the end-to-end transmission of T.38. T.38 fax gateways are not provided.« Zusammenfassend also: Fax-Devices müssen G.711-Pass-Through beherrschen, das NGN der Telekom leitet aber auch T.38 durch. Und zum anderen sollten beide Verfahren unterstützt werden, weil sich NGNs und IP-basierte Fax-Devices nun stark verbreiten. Dies soll mit den beiden folgenden Bildern verdeutlicht werden.

Hat der A-Teilnehmer sein Fax-Device mit einem NGN-Provider verbunden, der T.38 unterstützt, und sendet er ein Fax an einen B-Teilnehmer, der noch einen klassischen, PSTN/ISDN-Anschluss hat, so kann immer das T.38-Protokoll genutzt werden **(Bild 1),** da bei diesem Übertragungsweg immer die Netzübergangs-Gateways des NGN-Providers die T.38-Gegenstelle sind.

Wie in **Bild 2** gezeigt, koppeln sich NGN-Provider aber zunehmend auf Basis von IP mit Session Border Controllern (SBC). Hier kann das vom Fax-Device des A-Teilnehmers gewünschte T.38 auf seinem Weg zum Fax-Device des B-Teilnehmers von diesem



Grafik: VAF/Autoren

▲ **Bild 2:** Bei einer durchgängigen IP-Übertragung kann das Fax-Device oder der Provider des B-Teilnehmers T.38 ablehnen.

oder sogar schon vom Netzübergangs-SBC seines NGN-Providers abgelehnt werden, weil es von ihm nicht unterstützt wird.

Zum Glück sieht das SIP-Protokoll vor, dass bei stehender Medienverbindung von T.38 auf G.711-Pass-Through sozusagen zurückgeschaltet werden kann (Englisch: »Fax Fallback«). Dies erfolgt mit einem sogenannten re-INVITE-Befehl. Dieser Fallback-Mechanismus hat somit in letzter Zeit bei Fax-over-IP eine solch zentrale Bedeutung erhalten, dass er gewissenhaft in IP-Fax-Devices (Faxserver, ATAs und ISDN-Gateways) implementiert und ausführlich getestet sein sollte.

ITU-Norm	Bit/s	BAUD	Modulation	Einführung
V21 channel2	**300**	300	FSK	1962
V.27ter	**4.800/2.400**	1.600/1.200	PSK	1976
V.29	**9.600/7.200/4.800**	1.600/1.200	QAM/PSK	1976
V.17	**14.400/12.000/ 9.600/7.200**	2.400	Trellis	1991
V.34fax	**33.600/28.800**	3.200/3.429	Trellis	1994/1996
All-IP-Tauglichkeit:	**grün** = ☺	**gelb** = 😐	**rot** = ☹	

▲ **Tabelle 1:** Mit zunehmender Übertragungsrate und Schrittgeschwindigkeit der Fax-Codecs steigt die Abhängigkeit der Fax-over-IP-Übertragung von den QoS-Einstellungen.

Optimierung von Faxparametern

Mit dem Erstarken der Fax-Pass-Through-Übertragung in der Praxis müssen wir uns auch wieder mehr dem Thema Quality of Service (QoS) der IP-Übertragungsstrecke (d. h. Packet Loss, Delay, Jitter) widmen.

Ist einem Anwender Fax hinreichend wichtig, so kann man sicher dafür sorgen, dass das anwendereigene IP-Netz und die IP-Anbindung an das NGN seines ITSP (Internet Telephony Service Provider) eine gute QoS aufweist. Was aber kann man beim B-Teilnehmer voraussetzen, wenn dieser auch All-IP-basiert faxt? Sicherlich ein nicht unerhebliches Delay, wenn er in den USA oder gar Australien angesiedelt ist. Oder Paketverlust, weil er eine Internetanbindung ohne bidirektionale Priorisierung des Faxmedienstromes nutzt? Um solchen Unwägbarkeiten zu begegnen, sollte man sein Fax-Device besser so konfigurieren, dass es etwas langsamer, dafür aber robuster faxt. Konkret sollte man zunächst vom V.34fax **(Tabelle 1),** auch Super-G3-Fax genannt, runterschalten indem man Übertragungsraten von 33.600 und 28.800 Bit/s sperrt. Nur wenn das nicht genügend Stabilität bringt, wären auch 14.400 und 12.000 Bit/s zu unterbinden, indem man in den Voreinstellungen maximal 9.600 Bit/s erlaubt.

Eine weitere Einstellmöglichkeit, die die meisten Fax-Devices bieten, ist der Error Correction Mode (ECM). Wird er eingeschaltet und auch vom Empfänger unterstützt, kann dieser mit einer Checksumme jedes 256-Byte-Frame auf Richtigkeit überprüfen und im Fehlerfall vom Sender die wiederholte Übertragung anfordern. Dieses Vorgehen bringt auch bei All-IP-Übertragungsstrecken in der Regel eine stabilere Übertragung.

Migration der Faxrufnummern

Wenn die an den SIP-Trunk angeschlossene TK- oder UCC-Anlage – wie beispielsweise Microsoft Lync bzw. Skype for Business – Fax nicht oder nicht hinreichend gut unterstützt, können die Fax-Durchwahlrufnummern entweder CPE-basiert oder netzbasiert aus dem Rufnummernblock des SIP-Trunks auf andere Sprachanschlüsse weitergeleitet bzw. geschwenkt werden. Dazu im Einzelnen:

CPE-basiert: CPE (Customer Premises Equipment) bezeichnet Geräte, die beim Kunden stehen. Die hier benötigten Gerätefunktionen sind zum einen die E-SBC-(Enterprise-Session-Border-Controller-)Funktion, die den SIP-Trunk vom Provider zur IP-basierten UCC/TK-Anlage weiterleitet. Dies kann der E-SBC im Transparent-Mode oder im softwaretechnisch aufwendigeren Back-to-Back-User-Agent-Mode (B2BUA) tun (siehe dazu auch den Fachbeitrag von Mathias Hein auf S.16 ff. dieser Ausgabe). Zum anderen werden die Gateway- und Voice-Routing-Funktionen benötigt, die es ermöglichen, die Faxdurchwahlrufnummern nicht zum internen SIP-Trunk, sondern zu Faxgeräten und Faxservern (um-) zu leiten. Dies kann klassisch über ISDN- oder Analog-Ports, aber auch direkt per Software zu einem integrierten Faxserver erfolgen.

Netzbasiert steht für NGN-Funktionen des ITSP. Da im NGN sowieso ein Voice-Routing erfolgt, kann dieses zunehmend auch zur Unterstützung der Rufnummernmigration beim Kunden eingesetzt werden, und im NGN werden dann die Faxdurchwahlrufnummern vom SIP-Trunk auf einen anderen Sprachanschluss geschwenkt. Sind dies z. B. einfache Endgeräte-SIP-Accounts, so können an diese Analog-Telefon-Adapter (ATA) angebunden werden und an deren a/b-Port wiederum klassische Faxgruppe 3-Endgeräte. Bei höherem Faxvolumen oder einer Faxintegration in Computeranwendungen können die Faxdurchwahlrufnummern auf einen zweiten SIP-Trunk geschwenkt werden, der sie zu einem Faxserver leitet. Ist keine tiefe Computerintegration gefordert und das Faxvolumen geringer, können Faxdurchwahlrufnummern auch zu einem cloudbasierten Faxserver geschwenkt werden, der Fax über ein möglichst kompatibles Computerformat – wie PDF – empfängt und sendet. ■

Literatur:

[Deu01]: Deutinger, J.: Fax in Zeiten des Internets, VAF Report 2/2014, Seite 20ff.

[Ste01]: Steinkopf, A.: Was ist ein SIP-Trunk?, VAF Report 1/2015, Seite 20ff.

[DeT01]: 1TR118 Technical Specification of the SIPTrunking Interface between a SIP-PBX with DDI and the NGN Platform of Telekom Deutschland. Version 1.0, 30.06.2015, Hrsg.: Deutsche Telekom AG

Autorenkollektiv

Johann Deutinger, Jurgen Van Maele, Andreas Steinkopf

J. Deutinger ist Technik-Vorstand bei der Ferrari electronic AG
J. Van Maele ist Solution Director EMEA bei AudioCodes Ltd
A. Steinkopf ist Produktmanager für VoIP bei der QSC AG

Der Strom kommt bei VoIP nicht mehr aus der Telefonsteckdose

Weshalb sich Unternehmen mit USV befassen sollten

Bei einer Umstellung von ISDN auf VoIP bildet die unterbrechungsfreie Stromversorgung (USV) eine zusätzliche Anforderung für die Sicherstellung der Verfügbarkeit des Dienstes Telefonie.

Die amtliche Statistik weist für Deutschland im Jahr 2014 rund 147.800 Unterbrechungen der Stromversorgung im Niederspannungsbereich aus. Erfasst werden Unterbrechungen, die länger als drei Minuten dauern. Als durchschnittliche Versorgungsunterbrechung ermittelten die Statistiker daraus einen Wert von 16,2 Minuten/Jahr je Letztverbraucher, und in dem alternativ anwendbaren sogenannten SAIDI Index (System Average Interruption Duration Index) betrug der Wert für das Jahr 2014 dann 12,28 Minuten/Jahr. (Quelle: Monitoringbericht 2015 der Bundesnetzagentur zu den Energiemärkten, Seite 70 ff.). Um hier keinen falschen Eindruck zu erwecken: Die Verfügbarkeit der Stromversorgung kann in Deutschland, zumal im internationalen Vergleich, als sehr hoch angesehen werden. Dennoch sollten sich gerade Verantwortungsträger in Unternehmen vergegenwärtigen, dass es auch in Deutschland immer wieder zu kürzeren oder auch längeren Ausfällen der öffentlich bereitgestellten Versorgung mit Elektrizität kommt.

Die Auswirkungen stellen ein Risiko dar, das in das Risikomanagement des Unternehmens mit einbezogen werden muss und dem durch geeignete Maßnahmen entgegengesteuert werden kann. Mit der inzwischen flächenhaften Verbreitung des Wechsels von klassischer Analog/ISDN-Telefonie auf Voice-over-IP (VoIP) – sowohl im Bereich der TK-Systeme und der Telefone als auch hinsichtlich der sogenannten All-IP-Anschlüsse an die öffentlichen Telekommunikationsnetze – kommt nun hinzu: Bei einem Stromausfall kann nicht mehr ohne Weiteres telefoniert werden. Unternehmen brauchen darum mit Blick auf die Telefonie (neue) Lösungen. Denn sowohl die Kontinuität der geschäftlichen Kommunikationsprozesse als auch Forderungen aus dem Bereich des Arbeitsschutzes müssen hierbei bedacht werden.

Ermittlung der Abwärme in einem VoIP-Kabelschrank

Element *Leistungsaufnahme des Elements in Watt*	**Multiplikationsfaktor** *Gewichtung*	**Abwärme** *Resultierender Richtwert*
Switches ohne PoE-Stromversorgung	1,0	_____ Watt
Switches mit PoE-Stromversorgung	0,6	_____ Watt
Separate PoE-Netzteile (Midspan)	0,4	_____ Watt
Sonstige IT-Geräte	1,0	_____ Watt
USV-System	0,9	_____ Watt
Permanente Beleuchtung	1,0	_____ Watt
	Summe	_____ Watt

Tabelle: VAF, nach Angaben von APC / Schneider Electric

▲ **Tabelle 1:** Berechnung der Abwärme aus den angegebenen Leistungsaufnahmen der Elemente in Watt

Forderungen aus dem Arbeitsschutz

Gemäß § 10 Absatz 1 Satz 1 des Arbeitsschutzgesetzes (ArbSchG) hat der »Arbeitgeber (…) die Maßnahmen zu treffen, die zur Ersten Hilfe, Brandbekämpfung und Evakuierung der Beschäftigten erforderlich sind.« Und weiter heißt es im Satz 3: »Er hat auch dafür zu sorgen, dass im Notfall die erforderlichen Verbindungen zu außerbetrieblichen Stellen, insbesondere in den Bereichen der Ersten Hilfe, der medizinischen Notversorgung, der Bergung und der Brandbekämpfung eingerichtet sind.« Was darunter konkret zu verstehen ist, wird von der gesetzlichen Unfallversicherung in der Informationsschrift »Erste Hilfe im Betrieb« (DGUV BGI/GUV-509, Juli 2013) beschrieben. Der Abschnitt 5.1 »Alarm- und Meldeeinrichtungen« beginnt mit der geradezu lapidaren Feststellung: «Die gebräuchlichste Meldeeinrichtung ist das Telefon.«

Geschäftliche Anforderungen

Darüber hinaus hat der Ausfall der Telefonie in den meisten Unternehmen auch eine nicht unerhebliche Auswirkung auf die Geschäftsprozesse. Stehen die Telefone und die IP-Komponenten still, weil deren Stromversorgung unterbrochen ist, können keine

Bestellungen, Aufträge etc. mehr abgewickelt werden und es drohen entsprechende Einbußen. Es sollte darum vor dem Hintergrund des individuellen Geschäftsmodells geprüft werden, wie lange Überbrückungszeiten mit Ersatzstromversorgung erforderlich sind. Schließlich muss auch eine Strategie für das geordnete Herunterfahren (Shut-down-strategie) der IT-Komponenten zum Ende der kürzeren oder längeren Überbrückungszeit ermittelt werden, unter anderem auch, um z. B. Datenverlust oder Beschädigung der IT-Hardware zu vermeiden.

USV und VoIP-Technik

Bei der klassischen, analogen Telefonie kommt die Stromversorgung der Telefone aus dem Telefonnetz. ISDN-Telefonanlagen erfordern jedoch bereits eine zentrale Stromversorgung, und deren Verfügbarkeit wurde in der Regel schon in der Vergangenheit durch eine USV abgesichert. Durch die flächendeckende Umstellung von ISDN auf VoIP werden die Karten nun neu gemischt.

Ein Grundproblem der VoIP-Technik besteht in der Stromversorgung der IP-Telefone. Lokale Stromversorgungen bedeuten den Einsatz einer Vielzahl kleiner Steckernetzteile und jeweils die Belegung eines 220-V-Steckplatzes durch ein Telefon. Dies ist ein Rückschritt gegenüber den bisherigen Telefonlösungen. Die VoIP-Telefone werden darum typischerweise über die Netzwerkanschlusskabel mit Strom versorgt. Diese standardisierte Variante (IEEE 802.3 af bzw. 802.3 at) wird als Power-over-Ethernet (PoE) bezeichnet und versorgt die angeschlossenen Endgeräte über ein achtadriges Ethernetkabel mit Energie (802.3af: max. 15,4 W und 802.3 at: max. 25,50 W).

Die Auswahl eines USV-Systems im EV- und GV-Bereich beruht auf folgenden Faktoren:

- Gesamte erforderliche Leistungsaufnahme in Watt
- Erforderliche Überbrückungszeit in Minuten
- Gewünschte Stufe der Redundanz oder Fehlertoleranz
- Erforderliche Spannung und Anzahl der Steckdosen

Etagenverteiler

Die Energiequelle für PoE wird in der Regel im Etagenverteiler (EV) in Form eines Layer-2-/Layer-3-Switches/Routers untergebracht. Dies bedeutet, dass hier die Leistung für die Versorgung von unter Umständen hunderten IP-Telefonen bereitgestellt werden muss. Ein Stromausfall im EV hat dadurch auch einen Ausfall aller angeschlossenen Telefone zur Folge. Soll dieses Verfügbarkeitsrisiko abgefedert werden, ist für den EV eine entsprechend leistungsfähige USV vorzusehen. In den meisten EV stehen bisher weder USV noch (ausreichende) Möglichkeiten zur Lüftung oder Kühlung zum Schutz vor Überhitzung zur Verfügung. Durch die hohe Leistungsaufnahme der aktiven Komponenten im EV heizt sich die Luft jedoch zwangsläufig auf. Darum muss bei einem Umstieg auf VoIP unter Umständen die Klimaanlage des EVs neu dimensioniert werden **(Tabelle 1).** Ähnliches gilt auch für die eventuell vorhandenen Gebäudeverteiler (GV).

Rechenzentren

In den Rechenzentren werden nicht nur die Server und zentralen Rechner, sondern auch die VoIP-Telefonanlagen untergebracht. Meist operieren die modernen VoIP- und UC-Systeme als reine Anwendungen auf einem oder auf mehreren virtuellen Rechnern. Dieser zentrale Bereich ist in den meisten Unternehmen bereits mit USV-Systemen ausgerüstet. Hier ist zu überprüfen, ob die Überbrückungszeiten der bisher vorhandenen USV den höheren Verfügbarkeitsanforderungen der VoIP-Technologie genügen.

Planung und Betrieb

Mittels einer genauen Analyse der Anforderungen, der Infrastruktur und der sonstigen Systembedingungen (z.B. Virtualisierung) können die notwendigen Elemente eines USV-Konzepts ermittelt werden: die benötigten Überbrückungszeiten der USV bei Stromausfall, die optimale Shut-down-Strategie der Rechner und Netzressourcen, die Größe der USV, die benötigten Batteriemengen und die Anforderungen an die Kühlung. Über ein u. U. in der USV intergriertes Management und Monitoring auf Basis des SNMP-Protokolls lassen sich darüber hinaus die Temperaturen, die Luftfeuchtigkeit, die aktuelle Leistungsaufnahme, und der Zustand der Baterien ermitteln.

Die wichtigsten Schritte zur Realisierung der gesicherten Stromversorgung einer VoIP-Lösung:

- Genaue Definition der anfallenden Strom- und Kühllasten
- Festlegung der notwendigen Überbrückungszeit und der Shut-down-strategien
- Festlegung der USV-Lösung mit zugehörigen Batterieerweiterungen
- Verwaltung der USV-Systeme (Aktivität, Temperaturen, Batteriealter) über ein zentrales Management bzw. automatisierter Shut-down der angeschlossenen Rechnersysteme im Katastrophenfall

Fazit

Die Umstellung von Analog/ISDN auf VoIP erfordert unter dem Aspekt der Stromversorgung eine neue Beurteilung der Verfügbarkeit der Telefontechnik. Nur mittels eines durchgehenden USV-Konzepts lassen sich auch bei einem Stromausfall Notrufe noch absetzen, die Kontinuität der Geschäftsprozesse gestalten und geordnete Shut-down-Strategien realisieren. ■

Autor:

Christian Stolte ist im Bereich der USV-Lösungen/VoIP (Marke APC) als Systems Engineer und Solution Architect bei der deutschen Tochter des international agierenden Elektroherstellers Schneider Electric tätig. Ch. Stolte ist u. a. zuständig für Kundenberatung und Partnertrainings.
USV-Lösungen und Kühlsysteme werden in Deutschland über die ALSO Deutschland GmbH distribuiert.

www.schneider-electric.de
www.also.com

Bauprodukteverordnung (BauPVo)

Neue Anforderungen an Installationskabel für Gebäude

Foto: www.shutterstock.com

Spätestens ab 1. Juli 2017 dürfen nur noch Installationskabel in den Verkehr gebracht werden, die vorschriftenkonform die einheitlichen Euroklassen für das Brandverhalten (React to Fire) ausweisen. Wer Installationskabel vertreibt und verbaut, sollte sich schon jetzt darauf einstellen.

Die rechtliche Grundlage für die sich jetzt abzeichnenden, weitreichenden Neuerungen im Geschäft mit Installationskabeln bildet die Bauprodukteverordnung (BauPVo, englisch: Construction Products Regulation, CPR) aus dem Jahr 2011. Sie trat als EU-Verordnung Nummer 305/2011 bereits am 1. Juli 2013 in Kraft und muss für ihre Geltung in den EU-Mitgliedsstaaten nicht erst in nationales Recht übertragen werden. Kabel und Leitungen, die für den dauerhaften Einbau in Gebäuden vorgesehen sind, fallen als sogenannte Bauprodukte ebenfalls unter die Verordnung. Sie waren aber bisher in der Anwendung davon ausgenommen. Der Grund liegt darin, dass die EU-Kommission zunächst die europäischen Normierungsgremien CEN und CENELEC beauftragen musste, für Kabel einheitliche Euroklassen hinsichtlich des Brandverhaltens zu definieren und die Grenzwerte der einzelnen Parameter sowie die Prüfverfahren festzulegen. Die Klassenfestlegungen sind inzwischen erfolgt, die Prüfverfahren sind beschrieben und Zertifizierungsstellen notifiziert. Mit einer Übergangsfrist von zwölf Monaten ab dem 1. Juli 2016 wird die BauPVo nunmehr auf den Bereich der Installationskabel ausgedehnt.

React to Fire versus Resist to Fire

Der Regelungsgegenstand der BauPVo darf nicht verwechselt werden mit den im Markt weithin bekannten und beispielsweise auch in der Muster-Leitungsanlagen-Richtlinie (MLAR) und anderen Vorschriften sowie Richtlinien umfänglich berücksichtigten, normativen Forderungen an den Funktionserhalt von Kabeln und Leitungen im Brandfall gemäß DIN 4102-12. Wie lange widersteht eine Leitung einem Brand, sodass ihre Funktion erhalten bleibt, um beispielsweise einen Brandalarm übertragen zu können? Im Englischen wird dies auch als »Resist to Fire« bezeichnet. Im Zusammenhang der BauPVo geht es hingegen um das Brandverhalten im Hinblick auf die exotherme Brandleistung, die Rauchgasdichte, die Azidität und das abtropfende Verhalten der Kabel und Leitungen selbst (»React to Fire«).

Brandablauf und Baumaterialien

Brand in Gebäuden ist seit Menschengedenken eine der großen Gefahren für die sich darin aufhaltenden Personen. Neben der Hitze sind vor allem die Verrauchung der Räume und die verätzende Wirkung des Qualms lebensgefährlich. Gerade die ersten Minuten nach Ausbruch eines Feuers sind entscheidend für eine erfolgreiche Flucht aus einem brennenden Gebäude, und dafür sind eine brauchbare Sicht ohne zu viel Rauch und freie Atmung ohne toxische Gase notwendig. Längere, rauchfreie Zeiten tragen somit maßgeblich zu einer erfolgreichen Evakuierung bei, denn die massive Hitzeentfaltung (Flash over) folgt im Brandablauf in der Regel erst etwas später.

Erheblichen Einfluss auf das Brandverhalten haben die verbauten Materialien. Vor diesem Hintergrund erschließt sich auch die Bedeutung, die Kabeln und Leitungen in Gebäuden hinsichtlich ihres Brandverhaltens im Sinne von React to Fire in dreifacher Hinsicht zukommt:

- als Brandherd bzw. -ursache,
- als Brandfortleitungsmedium,
- als verbrennendes Bauteil (Brandlast).

Die Kabelindustrie hat diese Zusammenhänge schon vor Jahren aufgegriffen und neben den PVC- und PE-basierenden Isolationswerkstoffen gerade auch für Installationen in Gebäuden neue, halogenfreie und schwer entflammbare Kunststoffe eingeführt. Da die Produkte in der Regel einen höheren Preis haben, hat der Markt sie nur zum Teil angenommen. So gibt es einerseits Datenkabel heute fast ausschließlich in

Weblinks:
www.zvei.org
www.vde.de

Literatur:
Brandschutzkabel erhöhen die Sicherheit – Kabel als vorbeugender Brandschutz nach der europäischen Bauprodukteverordnung. White Paper des ZVEI – Zentralverband Elektrotechnik und Elektronikindustrie e. V., Frankfurt, April 2015.

Verordnung (EU) Nr. 305/2011 zur Festlegung harmonisierter Bedingungen für die Vermarktung von Bauprodukten (…), 9. März 2011.

schwer entflammbaren, nicht korrosiven Ausführungen (Flame Retardent non Corrosive, FRNC), wo hingegen 230 V-Stromleitungen immer noch überwiegend auf Basis von PVC-Werkstoffen (sog. NYM-Kabel) in den Markt gelangen.

Was kommt auf uns zu?

Vor dem Hintergrund der BauPVo entwickeln Hersteller verstärkt neue Granulatmischungen (Compounds) für die Kabelmäntel, um sich in der aktuellen Marktentwicklung geeignet zu positionieren. Unter dem Begriff »Brandschutzkabel« wird dabei auch der Ansatz verfolgt, diese als höherwertige Produktgruppe jetzt breiter am Markt zu etablieren. Die Erwartung ist auch nicht von der Hand zu weisen, denn mit der anstehenden Ausdehnung der BauPVO erfolgt die Einführung einer tiefgreifenden, neuen Regulierung des Markts für Kabel und Leitungen in Gebäuden als Bauprodukte mit durchaus maßgeblichem Einfluss auf das Brandverhalten. Im Folgenden werden wichtige Veränderungen kurz beschrieben.

Neue Klassen und externe Prüfungen

Bisherige Klassifizierungen für Rauchgasdichte, Korrosivität sowie Einkabel-/Mehrkabelbrandprüfung werden abgelöst und europaweit einheitlich durch die Brandklassen aus der EN 50575:2014 (ursprünglich beschrieben in der EU 2006/751) ersetzt. Die Klassen lauten A, B1, B2, C, D, E und F. Klasse A bedeutet »nicht brennbar« und wird wohl kaum am Markt zu finden sein. Klasse F ist reserviert für Kabel, die zwar in den Verkehr gebracht werden dürfen, jedoch nicht die Anforderungen der Klasse E erfüllen. In den Klassen D und E erfolgen lediglich Typmusterprüfungen, für die Erreichung der Klassen A, B1, B2 und C sind hingegen regelmäßige Prüfungen und Maßnahmen im Produktionsvorgang vorgeschrieben. Des Weiteren sind drei Unterklassen vorgesehen. Diese betreffen die Eigenschaften der Rauchentwicklung/-dichte (Unterklasse »s«), der Säureentwicklung/Korrosivität (»a«) sowie der brennenden Tropfen (»d«).

CE ist nicht mehr gleich CE

Das bekannte CE-Kennzeichen erhält in diesem Zusammenhang eine neue, zusätzliche Bedeutung. Denn bisher wurde es bei Kabeln und Leitungen regelmäßig lediglich dazu verwendet, die Einhaltung der Niederspannungsrichtlinie (2014/35/EU) anzuzeigen und nur gelegentlich auch die Einhaltung der RoHS-Richtlinie (2011/65/EU) sowie der REACH-Verordnung (1907/2006/EU).

Zudem war es bisher nur eine Selbsterklärung des Herstellers. Künftig ist in Bezug auf die Erklärung zu den Brandklassen für den Hersteller der Weg über eine notifizierte Stelle als externer Zertifizierer zwingend vorgeschrieben. Zusätzlich müssen auf der CE-Konformitätskennzeichnung die testierte Brandklasse und weitere Angaben zur Identifikation des Herstellers, des Prüfungsvorgangs und des vorgesehenen Produktgebrauchs enthalten sein. Die Kennzeichnung erfolgt mit einem entsprechenden Etikett an der Trommel oder am Wickelring; ggfs. können auch Informationen auf den Kabelmantel gedruckt werden. Künftig kann es sich einmal mehr empfehlen, auf der Baustelle das CE-Konformitätszeichen mit der Angabe in der Auftragsbestätigung abzugleichen.

Umsetzung und Hürden in der Praxis

Das Ziel der gesamten Maßnahmen ist es, den passiven Brandschutz in Gebäuden durch die Verwendung von hochwertigen Kabeln im Sinne des Brandverhaltens zu verbessern. Um nun die praxisgerechte Anwendung der neu klassifizierten Produkte hinzubekommen, werden anerkannte, konkrete Zuordnungslisten benötigt, denen zu entnehmen ist, in welcher Klasse von Gebäuden oder Gebäudebereichen welche Kabelklassen notwendig bzw. maximal noch zulässig sind. Fluchtwege unterliegen sicherlich strengeren Kriterien als andere Räume, Pflegeheime benötigen längere Evakuierungszeiten als freistehende, kleine Verwaltungsgebäude usw. Vom Industrieverband ZVEI liegt eine systematische Zuordnungsliste als Vorschlag vor. Die Verständigung auf eine allgemein anerkannte Liste und in der Folge die Umsetzung in Bauvorschriften sowie Richtlinien stehen noch aus und sind jetzt dringend geboten. Denn insbesondere Planer und Bauherren dürften sich aus Gründen der Investitionssicherheit jetzt zunehmend an den neuen Klassifizierungen orientieren und stehen derzeit noch vor der Herausforderung, diese für Projektvorhaben bzw. in Ausschreibungen geeignet zu formulieren.

Autor:


Foto: VAF

Dipl.-Ing. Stefan Schreiber ist in der Geschäftsführung von eku Kabel & Systeme GmbH & Co. KG in Bochum tätig. Das Unternehmen ist seit 1975 am Markt und mit rund 100 Mitarbeitern an acht Standorten als Mehrwertdistributor und Spezialist für passive Datennetzwerktechnik und Systemkabel vertreten.
E-Mail: s.schreiber@e-k-u.de
www.e-k-u.de

VAF-Projektbericht: Verkehrsmessungen sollen Muster erkennbar machen

Was läuft da so im LAN?

Um das Zusammenspiel von VoIP, Video und Daten im Netzwerkverkehr genauer zu untersuchen, fanden unter Leitung von Prof. Dr.-Ing. Gerd Siegmund erste Messungen in den LAN von Mitgliedsunternehmen statt. Das Projekt soll fortgesetzt werden und zu verbesserten Planungsgrundlagen für UC-Netze führen.

Autor: Prof. Dr.-Ing. Gerd Siegmund

Im Herbst vergangenen Jahres untersuchten im Rahmen einer VAF-Projektreihe Uwe Bernhardt und Alexander Muth, beide Studenten der Technischen Hochschule Nürnberg, den Verkehr in den LAN von drei VAF-Mitgliedsunternehmen. Im VAF wurde das Projekt von Jens Crins, ITK-Fachreferent begleitet. Die Vorarbeiten waren bereits im Frühjahr und Sommer des Jahres erfolgt. Im Vordergrund der ersten Projektphase stand die Suche nach typischen Verkehrsmustern für bestimmte Kommunikationsarten.

Die vorläufigen Erkenntnisse werden im Rahmen dieses Beitrags berichtet und sollen in einer zweiten Projektphase durch weitere Untersuchungen validiert und ergänzt werden. In der Folge könnten als drittes Teilprojekt dann belastbare Erkenntnisse über typische Muster als Basis für einen Generator genutzt werden, der in einem Testsystem als Verkehrsquelle für VoIP/Video/Datenverkehr dient.

Um die Vertraulichkeit der internen Daten der besuchten Firmen sicherzustellen, wurde eine einfache Software erstellt und eingesetzt, mittels derer die mit Wireshark aufgezeichneten Daten noch vor Ort gezielt statistisch ausgewertet werden konnten. Unmittelbar im Anschluss der Auswertung wurden die aufgezeichneten Originaldaten wieder gelöscht. Zur weiteren Analyse konnten dann nur noch unkritische Daten festgehalten werden. Dazu gehörten beispielsweise die Paketlänge, die Anzahl der Pakete, der Paket-Typ (UDP oder TCP) und die Information, zu welchem Zeitpunkt ein Paket übertragen wurde. Der ursprünglich weitergehende Gedanke, auch eine Software zur automatischen Anonymisierung der gesamten aufgezeichneten Daten selbst zu erstellen, sodass diese für weitere Analysen als Datenreservoir zur Verfügung stehen könnte, musste aus Zeit- und Aufwandsgründen – zumindest im Rahmen dieser Projektreihe – aufgegeben werden. Den Projektteilnehmern ist nach Recherchen nicht bekannt, dass Lösungen zur vollständigen Anonymisierung am Markt verfügbar wären.

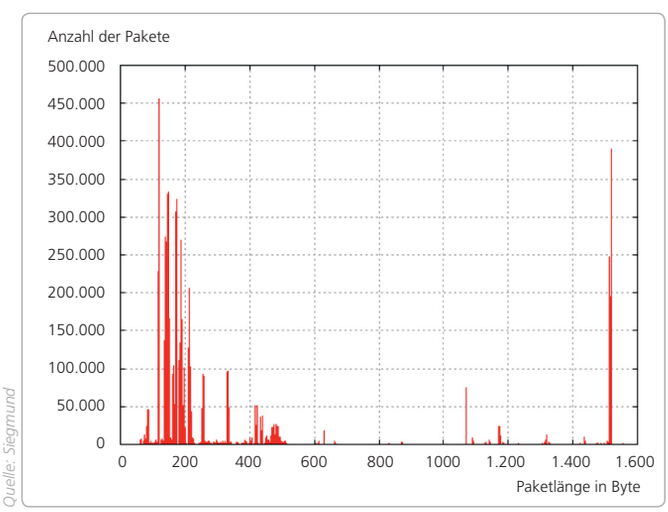
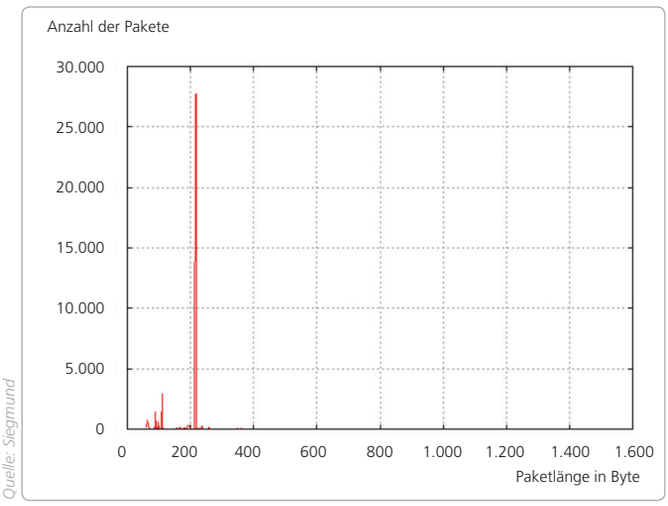


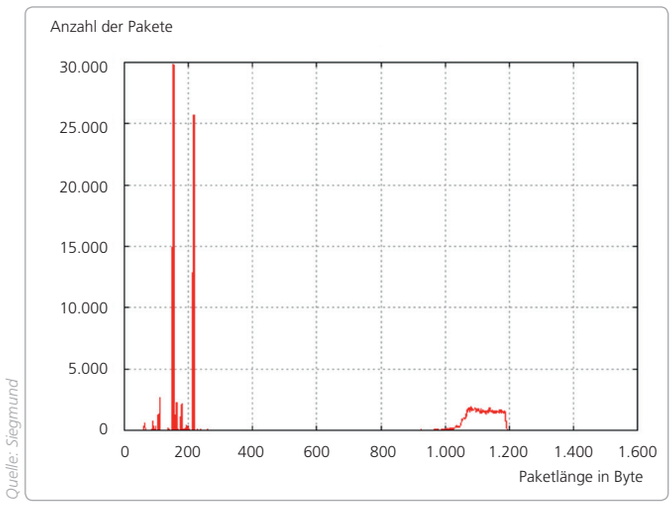
Bild 1: Beispiel für die Messung von Datenverkehr (hier mit Desktop-Sharing)

Motivation und theoretischer Hintergrund

Die Netzauslastung wird nur durch zwei Parameter festgelegt: zum einen durch die Last, also die Anzahl der Pakete, die pro Sekunde auf ein System (ein Netz, einen Router, einen Switch oder eine Leitung) treffen, und zum anderen durch die Anzahl der Pakete durchschnittlicher Länge, die das System pro Sekunde bearbeiten kann. Der zweite Wert beschreibt die Leistungsfähigkeit des Systems und ist durch die Bandbreite oder die »Performance« des Geräts (Router oder Switch) durch den Hersteller vorgegeben. Bei der Einführung von VoIP wird häufig zuerst nur die erforderliche Bandbreite für die Übertragung der Sprache und die Bandbreite des Übertragungssystems beurteilt. Das ist jedoch falsch, weil die übertragenen Pakete nicht »bit-weise« abwechselnd durch das System transportiert werden. Ein Router oder Switch bearbeitet immer Pakete, und wenn gerade ein Paket bearbeitet wird, müssen andere Pakete in einem Speicher warten. Die Bearbeitung eines Pakets im Netzelement hängt nicht von der Paketlänge ab. Ein Router analysiert den IP-Header und muss dann anhand der



▲ **Bild 2:** Beispiel für VoIP mit UDP



▲ **Bild 3:** Videoübertragung mit UDP

Routing-Tabelle eine Entscheidung für die Weiterleitung des Pakets treffen – völlig unabhängig von der Länge des Pakets. Wenn die Entscheidung getroffen ist, wird das Paket zum gewünschten Ausgangsport geleitet und »fließt« mit der gegebenen Übertragungsgeschwindigkeit ab. Wie lange das dauert, hängt dann wieder von der Länge des Pakets ab, ist aber für die Betrachtungen hier nicht von Bedeutung, da in der Regel der »Abfluss« keinen Engpassfaktor der Systemkomponenten darstellt. Bei VoIP werden mit RTP relativ kleine Pakete (160 Byte plus Overheads durch UDP, IP und Ethernet) transportiert. Diese werden aber mit einer festen Paketrate übertragen (alle 20 ms ein Paket ergibt 50 Pakete/s).

Durch die kleinen Pakete ist die umgerechnete Bandbreite für eine Sprachübertragung relativ gering und beträgt ungefähr 100 kbit/s. Die Paketrate ist mit 50 Paketen/s aber relativ hoch. Dies führt dazu, dass der VoIP-Verkehr häufig falsch eingeschätzt wird. VoIP stellt für ein lokales Netz also eine relativ große Belastung dar. Zudem bringt die Verbreitung von Anwendungen wie Videokonferenzen und Desktop-Sharing zunehmend Verkehr in die Firmennetze, der ein einfaches Festhalten an den bisher bewährten QoS-Regeln, wie z. B. der Verkehrstrennung von VoIP, auf den Prüfstand stellt. Um hier zu neuen und angemessenen Erkenntnissen zu kommen, müssen über verkehrstheoretische Betrachtungen hinaus auch die realen Netze genauer untersucht werden. Im Folgenden werden erste, vorläufige Erkenntnisse berichtet.

Die Messergebnisse

1. Datenverkehr

Die Messungen des Datenverkehrs zeigten einige Überraschungen: Zum einen wurden unerwartet viele sog. Jumbopakete mit über 7.000 Byte identifiziert. Die klassische maximale IP-Paketlänge liegt bei 1.518 Byte. Bei den drei Messungen wurden einmal 15 Prozent und einmal sogar 23 Prozent der aufgezeichneten Pakete mit einer Länge über 1.518 Byte verzeichnet. Die zweite Überraschung war der relativ große Anteil von Managementpaketen, die weder UDP noch TCP zugeordnet werden konnten. Dieser Anteil machte bei zwei von drei Messungen 19 Prozent aus, bei der dritten Messung waren es 9 Prozent des Gesamtverkehrs. Weniger überraschend war die Verteilung der Paketlängen. Hier kommen – typisch für IP-Verkehr – nur sehr viele sehr kleine und sehr große Pakete vor. Dieses Muster lässt sich durch die typischen kurzen Anfragen (Request – ein Klick auf einen Link) und die Übertragung der abgefragten Inhalte erklären: Es werden in der Folge eines Requests viele Pakete mit der maximalen Länge übertragen sowie ein Paket, das den Rest des Inhalts überträgt. **(Bild 1)** Genau dieser Zusammenhang macht eine vorausschauende Berechnung der IP-basierten Netze so schwer, weil der Mittelwert (ca. 770 Byte) keine gute Vorausschau ermöglicht. Ein anderes Wort für den »Mittelwert« ist der »Erwartungswert«. Das bedeutet: Wenn man von einem LAN den Verkehr aufzeichnet, würde man aus dem statistischen Durchschnitt heraus erwarten, dass ein IP-Paket mit 770 Byte transportiert wird. Die Messungen belegten, dass dies nicht stimmt. Das aufgezeichnete Paket ist typischerweise entweder ca. 50 oder 1.518 Byte lang, aber nicht 770 Byte. Bei Anwendungen wie »Desktop-Sharing« konnte zusätzlich eine Häufung von Paketen mit einer Länge zwischen 200 und 600 Byte festgestellt werden. Nur in einem Firmennetz wurde diese Anwendung während der Messung im Netz ausgeführt. Genauere Aussagen können daher noch nicht getroffen werden.

2. VoIP

Beim Transport von Sprache mit den RTP-Paketen sendet eine Quelle sehr regelmäßig in festen und immer gleichen Abständen (z. B. alle 20 ms bei G.711) ein Paket mit einer festen Paketlänge (z. B. 200 Byte bei G.711). Bei der Standardübertragung findet man diese einzelne Häufung mit einer Paketlänge von 200 Byte bei der UDP-Übertragung. **(Bild 2)** Bei Anwendung von TCP findet man die gleiche Spitze in der TCP-Übertragung. Dies bestätigten auch die Messungen – bei VoIP gab es also keine Überraschungen.

3. Video

Bei der Videoübertragung zeigten zwei Messungen eine auffällige Häufung von

	Messung 1	Messung 2	Messung 3	Mittelwerte
Pakete insgesamt	13.409.898	1.924.489	465.859	
TCP	10.424.712 **(78 %)**	1.387.144 **(72 %)**	319.961 **(69 %)**	73 %
UDP	463.425 **(3 %)**	182.578 **(9 %)**	102.778 **(22 %)**	3–22 %
Weder TCP noch UDP	2.521.760 **(19 %)**	354.766 **(19 %)**	43.059 **(9 %)**	9–19 %
Pakete über 1.580 Byte	3.034.794 **(23 %)**	281.921 **(15 %)**	5.640 **(1,2 %)**	1,2–23 %
Systemauslastung	0,44 %	0,16 %	0,86 %	
Ankunftsrate in Paketen/s ohne VoIP	675,32	207,3	800,18	
Zusätzliche Pakete/s durch VoIP	56,81 **(7,8 %)**	62,5 **(23 %)**	195,8 **(20 %)**	

▲ **Tabelle 1:** Zusammenfassung der Messergebnisse

UDP-Paketen mit einer Länge zwischen 1.000 und 1.200 Byte **(Bild 3)**, die bei anderen Übertragungen nicht auftraten. Die vielen Pakete um 160 bzw. 200 Byte entsprechen der Sprachübertragung im Video-Stream. Bei einer Messung traten zusammen mit der Videoübertragung Häufungen in der TCP-Übertragung zwischen 200 und 600 Byte auf, diese waren sehr ähnlich zu den Häufungen bei der Desktop-Sharing-Anwendung. Mehr kann aus diesen drei Messungen nicht abgeleitet werden. Die Videoübertragung lässt sich also mit den bisherigen Ergebnissen noch nicht ausreichend charakterisieren, hier müssen weitere, isolierte Messungen folgen.

4. Auslastung der gemessenen Netze

In allen Messungen war die gesamte Systemauslastung kleiner als 1 Prozent der maximal möglichen Systemauslastung **(Tabelle 1).** In der Praxis wären Echtzeitübertragungen ohne Probleme und ohne Störungen durch Jitter und Paketverlust möglich, dies entsprach auch der Beobachtung während der Messungen.

5. Belastung der Netze durch VoIP

Wie unerwartet stark VoIP das Netz belastet, kann ein Beispiel aus den Messungen belegen **(Tabelle 2).** Die Angabe in bit/s zeigt, wie viel Bandbreite die jeweilige Übertragung entspricht. Die Angabe in Paketen/s entspricht der Paketrate, also der Belastung, die in das Netz durch ankommende Pakete eingebracht wurde. Die resultierende Netzbelastung ist dann die durchschnittliche Paketrate im Netz (l) geteilt durch die durchschnittliche Paketrate, die das System bearbeiten kann (μ). Letztere ist hier nicht dargestellt. Die Werte in Tabelle 2 sind einer Messung entnommen, also nicht repräsentativ. Dennoch lässt sich für dieses Beispiel festhalten: Mit den gemessenen 349,9 Paketen/s ist die Systembelastung durch VoIP massiv höher als die durch Standard-IP-Pakete und durch Jumbopakete. Mit diesen Messwerten ergibt sich für die Datenkommunikation mit IP-Paketen der Länge 1.500 Byte eine Paketankunftsrate von 16,78 Paketen/s je 100 kbit/s, für Jumbopakete sind es nur 3,38 Pakete/s je 100 kbit/s und für VoIP beachtliche 57,34 Pakete/s je 100 kbit/s. VoIP ist eine unerwartet und häufig unterschätzte, große Netzbelastung.

Übertragung	bit/s	Pakete/s (λ)
Daten mit 1.500 Byte je Paket	476.740	79,5
Daten mit Jumbopaketen	811.200	27,4
VoIP (nicht immer mit G.711)	610.200	349,9

▲ **Tabelle 2:** Der Unterschied zwischen bit/s und Pakete/s

Ausblick

Im Rahmen des VAF-Fachbereichs Technik wird derzeit die Fortsetzung der Untersuchungen organisiert. Zunächst sollen durch weitere Messungen im laufenden Jahr die Daten validiert und verfeinert werden. Auf einer im Ergebnis breiteren und robusten Datenbasis können dann typische Verkehrsmuster als Referenzen für die verbesserte Planung von UC-Netzen abgeleitet werden. In der Folge könnte an das bereits im Jahr 2014 erfolgreich abgeschlossene Projekt für die Entwicklung eines VoIP-Verkehrsgenerators angeknüpft werden. Das mittelfristige Ziel ist somit die Entwicklung eines Verkehrsgenerators für VoIP/Video/Datenverkehr und damit eines äußerst nützlichen Werkzeugs für die Teststellung von UC-Netzen. Aber bis dahin muss noch einige Arbeit erbracht werden. ■

Literaturhinweis: Bandbreitenberechnungen in VoIP-Systemen, Autor: Prof. Dr.-Ing. Gerd Siegmund, Studie im Auftrag des VAF Bundesverband Telekommunikation e.V., 36 Seiten, Hilden 2012.

Autor:

Foto: VAF

Prof. Dr.-Ing. Gerd Siegmund,
Technische Hochschule Nürnberg
Georg Simon Ohm

VOB-Praxis

Übergabe an den Nutzer? **Kennt die VOB nicht!**

Was die **Fachfirma** beachten sollte.

Grafik: iStockphoto.com/zoljo

Problem:

Bei unserem Projekt »Kommunikationstechnik für den Erweiterungsbau eines Pflegeheimes« haben wir alle beauftragten Arbeiten ordnungsgemäß und termingerecht abgeschlossen. Als nächstes steht ja wohl die Abnahme nach VOB/B an. Nun verlangt unser Auftraggeber von uns, dass wir noch eine Übergabe der Telekommunikationstechnik an die Nutzer – also die Beschäftigten des Pflegeheimes – durchführen müssen. Erst danach will er unsere Arbeiten abnehmen.

Wir sind aber der Meinung, dass wir nicht für die Einweisung der Nutzer zuständig sind, sondern mit Montage und Einrichtung der Technik ein abnahmefertiges Produkt abgeliefert haben. Müssen wir die Nutzerübergabe vornehmen? Und kann die Verweigerung dieser Übergabe die Abnahme verhindern?

»Viele Auftraggeber verlangen von der Fachfirma eine Einweisung der Nutzer – zu Unrecht«

Antwort des VOB-Praktikers:

Nein, die Verweigerung einer Übergabe im Sinne einer Einweisung der Nutzer darf die Abnahme durch den Auftraggeber nicht verhindern, wenn sie vorher nicht vereinbart worden ist. Dies gilt aus dem einfachen Grund, dass eine solche Übergabe in der VOB nicht als Pflichtleistung vorgesehen ist. Die VOB regelt das Verhältnis zwischen dem Auftragnehmer und Auftraggeber – nicht dem Nutzer.

Leider kommt es aber bei vielen Projekten vor, dass der Auftraggeber tatsächlich von der Fachfirma vor oder auch nach der Abnahme noch eine Übergabe an den Nutzer verlangt, obwohl das im Vertrag so nicht vereinbart ist. Bestimmt kann hier nicht immer unterstellt werden, dass der Auftraggeber bewusst eine Leistung einfordert, die ihm nicht zusteht – oftmals ist es Unwissenheit oder eine Fehleinschätzung der Abnahmebedingungen.

Dabei wird in der Regel das Argument strapaziert, dass doch letztlich der Telefonienutzer mit den neu bereitgestellten Leistungen arbeiten müsse, und deshalb sei eine Einweisung (Übergabe) erforderlich. Da eine Übergabe zusätzlich zur Abnahme in der VOB aber nicht als Pflichtleistung geregelt ist, kann sie nur vom Auftraggeber verlangt werden, wenn sie vorab vereinbart wurde.

Empfehlung:

In dem Fall sollte der Unternehmer praktisch abwägen. Es gilt eigentlich der VOB-Grundsatz: »Keine (zusätzliche) Erbringung von Leistungen ohne vorherige Regelung der zugehörigen Vergütung.«

Die Abwägung besteht darin, ob man nun ein Nachtragsangebot erstellt, oder ob das Projekt »so gut gelaufen ist«, dass die Übergabe an den Nutzer nachträglich mit einkalkuliert werden kann. Festzuhalten ist, dass der Auftraggeber keinen generellen Anspruch auf eine Übergabe hat.

Autor:

Hartmuth H. Gawlik
TK-Planungsingenieur und
VAF-Fachberater für Projekte mit
VOB/VOL-Hintergrund

VAF-Mitglieder können sich kostenlos beraten lassen, Fragen einsenden oder weitere Themen für die Rubrik vorschlagen.

Telefonische Anfragen unter:
02103 700-250

@ Kostenlose Beratung für Mitglieder:

tk-projektberatung@vaf-ev.de

Ferrari electronic AG

Kosten sparen und sicher in der Cloud mit der Software OfficeMaster Suite 6

Cloud-Lösungen liegen im Trend, und zunehmend setzt sich Microsoft Office 365 in Unternehmen durch, allem voran im Bereich der E-Mail-Kommunikation. Ein Wechsel in die Cloud erspart die Kosten für die Wartung lokaler Exchange-Server. Allerdings funktionieren lokale Faxserverlösungen nicht mehr oder sie sind durch die Öffnung für eingehende SMTP-Nachrichten erheblichen Sicherheitsrisiken ausgesetzt. Bisher gab es zu diesem risikobehafteten Vorgehen keine ernsthaften Alternativen. Die Anbindung über einen lokalen Exchange-Server mit Office 365 Hybrid-Mode ist zwar möglich, allerdings mit zusätzlichen Kosten verbunden.

Lösung: Die OfficeMaster Suite 6 bietet die gewohnten Funktionen wie Faxversand und -empfang in Outlook zusammen mit Postfächern in der Microsoft-Cloud. Eine neu entwickelte Integration in Office 365 unter Verzicht auf SMTP benötigt keinerlei eingehende Verbindungen. Damit sind etwaige Sicherheitsrisiken ausgeschlossen, da keine möglichen Angriffspunkte von außen vorhanden sind.

Grafik: Ferrari electronic AG

Mit Version 6 der OfficeMaster Suite bringt Ferrari electronic AG ein wegweisendes Produkt für den All-IP-Markt heraus: vollständige Integration in Office 365, Unterstützung von Exchange und Office 2016 und erstmalig auch direkte IP-Anbindung des Faxservers sowie der Voice- und SMS-Funktionen.

Kontakt:

Ferrari electronic AG
Tel.: 03328 455-90
info@ferrari-electronic.de
www.ferrari-electronic.de

innovaphone AG

Maximale Sicherheit mit der innovaphone PBX

Maximale Sicherheit mit innovaphone

Foto: innovaphone

Moderne Telefonanlagen sind nicht mehr räumlich begrenzt. Durch die Umstellung auf All-IP ist die Telefonanlage jederzeit über die weite Welt des Internet erreichbar – und das ist so gewollt. Denn nur so lassen sich der Anschluss an den SIP-Provider oder sogenannte Anywhere-Workplace-Konzepte realisieren, bei denen die Telefonanlage stets da ist, wo sich der Mitarbeiter befindet. In der Folge wird das Smartphone zur vollwertigen Nebenstelle, oder man telefoniert gleich über den Webbrowser, der selbstverständlich Zugriff auf alle Daten der Telefonanlage haben soll.

innovaphone empfiehlt: ITK-Systemhäuser sollten bei der Wahl von IP-Telefonanlagen und UC-Lösungen genau auf die integrierten Sicherheitsmöglichkeiten achten. Bei innovaphone wird Sicherheit seit jeher großgeschrieben, und die innovaphone PBX verfügt unter anderem über folgende Sicherheitsmechanismen:

- »State of the Art«-Sicherheitsprotokolle garantieren einen hohen Sicherheitsgrad.
- Das eigenentwickelte Betriebssystem ist nicht anfällig für die verbreiteten Viren, Würmer und Trojaner.
- SBC (Session Border Controller) ist standardmäßig in jeder innovaphone PBX enthalten.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

- Integrierte »Reverse-Proxy-Funktionalität« ermöglicht sicheren Zugriff auf die PBX von überall, passend zum Anywhere-Workplace-Konzept.

Fazit

Die innovaphone PBX bietet maximale Sicherheit ohne zusätzliche Kosten im Bereich der IP-Telefonanlagen und UC-Lösungen.

Kontakt:

innovaphone AG
Tel.: 07031 73009-0
sales@innovaphone.com
www.innovaphone.com

Verbandstermine 2016

28.–29.04.2016	Frühjahrstagung	Mitgliederversammlung	Trier
16.–17.06.2016	27. Jahrestagung Vertrieb	Fachtagung	Lübeck
22.–23.09.2016	Herbsttagung der ITK-Systemhäuser	Fachtagung	Braunschweig
11.–12.11.2016	35. Jahrestagung Technik und Service	Fachtagung	Erfurt

Aktuelle Kurstermine

wissenswerkstatt
www.vaf-wissenswerkstatt.de

Schulungen

Datum	Kursbezeichnung	Ort
15.03.2016	VOB/A Fit für die Auftragsakquise Aufträge nach VOB gewinnen	Hilden
16.03.2016	VOB/B Projekte erfolgreich managen Aufträge erfolgreich abwickeln, Schulung mit Mustertexten und Arbeitshilfen	Hilden
04.–05.04.2016	WLAN im Unternehmenseinsatz Grundlagen, Konzepte, Protokolle und Standards	Hilden
20.–22.04.2016	Virtualisierung für den Mittelstand Einführung zu Technologien, Überblick zu marktrelevanten Lösungen	Hilden
11.–12.05.2016	Fit für den Vertrieb Intensivtraining des effektiven Verkaufens	Hilden

Gesamtes Kursprogramm: Eine Übersicht über alle Kurse im Standardangebot der Wissenswerkstatt sowie weitere Termine finden Sie auf **www.vaf-wissenswerkstatt.de.** Anfragen auch für Inhouse-Schulungen können Sie an die VAF-Geschäftsstelle richten: **Frau Simone Weislowski, Tel.: 02103 700-254** oder **weislowski@vaf-ev.de**

Impressum

VAF Report

Mitgliedermagazin und Informationsschrift für mittelständische Systemhäuser,
Ausgabe: 01/2016 (39. Jahrgang)

Anfragen für redaktionelle Beiträge und Anzeigen an den

Herausgeber:
VAF Bundesverband Telekommunikation e.V. (gegründet 1951)
Otto-Hahn-Straße 16, 40721 Hilden,
Tel.: 02103 700-250, Fax: -106,
Internet: www.vaf-ev.de, E-Mail: info@vaf-ev.de

Namentlich gekennzeichnete Artikel oder Firmenbeiträge geben nicht unbedingt die Meinung des Herausgebers wieder.

Redaktion:
Martin Bürstenbinder (Gesamtleitung, V.i.S.d.P.),
Mathias Hein (Fachleitung Technik),
Folker Lück (freier Mitarbeiter),
Simone Weislowski (Redaktionsassistenz)

Anzeigenannahme:
Simone Weislowski, weislowski@vaf-ev.de

Gestaltung:
Uwe Klenner, www.layout-und-gestaltung.de

Lektorat:
Stephanie Esser,
www.textschliff.de

Bildmaterial:
www.shutterstock.com (1, 3, 24),
VAF (3, 4, 8, 9, 19, 25, 28), ATRT (5), NTA (6), MTG (6), BFE (6), innovaphone (10, 11, 30), QSC (15), H. Gawlik (29), www.istockphoto.com (29), Ferrari (30), Teletrust (30)

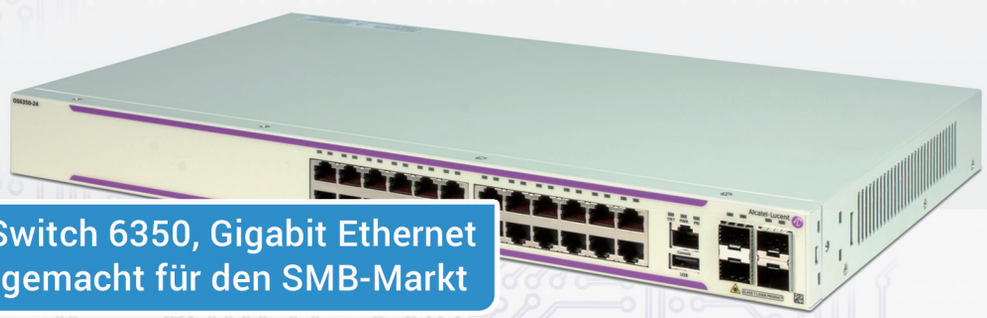
ISSN 1866-9743

ITANCIA

IHR DISTRIBUTOR MIT MEHRWERTEN

ITANCIA ist offizieller Distributor in Deutschland und in Österreich von

Alcatel·Lucent Enterprise



Neuer OmniSwitch 6350, Gigabit Ethernet LAN Switch, gemacht für den SMB-Markt

. **Jede DATA-Komponente** wird bei iTANCIA per default mit einem **AVR** (Advanced Replacement Service) **über 3 Jahre** ausgeliefert.

. ITANCIA ist seit Mai 2015 **offizieller Trainingspartner von Alcatel-Lucent Enterprise** im Bereich OXO, OXE, LAN und WLAN.

. Unsere refurbished Alcatel Produkte erlauben Ihnen **abgekündigte Produkte in perfektem Zustand** und zu besten Konditionen weiterhin anzubieten. Z. B. Mobile 400, 4029/28, 4039/38 Telefone.

. **Hotline**: unsere ACSE-zertifizierten Techniker stehen Ihnen für Ihre OXO-, OXE- und LAN-Angelegenheiten zur Verfügung.

Alcatel·Lucent Enterprise · ALCATEL home & business phones · CASTEL · C4B COM FOR BUSINESS · doro · Gigaset pro

Jabra · KONFTEL · Panasonic · plantronics · Polycom · snom

ITANCIA GmbH
Friedrichshafener Str. 3
82205 Gilching

+49- 8105-77225-400
info.de@itancia.com
www.itancia.com