ComConsult Research

Der Netzwerk Insider

November 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

von Dipl.-Inform. Petra Borowka-Gatzweiler

All-IP respektive SIP Trunking ist das Schlagwort, das den Wechsel des öffentlichen Telekommunikations-Netzes hin zu IP und SIP bezeichnet. Dies betrifft nicht nur die Sprachübertragung (VoIP) sondern auch Video, Erreichbarkeitsanzeige, Chat, A/VWeb-Konferenzen und alle weiteren UCC-Dienste.

Der Übergang auf IP im öffentlichen Telekommunikationsnetz birgt ähnliche Risiken wie wir sie seit Jahr(zehnt)en für IT-Kommunikation über Internet kennen. Das bedeutet, der Netzwerk-Perimeter muss besonders geschützt werden.

Und hier kommt der Session Border Controller (SBC) ins Spiel.

weiter auf Seite 9

Zweitthema

Kühltechniken im Rechenzentrum, Alternativen zur klassischen Raumkühlung

von Dipl.-Ing. Hartmut Kell

Die herkömmliche Methode zur Kühlung von Serverräumen ist die Raumkühlung. Dabei wird dem Serverraum von mehreren parallel arbeitenden Klimaanlagen Kaltluft zugeführt, zumeist über einen Doppelboden, und warme Abluft im Deckenbereich entzogen. Im Falle von Bestandsrechenzentren wird man in der Regel diese Technologie nach Möglichkeit weiterverwenden, jedoch kommt sie bei hohen Leistungsdichten in den Serverracks an ihre Grenzen. Auch ein Verzicht auf Doppelböden bzw. auf ausreichend hohe Doppelböden, wie sie sich durchaus bei Umbau von vorhandenen Räumlichkeiten wegen der fehlenden Raumhöhe ergeben kann, macht andere Kühlkonzepte notwendig.

Der nachfolgende Artikel beschäftigt sich mit Kühlkonzepten, die eine rack- oder reihenbasierende Kühlung als Basis-Technologie verwenden und soll im Rahmen der ein oder anderen RZ-Planung den interessierten Leser dazu anregen, auch diese Alternativen in Betracht zu ziehen.

weiter auf Seite 21

Geleit

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution oder entstehen sogar noch mehr Probleme?

auf Seite 2

Standpunkt

Vertrauenskrise bei Zertifikaten

auf Seite 19

Aktueller Kongress

ComConsult UC-Forum 2015

ab Seite 5

Aktuelles Seminar

Die neue EU-Datenschutz-grundverordnung

auf Seite 20

Aktuelles Intensiv-Seminar

Winterschule 2015

ab Seite 7

Zum Geleit

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution oder entstehen sogar noch mehr Probleme?

Ernst zu nehmende Prognosen von Herstellern, Providern und Marktforschern gehen davon aus, dass sich in den nächsten Jahren die Anforderungen an Mobilfunknetze durch die Steigerung der Anzahl der Endgeräte multipliziert mit der von jedem mobilen Endgerät benötigten Leistung grob um einen Faktor 1000 erhöhen werden. Das hört sich dramatisch an, ist aber letztlich nichts anderes als eine plakative Projektion der bisherigen Entwicklung. Die Prognose betrifft natürlich nicht nur Provider, sondern auch Betreiber von privaten wireless Infrastrukturen, weil es ja auf Dauer nicht hinzunehmen wäre, wenn ein Mitarbeiter mit seinen mobilen Endgeräten eine erhebliche Service-Degradation erfahren würde, wenn er das Unternehmens-WLAN benutzt.

Ein großer Teil der zusätzlichen Last wird auf Video entfallen. Natürlich benötigt man in einem Unternehmen oder einer Organisation kein Netflix, aber welche Konsequenzen hat die Einführung neuer Dienste wie sie für eine „gesteigerte Benutzererfahrung“ im Rahmen von Kooperationen z.B. zwischen IBM und Apple oder Apple und Cisco oder einfach durch höhere Video-Anteile bei UC mittelfristig flächig eingeführt werden können?

Mit IEEE 802.11ac Wave2 steht ab Herbst 2015 eine neue Evolutionsstufe für WLANs zur Verfügung. Vereinzelt wurde auch schon Wave3 mit einer theoretischen Leistung von 10 Gbps angekündigt. Die wichtigen neuen Funktionen von Wave2 und 3 müssen auf den Prüfstand. Was können sie bewirken? Und: sind sie überhaupt erlaubt? Für die Nutzung von 160 MHz breiten Kanälen in flächendeckenden Infrastrukturen ist eine Erweiterung der bisher zulässigen Frequenzbereiche notwendig. Die ist auf dem Weg, aber erreicht sie uns rechtzeitig?

Aber auch LTE ist in einer permanenten Entwicklung und es entstehen Begehrlichkeiten der Provider hinsichtlich der lizenzfreien Bänder, die bislang den WLANs vorbehalten waren. Betreiber sollten akzeptieren, dass ein Bereich, auf den man normalerweise kaum schaut, erheblich an Wichtigkeit gewinnt:

die Filter- und Verstärkertechnik der Wireless-Transceiver. Durch die immer weiter voranschreitende Füllung der Bänder entsteht die Notwendigkeit, die bisher recht großzügig ausgelegten Lücken zwischen den Bändern zu verdichten, z.B. durch Modulationsverfahren mit höherem Wirkungsgrad. Ohne weitere technische Erläuterungen werden dabei ältere Systeme, die nicht mit der neuesten Transceivertechnik ausgestattet sind, den Kürzeren ziehen.

Das IoT stellt eine eher schleichende Gefährdung dar. Auch hier kann es zu deutlichen Überschneidungen mit unternehmensinternen WLAN-Versorgungsstrukturen kommen.

Schließlich: wie werden die neuen Systeme in die Gesamt-Architektur integriert?

Spätestens bei der Sicherheit könnte man zu dem Schluss kommen, dass durchschnittliche Unternehmen und Organisationen mit konventioneller Technik hier schnell an Grenzen stoßen.

Video als Triebkraft des Massengeschäfts

Das Thema Video führt zu einem Bereich heftiger Entwicklungstätigkeit, nämlich Mobilfunk mit LTE. Provider gehen davon aus, dass Nutzer massenhaft Videos auf ihre immer besser werdenden Endgeräte streamen möchten und sie als Kunden verloren gehen, wenn das nicht richtig klappt. Dazu kommt, dass man mit zunehmender Netzleistung den Kunden relativ einfach Mehrwertdienste anbieten kann, die sie an einen Anbieter binden.

Bislang war die Ausgangslage für private Betreiber eher ungünstig, aber jetzt kommen die „Wave2“-Produkte von 802.11ac. Praktisch alle wichtigen Hersteller haben sie noch für das dritte oder letzte Quartal 2015 angekündigt. Sie erreichen zwar immer noch nicht den gesamten Funktionsumfang, der in 11ac definiert wurde, sind

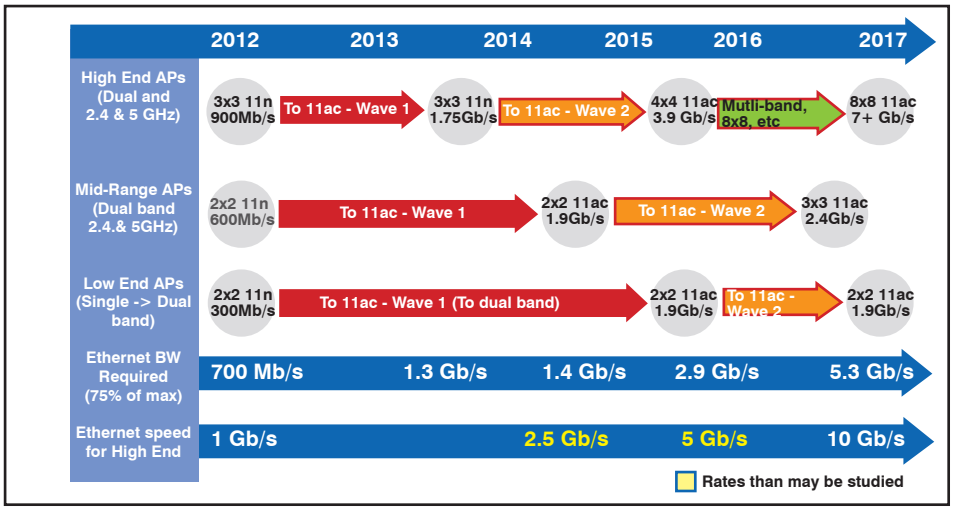

Abbildung 1: 802.11ac Enterprise AP Segmente und Trends

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution?

aber dennoch deutlich besser. Zur besseren Übersicht stellt die Abbildung 1 die Entwicklung differenziert nach Qualitätsbereichen für Access Points dar. In Unternehmen und Behörden benutzen wir mindestens Mid-Range Geräte, vorzugsweise aber High End. Weiter unten sieht man die Ethernet-Bandbreite, die man zur Unterstützung der jeweiligen Generation benötigt. In früheren Artikeln wurde die Entwicklung von 2,5 und 5 GbE ausführlich dargestellt. (siehe Abbildung 1)

Welche Herausforderungen entstehen für private Betreiber?

Private Betreiber von flächendeckenden Wireless-Infrastrukturen werden damit rechnen müssen, diesen generellen Trends nicht entgehen zu können. Die Mobilität ist eine Kernanforderung, die man nicht mehr wegdiskutieren kann. Mit der Zunahme interessanter Anwendungen wird auch die benötigte Leistung pro versorgtem Endgerät erheblich steigen.

Hier verweise ich gerne auf die Aktivitäten von Apple, IBM und Cisco. Basis ist eine Zusammenarbeit von IBM und Apple, die die Benutzerfreundlichkeit von Anwendungen knapp gesagt endlich in eine Dimension bringen wollen, wie sie für Privatanwender mit modernen mobilen Endgeräten längst selbstverständlich ist. Apple fällt es leicht, neue optimale Formfaktoren und Oberflächen zu entwerfen, wie das iPad Pro zeigt. Schöne Lösungen auf Anwendungs- und Endgeräteseite werden kaum sensationell funktionieren, wenn die Kommunikation klemmt. Also gibt es neben der schon länger bestehenden Kooperation zwischen IBM und Cisco auch eine neue Allianz zwischen Apple und Cisco. Ziel ist kurz gesagt die Optimierung des Verkehrs zwischen mobilen Endgeräten und realen oder Cloud-basierten RZ-Komponenten.

Damit entwerfen diese drei Hersteller ein Bild dafür, was Unternehmen und Organisationen eigentlich wirklich haben möchten: zusammenhängende, leicht zu betreibende, wirtschaftliche und sichere Lösungen statt einer Ansammlung unübersichtlicher, komplexer und undurchschaubarer Technologiehaufen.

Das definiert eine Leitlinie, die bei keiner Diskussion über neue Technologien oder Varianten außer Acht gelassen werden sollte. Wie tragen nun die neuen WLAN- und LTE-Entwicklungen zum Gesamtbild bei?

IEEE 802.11ac Wave2

Zwischen Wave1 und Wave2 gibt es eine Reihe von Unterschieden.

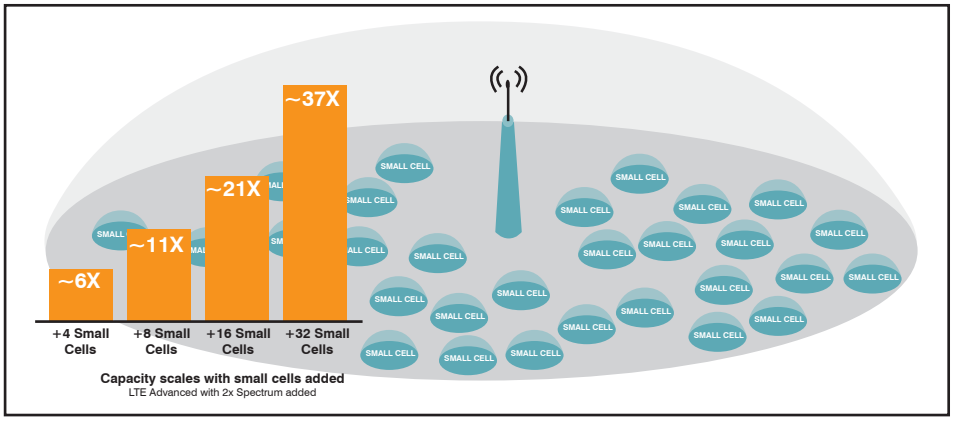

Abbildung 2: Steigerung der Leistung von LTE durch Small Cells Quelle: 3GPP

- Unterstützung von Brutto-Übertragungsgeschwindigkeiten bis 2,34 Gbps (statt 1,3 Gbps in Wave1) im 5 GHz-Band. Natürlich macht DCF dies wieder zunichte, aber Hersteller wie Cisco gehen davon aus, dass rund 1,5 Gbps übrig bleiben.
- Unterstützung von Multi-User MIMO (MU-MIMO)
- Option der Nutzung von 160 MHz breiten Kanälen für höhere Leistung
- Option der Nutzung eines vierten Spatial Streams für höhere Leistung
- Nutzung zusätzlicher Bänder im 5 GHz-Bereich, sofern definiert

Es gibt aber einen weiteren, wirklich wichtigen Punkt, den man leicht übersieht. Viele Leser werden noch wissen, dass es bei einem alten, analogen Radio vorkommen kann, dass man zwei Sender nicht richtig voneinander trennen kann oder sich Sendereinstellungen durch äußere Einflüsse wie z.B. Wärme, ändern können. Diese Effekte entstehen durch simple Filter, die die einzelnen Nutzfrequenzen bzw. Kanäle nicht sauber voneinander trennen. WLANs mit älterer Technik können ähnliche Probleme haben. Nur die neueste Technik für Filter und Antennen-Switches ist eine Gewährleistung für möglichst störungsfreie Arbeitsweise von WLANs. Hier kann man deutliche Fortschritte feststellen die, wie wir gleich sehen werden, für WLANs lebenswichtig sein können.

Entwicklungen bei LTE

Die Entwicklung internationaler Mobilfunkstandards ist deutlich aufwändiger als z.B. eine neue Ethernet-Norm. Weltweit arbeiten verschiedene Gremien im Grunde an den gleichen Entwicklungszielen. Dieser Prozess muss wegen seiner Komplexität einen deutlichen Vorlauf zum aktuellen Sachstand haben. Die meisten Kunden bekommen heute LTE nach Release. Rel. 10 bis ca. Rel .12 heißen auch „LTE Advanced“. Schon in diesen Versionen wird das Konzept aufgegriffen, die Leistung von LTE durch die Hinzunahme von passenden Zellenkonzepten zu erhöhen. Unter Voraussetzung eines guten Interferenz-Managements steigt die mögliche Leistung eines LTE-Versorgungsbereiches (einer Basis-Station) deutlich mit der Anzahl von kleinen Zellen (Small Cells). (siehe Abbildung 2)

Schon länger gibt es für „Provider WiFi“-Lösungen, die im Zusammenhang mit LTE-Geräten von den einschlägigen Herstellern angeboten werden und die Möglichkeit der Einbindung von WiFi-Zellen in verschiedenen Integrationsstufen besitzen.

Grob kann man sich das so vorstellen, dass eine Verbindung durch LTE aufgebaut und verwaltet wird, Uplink auch mit LTE erfolgt, aber der Downlink mit WiFi. Das einzige, was man dazu sonst noch benötigt, ist die Fähigkeit von Endgeräten, gleichzeitig an LTE und WiFi teilzunehmen. Da ist aber durch die integrierten Transceiver meist gewährleistet.

Ebenfalls mit LTE Advanced wurde der Gedanke eingeführt, LTE auch auf **lizenzfreie Bereiche** (also wo sonst die WLANs sind!) auszudehnen. Mit LTE Rel. 13 wird das weiter konkretisiert. Es gibt aktuell zwei Versionen, die diskutiert werden, nämlich LAA (Licensed Assisted Access) und LTE-U (LTE Unlizensed). Gemeinsam ist diesen Vorschlägen, dass es immer eine Verbindung zwischen Endgerät und LTE-Basisstation im lizensierten Bereich gibt, die die Verbindung im lizenzfreien Bereich steuert. LAA soll die Lösung für die EU werden und ist für Up- und Downlink nutzbar und besitzt die Koexistenzverfahren LBT, DFS und TPC. LTE-U für USA, ASIA-PAC und ROW kommt ohne sie aus, ist aber auch nur für den Downlink gedacht.

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution?

Ohne weitere Diskussion können wir aber folgendes feststellen: die Koexistenz von LTE und WLANs im gleichen lizenzfreien Bereich ist eine erhebliche Gefährdung für die WLANs! Untersuchungen zeigen, was schon der gesunde Menschenverstand nahe legt: wegen der fundamentalen Unterschiede der Funkdienste (WLAN ungeordnet und nicht deterministisch mit DCF, LTE geordnet mit sauberer Steuerung, WLAN als Zeit-Multiplex-System, LTE als Raum-Multiplex-System) ist die Koexistenz auf einem Frequenzbereich sehr schwierig und mit deutlichen Leistungseinbußen besonders bei WLANs belegt. Voraussetzung dafür, dass es überhaupt funktioniert, sind Filter, Antennen-Switches und Verstärker der neuesten Generation.

Konsequenzen für die Betreiber privater IT-Versorgungsstrukturen

Die Anforderungen an die mobile Versorgung steigen stark und man wird darauf Antworten finden müssen. Es wird sicher nicht zu weniger, sondern eher zu mehr WLAN-Zellen kommen. Das wird glücklicherweise durch die neuen Ethernet-Technologien für die Integration der vielen APs unterstützt. Bei mehr Zellen, mehr Teilnehmern und mehr Leistung pro Teilnehmer rücken natürlich die betrieblichen Aspekte und die Sicherheitsfragen noch deutlicher in den Vordergrund. Hier gibt es viele interessante Lösungen, auch Cloud-basiert, die uns noch beschäftigen werden.

Natürlich werden WLANs und LTE-Angebote zusammen wachsen, es sollte für einen Mitarbeiter problemlos möglich sein, die Abdeckung der unternehmenseigenen flächendeckenden WLAN-Umgebung zu verlassen ohne dass seine Verbindungen abreißen, die dann eben von LTE unterstützt werden.

Das Vordringen von LTE in unlizensierte Bereiche ist aber als sehr kritisch einzustufen. Auf einem Fabrikgelände oder Campus ist das sicher kein Problem, ich erinnere mich aber z.B. an Universitäten, bei denen sich viele Institute in Gebäuden befinden, die relativ wild über das Stadtgebiet verteilt sind. Das kann es auch bei Ämtern, Behörden oder Unternehmen mit vielen Filialen, wie z.B. Sparkassen, geben. In diesen Bereichen kann es zu erheblichen Störungen kommen, wenn tatsächlich LTE auf den gleichen Frequenzen betrieben wird. Es soll zwar ein „harmonisches Nebeneinander“ von LTE/LAA und WiFi geben, aber eher aus der Perspektive eines Providers, der beides betreibt. Private Betreiber haben an dieser Stelle praktisch keine Lobby.

In den nächsten Jahren müssen wir auch mit einer zunehmenden Verbreitung von öffentlichen WLAN-Netzen z.B. kommunaler Betreiber rechnen. Ein weiterer wichtiger Trend, der den Vormarsch von LTE in die lizenzfreien Kanäle beschleunigen könnte, ist das IoT. Hier gibt es mögliche technische Ansätze gleich im halben Dutzend.

Wie auch immer sollte ein privater Betreiber immer die neueste Technologie bei den Transceivern einsetzen, weil nur diese wenigstens die Chancen auf störungsfreien Betrieb einigermaßen wahren hilft.

Denn, wie auch immer man es sieht: es wird deutlich enger auf den Bändern!

Ihr Dr. Franz-Joachim Kauffels

Aktueller Kongress

ComConsult UC-Forum 2015
23.11. - 25.11.15 in Königswinter

Die ComConsult Akademie veranstaltet vom 23.11. bis 25.11.15 ihr diesjähriges "UC-Forum 2015" in Königswinter.

Die Ablösung der ISDN Technologie bis 2018 hat bei vielen Nutzern eine erhebliche Verunsicherung ausgelöst. Vielen ist Stand heute nicht klar, welche Änderungen bei der Anbindung ihrer TK und UC-Lösung an das öffentliche Kommunikationsnetz sich dabei ergeben.

Dabei gilt es aber jetzt schon sich mit den Änderungen vertraut zu machen. Fragen wie:

- Was ist ein SBC?
- Wo brauche ich ihn? Wer betreibt ihn?

sind nur einige von vielen.

Gerade der Wechsel von einer leitungsvermittelnden Technologie hin zu einer paketorientierten im WAN bringt ganz neue Herausforderungen für die Qualität der Unternehmenskommunikation.

Aber damit nicht genug. Aufgrund dieser radikalen technischen Änderungen müssen nun auch die Provider nach neuen Geschäftsmodellen Ausschau halten. Sie drängen daher verstärkt in den Markt der Lösungsanbieter.

Damit werden jetzt auch die Karten neu gemischt bei der Frage:

Soll ich TK & UC selber betreiben oder einen Cloud-Dienst nutzen?

Neue attraktive Modelle für cloudbasierte Kommunikation drängen verstärkt auf dem Markt. Waren bis vor wenigen Jahren nur reine Sprachlösungen verfügbar, verschiebt sich dieses Bild zunehmend in Richtung UCC auf Basis etablierter Lösungen von Microsoft, Cisco oder Unify.

Daher widmet sich dsás diesjährige UC-Forum intensiv den folgenden Fragen:

- Das ISDN stirbt - aber was folgt?
  - Wie funktioniert SIP Trunking mit dem Provider?
  - Gibt es Alternativen?
- Welche Argumente sprechen für und gegen die Cloud?
  - Wo steht UC(C) heute?
  - Was bieten die Provider?
- Welche Vorteile verspricht eine neue Technologie wie WebRTC?
  - Eine junge Technologie entwickelt sich. Wo stehen wir aktuell?
  - Mit welchen Problemen sollte man rechnen?

Diese und viele weitere Themen werden wie gewohnt von unseren etablierten und bekannten Spezialisten präsentiert. Die Analysen und Empfehlungen werden wie immer ergänzt um Praxis-Beispiele und Erfahrungs-Berichte aus Projekten.

Das ComConsult UC-Forum 2015 ist die richtige Veranstaltung zum richtigen Zeitpunkt. Erhalten Sie Analysen und Empfehlungen von Top-Experten und bereiten Sie sich jetzt auf eine der größten Umstellungen der Kommunikations-Industrie der letzten 40 Jahre vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult UC-Forum 2015

Ich buche den Kongress
ComConsult UC-Forum 2015

☐ 23.11. - 25.11.15 in Königswinter
zum Preis von € 2.390,-- netto

☐ inkl. Report " ComConsult Communications Index"
zum Preis von 338,- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

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

Programmübersicht ComConsult UC-Forum 2015

Montag 23.11.2015 - UC 2016 - Markt & Technik

9:30 - 10:15 Uhr
Keynote
- UCC – von On-Premise in die Cloud
- Arbeitsplatz – vom Telefon zur Browseranwendung
- Amtsanbindung – vom PSTN-Gateway zum SBC
- Amt – von ISDN zu All-IP • Markt – von der Vielfalt zur Einfalt?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
UC Aktuell - Cloud vs. OnPrem
- Einsatz-Szenario Cloud / On Premise
- Funktionalität und Vorteile: Cloud Lösungen / On Premise Lösungen
- Nachteile: Cloud Lösungen / On Premise Lösungen
- Fazit: Welche Lösung eignet sich für wen?

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN
Markus Geller, ComConsult Research GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:00 Uhr
Collaboration auf dem Weg in die Cloud
- Veränderungen im Markt, Anforderungen der Kunden, Innovation, warum Cloud?
- Cisco Collaboration Cloud aber sicher! Enterprise Security mit Cloud Deployments • Hybrid Cloud Lösungen, Schutz bestehender Investitionen, Integration im Zusammenspiel mit den Vorteilen der Cloud • Kunden Use Cases, neuste Innovationen in Cisco Collaboration und deren Anwendung in Projekten

Tobias Neumann, Cisco Systems GmbH

12:00 - 12:30
WebRTC – Aktuelle Situation und Trends
- Google Roadmap
- Video Codecs (VP8 HW Encoding, VP9, H.264)
- Microsoft IE und WebRTC
- SCTP vs. QUIC
- ORTC: Das Ende von SDP
- Ericsson: Open WebRTC Project

Markus Geller, ComConsult Research GmbH

12:30 - 13:00
Evolution der Kommunikation aus der Sicht eines Carriers
- Zukunftstrends in der Kommunikation (Von ISDN zur Cloudlösung, neue Möglichkeiten mit der Cloud, Sicherheitsanforderungen an eine as-a-Service Kommunikationsumgebung)
- Transition und Transformation (Managed Take over von PSTN auf Unified Communications, neue Umgebung, neue Services)
- Professional Services im Bereich Cloud & UC
- Transport Mechanismen für IP Voice (SIP trunking, Secure Cloud Interconnect, Einbindung von Lync/S4B Voice)

Thomas Markus Meyer, Stefan Brandes, Verizon Deutschland GmbH

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:00 Uhr
Neue Kommunikationswege für UCC
- Trend 1: schlankere Nutzeroberfläche
- Trend 2: All-IP Multimedia durch den Einsatz von Enterprise SBCs
- Trend 3: der Shift vom separaten UC-Client zur Anwendungs-Integration
- Trend 4: Maßgeschneidertes UCC durch Anwendungen und Snap-Ins

Thomas Römer, Avaya Deutschland GmbH

15:00 - 16:00 Uhr
Musterprojekt Teil 1:
Ausschreibung einer UC-Lösung
- Vorstellung der Vorgehensweise
- Hersteller-Auswahl • Ausschreibungsszenario
- Bewertungskriterien • Arbeitsplatzmodelle

Dipl.-Math. Leonie Herden, ComConsult Beratung und Planung GmbH

16:00 - 16:30 Uhr Kaffeepause

16:30 - 17:30 Uhr
Musterprojekt Teil 2:
Präsentation der Ergebnisse
- Vorstellung der eingegangenen Angebote
- Architektur und Lösungsdesign im Überblick
- Aktuelle Clients und Arbeitsplatzlösungen
- Preise & Wirtschaftlichkeit

Dipl.-Math. Leonie Herden, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr Happy Hour

Dienstag 24.11.2015 - VoIP im WAN, Übergang zum öffentlichen Netz

9:00 - 9:45 Uhr
Session Border Controller:
Funktionalität und Einsatz-Szenarien
- Einsatzbereiche: UNI, NNI, E-SBC
- Funktionsbereiche: Sicherheit / Interoperabilität / Robustheit, Hochverfügbarkeit, Qualität, SLAs / Regulatorische Compliance

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

9:45 - 10:45 Uhr
Session Border Controller:
Architektur- und Design-Konzepte
- Zentral vs. dezentral – Referenzarchitekturen für SBCs • Anschaltung von herstellereigenen Lösungen und Third-Party-Produkten
- SBCs als zentrale Routing-Instanz
- Firewall Bypass vs. Firewall Traversal
- Wie sieht ein SBC-Design nach BSI TLSTK 2.0 aus?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause

11:15 - 11:45 Uhr
Einsatzszenario für WebRTC und Session Border Controller aus Sicht von Alcatel-Lucent
- Einführung und Vorteile von WebRTC
- Definition • Vorteile • Architektur
- Kompatible Browser und deren Verbreitung

Christian Sailer, ALE Deutschland GmbH

11:45 - 12:15 Uhr
Beispiel einer WebRTC-Lösung
Kerninfrastrukturstandards (DTLS, ICE, Turn etc.)

Lars Dietrichkeit, innovaphone AG

12:15 - 13:00 Uhr
SIP Trunking Standards: UNI
- Wofür sind SIP Trunking Standards gut?
- ITU-T • ETSI • SIP Forum: SIPconnect
- Positionen der Hersteller

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:15 Uhr
Anwendervortrag: Der Wechsel von PSTN auf SIP Trunking
- Die Private Telefonie Cloud der TK
- Was steckt in der Private Cloud drin? Herausforderungen bei der Implementierung
- Entwicklungsstrategie All over IP • Fazit

Dipl.-Ing. Rolf Nagelfeld, Techniker Krankenkasse Hamburg

15:15 - 15:45 Uhr
Microsoft Skype for Business/Lync
- Unterstützung klassischer Telefonie
- CallControllGateways
- Unterschiede zwischen den Produktversionen (Lync und Skype for Business)

Joachim Frenzel, estos GmbH

Worüber bei WebRTC keiner spricht
- Warum Google in WebRTC investiert
- Safari on the Edge of WebRTC
- Wie Sie Ihr Unternehmen auf WebRTC vorbereiten

Raphael Bossek, estos GmbH

15:45 - 16:15 Uhr Kaffeepause

16:15 - 17:15 Uhr
Voice & Video Codecs im WAN
- Welche Voice- und Video-Codecs spielen in der Praxis eine Rolle? • Wie funktionieren adaptive Codecs? • Welche Mechanismen zur Fehlerkorrektur existieren?
- Welche Codecs eignen sich für den Einsatz im WAN? • Welche Codecs werden von den Herstellern präferiert?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

Mittwoch 25.11.2015 - ISDN Abschaltung 2018: der Weg zu All-IP

9:00 – 9:30 Uhr
Motivation für All-IP
- Die weltweite Abschaltung der öffentlichen PSTN-Netze ist angekündigt
- Bisheriges Design einer VoIP-Enterprise-Lösung
- Zukünftiges Design einer VoIP-Enterprise-Lösung
- Die „VoIP"-Welt wird auf UC erweitert werden
- Welche Probleme müssen in der neuen All-IP Welt gelöst werden? • All-IP und IPv6

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

9:30 - 10:15 Uhr
E-SBC Produkte im Vergleich
- Funktionsweise eines SBC
- Welche Leistungsmerkmale sollte ein SBC haben?
- Herstellerübersicht der führenden Anbieter

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:15 – 10:45 Uhr
ISDN vs. VoIP – Was ist anders?
- Leitungsvermittlung vs. Paketvermittlung
- Überbuchungssituation, CAC
- Comfort Noise: Woran erkenne ich eine freie Leitung?
- Die Abhängigkeit der Sprachqualität von Zeitinformationen und deren Herkunft
- Über welche Datenleitung kommuniziere ich?

Markus Geller, ComConsult Research GmbH

10:45 – 11:15 Uhr Kaffeepause

11:15 – 12:45 Uhr
SIP Trunk Lösungen & Produkte - Teil 1
- Vortrag: T-Systems

Dipl.-Ing. Wilfried Meer, T-Systems International GmbH
- Vortrag: Vodafone

Dipl.-Ing. Jindrich Slavik, Vodafone GmbH

12:45 - 13:45 Uhr Mittagspause

13:45 - 15:15 Uhr
SIP Trunk Lösungen & Produkte - Teil 2
- Vortrag: Telefónica Deutschland

Dipl.-Ing. Frank Düpmann, Telefónica Deutschland GmbH & Co OHG
- Vortrag: BT Deutschland

Jan Riechers, BT (Germany) GmbH & Co oHG

15:15 - 15:45 Uhr Kaffeepause

15:45 - 16:15 Uhr
NNI – der Weg zu All-IP
- Was fehlt für die globale SIP/IP Kommunikation?
- Welche Lösungsansätze gibt es?
- Wo liegen die Probleme?

Markus Geller, ComConsult Research GmbH

Der Veranstalter behält sich Änderungen im Programm vor

Aktuelles Intensiv-Seminar

Winterschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik 07.12.-11.12.15 in Aachen

Die ComConsult Akademie veranstaltet vom 07.12. bis 11.12.15 in Aachen ihre diesjährige "Winterschule".

Die Winterschule 2015 bringt Sie in 5 Intensiv-Tagen auf den neuesten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik. Wir analysieren mit Ihnen, wie sich IT-Architekturen verändern, welche Auswirkungen das hat und welche Änderungen und Investitionen auf Ihrer Seite erforderlich sind.

Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen und welche Anforderungen generiert das auf Infrastrukturen
- Was passiert auf der WAN-Seite, wie sieht eine Zukunfts-orientierte WAN-Lösung aus?
- Wie sieht die Zukunft des LAN aus? Welche der neuen Technologien werden sich durchsetzen? Wie können skalierbare und sichere LAN-Infrastrukturen geschaffen werden?
- Unified Communications, das Ende von ISDN: wie sieht die Kommunikations-Lösung der Zukunft aus? Was bedeutet das für Infrastrukturen?
- WLAN-Technik erreicht immer neue Leistungsklassen: aber wie sieht die Zukunft aus? Wo ist die Abgrenzung zum Mobilfunk?
- IPv6 ist Realität: wie sieht eine erfolgreiche Migration aus? Welche Projekterfahrungen können helfen?
- Sicherheit wird immer mehr zum Schlüssel für erfolgreiche IT-Infrastrukturen: LAN, mobile Endgeräte, UC: erfolgreiche Lösungen und Erfahrungen aus der Praxis

Top Experten der Branche gestalten das Programm dieser Intensiv-Schulung und bringen systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen in diesen Kurs ein. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

Frühbucherphase bis zum 10.11.2015

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Winterschule 2015

Ich buche das Seminar
Winterschule 2015

☐ 07.12.-11.12.15 in Aachen
zum Preis von € 2.290,-- netto*

* Preis gültig bis zum 10.11.15 - danach regulärer Preis € 2.490,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Programmübersicht Winterschule 2015

Montag, der 07.12.15 - IT-Architekturen und Auswirkungen auf Infrastrukturen

IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand. Ohne Zweifel wird unsere IT-Landschaft in fünf Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

9:30 - 12:30 Uhr
Wir analysieren für Sie:
- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:00 - 17:00 Uhr
Rechenzentren sind unter Druck:
- Die Cloud puscht das Thema Wirtschaftlichkeit, Kosten und Transparenz
- Mobile Endgeräte erfordern mindestens eine Private Cloud Infrastruktur und einen Übergang zu Benutzer-zentrischen Lösungen
- Server- und Speicher-Konsolidierung gehen permanent weiter, hoch-skalierende Infrastrukturen sind gefordert
- Virtualisierung geht in die nächste Runde und öffnet die Tür zu automatischen Lastausgleichen und Provisionierungen mit erheblichen Anforderungen an Infrastrukturen

Wir analysieren für Sie:
Strategien für das Rechenzentrum der Zukunft:
- Software-Defined Data Networks SDN
- Cloud Computing

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

11:00 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, der 08.12.15 - LAN-Technologien: aktuelle Entwicklungen

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Programmierbare Netzwerke als Teil des Software Defined Data Center und als Teil von Software Defined Infrastrukturen sind ein Beispiel dafür. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Wir erklären, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten.

9:00 - 17:00 Uhr
Sie lernen in diesem Themenblock:
- Welche neuen LAN-Technologien gibt es, welche Konsequenzen hat das?
- Netzwerk-Design mit 10/25/50/100 Gigabit, wie sehen Anforderungen und Planungs-Ansätze aus?
- Fabric-Konzepte verdrängen traditionelle Architekturen: was leisten sie und wie können sie sinnvoll eingesetzt werden?
- Edge/Core-Architekturen mit neuen Formen von Labbel-Switching: ist hier die Zukunft?
- Wie kann eine Hersteller-neutrale Lösung aussehen?
- Quo Vadis VLAN-Technik: werden VLANs durch Edge-Provisioning und Overlays verdrängt?

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Mittwoch, der 09.12.15 - Unified Communications, das Ende von ISDN

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons. Gleichzeitig ist ISDN am Ende, es wird 2017 abgeschaltet. Dies erfordert eine Neubestimmung des Verständnisses von Kommunikation: was gehört dazu, wie kommunizieren wir in Zukunft mit Externen?

9:00 - 17:00 Uhr
In diesem Themenblock lernen Sie:
- Motivation: Warum All-IP? Einführung in das Thema
- SIP Trunking vs. PSTN: Was sind die wesentlichen Unterschiede? • Was kommt nach 2018?
- Standards für Enterprise- und Provider-Peering
- Session Border Controller: Funktionalität und Markt
- Provider-Marktübersicht: Geschäftsmodelle und Angebote • Architektur einer globalen All-IP Kommunikation • Wie sieht das Kommunikations-Endgerät der Zukunft aus?

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN
Markus Geller, ComConsult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Donnerstag, der 10.12.15 - WLAN und Mobilfunk / IPv6: aktueller Stand bei Unternehmen

Mit der rasanten Zunahme mobiler Endgeräte bekommt der Zugang dieser Geräte zu den Unternehmens-Infrastrukturen eine zentrale Bedeutung. In Zukunft werden deutlich mehr Endgeräte diesen Zugang wählen als die Kabel-basierte Alternative. Denkt man einen Schritt weiter zum Internet of Everything, dann wird die zukünftige strategische Bedeutung des Zugangs über WLAN und Mobilfunk deutlich. Sowohl die schiere Anzahl der Teilnehmer als auch der damit verbundene Schutz- und Kontrollbedarf machen Änderungen an der Netzwerk-Infrastruktur erforderlich.

9:00 - 12:30 Uhr
In diesem Themenblock lernen Sie:
- Welche Optionen Ihnen das moderne WLAN bietet
- Wie sich Mobilfunk-Alternativen demgegenüber positionieren

Dr. Franz-Joachim Kauffels, Technologie-Analyst

IPv6 Projekte sind angelaufen. IPv6 existiert nicht mehr nur in Forschungsumgebungen, bei den Providern und in Testnetzen von Unternehmen. Immer mehr Firmen haben mit der Migration begonnen, von DAX 30 bis Mittelständler, von Finanzinstituten bis zur Fertigung. Nicht nur der Internet-Auftritt, der Provider-Anschluss und die Homeoffice VPNs werden migriert. Auch in den Unternehmen selbst, hat die Migration begonnen. In diesem Themenblock wird der aktuelle Stand der IPv6 Migration vorgestellt. Weiterhin werden erfolgreiche Migrationsstrategien anhand laufender Projekte erörtert.

14:00 - 17:00 Uhr
In diesem Themenblock lernen Sie:
- Welche Entscheidungen wann getroffen werden müssen • Wie man ein IPv6 Projekt planerisch und organisatorisch umsetzt
- Wie man die IPv6 Migration in den Lifecycle von Hard- und Software integriert
- Warum ein Migrationsprojekt nicht so teuer ist, wie viele annehmen
- Wo mit Schwierigkeiten zu rechnen ist und wo nicht
- Wie man die Internet-Präsenz schrittweise migriert
- Worauf bei Software und Appliances in Bezug auf IPv6 zu achten ist

Markus Schaub, ComConsult Study.tv

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Freitag, der 11.12.15 - Sicherheit / WAN

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume sondern um Informationssicherheit als integraler Bestandteil der IT-Architektur.

9:00 - 12:30 Uhr
Sie lernen in diesem Themenblock:
- Abwehr zielgerichteter Angriffe: Notwendigkeit sys tem- und anwendungsübergreifender Strategien
- Netzbasierte Sicherheit: Praxiserfahrungen aus den Bereichen Verschlüsselung, Zonenkonzepte, NAC und Testumgebungen
- Sicheres Cloud Computing und sicheres Mobile Computing: Möglichkeiten und Grenzen
- Sicherheit und UC: Immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Wide Area Networks unterliegen weitgehend den Investitions- und Betriebspräferenzen der Provider. Die sich dadurch ergebenden Trends und Restriktionen müssen in WAN-Strategien und -Konzepten der die WANs nutzenden Organisationen berücksichtigt werden.

14:00 - 15:30 Uhr
Sie lernen in diesem Themenblock:
- Welchen technologischen Trends folgen die WAN Provider (MPLS, OTN, Ethernet, ...)?
- Wie wirkt sich der Cloud-Trend auf die WANs aus?
- Kupfer, Glasfasern oder drahtlos: was sitzt sich als WAN Access durch?
- Welche Folgen haben aktuelle Entwicklungen in den Bereichen Voice und Video für das WAN?
- Welche Anwendungen sind WAN-tauglich, welche nicht? • Was bedeuten aktuelle WAN Trends für Außenstellenkonzepte von Unternehmen?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor

Schwerpunktthema

Session Border Controller: Die Perimeter-Komponente für All-IP

Teil 1

Fortsetzung von Seite 1

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

1. Wofür brauchen wir SBCs?

Da die durchschnittliche Vertrautheit der ICT-Welt mit Session Border Controllern bislang nur mittelmäßig ausgeprägt ist, rollt dieser Beitrag das Thema von der Basis her auf (siehe Abbildung 1.1, Quelle: 2015 UC, SIP and SBC Plans and Priorities; Webtorials 12/2014).

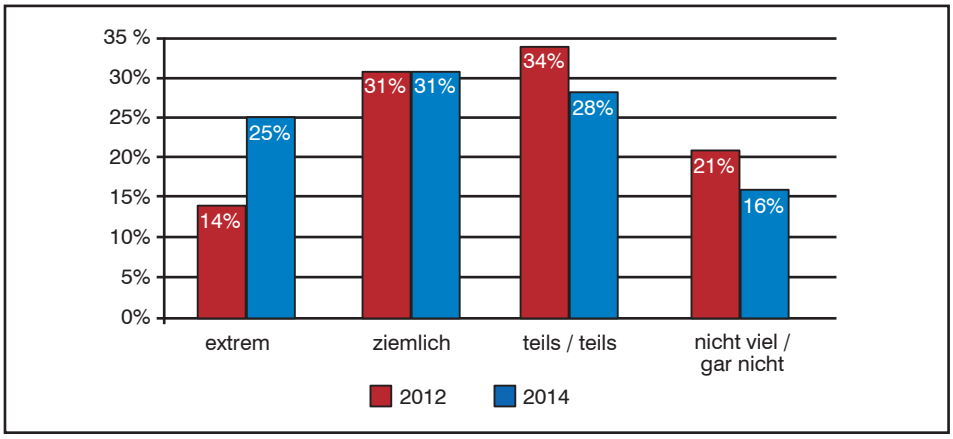

Abbildung 1.1: Vertrautheit mit Session Border Controllern
Quelle: 2015 UC, SIP and SBC Plans and Priorities; Webtorials 12/2014

Früher - ja früher war nicht nur alles besser, sondern hatten wir statt IP-basierter Telefonie das ISDN/PSTN Netz. Die Endgeräte waren autorisierte völlig unkriminelle Telefone, das Telko-Netz war ein privates Netz des Telko Providers, die betriebene Anwendung war Voice-only: soll heißen simple Telefonie, auf der Basis vergleichsweise sicherer Leitungsvermittlung (siehe Abbildung 1.2).

Heute sind wir dabei, diese friedliche Umgebung mit einer wesentlich chaotischeren zu tauschen: genutzt werden beliebige Endgeräte, das Netzwerk besteht aus mehreren kaskadierten öffentlichen Netzwerken, die betriebenen Anwendungen sind Multimedia, auf der Basis eines vergleichsweise unsicheren paketvermittelten Netzwerks (wie Abbildung 1.3 zeigt).

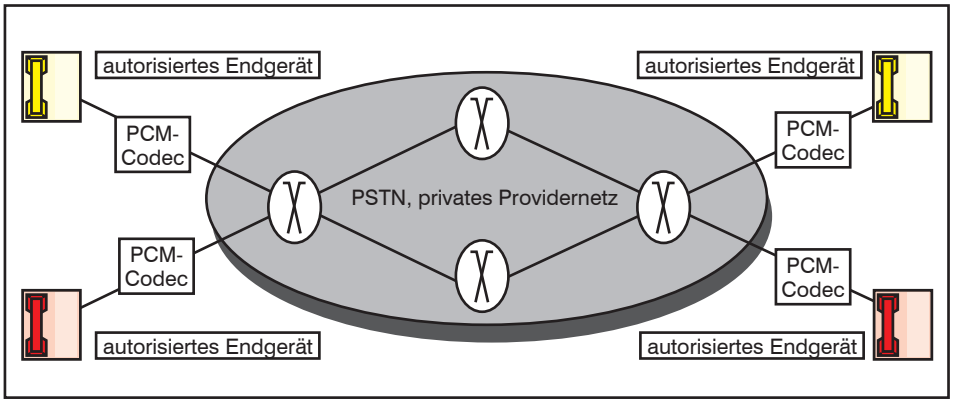

Abbildung 1.2: ISDN Telefonie auf Basis leitungsvermittelter Verbindungen

Der Session Border Controller steht – nicht nur als Schutz- und Trutz-Komponente – an der Grenze zweier unterschiedlicher Netzwerkbereiche und kontrolliert diese, wie der Name "Border Controller" schon sagt. Somit gibt es mindestens eine Aufgabe, die er zuverlässig erledigen muss: den Perimeterschutz. Dies gilt sowohl für Enterprise-Provider-Übergänge als auch für Provider-Provider-Übergänge. Der direkte Übergang zwischen zwei Enterprise-Netzen würde auch unter diesen Schutzbedarf fallen, soweit er tatsächlich ohne zwischengeschaltetes öffentliches Netz vorhanden ist. Letzteres könnte beispielsweise bei der Verbindung zweier Mandanten innerhalb eines privaten Campus-Netzes der Fall sein.

Der Session Border Controller übernimmt die Aufgabe eines Firewalls für Voice, Video und Multimedia Echtzeitkommunikation.

Das Wort "Session" im SBC bezieht sich auf SIP Sessions. Jetzt werden Sie vielleicht fragen: Warum macht das nicht mein "normaler" Perimeterschutz – der Firewall? Die Antwort ist ebenso leicht wie ärgerlich: Der kann es eben nicht ordentlich. Insbesondere die höchst dynamisch bei Sessionbeginn eines Mediastreams ausgehandelten und dann nur für die Dauer der Session gültigen beliebigen UDP Portnummern zwischen 1024 und 65535 sind der Feld-, Wald- und Wiesen-Firewall ein Greuel. Kurz gesagt:

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

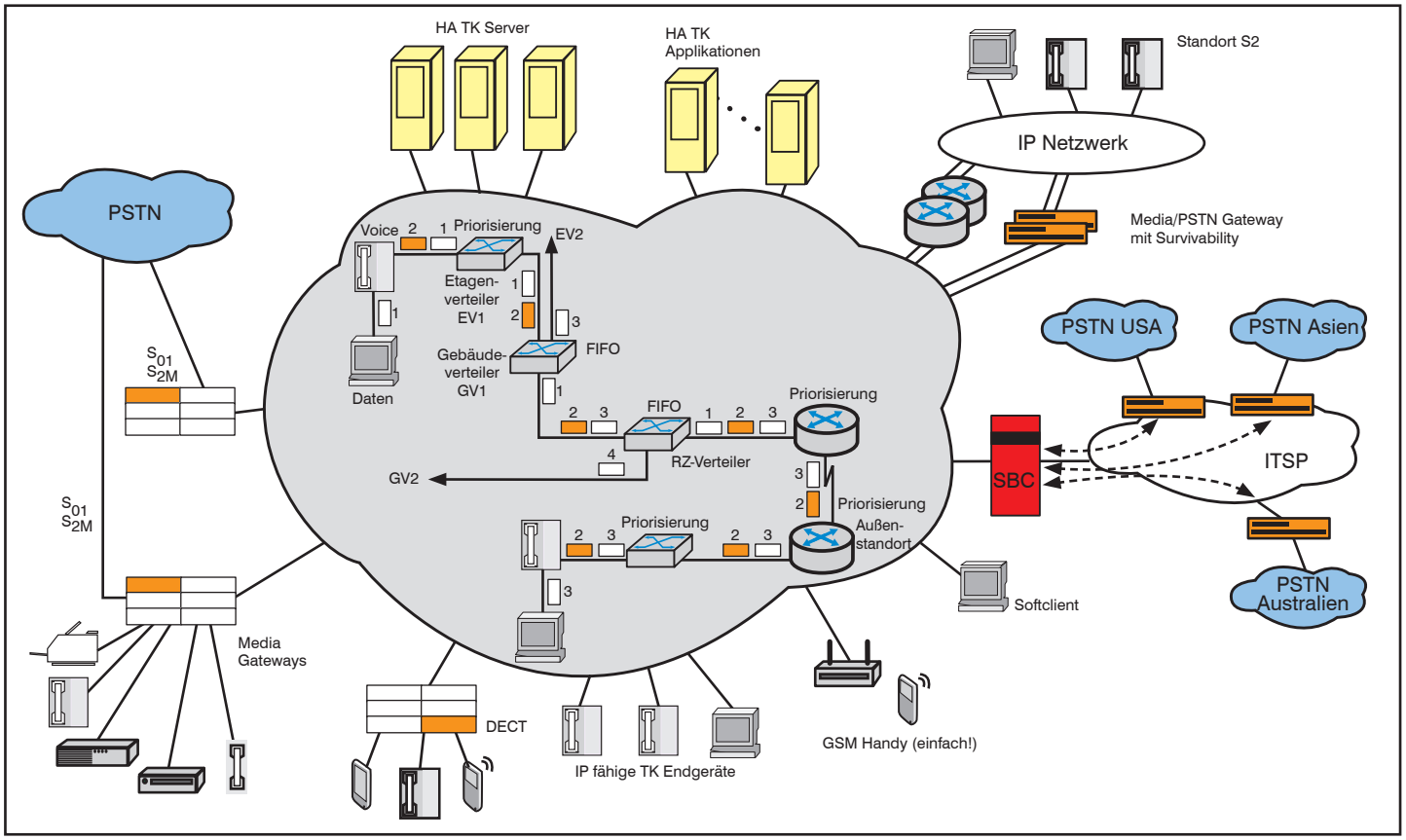

Abbildung 1.3: Multimedia VoIP / SIP Universum auf Basis paketvermittelter IP-Netze

Voice und Video war nie ein Kern-Markt der traditionellen Firewall-Hersteller.

Session Border Controller sind aktuell die einzigen Netzkomponenten, die für den Perimeterschutz und andere Border-Funktionen der Echtzeit-Kommunikation sowohl die Control Plane (SIP Signalisierung) als auch die Data Plane (RTP/RTCP Media Streams) vernünftig integrieren können. Weder Router noch Softswitches/TK-Server noch Firewalls leisten diese Integration. Somit hat sich in den letzten Jahren ein eigener Session Border Controller Markt entwickelt, der den Firewall-Herstellern inzwischen so weit voraus ist, dass sie diesen Vorsprung kaum noch aufholen könnten, wenn sie es denn wollten. De facto ist aber auch gar nicht erkennbar, dass sie es wollen. Vielleicht ist das auch gut so, denn der Session Border Controller als solches ist funktional gewiss ausreichend komplex und kann somit gut auf die spezifischen IT-Firewall-Funktionen verzichten.

Das führt wiederum sofort zu folgender Frage: Wird der Voice- und Video-Verkehr dann gar nicht über den normalen Firewall geführt? Diese Frage lässt sich mit einem klaren Jein beantworten: Typischerweise leistet der IT-Firewall einen Basis-Schutz für den SBC selbst und die Verkehrslasten, die zum SBC durchgelassen werden: Soll heißen, der SBC steht zwischen den IT-Firewalls und diese lassen nur Verkehr von und zu der IP-Adresse des SBC durch: Abbildung 1.4 zeigt die Positionierung eines SBC in der DMZ am Enterprise Perimeter.

Aktuell sind Session Border Controller noch ziemlich Voice-fokussiert, zunehmend erhalten sie jedoch mehr und mehr Multimedia Funktionen, das bedeutet zusätzlich zur Telefonie auch Video, Text-Nachrichten, Datei-Anhänge, Online-Kollaboration und ähnliche Streams zu handhaben. In dieser Rolle sind sie kritische zentrale Echtzeitkommunikations-Komponenten, die zusätzlich zum Perimeterschutz weitergehende Funktionen hinsichtlich Quality of Service und Ver-

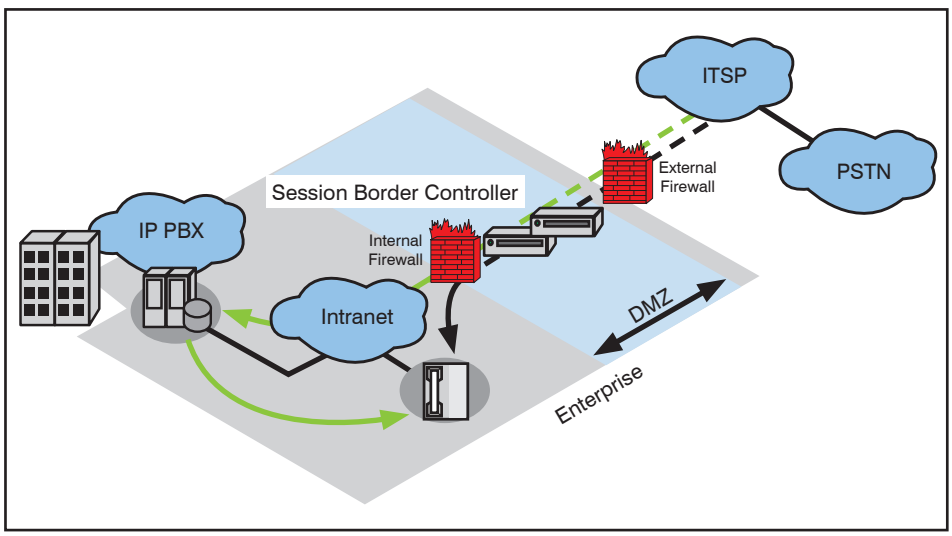

Abbildung 1.4: Positionierung des Session Border Controllers am Enterprise Perimeter

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

fügbarkeit leisten. Als erste Annäherung an eine Definition fassen wir daher zusammen:

Session Border Controller ermöglichen eine sichere und interaktive Hochqualitäts-Kommunikation über verschiedene und mehrfach kaskadierte IP Netzwerke hinweg.

2. Welche SIP Trunking Szenarien sind zu betrachten und wo steht welcher SBC?

Sowohl bei der ISDN- als auch Internet-Technologie sind typischerweise zwei grundsätzliche Netzübergangstypen zu beachten: das User-to-Network Interface (UNI) als Übergang zwischen einem Unternehmens- und einem Provider-Netz und das Network-to-Network Interface (NNI) als Übergang zwischen zwei Provider-Netzen.

SBCs kommen entsprechend an UNI- und NNI-Netzübergängen zum Einsatz. Im Regelfall vertraut bei Standort-Übergängen keiner dem anderen, somit stehen sich jeweils zwei SBCs beider beteiligten Netze gegenüber. Das Beispiel aus Abbildung 2.1 zeigt einen NNI-Übergang zwischen Provider 1 und Provider 2 sowie einen UNI Übergang zwischen Enterprise und Provider 1.

Erhalten kleinere Unternehmens-Standorte keinen direkten Übergang ins öffentliche Netz, weil der Session Border Controller hier zu teuer ist, so werden sie über Corporate WAN an einen zentralen Standort und von dort über einen zentralen SBC ins öffentliche Netz angebunden.

User to Network Interface

Der Enterprise UNI Übergang ist sicher das älteste SBC-Einsatzszenario. Hier geht es nicht nur um die Anbindung an das öffentliche Netz, sondern zum Beispiel auch um die unternehmensinterne Verbindung von "SIP-Inseln", die über öffentliches WAN miteinander kommunizieren sollen, um die Anbindung von remote Nutzern ebenso wie um die Einrichtung von Föderationen zur B2B Kommunikation mit anderen Unternehmen.

Bei der detaillierteren Beschreibung der SBC-Funktionen wird sich dieser Beitrag daher auf den ESBC konzentrieren. Das Enterprise UNI entstand nach dem internen Wechsel von ISDN TK-Anlagen auf VoIP und der nachfolgenden Nutzung von SIP Trunking als kostengünstige Telefonie-Fernverbindung.

Hier wird der Session Border Controller eingesetzt, um eine sichere Grenze zwischen der VoIP-Welt mit all ihren Komponenten wie TK-Server, PSTN Gateways, SIP Server und TK/UC-Applikationsservern einzurichten. Diese Grenze benötigt oft einen besonders hohen Funktionsumfang, daher hat sich ein eigener ESBC Markt (Enterprise Session Border Controller) etabliert.

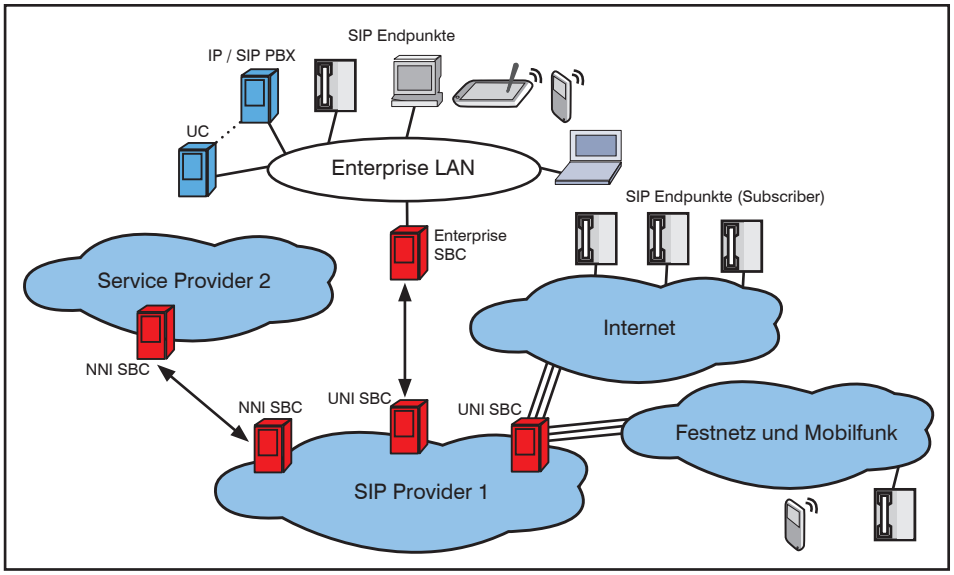

Abbildung 2.1: SBC-Einsatzszenario für Provider, Unternehmen und Einzelanbindungen

Bei Einzelanbindungen über SOHO, Internet, Fixed Mobile Conversion (FMC) Zugangsnetzen wie Festnetz, Mobilfunk, DSL ist der SBC auf der Kundenseite vielfach zu teuer und entfällt. Dieses UNI Interface wird auch Subscriber-Interface genannt. Hier finden wir typischerweise nutzerseitig keinen Session Border Controller sondern nur am Netzübergang des (SIP) Providers zum Subscriber. Das Beispiel aus Abbildung 2.2 zeigt Subscriber UNI Übergänge aus dem Internet, Festnetz und Mobilfunknetz.

Network to Network Interface

Obwohl die meisten Provider ihre internen SS7 Backbones längst durch SIP ersetzt haben, wird am Übergang zwischen verschiedenen Providern meistens weiterhin ISDN und SS7 eingesetzt! Das bedeutet eine SIP-ISDN und danach wieder ISDN-SIP Konvertierung – soweit zu All-IP… Abgesehen von den resultierenden Interworking Themen (SIP ist nicht gleich SIP) beseitigt diese unselige Doppelkonvertierung nicht das gegenseitige Sicherheits-Bedürfnis: Ganz ähnlich wie der Bedarf nach einer sicheren Grenze zwischen Unternehmen und Provider haben auch zwei Provider gegeneinander das Bedürfnis, sich abzuschotten. Die Netzwerke im Provider-Umfeld sind nicht nur IP-Netzwerke, sondern auch Festnetz (PSTN), Funknetze (GSM, UMTS, LTE) bis hin zu Kabel(modem)netzen.

Hier geht es jedoch nicht nur um die Abwehr möglicher Seuchen und Angriffe, sondern auch ganz explizit um Wettbewerbs-Schutz: Durch das Entfernen von Routing Headern zum Beispiel verbirgt ein Provider 1 nicht nur die eigenen internen Netzstrukturen vor einem Provider 2, sondern löscht auch alle Informationen, die Provider 2 den direkten Zugang zum Kunden zeigen und ihm so ermöglichen könnten, diesen abzuwerben.

Da sich noch kein definierter Standard für SIP Trunking durchgesetzt hat, gibt es funktional immer wieder Unterschiede zwischen SIP Dialekten verschiedener Provider. Somit ist eine SIP-Normalisierung beziehungsweise Anpassung verschiedener Provider-SIP-Implementierungen aneinander eine weitere wesentliche NNI SBC Funktion.

Gegenseitige Abrechnungs- und SLA-Monitoring-Funktionen sind ebenfalls ein wichtiger Funktionsbereich bei NNI Session Border Controllern, hier ersetzen sie die frühere Funktionalität entsprechender PSTN-Knoten im SS7 Umfeld.

Das NNI wird in zweifacher Hinsicht benötigt: Zum einen für reine Durchleitung, da nicht jeder Provider flächendeckend in allen Ländern eine Netzwerk-Infrastruktur besitzt. Zum anderen aber auch für die gegenseitige Nutzung von Diensten, die ein Provider selbst nicht bereitstellen kann oder will: Das Beispiel aus Abbildung 2.2 zeigt zwei Provider, die einen unterschiedlichen Dienst-Fokus haben: Service Provider SP1 hat flächige PSTN-Gateways installiert, Service Provider SP2 stellt TK, UC und weitere Kommunikations-Applikationen zur Verfügung. Mittels entspre-

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

chender Durchleitungs-Vereinbarungen sind nun beide in der Lage, ihren Kunden sowohl die Applikationen als auch den optimierten PSTN-Zugang anzubieten – für beide eine Win-Win Situation. Die entsprechenden gegenseitigen SLAs sowie die interne Abrechnung der gegenseitig geleisteten Dienste werden hier einen erheblichen Teil der Vertragsgestaltung ausmachen. Wie schon zuvor erläutert, werden auch in diesem Beispiel beide Provider an ihrem jeweiligen NNI Session Border Controller die Routing Header mit Kundeninformationen entfernen, um den direkten Kundenzugang für den jeweils durchleitenden Provider zu unterbinden.

Hochverfügbarkeits-Szenarios für Enterprise SBCs

Da ein Enterprise SBC (ESBC) oft ein zentraler Übergangspunkt ins öffentliche Kommunikations-Netz (SIP Netz) für viele Teilnehmer / Nutzer ist, muss hier am ehesten über Hochverfügbarkeits-Lösungen nachgedacht werden. In erster Linie wird natürlich der SBC selbst in diesem Fall zu doppeln sein. Um dies katastrophengeeignet zu bewältigen, erfolgt eine Positionierung in zwei getrennten (mindestens 5 Kilometer voneinander entfernten) Rechenzentren. Ob hierfür separate Appliances einzusetzen sind oder zwei virtualisierte Session Border Controller zum Einsatz kommen können, ist vielfach eine Frage der gewünschten Leistung und Skalierbarkeit. Die jeweiligen SBCs werden zum Provider Edge hin mindestens mit einem Router (wie in Abbildung 2.3), oder darüber hinausgehend wie unter Kapitel 1 beschrieben mit dem IT-Firewall geschützt.

Das Beispiel-Szenario aus Abbildung 2.3 zeigt ein Unternehmensnetzwerk, in dem alle Standorte an zwei vollredundante zentrale Data Center angebunden sind. Somit haben die in den Standorten installierten Telefone keine eigenen Server und keinen eigenen Zugang zum öffentlichen SIP Netz, sondern nutzen stattdessen die zentralen Data Center 1 und 2 und die dortigen SIP Trunks. Die Standorte selbst sind mit einem Einzelrouter (Single Point of Failure) an das MPLS-Netz angebunden, das heißt hier sieht das Unternehmen keinen HA-Bedarf für das Ausfallrisiko aller Telefone eines Standortes. Fällt jedoch ein singulärer ESBC aus, so verlieren ohne Vollredundanz sofort alle Standorte - das heißt alle Nutzer - den Zugang zum öffentlichen SIP-Netz, was natürlich eine wesentlich gravierendere Ausfallsituation darstellt und somit per HA abgesichert wurde. Gleichermaßen ist die zentrale TK/UC Serversuite vollredundant ausgelegt – denn was nutzt ein HA Enterprise Session Border Controller, wenn ein einziger verfügbarer TK/UC Server ausfällt? Genau - der HA-ESBC nutzt in

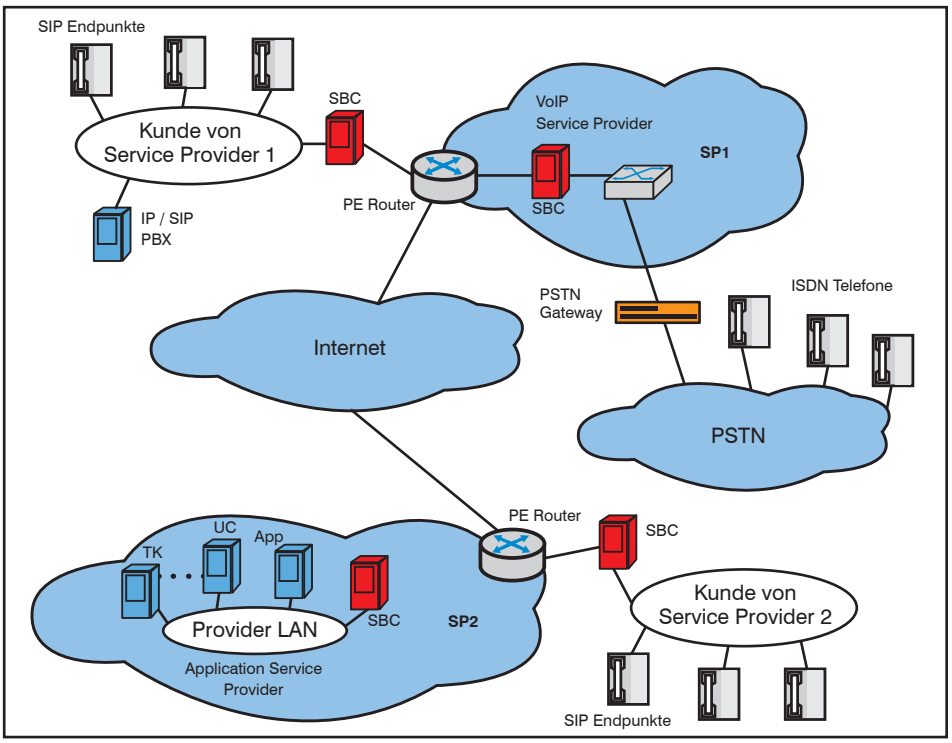

Abbildung 2.2: NNI SBCs zwischen Providern mit unterschiedlichen Dienstangeboten

diesem Fall gar nichts mehr. Gleiches gilt natürlich für die physische SIP Trunk Anbindung an Provider 1: Zur Vermeidung eines SPOF muss sie wegeredundant über verschiedene Hauszuführungen und Trassen sowie an zwei POPs geführt werden.

Das dargestellte Beispiel hat über die übliche Hochverfügbarkeit hinausgehend noch zwei weiterführende "UHA"-Redundanzerweiterungen (Ultra High Availability): Erstens wurde das Management gedoppelt (ein Ausfall des Managements bedeutet ja noch keinen Ausfall der SBCs), zweitens gibt es von jedem Data Center aus zwei SIP Trunks zu zwei unterschiedlichen Providern. Letzteres soll auch noch den Komplettausfall eines Providernetzes absichern. Bei einer solchen UHA ist natürlich vorab zu vereinbaren

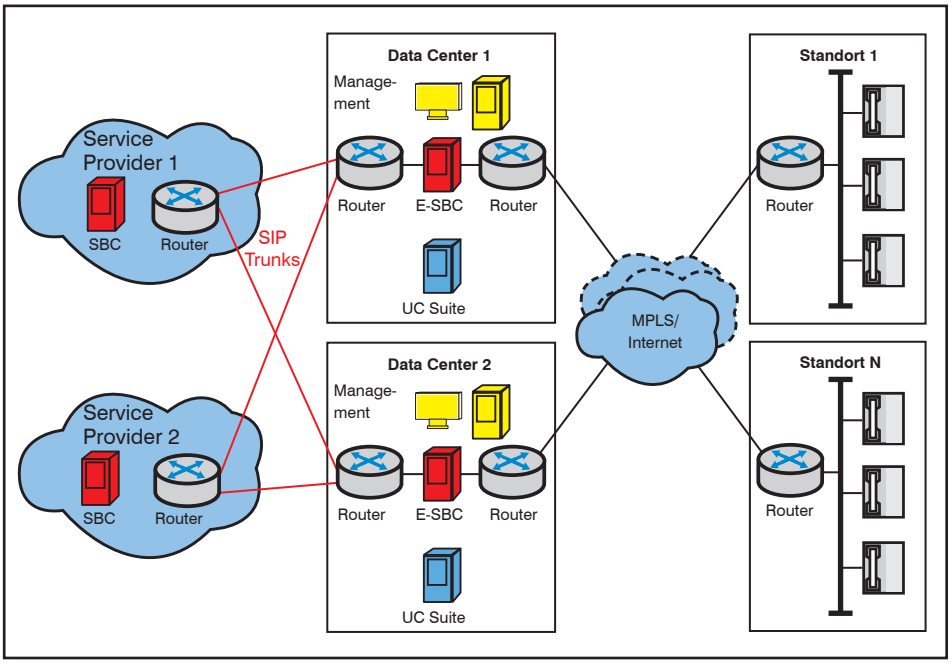

Abbildung 2.3: UHA-Szenario für Enterprise SBCs

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

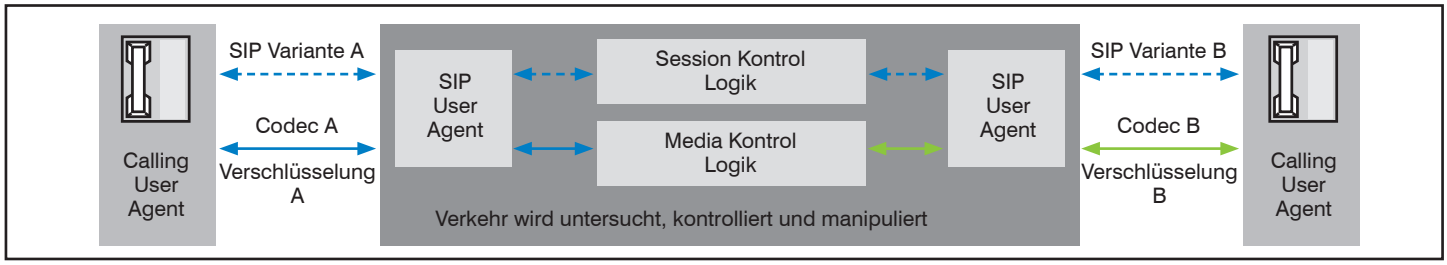

Abbildung 3.1: Der Session Border Controller als B2BUA Agent

und auch im Nachgang gelegentlich zu testen, wie sich die Umschaltung zwischen den beiden gewählten Providern automatisieren lässt und welche Schaltzeiten dann machbar sind. Die Schwierigkeit hierbei ist die, dass ja im Normalfall alle eingehenden Telefonate (Calls) beziehungsweise SIP Sessions nur bei jeweils einem der beiden Provider ankommen und bearbeitet werden sollen, also ein eindeutiges Call Routing gefahren wird. Für eine automatisierte Umschaltung müssen beide Provider gegenseitig ihre Konfiguration oder zumindest Teile davon offenlegen, was meistens zu erheblichen Widerständen bei beiden Providern führt.

Hinsichtlich der Kosten einer solchen UHA-Lösung können diese bei entsprechend vielen Standorten immer noch niedriger liegen als die Kosten für Konfiguration und Betrieb von lauter dezentralen DMZ / ESBC Konfigurationen. Zudem ist das Risiko von Inkonsistenzen und Sicherheitslücken bei einer zentralen Lösung niedriger als bei einer dezentralen.

3. Die Funktions-Elemente des SBC

Session Border Controller stehen typischerweise in den DMZs und bearbeiten den Verkehr von und zu SIP Trunks und anderen Kommunikations-Netzverbindungen, insbesondere für Echtzeit-Kommunikationsprotokolle. Sie verbinden also nicht nur das Unternehmen über SIP Trunks mit dem öffentlichen SIP-Kommunikationsnetz und kontrollieren hierüber auch die Kommunikation mit dem PSTN sowie mit gehosteten TK/UC Cloud Diensten. Darüber hinaus verbinden Enterprise SBCs auf der Enterprise Seite verschiedene Standort-Netzwerke eines einzelnen Unternehmens, die über Corporate WAN zusammenhängen oder auch verschiedene Standorte verschiedener Unternehmen über öffentliches Internet. Letzteres wird als Föderation bezeichnet, beispielsweise zwischen einer TK-Lösung von Avaya und Alcatel-Lucent, zwischen einer UC-Lösung von Cisco und Microsoft Lync oder zwischen einer Contact Center Lösung von Luware und von Unify.

SBCs tun mehr als Firewalls

Während eine Firewall erlaubten Verkehr (unverändert) durchlässt und unerlaubten Verkehr blockiert, leistet der SBC Session Management und Kontrolle für Multimedia Kommunikation. Die meisten IP Firewalls leisten Basis-Unterstützung für SIP: Access Control Listen, die basierend auf Adress-Informationen IP/TCP/SIP Header den SIP Verkehr zulassen oder blockieren können. Der Unterschied liegt in der unterliegenden Architektur von SBCs: In "SIP-Sprache" ist eine SIP Firewall ein SIP Proxy Server, der für die Weiterleitung und Kontrolle der SIP Signalisierung zuständig ist, jedoch nicht aktiv etwas mit der Bearbeitung der Media Streams zu tun hat.

Ein SBC ist als so genannter Back-to-Back User Agent (B2BUA) implementiert, der sowohl Signalisierung als auch Media Stream aktiv bearbeitet.

Laut RFC 3261 muss zwar bei einem Back-to-Back User Agent nur die Signalisierung und nicht der Media Stream zwingend über den B2BUA laufen, im Fall SBC als B2BUA läuft jedoch auch der Media Stream über den Session Border Controller. Wie Abbildung 3.1 zeigt, terminiert der SBC als B2BUA die Session einer SIP Entität (hier anrufender Teilnehmer) und richtet eine separate Session zu einer anderen SIP Entität (hier angerufener Teilnehmer) ein. Hierbei verbirgt er vor beiden SIP Entitäten die Topologie und Architektur der jeweils anderen SIP Entität, insbesondere interne IP Adressen von Servern und Telefonen. Im Gegensatz zu Firewalls hält der SBC alle Session Stati vor, kontrolliert und manipuliert die Signalisierung und die assoziierten RTP Media Streams.

Insbesondere ist der SBC state-aware für SIP, RTP und RTCP, das heißt er hält für die Dauer der Session entsprechend durchlaufende Pinholes für die jeweils dynamisch gewählten Portnummern offen. Ein Firewall dagegen könnte ein Pinhole schließen und mit einer anderen Portnummer wieder öffnen, was bei SIP / RTP / RTCP jedoch zum Session-Abbruch führen kann.

Da der SBC das Paket aktiv auf Schicht 5 bearbeitet, kann er alle NAT-Änderungen auch in die entsprechenden SIP/RTP/RTCP Header übertragen. Somit ist ein wichtiges Problem gelöst: der NAT Traversal. Er scheitert bei "normalen" Firewalls daran, dass diese mittels Adress- und Portnummern-Änderung lediglich Schicht 3 und 4 manipulieren, die getätigten Änderungen jedoch nicht in die Schicht 5 übertragen. Der Empfänger schmeißt – im Wissen, dass er alle Informationen nochmals auf Schicht 5 findet – Schicht 3 und 4 jedoch weg und findet dann in Schicht 5 die originären, inzwischen leider (weil durch NAT geändert) falschen Informationen. Der Rückweg ist mit diesen "falschen" Adressen dann nicht mehr möglich. In der Praxis haben sich zur Lösung des NAT Problems STUN und ICE (RFC 5389) etabliert.

Die Paket-Bearbeitung findet auf der Session-Schicht statt und beinhaltet auch die Änderung, Anpassung und Konvertierung von Paketen. Wesentlich ist, dass SBCs für jede Session sowohl Signalisierung als auch Media Stream terminieren und neu aufsetzen. Das versetzt einen SBC als zentralen Demarkationspunkt in die Lage, Beliebiges mit den Paketen anzustellen, insbesondere sie auf der Basis granularer Sicherheits- und Qualitäts-Regeln zu überprüfen, in eine vorrangige oder nachrangige Warteschlange einzuordnen, gewissen Senderaten-Limitierungen zu unterwerfen, sie anzupassen und zu ändern, bis hin zur kompletten Unterdrückung unerwünschter Verkehrslasten.

Zusätzlich ist der SBC natürlich die geeignete Komponente für ein Gesamt-Monitoring aller durch ihn bearbeiteten Verkehrslasten.

In dem zuvorigen Zusammenhang leistet der SBC eine ganze Reihe von Funktionen:

- Protokoll-Manipulation: für Interoperabilität / Interworking zwischen der SIP Enterprise Lösung und dem SIP Trunk / SIP Provider sowie für Interoperabilität zwischen verschiedenen Enterprise Lösungen

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

- Protokoll-Konvertierung: zum Beispiel zwischen SIP und H.323, soweit letzteres noch vorhanden ist
- Sicherheit: durch Deep Packet Inspection und Anwendung entsprechender Sicherheits-Regeln
- Verschlüsselung: Terminieren und Neu-Aufsetzen von Verschlüsselung oder Konvertierung von SRTP auf IPsec
- Quality of Service: SLA Überwachung oder auch Notruf (112)
- Session Routing: Optimierung der Wegwahl hinsichtlich Fehlerumschaltung, Lastverteilung, Least Cost Routing
- Codec Anpassung
- Session-Replizierung: für Aufzeichnungen (intern oder gesetzlich)

Insbesondere ESBCs sind speziell dafür entwickelt, die vergleichsweise komplexen Sicherheits-, Interoperabilitäts- und Quality of Service Anforderungen im Umfeld von IP-Telefonie, Unified Communications und beliebigen Endgeräten bis hin zu BYOD handhaben zu können.

Wie kommt nun ein SIP- oder RTP-Paket von der einen auf die andere Seite? Die Signalisierung nutzt intern den Port 5060 oder 5061, der SBC kann dies intern z.B. in einen TCP Tunnel zwischen "SBC-Eingang, Firewall und SBC-Ausgang" wandeln, der die interne Signalisierung terminiert und nach außen erneut den Port 5060 oder 5061 verwendet, jedoch mit geändertem Source-Port und geänderter IP-Quelladresse. Der Media Stream (z.B. Audio Datenstrom) nutzt intern freie UDP Ports (>1023), die über definierte Ports zwischen "SBC-Eingang, Firewall und SBC-Ausgang" terminiert werden und nach außen als freie UDP Ports neu aufgesetzt werden. Entsprechende Beispiele zeigen die Abbildungen 3.2 und 3.3.

4. Die Leistungsmerkmale eines SBC

Der Funktionsumfang von Session Border Controllern lässt sich grundsätzlich in die nachfolgenden Bereiche unterteilen:

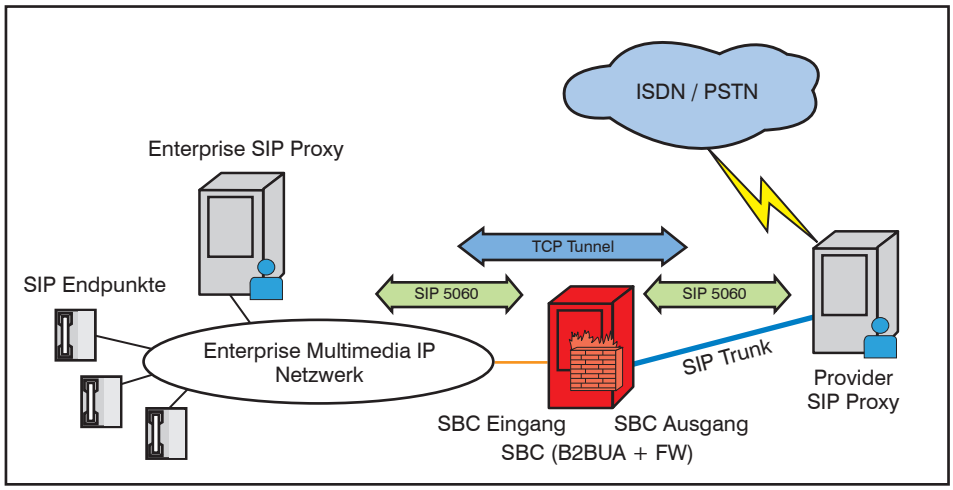

Abbildung 3.2: Weiterleitung von SIP Paketen durch den SBC

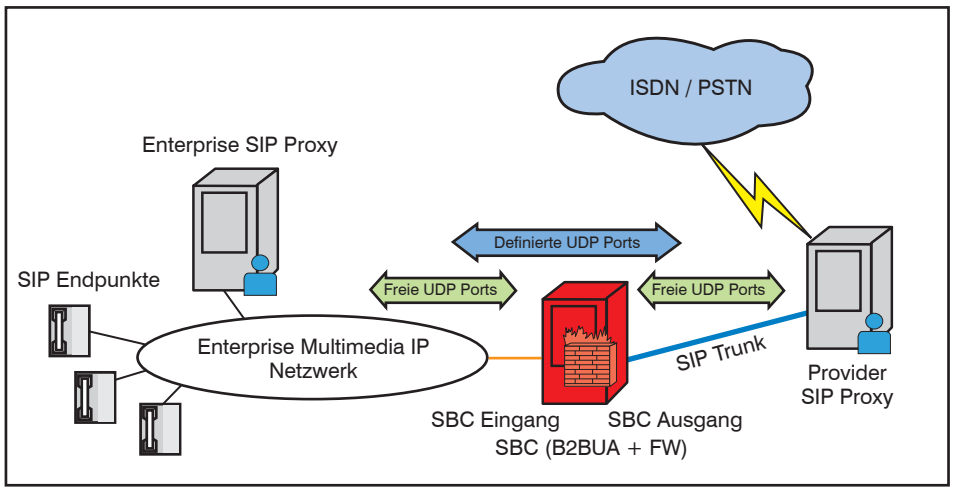

Abbildung 3.3: Weiterleitung von RTP Paketen durch den SBC

- Sicherheit
- Interoperabilität / Interworking
- Verfügbarkeit, SLA-Sicherstellung
- Regulatorische Compliance
- Management
- Architektur, Leistung, Skalierbarkeit

Die Grafik in Abbildung 4.1 zeigt die Ergebnisse einer Webtorials Umfrage zu Enterprise Session Border Controllern (2015 UC, SIP and SBC Plans and Priorities; Webtorials 12/2014), welche Wichtigkeit einzelne Funktionen für die befragten Unternehmen haben.

Dass die Sicherheit hier ganz oben und Integration mobiler Geräte auf Platz drei steht, ist nicht überraschend. Dass aber Voice Transcoding den zweiten Platz hält, belegt eindrucksvoll, wie wenig einheitlich SIP Kommunikation über verschiedene Netze hinweg heute immer noch implementiert ist. Hinsichtlich WebRTC ist zu erwarten, dass sich diese Position vom aktuell letzten Platz in den nächsten Jahren schnell nach oben arbeiten wird.

4.1 Sicherheit

Vorrangig schützen SBCs sowohl Session Agenten und UC-Diensterbringer der Unternehmens-Infrastruktur als auch sich selbst. Hierfür leisten sie als erstes Zugangsschutz im Sinne einer Überprüfung gehender und kommender Sessions (Access Control), schützen im Nachgang die einzelnen zugelassenen Sessions und bieten Schutz gegen externe Angriffe sowie bei "normalen" (nicht-kriminellen) Überlasten.

Bedrohungen

Im Rahmen der Schutzfunktionen leisten sie insbesondere die nachfolgenden Funktionen:

- Schutz gegen unberechtigte Ressourcen-Nutzung (Service-Theft) und Toll Fraud: Bei solchen Angriffen dringen Hacker in ein ungenügend gesichertes VoIP System ein und routen IP-Telefonie darüber ohne dafür zu bezahlen. Hierbei nutzen sie die Netzwerk-Ressourcen des angegriffenen Unternehmens und generieren bezahlpflichtige Anrufe, die dann aber das Unternehmen vom Provider in Rechnung gestellt bekommt.

- Schutz gegen Spoofing: Der Angreifer verschleiert seine eigene Identität (zum Beispiel Caller-ID, Telefonnummer) und gibt sich als jemand Anderes aus, entweder um dessen Anrufe auf sich zu ziehen oder auch nur um Verwirrung zu stiften.

- Schutz gegen DoS/DDoS: Diese Angriffe versuchen, TK-/UC-Server oder den

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

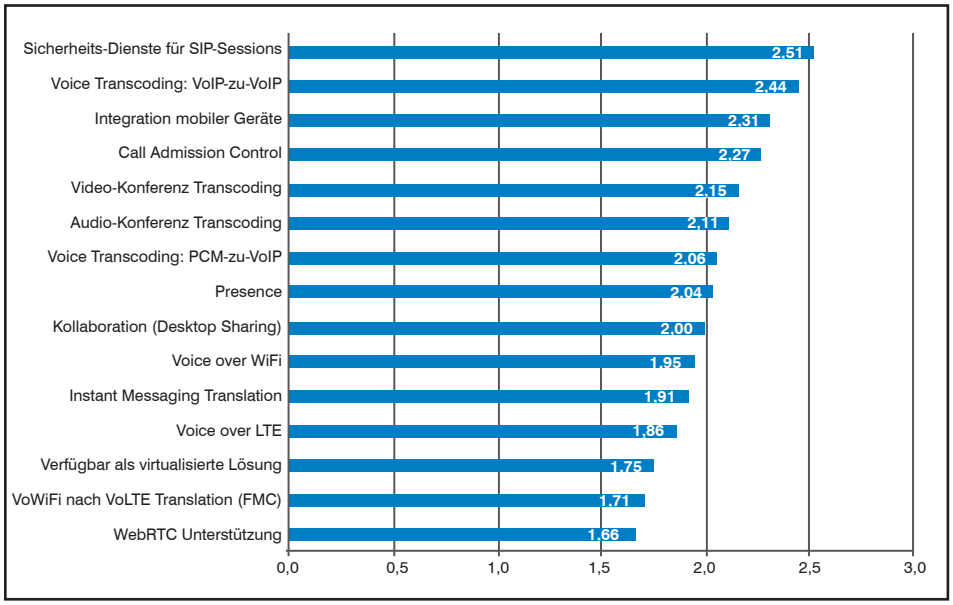

Abbildung 4.1: Wichtigkeit von ESBC Funktionen

SBC selbst zu fluten oder anderweitig zu kompromittieren, so dass die normale Paketbearbeitung völlig zum Erliegen kommt und de facto für den TK-/UC-Dienst eine Ausfallsituation entsteht.

- Registrierungs-Storms: entweder gezielt kriminell oder aufgrund vorhergegangener (Netzwerk)-Fehlersituationen versuchen tausende bis zigtausende Geräte gleichzeitig, sich neu zu registrieren.

Angriffsschutz
ESBCs stellen zum Schutz gegen die zuvor genannten Bedrohungen eine Applikations-Firewall für Voice, Video und Multimedia dar, insbesondere mit folgenden Leistungsmerkmalen:

- Zugangsschutz für Voice, Video und Multimedia auf Applikations-Ebene
- Überprüfung und Überwachung erlaubter Sessions
- Schutz gegen TDoS (Telephony Denial of Service)
- Schutz gegen VDoS (Video Denial of Service)
- Schutz der Vertraulichkeit (Abhören, Mitschneiden, Man in the Middle)
- Schutz der Authentizität (Prüfsummen)
- Deep Packet Inspection
- Topology Hiding

Die Schutzfunktionalität wird ähnlich wie bei Firewalls mittels komplexer Regeltabellen umgesetzt, ein Beispiel hierfür zeigt Abbildung 4.2.

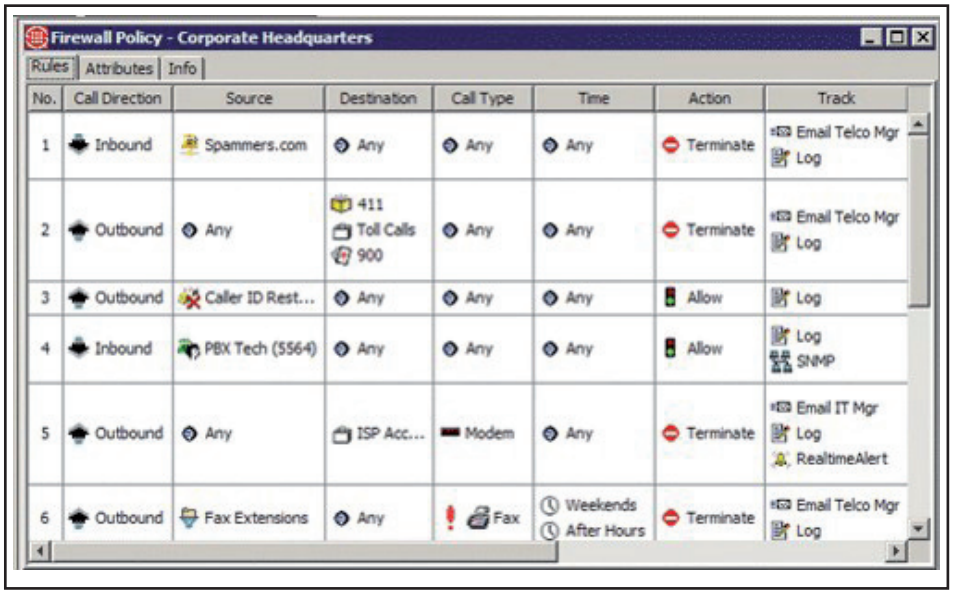

Abbildung 4.2: Access Control Tabelle eines SBC

Für die Zugangskontrolle auf Applikations-Ebene überprüft der SBC entsprechende Zertifikate oder Credentials der beteiligten Endgeräte, beispielsweise mit dem Online Certificate Staus Protocol (OSCP) oder ähnlichen Protokollen. Zusätzlich handhaben SBCs für alle Registrierungen, alle ausgehenden und alle eingehenden Verbindungen eine komplexe ACL-Listenüberwachung mit

- Whitelisten (uneingeschränkter Zugang)
- Blacklisten (unerlaubter Zugang)
- Greylisten (regelbasiert eingeschränkter Zugang)

Hierbei kann ein Session Border Controller den erlaubten Verkehr automatisch gegenüber nicht erwünschtem Verkehr priorisieren, so dass auch während eines DoS Angriffs der erlaubte Verkehr vorrangig bearbeitet wird. Wird eine Verbindung erlaubt, so richtet die Signalisierung durch den SBC hindurch eine Punkt-zu-Punkt Verbindung ein, der SBC öffnet die ausgewählten Ports und richtet einen "RTP Flow" zwischen den beteiligten Endgeräten ein. Der SBC fügt seiner ACL-Tabelle eine Regel für den aktuell zugelassenen Flow hinzu, so dass die zugehörigen RTP Pakete überprüft und danach zum routingtechnisch günstigsten Next Hop (zum Beispiel delay-optinmiert) weitergeleitet werden können. Ist eine Verbindung einmal zugelassen, wird sie im Fall einer Greylist auf erlaubte und unerlaubte Aktionen überwacht.

Sicherung der Authentizität und Vertraulichkeit erfolgt durch die Bildung von Prüfsummen (SRTP, TLS) sowie durch Verschlüsselung und deren Anpassung am Übergang zum öffentlichen Netz / beim Internet Traversal. Typischerweise erfolgt die Verschlüsselung der Signalisierung mit Signalisierung mit TLS (setzt TCP auf der Transportschicht voraus), die Verschlüsselung des Media Streams mit SRTP. Soweit erforderlich, können Session Border Controller auch Konvertierung zwischen SRTP und IPsec durchführen.

Egal ob es um Terminierung und Wiederaufsetzen der Verschlüsselung oder Anpassung der Verschlüsselung (SRTP / IPsec) geht, in jedem Fall ist eine entsprechend hohe Leistung wichtig, um die Bearbeitungszeit möglichst niedrig zu halten. Teilweise sinkt bei Einsatz von Verschlüsselung die Anzahl maximal möglicher Sessions bis auf 50% der maximalen Sessionzahl ohne Verschlüsselung! Hier sind spezielle Appliances den OTS Servern vielfach überlegen, deren Architektur eigene Prozessoren zum Offload der Verschlüsselungs-Prozesse hat.

SBCs schützen das Enterprise Netz, die

dort positionierten Server und Kommunikationsbeziehungen zum Provider, indem sie die interne Netzwerk Topologie durch Nutzung von Network Address Translation (NAT) auf Layer 3 (IP) UND Layer 5 (SIP) Topologie verbergen, die Service Infrastruktur gegen DoS/DDoS schützen und VPN Trennung umsetzen. Im Rahmen dieses Topologie Hidings werden insbesondere interne IP Adressen von Netzkomponenten, Servern und Telefonen verborgen.

4.2 Interoperabilität, Interworking

Session Border Controller übernehmen mehr als nur Sicherheits-Funktionen. Manchmal geht die Rede: Es ist die Sicherheit, die das Interesse am SBC weckt, aber tatsächlich sind es seine anderen Funktionen, die letztendlich zu Kauf und Implementierung führen. Dies gilt insbesondere in den Bereichen Interoperabilität und Interworking mit Funktionen wie Mediation und Konvertierung zwischen verschiedenen Protokollen für Signalisierung, Transport und Verschlüsselung.

SIP Normalisierung

SIP ist aktuell DAS vorrangige Echtzeit-Kommunikationsprotokoll und ist somit elementar wichtig, um verschiedene Netze, TK-/UC-Lösungen, Hersteller und Provider miteinander kommunizieren lassen zu können. SIP ist eine globale IETF-Kommunikations-Standard-Suite, aber Hersteller und Provider haben jeweils ihre eigenen SIP Dialekte implementiert, die zwar technisch grundsätzlich zu den SIP Standards, aber nicht notwendigerweise gegeneinander kompatibel sind. Teilweise liegen im Gegenteil die Implementierungen zweier miteinander verbundener SIP-Systeme in Syntax und Dialekt so weit auseinander, dass sie wie zwei verschiedene Sprachen aneinander vorbei reden. Dies liegt einerseits an nicht immer bis ins letzte durchspezifizierten RFCs, andererseits an unterschiedlichen Interpretationen eines RFCs. Teilweise wurde von 3GPP Providern eher IETF RFC 3261 implementiert, von Festnetz Providern eher TISPAN, im Mobilfunknetz die IMS Spezifikationen, in bestimmten frühen SIP Trunking Szenarien eher SIP-I nach ITU-T 2004 Q.1912.5. Diese "SIP Dialekte" sind jeweils auf die Nutzung bestimmter Header, Authentisierungen und spezielle SIP Erweiterungen (wie NOTIFY/SUBSCRIBE) beschränkt. Neben den Header-Unterschieden fügt SIP-I zusätzlich einen weiteren SIP Body Typ, den ISUP Teil, in das SIP Paket ein; was wiederum der Rest der SIP Dialekte dann gar nicht mehr verstehen kann und will.

In allen beschriebenen Fällen werden jedenfalls die jeweils beteiligten Hersteller / Provider alle im Brustton der Überzeugung darauf beharren, dass sie den Standard implementiert haben…

Abbildung 4.3: Verschlüsselung sichert Vertraulichkeit

Und noch schlimmer: Interoperabilitätsprobleme können wie Angriffe wirken, das heißt ein TK-Server wird gegebenenfalls SIP Header mit Parametern, die ihm unbekannt sind, verwerfen, weil er sie für einen Angriff hält. Tatsächlich gibt es diese Angriffe ja auch, die durch manipulierte SIP Header den TK-Server bis hin zum Core Dump kompromittieren können.

Und hier kommt der Session Border Controller ins Spiel: Seine Rolle ist es, alle benötigten Dialekte zu sprechen und bei zwei Dialekten "X" und "Y" die Teile von X und Y, die nicht zueinander passen, "mit wirespeed" ineinander zu übersetzen.

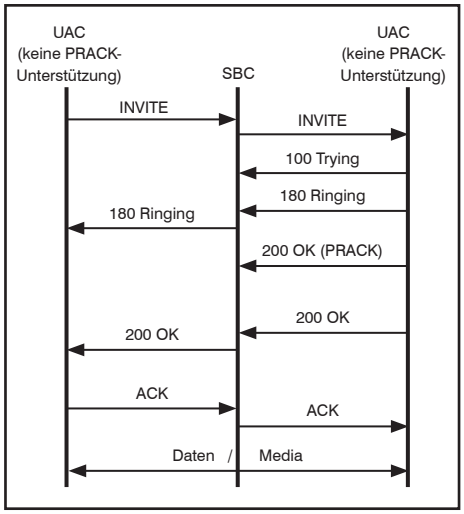

Abbildung 4.4: Callflow Anpassungsbeispiel für PRACK zwischen IMS und non-IMS SystemenVertraulichkeit

Je nahtloser er das tut, umso besser erledigt er seinen Job. Er hat hierfür entsprechende Header Manipulation Rules (HMRs), die jeweils Dialekt X in Dialekt Y wandeln. Für den einfachen Fall gibt es die zustandslose Header-Manipuliation, bei der der SBC bestimmte Header entfernt und stattdessen andere Header einfügt. Für den komplexeren Fall gibt es die zustands-orientierte Paketbearbeitung, in der ein kompletter Call Flow angepasst wird. So arbeitet beispielsweise das IMS sehr oft mit PRACK (Provisional Acknowledgement) während PRACK in RFC 3261 Umgebungen wenig verbreitet ist. Das Beispiel in Abbildung 4.4 zeigt, wie ein Session Border Controller die Call Flows zwischen IMS und IETF RFC 3261 anpassen kann.

Der typische Anpassungsfall sind SIP Dialekte zwischen der Provider SIP Lösung auf der einen und der Enterprise SIP Lösung auf der anderen Seite. Wichtige Leistungsmerkmale sind hier Translation-Funktionalität für:

- Telefon-Nummer
- Adresse
- Antwort Codes

Über die SIP Signalisierung hinausgehend kann auch eine Konvertierung der Signalisierung (Transsignalling) notwendig werden, zum Beispiel zwischen SIP und H.323, soweit dieses noch im Einsatz ist.

SIP Mediation

Ein wichtiger Funktionsbereich ist die Anpassung verschiedener Media Streams und Codecs aneinander mittels Transcoding und/oder Transrating: Der SBC

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

weiß, welche Codecs beide Seiten unterstützen, ob es einen gemeinsamen Codec gibt, ob er diese in der Senderate gegeneinander angepassen muss oder ob er zwei möglichst geeignete Codecs ineinander konvertieren muss. Er nutzt dazu eine Mischung aus Software und DSPs, die Voice und Videosignale in Echtzeit decodieren und wieder neu codieren. Hierzu zählen Leistungsmerkmale wie

- Anpassung zwischen HD Voice bei neueren und G.711 bei älteren Geräten
- Anpassung zwischen G.711 und G.729 bei Bandbreiten-Restriktionen
- Neu-Auswahl des Codec (Renegotiation), um Bandbreite zu optimieren
- Fax- und Faxton-Erkennung
- Fehlerkorrektur (z.B. Echo Unterdrückung)
- Media-Einspielung (z.B. Musik, MoH)
- Media Replizierung für Aufzeichnung (Standards SIPREC: "Session Recording Protocol", "Session Initiation Protocol (SIP) Recording Metadata")

Da es sich so gut in das Mediations-Portfolio einfügt, spielen Session Border Controllern bei Bedarf auch Media Bridge und sparen so die Implementierung separater Gateways zwischen verschiedenen Konferenzlösungen für Voice und Video (siehe Abbildung 4.5).

Ein weiterer Anpassungsbereich für SBCs, der ebenfalls nicht vernachlässigbar ist, tut sich aktuell bei der IP-Adressierung auf: Bridgefunktion und Konvertierung zwischen IPv4 und IPv6 für private und öffentliche IPv4 und IPv6 Adress-Räumen.

In Teil 2 lesen Sie:

- Funktionen von SBCs:
  - Verfügbarkeit, SLA-Sicherstellung
  - Regulatorische Compliance
  - Management
  - Architektur, Leistung, Skalierbarkeit
- Markt und Hersteller: Einige Produktbeispiele

Lesen Sie auch folgende Artikel zum Thema von Frau Borowka-Gatzweiler

"SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen - Teil 1", Netzwerk Insider Ausgabe August 2008

"SIP Trunking und SIPconnect bieten neue Möglichkeiten für standortübergreifende TK-Anwendungen - Teil 2", Netzwerk Insider Ausgabe April 2009

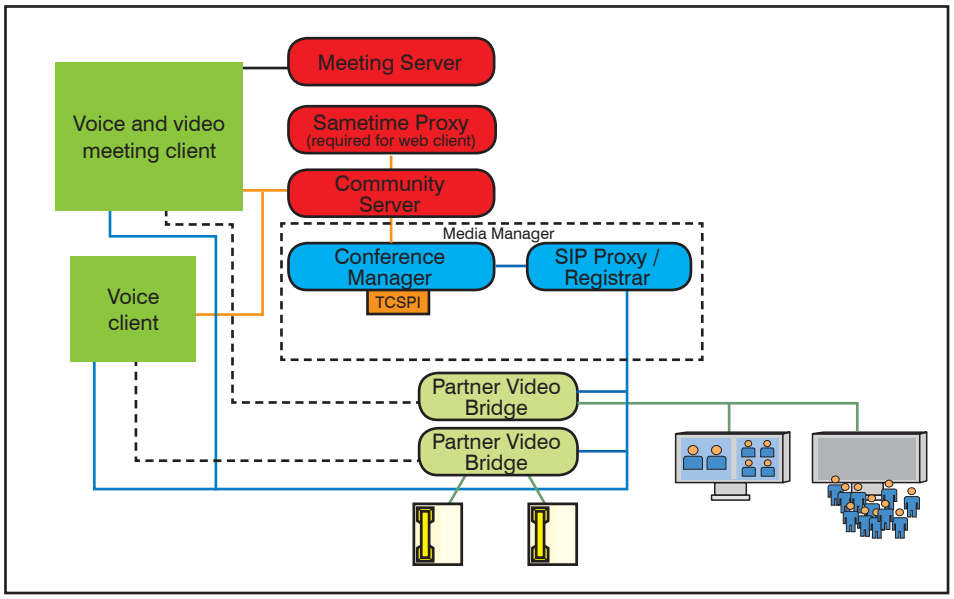

Abbildung 4.5: Der SBC als Media Bridge

Abkürzungen, Links, Literatur

ACL	Access Control List(e)
ALG	Application Layer Gateway
A/V	Audio / Video
B2B	Business to Business
B2BUA	Back-to-Back User Agent
BRI	Basic Rate Interface
BYOD	Brind Your Own Device
CAC	Call Admission Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DSP	Digital Signal Processor
ESBC	Enterprise SBC
FMC	Fixed Mobile Conversion
FW	Firewall
GW	Gateway
GSM	Global System for Mobile Communications
HA	High Available
HMR	Header Manipulation Rules
ICE	Interactive Connectivity Establishment
ICT	Informations and Communications Technology
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITSP	Internet Telephony Service Provider
ITU-T	International Telecommunication Union-Telecommunication Standards
LCR	Least Cost Routing
LTE	Long Term Evolution
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NNI	Network to Network Interface
OCSP	Online Certificate Status Protocol
OTS	Off the Shelf
PBX	Private Branch eXchange
POP	Point of Presence
PRI	Primary Rate Interface
PSTN	Public Switched Telephony Network
QoS	Quality of Service
QSIG	Q-interface SIGnalling protocol
RFC	Request for Comment
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Communications
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIP-I	SIP - ISUP Interworking
SIPREC	SIP RECording
SP	Service Provider
SPOF	Single Point Of Failure
SRTP	Secure RTP
SS7	Signaling System #7 / Signalisierungssystem Nummer 7
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TCSPI	Telephony Conferencing Service Provider Interface
TDM	Time Division Multiplexing
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TK	Telekommunikation
TLS	Transport Layer Security
UC	Unified Communications
UCC	Unified Communications and Collaboration
UDP	User Datagram Protocol

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

UHA	Ultra High Available
UMTS	Universal Mobile Telecommunications System
UNI	User to Network Interface
URI	Universal Resource Identificator
VDOS	Video Denial of Service
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

Links

www.ietf.org
www.sipforum.org
www.sonus.net

Literatur

- Pat Hurley: Session Border Controller for Dummies; Wiley & Sons, 2nd Edition 2013
- Session Boder Controllers: A Primer; Oracle White Paper 2013
- Market Guide for Enterprise SBC; Gartner, Juni 2014
- John Hardwick: Session Border Controllers, Enabling The VoIP Revolution; Data Connection Whitepaper, 2005

Standpunkt

Vertrauenskrise bei Zertifikaten

Der Standpunkt von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Zertifikate sind als Instrument zur Authentisierung unverzichtbar geworden. Schließlich basiert die gesamte SSL-/TLS-geschützte Kommunikation und damit die Absicherung vieler Web-Anwendungen und Web-Services darauf.

Wesentliches Element der Authentisierung mit Zertifikaten ist ein kryptographisches Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel, der Bestandteil des Zertifikats ist, und einem geheimen Schlüssel, der besonders geschützt beim Eigentümer des Zertifikats gespeichert wird. Bei der Ausstellung eines Zertifikats signiert die entsprechende Zertifizierungsstelle (Certificate Authority, CA) das Zertifikat mit ihrem eigenen privaten Schlüssel. Damit kann bei der Authentisierung mit dem Zertifikat anhand des öffentlichen Schlüssels der ausstellenden CA geprüft werden, ob das Zertifikat gefälscht bzw. manipuliert ist. Weiterhin kann unter Verwendung des öffentlichen Schlüssels eines Zertifikats geprüft werden, ob der Kommunikationspartner, der sich über ein Zertifikat authentisiert, auch im Besitz des zugehörigen privaten Schlüssels ist. Besteht ein Zertifikat diese Prüfungen und ist das Zertifikat noch gültig, dann ist die Authentisierung erfolgreich, sofern man der Stammzertifizierungsstelle (Root CA) traut, die das Zertifikat selbst bzw. in dessen Namen eine Intermediate CA das Zertifikat stellvertretend ausgestellt hat. Die Browser haben hierzu eine (recht große) Liste von vertrauenswürdigen Root CAs. Ist eine CA nicht auf dieser Liste, wird der Nutzer vom Browser entsprechend informiert und ihm die Möglichkeit gegeben dem Zertifikat trotzdem zu trauen.

Es ist klar, dass Root CAs und Intermediate CAs ihre Infrastrukturen besonders schützen müssen, denn ein Einbruch in eine CA, der zu einem Zertifikatsdiebstahl (im Sinne von missbräuchlich ausgestellten Zertifikaten) führt, kann einen erheblichen Schaden verursachen und für die betroffenen Nutzer die Authentisierung wertlos machen. Solche Vorfälle sind in der Vergangenheit leider schon vorgekommen. Mit einem gestohlenen Zertifikat könnte sich ein Angreifer beispielsweise als ein Google-Server ausgeben und so als Man in the Middle (MitM) trotz SSL-Verschlüsselung z.B. den Gmail-Verkehr eines Nutzers mitlesen.

Noch schlimmer ist es, wenn eine CA selbst missbräuchlich Zertifikate ausstellt, wie beim Zertifikatsdiebstahl zerbricht die Vertrauenskette. Wir haben leider eine recht unüberschaubare Vielzahl von Intermediate CAs und einen entsprechenden Missbrauch hat es auch schon gegeben. Das populärste Beispiel ist Google. Dieses Jahr ist aufgeflogen, dass eine Intermediate CA der Root CA des CNNIC (China Internet Network Information Center) für den Zweck der Überwachung durch die chinesische Regierung gefälschte Google-Zertifikate ausgegeben hat [1].

Wir benötigen daher dringend einen Mechanismus, der die grenzenlose Macht von CAs einschränkt und mit dem wir prüfen können, ob eine CA überhaupt berechtigt ist, ein Zertifikat auf einen Namen auszustellen. Ein solches Instrument ist mit Certificate Pinning gemäß RFC 7469 inzwischen verfügbar. Dabei wird meist über den öffentlichen Schlüssel einer CA ein Hash gebildet und dem Browser dieser Hash mitgeteilt. Der Browser kann jetzt prüfen, ob ein Server-Zertifikat auch von einer erlaubten CA erstellt wurde. Chrome und Firefox unterstützen Certificate Pinning, von Microsoft gibt es lediglich die Aussage, dass für den Internet Explorer Certificate Pinning in Betracht gezogen wird [2]. Certificate Pinning wird neben Google, Facebook und Twitter von immer mehr Diensten genutzt, um SSL gegen MitM-Angriffe zu schützen. Es spricht insbesondere auch nichts dagegen, die eigenen Web-Anwendungen und Web-Services einer Institution auf diese Weise abzusichern. Certificate Pinning bietet zwar keinen perfekten Schutz, ist jedoch eine wesentliche Verbesserung der aktuellen Lage.

Es wird außerdem noch an weiteren Mechanismen gearbeitet, um die Vertrauenskrise für Zertifikate noch stärker zu entschärfen. Google forciert z.B. mit Certificate Transparency [3] kryptographisch abgesicherte Logbücher (Certificate Logs), in denen ausgestellte Zertifikate manipulationssicher geführt werden. Certificate Logs sollen öffentlich einsehbar sein und ein jeder (speziell CAs) soll Zertifikate melden dürfen. Certificate Logs können dann insbesondere auch missbräuchlich ausgestellte Zertifikate enthalten, die damit sofort auffallen, sobald eine berechtigte CA Certificate Logs auswertet. Certificate Transparency ist zwar noch in einem experimentellen Status, es hat jedoch nicht lange gedauert, bis die ersten unberechtigt ausgestellten Zertifikate über Certificate Transparency gefunden wurden [4]. Wenn zudem eine Meldepflicht für CAs für Zertifikate bestünde (was auch ein Element von Certificate Transparency ist), könnte man für ein Zertifikat alleine dadurch, dass es in keinem Certificate Log auftaucht, bereits vermuten, dass es sich um ein missbräuchlich ausgestelltes Zertifikat handelt und es bei einer Authentisierung ablehnen. Certificate Transparency hat das Potential einen entscheidenden Beitrag zur Absicherung von Zertifikaten zu leisten, sofern es eine breite Unterstützung findet und von den gängigen Browsern unterstützt wird.

[1] Siehe **https://googleonlinesecurity.blogspot.de/2015/03/maintaining-digital-certificate-security.html**

[2] Siehe **https://dev.windows.com/en-us/microsoft-edge/platform/status/publickeypinningextensionforhttp**

[3] Siehe **https://www.certificate-transparency.org/**

[4] Siehe **https://googleonlinesecurity.blogspot.de/2015/10/sustaining-digital-certificate-security.html**

Aktuelles Seminar

Die neue EU-Datenschutz-grundverordnung
30.11.15 in Bonn

Die ComConsult Akademie veranstaltet am 30.11.15 ihr Seminar "Die neue EU-Datenschutzgrundverordnung" in Bonn.

2015 wird ein neues einheitliches Datenschutzrecht in der Europäischen Union vom Europäischen Rat und vom Europäischen Parlament beschlossen. Die Verordnung ist noch nicht endgültig verabschiedet, aber die wichtigsten Regelungen sind bereits jetzt weitgehend klar. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Informieren Sie sich über die geplanten Regelungen, damit Sie bei Inkrafttreten der Richtlinie wissen, was auf Ihr Unternehmen zukommt.

Zum Inhalt
- Entwicklung des Datenschutzes
- Entstehung der Verordnung
- Datenschutz ab 2015
- Direkt in allen Mitgliedsstaaten gültige Verordnung statt nur indirekt gültiger Datenschutz-Richtlinie 95/46/EG
- Einheitliche Datenschutzvorschriften in der EU
- Erweiterung von EU-Vorschriften auf Auftraggeber in Drittstaaten
- Konzentration der Aufsicht für Organisationen auf die nationale Datenschutzbehörde des Mitgliedsstaates des Hauptsitzes
- Recht auf Vergessen werden
- Recht auf Datenübertragbarkeit
- Notifizierung von Datenschutzverletzungen
- Definition von Binding Corporate Rules
- Datenschutzrechtliche Zustimmung nur noch explizit möglich
- Datenschutz bei Kindern
- Verarbeitung von sensiblen Daten wird untersagt (ausgenommen explizit erwähnte Ausnahmen)
- Dokumentationspflicht in den Unternehmen (Artikel 28)
- Datenschutzkonzept nach Artikel 22
- Sicherheitskonzept nach Artikel 30
- Ggf. Pflicht des Auftraggebers zur Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 33 statt Vorabkontrolle
- Einrichtung verpflichtender Datenschutzbeauftragter (neue Grenzen)
- Datenschutz durch Technik
- Pflicht zur Überprüfung der verwendeten technischen Mittel zum Schutz der Daten
- Prüfung des gesamten Lebenszyklus der Daten von der Entstehung bis zur Löschung
- Meldung von Sicherheitsvorfällen
- Datenschutzaudit
- Aufgaben Datenschutzbeauftragter

Durch die Veranstaltung führt Sie Rechtsanwalt Ulrich Emmert.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Die neue
EU-Datenschutzgrundverordnung

Ich buche das Seminar
Die neue
EU-Datenschutzgrundverordnung

☐ 30.11.15 in Bonn
zum Preis von € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Zweitthema

Kühltechniken im Rechenzentrum, Alternativen zur klassischen Raumkühlung

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH vermittelt er sein Fachwissen aus umfangreichen Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken in Form von Publikationen und Seminaren.

Methoden der Server-Kühlung

Grob unterteilt erfolgt die Kühlung von Servern in den meisten Rechenzentren mit Hilfe der folgenden Techniken:

Bei der Methode 1 wird der gesamte Raum über einen Doppelboden mit kalter Luft versorgt und auf dem Doppelboden stehen die zu kühlenden Server-Racks relativ unsortiert bzw. verteilt. Die kalte Luft strömt über mehr oder weniger gut verteilte Lochplatten in den Raum oberhalb des Doppelbodens. Diese Methodik findet man eher in kleineren Server-Räumen, wie z.B. bei einer Stadtverwaltung einer kleineren Stadt.

Eine erste und noch einfache Optimierung besteht bei der 2. Methode darin, die zu kühlenden Schränke sinnvoll zu platzieren. Die Schränke werden in Gruppen so aufgestellt, dass die aus dem Schrank rausgeblasene warme Luft nicht durch benachbarte Schränke wieder angesaugt werden kann. Man bildet einen Kaltgang und/oder einen Warmgang. Dieser Gang entsteht zunächst nur durch die geschickte Platzierung der Schränke. Ein großes Problem besteht darin, dass man durch einfaches Platzieren der Schränke nur schwer verhindern kann, dass warme Luft doch auf unterschiedlichen Wegen in den Bereich der kalten Luft geblasen wird und damit natürlich die Effektivität sinkt. Das führt zu Methode 3.

Methode 3 unterscheidet sich zu Methode 2 darin, dass einer der beiden Gänge – der Warm- oder Kaltgang – mit baulichen Maßnahmen gekapselt wird, das nennt man Einhausung. Man verhindert „Luftkurzschlüsse“ und steigert die Effektivität. Diese Methode 3 stellt heute DIE Standardmethode dar zur Kühlung von Server-Schränken in den meisten Server-Räumen. Doch wie die Tabelle unten zeigt, stößt auch diese Methode bei Server-Schränken mit Hochleistungs-Servern irgendwann an ihre Grenzen.

Es ist nachvollziehbar, dass eine Kühlung umso besser funktioniert, je näher das kühlende Element an die zu kühlende Einheit gebracht wird. Darauf zielt die Methode 4 bzw. 5 hin. Bei Methode 4 spielt der Doppelboden als kaltluftzuführendes Element keine Rolle mehr, stattdessen wird kaltes Wasser (oder auch ein anderes Kühlmedium) zu der Server-Rack-Reihe (am besten natürlich mit Einhausung) über eine entsprechende Verrohrung geführt und dort in einen Wärmetauscher. Luft wird über diesen Wärmetauscher geblasen, kühlt sich ab und wird durch die Server geführt.

Methode 5 unterscheidet sich zu Methode 4 darin, dass pro Rack (oder auch pro 2 Racks) ein Kühlgerät bereitgestellt wird und die warme Luft nicht in den Raum geblasen wird, sondern im Schrank oder der Schrankreihe bleibt und durch das Kühlgerät heruntergekühlt wird.

Der wesentliche Unterschied zwischen den Methoden liegt also in der Luftverteilung, das Liefern der Gesamtkühlkapazität und der damit verbundene Energieaufwand bleibt gleich. Die Bitkom gibt für diese Methoden unterschiedliche maxi-

male Kühlleistungen an (siehe Tabelle 1). Deutlich wird, dass die zu wählende Methode im Wesentlichen von der zu erwartenden benötigten Kühlleistung abhängt, sie ist im Prinzip gleich der elektrischen Leistung der im Rack vorgesehenen Komponenten. Ab einer bestimmten geforderten Leistung hat man keine Wahl mehr und wird wassergekühlte Lösungen einsetzen müssen. Nicht alle Klimafachplaner setzen diesen Schwellwert wie in der Tabelle dargestellt erst bei 10 kW/Rack an, häufig wird bereits bei niedrigeren Werten auf Methode 4 oder 5 zugegriffen.

Beschreibung der Lösung	Maximal mögliche Kühllast
Klimatisierung über Doppelboden ohne Bildung von Kalt/Warm-Gang	max. 1 kw/qm bzw. 4 kW/Rack
Klimatisierung über Doppelboden mit Bildung von Kalt/Warm-Gang	max. 2 kw/qm bzw. 8 kW/Rack
Klimatisierung über Doppelboden und Einhausung der Kaltgänge	12-20 kW/Rack
Eigene Klimageräte werden in die Schrankreihen (1 Gerät versorgt mehrere Schränke) gestellt und Warmgang wir eingehaust	ca. 10-25 kW/Rack
Klimatisierung über wassergekühltem Rack (geschlossenes System)	ca. 20-45 kW/Rack

Tabelle 1: Leistungsfähigkeit der verschiedenen Kühlmethoden

Grundprinzip: Kalte Luft in den Server und warme Luft aus dem Server

Bei allen Methoden besteht die Grundforderung, eine kalte Lufttemperatur am Luftansaugbereich der Server- oder Switch-Einheiten bereitzustellen. In sehr vielen Planungskonzepten beruft man sich bei der Festlegung des Temperaturbereiches für die zugeführte kalte Luft auf die ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) einem Berufsverband aller in Heizungs-, Kühlungs-, Lüftungs- und Klimaanlagenbau Tätigen in den USA. Diese empfiehlt einen Bereich von 18 bis 27 Grad Celsius. Die Effizienz der Kühlungstechnik nimmt zu, wenn die Temperaturdifferenz zwischen der eintretenden und der austretenden Luft (oder anderen Kühlmitteln) am Kälte erzeugenden Gerät möglichst groß ist, deshalb ist man zunächst einmal bestrebt, möglichst kalte Luft am Klimagerät zu erzeugen und diese mit so wenig Aufwand wie möglich zum zu kühlenden Gerät zu bringen. Dies erfolgt immer mit Hilfe von Lüftereinheiten, welche am effektivsten eingesetzt werden, wenn sie nicht unter Vollast laufen. Das hat zur Folge, dass bei langen „Luftwegen“ entweder die eingeführte Lufttemperatur sehr niedrig sein muss (z.B. 13 Grad Celsius) oder aber die Luftgeschwindigkeit bzw. der Druck sehr hoch. Die zugeführte Luft darf nicht zu kalt sein, sonst wird man mit Kondensationsproblemen rechnen müssen.

Kühlung über den Doppelboden

Da die meisten Serverräume über einen Doppelboden verfügen und auch bei neuen Rechenzentren der Doppelboden in der Regel mitgeplant wird, stellen die Lösungen mit einer Kaltluftzuführung über den Doppelboden die gängigste Lösung dar; ältere Serverräume häufig noch mit Methode 1 und 2, neu geplante Rechenzentren eher mit Methode 3. Das bedeutet, dass ein Großteil der Serverracks in Gruppen angeordnet und eingehaust wird. Die Planung bzw. Dimensionierung einer solchen Kühlung muss sorgfältig durchgeführt werden, u.a. muss festgelegt werden,

- wie hoch der Doppelboden mindestens sein muss, um die Kaltluft zu allen Doppelbodenplatten mit Luftaustritt bringen zu können,
- wie stark die Klimaanlage insbesondere die Lüftereinheit(en) sein muss, um die Luft dorthin zu bringen,
- mit welcher Temperatur die kalte Luft in den Boden eingeblasen wird.

Die geplante raumspezifische Klimainfrastruktur schränkt gegebenenfalls auch die Planungsmöglichkeiten des eigentlichen Rechenzentrumsnutzers oder IT-Fachplaners ein. Beispielsweise die Grundrissplanung bzw. Positionierung der Serverracks kann nicht losgelöst von den vorausgegangenen Planungen der Raumklimatisierung stattfinden, dazu zwei Beispiele.

Das Vorhandensein einer funktionierenden Kühlung über einen Doppelboden bedeutet nicht automatisch, dass die geplante Klimatechnik an jedem Punkt eine ausreichende Kaltluft zur Verfügung stellt. Der Abstand zwischen dem Serverrack und dem Klimagerät, welches häufig auch als CRAC bezeichnet wird (= Computer Room Air Conditioner), kann nicht beliebig groß sein. Ein Irrtum ist die Annahme, dass man mit einer entsprechenden Steigerung der Luftmenge (das erfolgt z.B. über eine Erhöhung der Lüfterdrehzahl am CRAC) jede noch so weite Ecke im Raum erreichen kann. Wird die Luftgeschwindigkeit im Doppelboden zu stark erhöht, so kann dies im Extremfall dazu führen, dass die wärmere Luft oberhalb der Doppelbodenplatten mit Luftaustrittsöffnungen nach unten in den Doppelbodenhohlraum gezogen wird und damit „warme“ Luft in den Boden gelangt. Fachleute sprechen von der maximalen „Wurfweite“ einer CRAC, man empfiehlt als Anhaltspunkt diese auf 12 bis 15 m zu begrenzen.

Sehr häufig steht die Planung der Kabelführung im Doppelboden unmittelbar in Zusammenhang mit der Planung der Schrank- bzw. Reihenpositionen und es muss durch den IT-Planer berücksichtigt werden, dass etwaige Trassen nicht zu einer starken Beeinträchtigung des Luftstromes führen dürfen. Gerade in Räumen, bei denen der Doppelboden aus unterschiedlichen Richtungen mit Luft versorgt wird, erschwert dies die Lage bzw. Ausrichtung der Trassen. Die EN 50174 gibt hierzu beispielsweise eine Empfehlung,

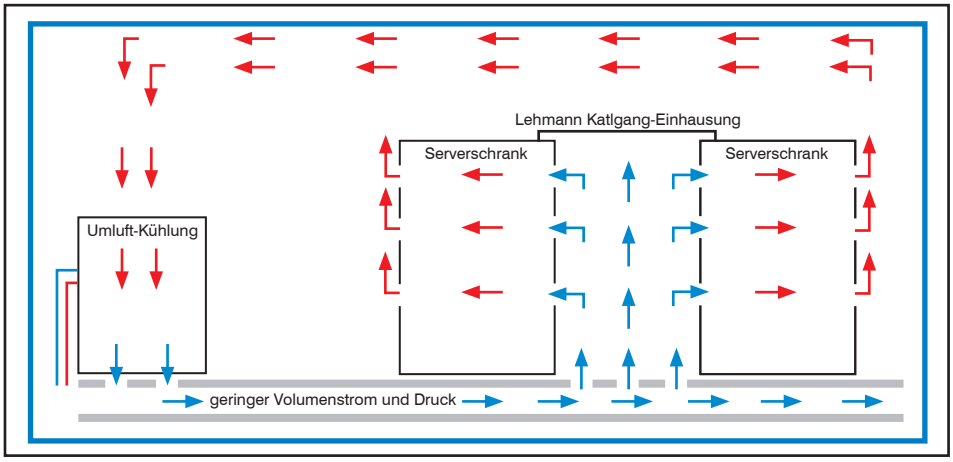

Abbildung 1: Prinzip der Kaltgangeinhausung

Trassierungen der Datenkabel in den Warmgang zu verlegen und Trassierungen der Stromkabel in den Kaltgang. (siehe Abbildung 1)

Kaltgang- vs. Warmgangeinhausung

In den meisten Serverräumen erfolgt eine Einhausung des Kaltgangs, also des Bereiches, in dem die kalte Luft aus den perforierten Bodenplatten des Doppelbodens nach oben gedrückt wird. Dazu wird dieser Bereich zwischen den gegenüberliegenden Schränken mit Hilfe von Kunststoffplatten im Wand- und Deckenbereich sowie einer oder zweier Türen eingekapselt. Einige Hersteller bieten Einhausungen mit Hilfe von Folientechniken an, was ein Nachrüsten von Einhausungen in vorhandenen kleineren Serverräumen deutlich vereinfachen kann und kostengünstiger macht. (siehe Abbildung 2)

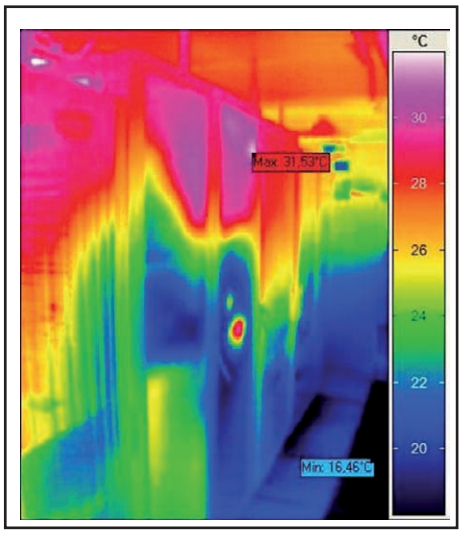

Abbildung 2: Wärmebildmessung Serverrack
Quelle: Emerson

Der Gang sollte etwas höher sein als die Höhe der Schränke, in der Regel empfiehlt man ca. 100 bis 200 mm höher. Dies hat den Vorteil, dass zum einen der Arbeitsbereich in den obersten Höheneinheiten etwas besser zugänglich ist, als wenn der Deckel der Schränke unmittelbar bündig zum Dach des Kaltganges wäre. Als weiteren Vorteil nennen die Schrankhersteller die – mit Wärmekameras gut darstellbare – Reduzierung der Lufttemperatur in den oberen Höheneinheiten, denn warme Luft steht immer im Dachbereich der Einhausung. Diese grundsätzlich immer höhere Temperatur im Dachbereich führt nebenbei auch zur Empfehlung, nach Möglichkeit in den Serverracks oben wärmeunkritische Komponenten wie z.B. passive Rangierfelder zu montieren. (siehe Abbildung 3)

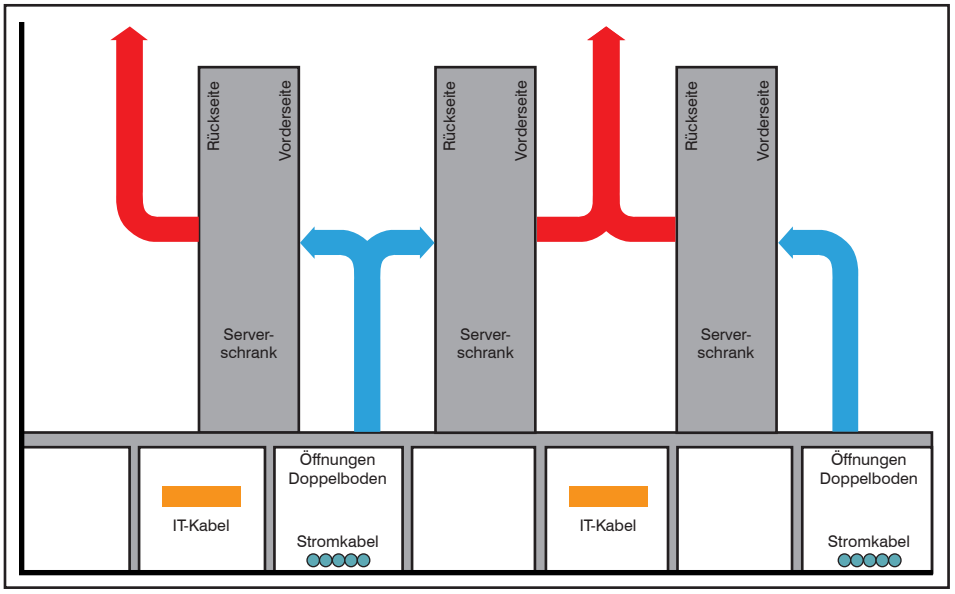

Abbildung 3: Kabelführung im Doppelboden nach EN 50174

Unterschiedlich bewertet wird von den verschiedenen Anbietern die Befestigung der Dachplatten, einige bevorzugen eine feste Verschraubung mit der Begründung, dass bei Ausfall der Raumklimaanlage diese zunächst mit 100% der Lüfterleistung hochfährt und dass das ggf. zu einem Hochdrücken bzw. Verrutschen der Platten führen kann. Andere Anbieter lassen diese Platten lose oben aufliegen, begründet durch die Sicherstellung eines Druckausgleiches bei Einströmen eines Löschgases in den Kaltgang und damit Vermeidung von Plattenbeschädigungen. Der VdS lässt den Verzicht auf Druckentlastungsklappen bei Bildung von Einhausungen zu, hier wird davon ausgegangen, dass die Server-Racks eine ausreichende Öffnungsfläche bereitstellen, demzufolge könnten die Deckenplatten also befestigt werden. Aus eigenen Erfahrungen des Autors heraus haben lose aufliegende Platten zumindest den Vorteil, dass bei Querverkabelungen/Rangierungen von einer Schrankreihe zur gegenüberliegenden die Zugänglichkeit des Kabelweges deutlich besser ist, als wenn die Platten erst losgeschraubt werden müssen.

Bei einem Ausfall der Stromversorgung und/oder Kühlung weist die Kaltgang-Einhausung den Nachteil auf, dass die zur Verfügung „stehende“ kühle Luft (Kaltluftvolumen) in dem eingehausten Bereich deutlich kleiner ist als bei Verzicht auf diese Einhausung und damit die Gefahr einer schnelleren Überhitzung besteht (eine Überhitzung im Sekundenbereich muss ggf. einkalkuliert werden). Auch die Einhausung von „Nicht-19“-Komponenten“ ist bei einem Kaltgangprinzip schwierig zu gestalten, hier bietet es sich weiterhin an, das gesamte Volumen des Raumes zur Kühlung von z.B. freistehenden Komponenten sicherzustellen.

An dieser Stelle lohnt sich die Betrachtung eines alternativen Einhausungs-Prinzips, die Warmgangeinhausung. Bei dieser eher selten zum Einsatz kommenden Einhausung gilt das gleiche Prinzip, jedoch wird der Bereich, in dem die warme Luft austritt, abgeschottet zum restlichen größeren (kalten) Raumvolumen und die warme Luft gezielt nach oben abgesaugt. Falls die dazu notwendigen Baumaßnahmen nicht möglich sind, können alternativ eigenständige Kühleinheiten in der Reihe vorgesehen werden, welche die warme Luft aus dem Warmgang ansaugen und nach vorne als kalte Luft wieder rausblasen (Prinzip der Direktkühlung, siehe unten).

Folgende Vorteile sind zu nennen:

- Die gezielte Rückführung von Luft mit sehr hoher Temperatur verbessert den Wirkungsgrad der Klimageräte.
- Bei Ausfall der Stromversorgung der Lüfter bleibt „lediglich“ die Luft im Warmgang stehen, ein relativ großes Reservoir an kalter Luft ist im Gesamtraum vorhanden und reduziert die Geschwindigkeit, mit der sich die Server erhitzen können.
- „Free-Standing-Systems“ lassen sich einfacher kühlen, da der Raum das Hauptreservoir an kalter Luft bereitstellt.
- Mit einer Warmgangeinhausung wird das Problem eines „Wärmenestes“ wie im Kaltgang vermieden, denn es können sich keine Wärmenester im Dachbereich bilden.

- Allgemein wird das Arbeiten in Warmgängen bzw. der Übergang von einem „leicht“ gekühlten Raum in einen Warmgang als angenehmer empfunden, als ein Betreten eines sehr kalten Kaltganges.

- Im Falle einer Raumkühlung benötigt die Kaltgangeinhausung einen Doppelboden zur Luftzuführung. Ohne diesen kann die gekühlte Luft nicht mehr von außen in den abgeschlossenen Kaltgang zwischen den Server-Racks gelangen. Darauf kann beim Warmgang verzichtet werden.

Viele Hersteller von Serverracks bzw. den damit verbundenen Klimatechniken analysieren diese Unterschiede, zeigen die Vor-/Nachteile ein und resümieren, dass Systeme für die Warmgang-Einhausung eine effizientere Lösung als Kaltgang-Einhausungen sind. Gerade auch der mögliche Wegfall des Doppelbodens vereinfacht im Einzelfall die Einrichtung von Serverräumen, insbesondere in bestehenden Räumen mit niedriger Deckenhöhe. Die Einhausung des Warmganges ietet sich auch dann in Rechenzentren an, wenn Racks mit hohen Leistungen in einem Bereich des Serverraumes konzentriert werden können, dann muss die bestehende Raumklimatisierung die Wärmeleistung dieser Hotspots nicht bewältigen. Die grundsätzliche Einbeziehung dieser Alternative ist aus Sicht des Autors zumindest überlegenswert.

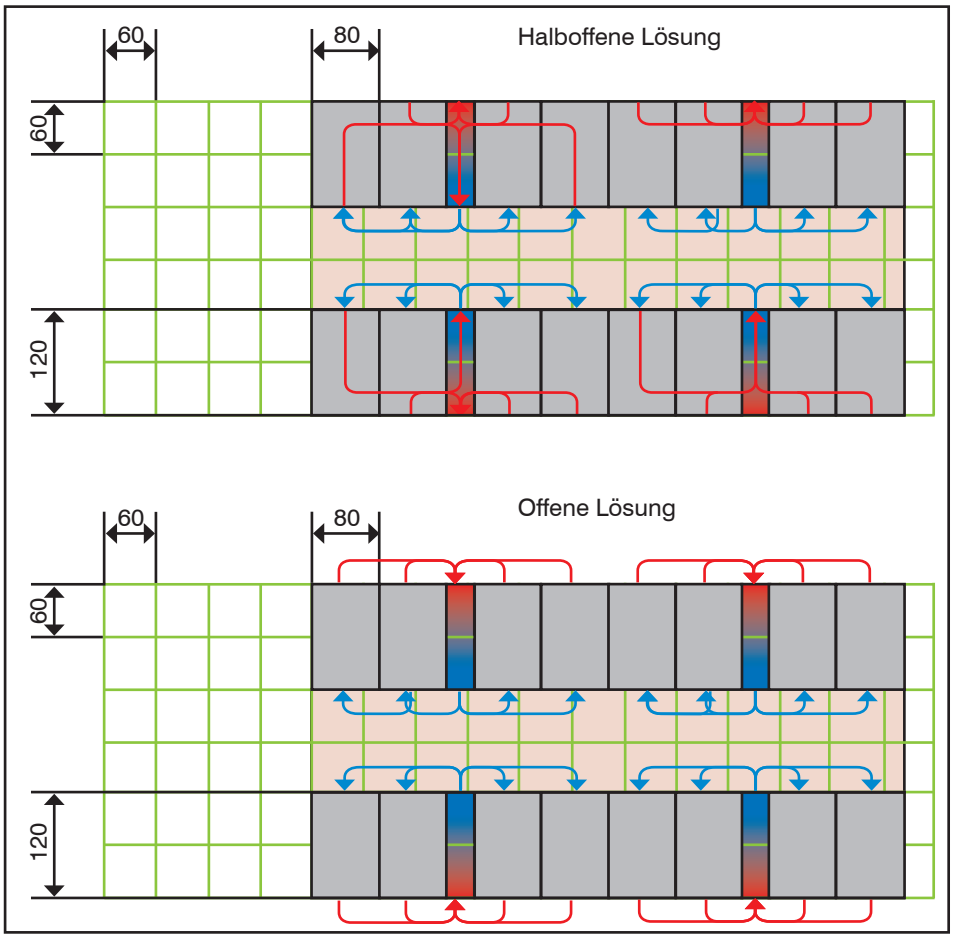

Abbildung 4: Unterschied offene und halboffene Lösung

Der VdS fordert zur Sicherstellung von ausreichenden Flutungszeiten (VdS 2380/2381/2093) Löschdüsen und Branddetektionselemente sowohl in Warm- als auch in Kaltgängen.

Direktkühlung

Reicht die Kühlleistung eines Doppelbodens – ob mit oder ohne Einhausungen - nicht mehr aus, so muss eine direkte Kühlung der Schränke durch Platzierung der Kühleinheiten (CRAC) in die Nähe des Schrankes erfolgen. Man unterscheidet zwischen zwei Kühlungskonzepten, der „Einzelschrank-“ und der „Reihen“-Kühlung. Bei der Einzelschrankkühlung steht für jeden Schrank ein eigenes Kühlgerät zur Verfügung und bei der Reihenkühlung teilen sich mehrere Schränke in der Reihe ein Kühlgerät. Beginnen wir mit der Reihenkühlung.

Es gibt wiederum zwei Lösungsansätze bei der Reihenkühlung, die offene und halboffene Lösung. Bei der offenen Lösung sorgen in der Reihe montierte Klimageräte für ein Ansaugen der warmen, die Serverracks hinten umgebenden Luft, diese wird durch die Kühleinheit bzw. Kühlregister abgekühlt und dann nach vorne in den eingehausten oder auch nicht eingehausten Kaltgang geblasen. Die beim Durchströmen der Server erzeugte warme Luft wird immer in den gesamten Serverraum geblasen. Bei der halboffenen Lösung wird die erwärmte Luft nicht in den offenen Raum geblasen, sondern sie bleibt in einem geschlossenen Bereich (z.B. einer Warmgangeinhausung oder in der Schrankreihe selber), damit beeinträchtigt die halboffene Lösung nicht die Komponenten außerhalb der Schrankreihe. (siehe Abbildung 4)

Eine Reihenkühlung setzt zur Effizienzsteigerung voraus, dass die erzeugte kalte Luft nicht in den freien Raum außerhalb der Reihe gelangen kann. Dies wird entweder dadurch erreicht, dass die Kühleinheit die kalte Luft in einen Kaltgang bläst (also vor die Serverschränke) und dort, wie beim klassischen Doppelbodenprinzip von vorne durch die Server nach hinten geblasen wird. Dies erfordert dann eine Kaltgangeinhausung und gelochte Fronttüren. Alternativ bieten die Hersteller eine Technik an, bei der die kalte Luft innerhalb der in Reihe positionierten Serverschränke nach vorne und seitlich geblasen wird, also die Schränke nicht verlässt. Damit kann auf eine Kaltgangeinhausung verzichtet werden, allerdings dürfen innerhalb der Schrankreihe keine Trennwände zwischen den Schränken sein, sonst kann sich die Kaltluft nicht ausbreiten (man wäre wieder bei einer Einzelschrankkühlung). Die Fronttüren müssen natürlich geschlossen sein (z.B. Glastüren). Die meisten Hersteller bieten Kühlelemente an, die eine Breite von 300 mm haben. (siehe Abbildungen 5 und 6)

Der Wechsel von einer Reihenkühlung zu einer Einzelschrankkühlung ist z.B. bei dem Hersteller Rittal möglich, ohne die Kühleinheit austauschen zu müssen. Durch Herausziehen der 300mm breiten Kühleinheit nach vorne kann die vorne seitlich ausgeblasene kalte Luft in einen Kaltgang geführt werden und wirkt dort wie ein Kaltluftvorhang (was natürlich zu einem in der Reihe vorstehenden Gerät und damit zu einer Beeinträchtigung des Frontbereiches an den Servern führt). Umgekehrt würde man bei Reinziehen der Kühleinheit in die Schrankreihe die kalte Luft dann gezielt nur in die Schränke blasen (analog zur Einzelschrankkühlung). Bei Umstellen des Luftaustritts kann die-

Abbildung 5: Beispiel für Seitenkühlgerät (Hersteller Schäfer)

Abbildung 6: Beispiel für eingebautes Seitenkühlgerät (Hersteller Rittal)

ses System auch benutzt werden, ohne in den Kaltgang hinausgezogen zu werden.

Sollte der Platz ein weiteres Element in die Reihe zu integrieren nicht zur Verfügung stehen, so bieten die Hersteller Kühlsysteme an, die entweder auf dem Dach, im Bodenbereich oder auch als Rückwand ausgelegt sind. Dazu zwei Beispiele:

- Rückwandwärmetauscher kühlen die warme Luft der Server auf 23 Grad runter und führen sie der Raumluft als kalte Luft wieder zu. Diese Tauscher arbeiten je nach Hersteller mit oder ohne eigenen Lüfter (Idee bei lüfterlosen Systemen: Lüfter der Server reichen zur Erzeugung des Luftstromes aus).

- Unter dem Rack angebrachte Wärmetauscher (Wärmetauscher befinden sich aber auf dem Doppelboden und benötigen damit weitere 12 HE im Raum) kühlen die aus dem Raum angesaugte Luft gezielt ab und blasen diese nach oben in das Serverrack. Bei dem Hersteller Schäfer sind damit z.B. Kühlleistungen von bis zu 21 kW möglich.

Solche Systeme bieten sich sowohl zur Einzelschrankkühlung als auch zu einem nachträglichen Einbau an. (siehe Abbildung 7)

Die eigentliche Kühlleistung bezieht sich bei allen Varianten auf die Kühlleistung der eingebauten Kühleinheit. Sieht man für jeden Serverrack eine eigene Kühleinheit vor, so steht natürlich dessen Kühlleistung explizit diesem Rack zur Verfügung. Platziert man die Kühleinheit zwischen zwei Racks und versorgt beide Racks mit dieser Einheit, so halbiert sich die Leistung. Gerade bei der Reihenkühlung werden Kosten dadurch gespart, dass sich mehrere Schränke eine Kühleinheit teilen.

Eine wichtige Frage stellt sich häufig, wie der Ausfall einer Kühleinheit „abgefangen“ wird. In diesem Falle besteht die Gefahr, dass sich die Temperatur in den Serverracks sehr schnell erhöht, denn das zur Restkühlung verfügbare Luftvolumen ist deutlich kleiner als bei einer klassischen Raumkühlung. Um dieses Risiko bewerten zu können werden nachfolgend die wichtigsten Teilelemente der Kühleinheit erläutert.

Zentrale Elemente der Direktkühlung

Die Kühlung jeder Einheit hängt davon ob, ob das von einem zentralen Punkt aus zugeführte Kühlmittel (in der Regel Wasser) garantiert und hochverfügbar bereit-

Abbildung 7: Beispiel für Kühlgerät in Rücktür (Hersteller Emerson)

gestellt werden kann. Dies sicherzustellen ist Aufgabe der Fachplanung für den Serverraum bzw. gehört zur Infrastruktur des Raumes. Möglichkeiten zur Verbesserung der Verfügbarkeit sind z.B. die Bereitstellung von zwei Kühlmittelkreisläufen, die dann sinnvollerweise auch zwei Kühlregister (= Einheiten, die warme Luft in kalte Luft umwandeln) in der Kühleinheit versorgen. Die Bereitstellung von zwei redundanten Kühlregistern ist aber nicht bei jedem Hersteller gegeben.

Ein weiteres zentrales Element, welches zur Rauminfrastruktur gehört ist der Strom, der die Lüfter betreibt. Hier gelten im Prinzip die auch sonst üblichen Betrachtungen bei einer redundanten RZ-Stromversorgung, d.h. also z.B. Anschluss der Lüfter an USV und Netzersatzanlage.

Wie bereits angesprochen arbeiten Lüfter besonders effektiv und stromsparend unter Teillast, das bedeutet, dass bei „n“ benötigten Lüftern (Minimalanzahl) es effektiver ist mehr als „n“ Lüfter einzubauen, damit die „n“ Lüfter nicht mit maximaler Drehzahl laufen, unabhängig vom Redundanz-Gedanken.

Damit ist das Risiko, dass eine Kühleinheit komplett ausfällt, als sehr gering einzustufen. Möchte man dieses dennoch komplett ausschließen, gibt es folgende Möglichkeiten:

Fall 1: Die Leistung der Kühleinheit wird vollständig zur Kühlung eines einzigen Serverracks benötigt. In diesem Fall kann die Ausfallsicherheit nur erreicht werden, indem eine zweite Kühleinheit ergänzt wird.

Fall 2: Die Leistung der Kühleinheit wird zur Kühlung von mehr als einem Serverrack benötigt (ähnlich der Reihenkühlung), setzt aber ein Wegfallen der Trennwände zwischen den Racks voraus. In diesem Fall kann durch Einplanung von mehreren Kühleinheiten dafür gesorgt werden, dass bei Ausfall einer Einheit die „verbleibende(n) Einheit(en)“ die Kühlung vollumfänglich sicherstellen. Dies hat zusätzlich den Vorteil, dass bei einer betriebsbedingten Öffnung der Fronttüre z.B. im Rahmen von Wartungsarbeiten, zusätzliche kalte Luft von den benachbarten Schränken einströmen kann und die Erhitzung verlangsamt wird.

Einige Hersteller bieten eine automatische Türöffnung an, falls die Kühleinheit ausfällt, in diesem Falle würde – zumindest theoretisch – die kalte Raumluft für eine zeitlich begrenzte Notkühlung der Server genutzt werden können.

Kühleinheiten können entweder mit Wasser betrieben werden oder mit einem speziellen Kältemittel. Es gibt eine weit verbreitete grundsätzliche Abneigung gegen Wasser als Kühlmittel, alle Hersteller verweisen aber darauf, dass durch die „gehäusetechnische“ Trennung der Kühleinheit und des Serverracks auch bei massiven Undichtigkeiten kein Wasser in die Server eindringen kann, derartige Fälle hätte es noch nie gegeben. Auch interne Detektorsensoren in den Kühleinheiten erkennen solche Lecks und melden diese an ein zentrales Managementsystem.

Branderkennung und -löschung

Neben der eigentlichen „Kühlthematik“ sind die begleitenden Techniken zu betrachten, insbesondere die Branderkennung und Löschung. Ein Prinzip, bei dem kalte oder warme Luft mit dem Serverraum ausgetauscht wird (offene oder halboffene Lösungen) lässt die Möglichkeit der Branddetektion im umgebenden Raum zu, was wiederum keine Anpassung dieser Technik in einem vorhandenen Raum zwingend notwendig macht. Sieht man dagegen ein geschlossenes System vor, muss die Detektion zwingend im Schrank erfolgen, Rauchansaugsysteme müssen vorgesehen bzw. nachgerüstet werden. Ähnliches gilt für die Löschung: Im Falle eines Brandes im Schrank muss ein Löschmittel in den Schrank einströmen, hier stehen folgende Varianten zur Auswahl:

Variante 1, Mitnutzen der Raumlöschung: Ein Brand innerhalb oder außerhalb des Schrankes wird detektiert und nach dem Erreichen der vordefinierten Eskalationsstufe strömt in den kompletten Serverraum Löschgas ein, die Türen der geschlossenen Schränke müssen sich automatisch öffnen und das Gas kann einströmen. Diese Technik lässt sich sehr einfach einrichten, es muss lediglich ein automatisches Öffnen der Schranktüren vorgesehen werden. Aber Achtung: So ausgerüstete Schränke sind deutlich teurer als „normale“ Schränke ohne automatische Türöffnung. Bei jedem Brand (auch einem kleineren lokalen Schwelbrand) wird das gesamte Löschgas verwendet, was zu unnötig hohen Kosten bei Fehl-

alarmen oder räumlich stark begrenzten und kleineren Bränden führt.

Variante 2, Einrichtung einer schrankspezifischen Löschanlage: Im Schrank wird eine eigene Löschanlage mit einer kleineren Löschgasmenge vorgesehen und diese Anlage löst dann selektiv aus, wenn in diesem Schrank (oder der Schrankreihe) ein Brand entdeckt wird. Damit werden Folgekosten durch notwendige wie auch fehlerhafte Löschungen deutlich reduziert, denn der umgebende Raum (eventuell mit einer eigenen Löschanlage) ist davon nicht betroffen.

Vergleich Reihen- und Einzelschrankkühlung

Wie dargestellt, hat jede der beiden Technologieansätze unterschiedliche Stärken bzw. Schwächen und eine pauschale Bevorzugung einer der beiden Techniken wäre nicht richtig.

Vergleicht man Reihen- und Einzelschrankkühlung, so sind folgende Vor-/Nachteile zu nennen:

- Bei der Einzelschrank-Kühlung kann die Kühlleistung pro Schrank deutlich höher ausgelegt werden, dafür werden aber die zusätzlichen Kosten für die Kühlgeräte ebenfalls höher sein.
- Die Kühlleistung lässt sich bei der Einzelschrank-Kühlung wesentlich präziser an den Kühlbedarf jedes einzelnen Schrankes anpassen.
- Die Schallemission ist bei der Einzelschrank-Kühlung in der Regel geringer, da es sich um ein geschlossenes System handelt.
- Brandschutz (Detektion und Löschung) hat in beiden Fällen unterschiedliche Vor- und Nachteile.
- Eine Reihenkühlung erfordert in der Regel eine Einhausung, bei einer Einzelschrankkühlung wird man darauf verzichten können.
- Die Redundanz in einer Reihenkühlung lässt sich kostengünstiger einrichten.
- Die Verrohrung ist bei einer Einzelschrank-Kühlung deutlich aufwendiger.
- Die Einzelschrank-Kühlung ist unbeeinflussbar durch Raumbedingungen und die Rack-Anordnung kann willkürlich sein. Eine Reihenkühlung setzt Gruppierungen von Schränken oder je nach Konzept auch Einhausungen voraus.
- Werden bei einer Einzelschrank-Kühlung die im Rack angebotenen Kühlleistungen nicht benötigt, so stehen sie auch keinem anderen Rack zur Verfügung.

Nimmt man die klassische Raumkühlung noch als dritte Alternative hinzu, so ist die Ausstattung eines Serverraumes mit allen drei Kühltechnologien durchaus denkbar. (siehe auch Herstellervergleich am Ende des Artikels)

Fazit

Unabhängig von der Größe des Serverraumes und auch der in diesem Serverraum betriebenen Server bzw. zu kühlenden Einheiten lohnt es sich, die verschiedenen Kühlungskonzepte zu vergleichen und für den jeweiligen Einsatzfall zu bewerten. Die Standard-Lösung der reinen Raumkühlung wird sehr häufig nicht die ausreichende Kühlleistung bringen und sie setzt Rahmenbedingungen voraus, die sich nicht bei jedem Serverraum-Neubau sicherstellen lassen. Hohe Kühlleistungen, eine Abkehr vom Doppelboden als kühlendes Element und die Verbesserung der Energieeffizienz erfordern eine Positionierung von Kühlelementen in unmittelbarer Nähe der Serverracks. Dies gelingt sowohl mit Reihenkühlungen als auch mit direkter Einzelschrankkühlung und ist bei den gängigen Schrankherstellern in unterschiedlichen Ausbaustufen zu bekommen.

Kühltechniken im Rechenzentrum, Alternativen zur klassischen Raumkühlung

Hersteller	Schäfer	Rittal	Emerson-Liebert	Emerson-Liebert	Pentair
Die Informationen in der Tabelle sind Herstellerangaben	Typ: Sidecooler; Ausführung offen, geschlossen oder als Hybrid lieferbar	Typ: LCP Inline CW	Typ CRV CR38 und CRV CR60.	CRV CR40 und CR50	Typ LHX20, SHX30, LHX40
Maße des Kühlelementes (B/T/H) in mm	Verfügbar in 300/1200/2000 oder 300/1000/2000 oder 300/1000/2200 oder 300/1200/2200	300b, 1000 oder 1200 t, 2000 oder 2200h	300x1100x2000, 300x1100x2200,300x1200x2200,300x1200x2000	600x1175x2000	Einzelschrank (Stand-Alone) mit integriertem Kühlgerät Abmessungen: 2000 H (42 HE) bzw. 2200 H (47 HE) x 800 B x 1200 T Andere Abmessungen auf Anfrage möglich Hier hat der Kunde zusätzlich noch eine 19"-Ebene direkt im Schrank integriert.
Einbaumöglichkeit in Fremdschranksysteme möglich?	Bedingt, bei Beachtung der 19" Ebene	Generell ja ohne Berücksichtigung der Gesamtoptik	Ja	Ja	Das Kühlaggregat kann als Einzelteil bestellt werden. Sicherlich ist es möglich, das Gerät in einen Fremdschrank einzubauen. Hier muss jedoch der Kunde selbst dafür Sorge tragen, dass die notwendigen Adaptionen am Fremdschrank erfolgen. Wir übernehmen für diesen Fall keinerlei Gewährleistung.
Nutzkühlleistung pro Einheit in kW (bei Anzahl von Lüfter); red. Lüfter möglich	34 kW, Sidecooler sind ohne Ventilatoren lieferbar, d.h. bis ca. 15 kW reichen die Ventilatoren in den Servern aus um die Luft über die Wärmeübertrager vom Sidecooler zu fördern (abhängig von den eingebauten Servern), Ventilatoren können jederzeit nachgerüstet werden (Modular); Lüfter immer redundant n+1 möglich. Lüfteranzahl zwischen 0 und 6 Stück beliebig wählbar.	Das muss ausgelegt werden. Mit Klimakaltwasser und 15°C sind etwa 36kW bis 40kW netto verfügbar. Je nach Anforderung werden 1 bis 6 Lüfter je Einheit eingesetzt. Die Leistung hängt nicht nur von der Anzahl der eingesetzten Lüfter ab, sondern insbesondere von der durchgesetzten Medienmenge und dem tolerierten Druckverlust. Man kann zur Reduzierung der elektrischen Leistungsaufnahme auch bei kleinen Kühlleistungen eine größere Stückzahl an Lüftern einsetzen. Ein Auslegungsprogramm ist verfügbar.	14-36KW 4 Lüfter, 20-48KW 6 Lüfter	25-40KW 2 Lüfter, 30-48KW 3 Lüfter	Abhängig vom Gerät: LHX20: max. 20 kW, Anzahl Lüfter: 6 SHX30: max. 30 kW, Anzahl Lüfter: 6 LHX40: max. 40 kW, Anzahl Lüfter: 7 --> keine Redundanz möglich
Lüfterkassetten modular?	Ja	Die Lüfter bilden mit den konstruktiven Montageblechen jeweils eine Einheit (Modul), die einzeln ausgetauscht und erweitert werden können bis zur max. mögl. Stückzahl je Gerätetyp	Einzeltauschbar	Einzeltauschbar	Der Basisschrank bietet die Möglichkeit, alle genannten Kühlaggregate aufzunehmen, abhängig von den Kundenanforderungen. D.h. sowohl ein LHX20 / LHX40 oder SHX30 Aggregat kann in den selben Basisschrank eingebaut werden.
Lüfter im lfd. Betrieb austauschbar?	Ja	Ja	Ja	Ja	Ja
Lüfter stufenlos regelbar?	Ja	Ja, wir setzen EC-Lüfter ein, die stufenlos geregelt werden. Im Störfall erhalten die Lüfter 100% Stellsignal und laufen mit voller Drehzahl.	Ja	Ja	Die Regelcharakteristik ist werkseitig vorgegeben, kann jedoch durch einen lizenzierten Servicetechniker angepasst werden. Werkseinstellung: Lüfterdrehzahl 80%. Wird die Luftaustrittstemperatur überschritten, wird auf max. Kühlbetrieb geschaltet, d.h. das Regelventil wird zu 100% geöffnet und die Drehzahl der Lüfter auf 100% Nenndrehzahl erhöht.
Red. Stromversorgung der Lüfter über unterschiedliche Stromkreise möglich?	Ja	Ja, als Option können die LCP mit redundanter Einspeisung geliefert werden.	Ja	Ja	Ja, über AC-Netzumschaltung, also Zubehör bestellbar.
Lüfter befinden sich im Warm- oder Kaltbereich?	Im kalten Bereich	Im Kaltbereich in Luftrichtung hinter dem Wärmetauscher	Kalt	Kalt	Das gesamte Register befindet sich sowohl im Kaltbereich als auch im Warmbereich. Die Lüfter selbst sind im Kaltbereich positioniert.
Nutzbar für Einzelschrank- und Reihenkühlung? Wie?	Ja, durch unterschiedliche Seiten- und Frontwände	Ja. LCP muss entsprechend bestellt werden, kann bei Bedarf aber durch Anbauen bzw. Entfall von Abdeckblechen und Austausch von Türen umgebaut werden. Reihenkühlung erfordert Gangschottung, Typenabhängig (Baureihe "Protruding") muss das LCP bei Reihenkühlung um 200 mm in den Kaltgang vorgezogen installiert werden. Hierbei Tiefenausgleich durch Adaptergehäuse. Die kleinere Baugröße wird auch bei Reihenkühlung bündig in die Schrankreihe eingebaut.	Ja. Keine Veränderung.	Ja. Keine Veränderung nötig.	Ja, nutzbar als Einzelschrank und Reihenkühlung. Bei der Reihenkühlung wird der eigene SideCooler verwendet, das Aggregat wird in einen 300 B Schrank eingebaut und dem Schrank beigestellt.
Redudante Kühlregister?	Nein	Nein	Nein	Nein	Nein
Regelung des Kaltwasserstromes erfolgt ….	Durch 2-Wege Ventil stetig, durch integrierten Kugelhahn kann das Ventil auf ein 3-Wege-Ventil umgeschaltet werden	Durch Regelkugelhahn mit Federrücklaufmotor. Im Störfall wird der Kugelhahn fremdenergielos auf 100% Durchgang geöffnet.	2- oder 3-Wegeventil	2- oder 3-Wegeventil	Die Ventilatoren und das Regelventil des Wasserkreislaufs werden von einer mikroprozessorgesteuerten Regel- und Steuereinheit angesteuert. Ein PID Regelkreis regelt den Wasserdurchfluss durch den Wärmetauscher in Abhängigkeit von der Luftaustrittstemperatur des Kühlmoduls.

ComConsult Veranstaltungskalender

TCP/IP-Netze erfolgreich betreiben, 11.11.-13.11.15 in Bonn

Garantietermin

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwendige Wissen.

Preis: € 1.890,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 11.11.-13.11.15 in Bonn

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 16.11.-17.11.15 in Nürnberg

Garantietermin

Ziel der Schulung ist es, den Teilnehmern einen Überblick über die aktuelle Situation im Bereich des Datenschutzes im Kommunikationsumfeld zu verschaffen. Datenschutz und Datensicherheit werden zunehmend wichtiger im Umgang mit Kunden und Mitarbeitern. Gerade mit der Einführung von IP basierten Lösungen in den Bereichen Telefonie oder Contact Center, stellen sich neue Herausforderungen in Bezug auf personenbezogene Informationen. Um Ihnen eine Überblick über den rechtlichen Rahmen zu geben beschäftigt sich dieses Seminar u.a. mit Fragen zur Abhörsicherheit, Vorratsdatenspeicherung, Datenverlust und den dazugehörigen Aspekten. Weitere Schwerpunkte bilden die etwaigen Vorgaben seitens der Bundesnetzagentur oder auch von Betriebsvereinbarungen, die es zu beachten gilt.

Preis: € 1.590,-- netto

Trouble Shooting für Netzwerk-Anwendungen, 17.11.-20.11.15 in Aachen

Garantietermin

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzten Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

Die neue EU-Datenschutzgrundverordnung, 30.11.15 in Bonn

Garantietermin

2015 wird ein neues einheitliches Datenschutzrecht in der Europäischen Union vom Europäischen Rat und vom Europäischen Parlament beschlossen. Die Verordnung ist noch nicht endgültig verabschiedet, aber die wichtigsten Regelungen sind bereits jetzt weitgehend klar. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Informieren Sie sich über die geplanten Regelungen, damit Sie bei Inkrafttreten der Richtlinie wissen, was auf Ihr Unternehmen zukommt.

Preis: € 1.090,-- netto

IPv6 Grundlagen - SeminarPlus, 30.11.-01.12.15 in Köln

Garantietermin

IPv6 betreiben, bedingt IPv6 verstehen. In diesem Seminar werden die Grundlagen des neuen IP Protokolles verständlich und praxisnah vermittelt. Die Schulung richtet sich gleichermaßen an Planer, Betreiber, Administratoren und Software-Entwickler.

Preis: € 1.790,-- netto

Das mobile Unternehmen, 30.11.-01.12.15 in Köln

Garantietermin

Dieses 2-tägige Seminar gibt Ihnen einen umfassenden Überblick über Einsatzmöglichkeiten, Risiken und Chancen sowie Anforderungen und Auswirkungen mobiler Technologien im Unternehmen. Es werden die grundlegenden Veränderungen in Arbeitsweise und Arbeitsausstattung aufgezeigt, die die steigende Mobilität mit sich bringt und die Auswirkungen auf den IT-Betrieb, die Infrastruktur und das Management von mobilen Geräten diskutiert. Zum einen werden mögliche Gefährdungen aufgezeigt, die durch die zunehmende Konsumerisierung und den damit verbundenen Anstieg von privat genutzten Geräten entstehen. Zum anderen werden aber auch Möglichkeiten und Chancen, die mobile Applikationen und die lückenlose Vernetzung im „Internet of Things“ bieten, erläutert.

Preis: € 1.590,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 30.11.-02.12.15 in Bonn

Garantietermin

IT-Sicherheit konform ISO 27001 und BSI Grundschutzkatalog - klingt kompliziert? Ist es auch. Gerade angehende IT-Sicherheitsexperten fühlen sich schnell überfordert! In diesem Seminar gehen Experten aus der Praxis deshalb nicht nur auf die Theorie, sondern auf die Praxis und den Betrieb ein.

Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 30.11.-01.12.15 in Köln

Garantietermin

Im Zuge stetig zunehmender Konsolidierung ist Virtualisierung längst zum Standard in jedem Rechenzentrum geworden. Doch der Blick hinter die Kulissen offenbart einen rapide wachsenden Komplexitätsgrad, dessen Beherrschung ein tieferes Verständnis dieser Technologie erfordert. In diesem Seminar werden die Zusammenhänge zwischen Server, Netzwerk und Storage im Umfeld der Virtualisierung analysiert.

Preis: € 1.590,-- netto

Winterschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Garantietermin

Die Winterschule 2015 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik. Wir analysieren mit Ihnen, wie sich IT-Architekturen verändern, welche Auswirkungen das auf Netzwerke, Kommunikations-Technik und Infrastrukturen hat und welche Änderungen und Investitionen auf Ihrer Seite erforderlich sind.

Preis: € 2.490,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
15.02. - 19.02.16 in Aachen
09.05. - 13.05.16 in Aachen
19.09. - 23.09.16 in Aachen

TCP/IP-Netze erfolgreich betreiben
11.11. - 13.11.15 in Bonn
14.03. - 16.03.16 in Berlin
20.06. - 22.06.16 in Bonn

Internetworking
04.04. - 08.04.16 in Aachen
04.07. - 08.07.16 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
10.05.-13.05.16 in Aachen
27.09.-30.09.16 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
14.06.-17.06.16 in Aachen
15.11.-18.11.16 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
14.03. - 16.03.16 in Köln
11.05. - 13.05.16 in Bonn
24.10. - 26.10.16 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
11.11. - 13.11.15 in Bonn
11.04. - 13.04.16 in Stuttgart
20.06. - 22.06.16 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
25.04.-27.04.16 in Bonn
04.07.-06.07.16 in Stuttgart
28.11.-30.11.16 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
22.02. - 23.02.16 in Bonn
25.04. - 26.04.16 in Düsseldorf
19.09. - 20.09.16 in Frankfurt

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

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

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

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

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