

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

von Dipl.-Ing. Hartmut Kell

Zugegeben, die Auswahl eines Lichtwellenleiterkabels gehört mit Sicherheit nicht zu den neuesten Herausforderungen im Rahmen der Planung von anwendungsneutralen Kommunikationsverkabelungen, aber trotz der vielfältig im Internet bereitstehenden Informationen gibt es weiterhin viele Fehlentscheidungen, unverständlich hohe Preisschwankungen bei Preisanfragen, trotz vermeintlich klarer Spezifizierung.

Deshalb lohnt sich auch 2017 noch eine genaue Betrachtung und Erläuterung der zur Wahl stehenden Materialien, welche in Zusammenhang mit der Auswahl eines Kabels eine Rolle spielen. Der nachfolgende Arti-



kel verdeutlicht die grundlegenden Materialunterschiede, vermittelt auf Basis von Erfahrungen einige Tipps, zeigt typische Fehler bei der Auswahl und listet eine kleine Auswahl an marktverfügbaren Kabeltypen.

Die „nichtoptischen“ Eigenschaften eines Glasfaserkabels werden durch wenige, aber wichtige Hauptbestandteile geprägt, die richtige Auswahl und Zusammenstellung dieser Bestandteile nimmt erheblichen Einfluss darauf, wo sich das Kabel am besten einsetzen lässt und es erklärt bei einem Produktvergleich, worin die qualitativen Unterschiede begründet sind.

weiter ab Seite 7

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

von M.Sc. Daniela Gies und Dipl.-Inform. Thomas Steil

Wer sich heute mit der Planung und dem folgenden Betrieb eines modernen Gebäudes befasst, wird vermutlich schon oft über den Begriff des „Smart Building“ gestolpert sein. Ähnlichkeiten der Namensgebung mit einer Fahr-

zeug-Marke sind zufällig. Smart meint schlau, intelligent.

Die Gebäude wandeln sich von einfachen Beton- und Backstein-Türmen mit Metall- und Glasanteilen in vernetzte Rechenma-

schinen - man könnte sagen: vom Eternit zum Ethernet. Unter diesen Aspekten ist ein Vergleich mit der Entwicklung, die unsere Automobile in den letzten Jahren genommen haben, nun doch zulässig.

weiter auf Seite 16

Geleit

Die Zeit nach ISDN ist die Zukunft von UC: wie konzipiert man eine zukunftssichere Kommunikations-Lösung? Brauchen wir Kollaboration?

auf Seite 2

Standpunkt

Verschlüsselung in der Cloud: Licht am Ende des Tunnels

auf Seite 24

Sonderveranstaltungen

ComConsult RZ-Tage
Netzwerk-Architekturen der Zukunft im RZ
Integration von Cloud-Lösungen in die RZ-Infrastruktur

ab Seite 25

Wireless und Mobility

ab Seite 22

Aktuelle Kongresse

ComConsult UC-Forum

ab Seite 4

ComConsult Technologie-Tage

ab Seite 14

Geleit

Die Zeit nach ISDN ist die Zukunft von UC: wie konzipiert man eine zukunftssichere Kommunikations-Lösung? Brauchen wir Kollaboration?

Mit dem Abschalten von ISDN verschwindet die zentrale Drehscheibe unserer Sprachkommunikation und mit ihr das schöne alte PSTN. Dies produziert naturgemäß ein Vakuum und somit viele neue Fragen:

- wie kommt die neue Drehscheibe her?
- was leistet sie und welche Dienste unterstützt sie?
- wie schließen sich Unternehmen an die Drehscheibe an?

Die Antwort der Provider ist IP-Telefonie der einfachsten Form. Wirklich? Im Zeitalter von Skype, Facebook Messenger, Google Hangouts, WhatsApp wird Telefonie durch Telefonie ersetzt? Das akzeptieren doch nicht einmal mehr die Endkunden, die immer mehr auf die gerade angesprochenen Dienste setzen. Es liegt auf der Hand, dass ein Telefonie-Angebot der alten Art in wenigen Jahren nur noch dazu dienen kann, dass Großeltern ihren Enkeln zeigen können wie es früher einmal war (und die Enkel werden fassungslos davorstehen).

Aber wie sollte eine Vision für die Kommunikations-Lösung der Zukunft aussehen? Was sollte das Fundament sein?

Die bekannten Anbieter von UC-Lösungen tragen nicht unbedingt dazu bei, eine einfache Antwort auf die Frage zu geben. Cisco bietet zum Beispiel die Kombination aus CUCM, WebEx und Spark und scheint der Ansicht zu sein, dass der Endbenutzer ohne Probleme mit mehreren Clients und redundanter Funktionalität je nach Situation arbeiten kann. Unify geht mit Circuit einen ähnlichen Weg und Microsoft toppt mit einem Bauchladen von Tools inklusive Teams das Angebot. Aber kann eine Sammlung von Tools je nach Bedarf und eine Überfrachtung der Clients wirklich die Lösung sein? Haben wir so viele Spezialanforderungen, dass diese Ansammlung unterschiedlicher Funktionen und Clients gerechtfertigt ist?

Zu einer ersten Antwort auf diese Frage lösen wir uns am besten von den Produkten und stellen uns vor, dass wir auf einer grünen Kommunikations-Wiese sind. Naturgemäß hat man dabei zwei Seiten zu beachten:



- die ideale Funktionalität, die man auf der eigenen Seite zum Kommunizieren haben will
- die damit verbundenen Erwartungen an die Gegenseite, speziell, wenn die Gegenseite außerhalb des eigenen Unternehmens ist

Die Erwartungen an die Gegenseite sind ein wesentlicher Teil des Design-Problems. Sobald wir uns von Sprache entfernen müssen wir feststellen, dass es bisher keinen im Markt etablierten Standard für Funktionalität in der Kommunikation zwischen Unternehmen oder mit Privatpersonen spricht Kunden gibt.

Dies führt zu vier Alternativen:

- wir reduzieren uns auf den kleinsten gemeinsamen Nenner: eine reine Sprachkommunikation. Dies ist die Haltung der Provider, aber auch Anbieter wie Spinate bieten nicht mehr. Hier kann man sofort sagen, dass das nicht ausreichen wird. Zwar ist Sprache ein unverzichtbares Muss, aber für sich alleine gesehen ist sie ein Teil der Vergangenheit. Das Design einer UC-Lösung auf der Basis von Sprache ist im Kern die Ursache für die Bauchladen-Situation, die wir dann bekommen.
- wir warten, bis sich ein neuer Funktions-Standard im Markt durchgesetzt hat. Immerhin unterstützt SIP ja Chat, Sprache und Video. Da liegt es nahe hier ei-

nen Minimal-Kern zu sehen, der überall zur Verfügung stehen sollte. Die Provider blockieren diese Entwicklung bisher. Meine Hoffnung ist Null, dass sich das ändert. Aber wir brauchen die Provider ja nicht unbedingt. Im Prinzip kann SIP ohne zentrale Instanz leben. Die Vermittlung könnte durch DNS ersetzt werden. Die Provider haben aus meiner Sicht bereits kapituliert und geben den Markt an die Cloud ab. Wem Sprache nicht ausreicht, der geht eben zu Apple, Facebook, Google und Microsoft. Wer sein mobiles Endgerät nutzen möchte, kann auch gleich folgen. Mobile Endgeräte existieren im Weltbild von Telekom, Vodafone und Co nicht, wer will schon die Einnahmen aus GSM-Kommunikation so einfach aufgeben. Das Leitbild der Provider scheint hier Kodak zu sein, RIP.

- wir liefern dem Kommunikations-Partner die Funktionalität temporär für die Dauer einer Kommunikation in Form eines Web-Clients oder wir verlangen, dass er einen Client, der zu unserer Installation passt, installiert. Diese Installation müsste aber in jedem Fall Lizenzfrei sein. Dies ist mit hoher Wahrscheinlichkeit die Übergangs-Lösung, um die wir nicht herumkommen. Technisch gesehen könnte WebRTC im Kern einer solchen Lösung stehen, es hätte den großen Vorteil, dass die Funktionalität schon im Browser existiert (nicht in jedem).

- wir gehen davon aus, dass der externe Kommunikationspartner mindestens einen der verbreiteten Standard-Dienste von Facebook, Google oder Microsoft (Skype) betreibt und wir haben eine Schnittstelle dazu. Auch dies kann ein Element einer Übergangslösung sein.

Damit sind wir dann bei der idealen Funktionalität, die wir uns für uns selber wünschen. Wie sähe die aus? Bei allen individuellen Unterschieden, die es zwischen Unternehmen und Behörden geben kann, ist doch unübersehbar, dass eine Kombination aus Chat, Sprache und Video die absolute Basis darstellen muss. Ob wir eine Realzeit-Umschaltung zwischen den Diensten im Laufe einer Kommunikation brauchen, mag eine individuelle Ent-

Die Zeit nach ISDN ist die Zukunft von UC: wie konzipiert man eine zukunftssichere Kommunikations-Lösung?

scheidung sein. Aber es kann nicht sein, dass wir eine Zukunfts-fähige Lösung planen, die hinter dem Standard, der von Facebook, Google und Microsoft (Skype) gesetzt wird, zurückfällt. Wir können einfach nicht so tun als wäre es noch 1990. Ein Dienst, der dabei nicht unterschätzt werden darf, ist Chat/Messaging, der sich allerdings in sehr unterschiedlichen Ausführungen umsetzen lässt. Der Trend geht dahin, dass Sprache und Email durch irgendeine Form von Chat abgelöst werden.

Damit sind wir aber auch automatisch bei der Diskussion von Kollaborations-Lösungen. Also Cisco Spark, Microsoft Teams und Unify Circuit. Google lasse ich hier mal raus, obwohl sie in den USA verbreitet sind und die Produkte überwiegend gut sind. Das basiert auf meiner Grundsatz-Entscheidung, Google-Produkte wenn möglich zu vermeiden. Auch bietet Google keinerlei Garantie für die zukünftige Verfügbarkeit seiner Produkte. Auch hochgradig akzeptierte und verbreitete Produkte werden da schon mal eben ohne Grund eingestellt, siehe NIK.

Cisco, Microsoft und Unify vermarkten ihre Kollaborations-Lösungen als neuen Ansatz, als neue Dimension der Kommunikation. Dazu ist anzumerken, dass das Marketing-Unfug ist. Wir haben seit 2001 Jive im Markt mit einer persistenten Chat-Lösung. Redbooth bietet seine komplette Plattform seit 2008/2010. Und seit 2009 rollt Slack diesen Markt auf. Von neu kann man also hier kaum sprechen. Produkte dieser Art haben seit Beginn ihrer Einführung ein zentrales Problem: die Akzeptanz durch die Benutzer und die Komplexität der Einführung in die Unternehmen. Tatsächlich hat aber gerade Slack gezeigt, dass eine erfolgreiche Nutzung möglich ist. Das Produkt setzt im Moment die Messlatte für Kollaborations-Lösungen. Microsoft stand in Verhandlungen zur Übernahme von Slack und hat sich aufgrund des Preises (Slacks Marktwert wird im Moment auf drei Milliarden USD geschätzt) die Entscheidung getroffen, ein eigenes Produkt zu entwickeln. Das Ergebnis ist Teams, das sich natürlich an den Erfolgsfaktoren von Slack orientiert. Das Produkt ist für eine erste Version zumindest auf dem Desktop erstaunlich gut. Schwer zu verstehen ist die Entscheidung, auf mobilen Endgeräten mit anderen Benutzer-Schnittstellen und einer eingeschränkten Funktionalität zu arbeiten. So lassen sich auf einem iPad noch nicht einmal neue Channel anlegen (KO-Kriterium). Auch fehlt bisher eine gelungene Integration externer Benutzer, was aus meiner Sicht ein weiteres KO-Kriterium ist (alle Teilnehmer müssen zwingend eine Business Office 365 Lizenz haben). Auch lassen sich im Chat

keine externen Messenger einbinden. Die Anzahl der für Channel angebotenen Connectoren ist im Vergleich zu Slack mager.

Aber zurück zur Grundfrage der Vision einer UC-Lösung, die wirklich zukunfts-tauglich ist. Welche Fragen entstehen diesbezüglich durch diese Kollaborations-Lösungen:

- alle genannten Kollaborations-Lösungen sind Cloud-basierte Lösungen. Dies generiert sofort die Frage, wie das mit einer On-Premise-Installation zusammenpasst. Auch muss sich der Kunde damit der Cloud-Frage stellen.
- alle diese Produkte haben einen ähnlichen Funktionsumfang, wenn auch die Bedienung und einzelne Merkmale voneinander abweichen. Ist das die Messlatte für die Zukunft von UC?
- alle angebotenen Kollaborations-Lösungen decken nicht die volle Funktionalität eines Arbeitsplatzes ab. Damit wird eine zusätzliche Installation eines "normalen" UC-Clients unvermeidlich. Damit entsteht aber eine erhebliche Funktions-Redundanz, die den gesamten Wert der Lösung in Frage stellt.

Die Antwort auf die erste Frage ist fast eine Glaubensfrage. Sie ist klar mein persönlicher Standpunkt und mir ist klar, dass die Mehrheit unserer Kunden hier anderer Meinung ist. Mein Standpunkt ist klar und einfach: Kollaboration und UC-Lösungen gehören für mich zukünftig in die Cloud. Ich akzeptiere keine Parallel-Welten. Dies hat viele Facetten, die ich hier nicht ansprechen will und deren Diskussion ich auf unser UC-Forum im November verschiebe. Mein typisches Endgerät ist mein iPhone, meine Clients sind ein SIP-Client und Zoom für Videokonferenzen. Den Sinn und die Kosten eines Tischtelefons kann ich schon lange nicht mehr nachvollziehen (meine eigene Meinung sei mir gestattet, in Projekten muss natürlich der Bedarf des Kunden und sein Wunsch die höhere Priorität haben). Ich hätte auch nichts gegen Skype for Business als Cloud-Lösung einzuwenden. Aber zum einen tritt Microsoft trotz vieler Ankündigungen immer noch nicht als Provider auf (was sie für mich extrem unglaubwürdig macht) und zum anderen gibt es bei mir auf iPhone und iPad immer wieder technische Probleme. Und im direkten Vergleich bietet Zoom als Videokonferenz die deutlich bessere Qualität und deutlich mehr Optionen. Auch hat Microsoft eine merkwürdige Lösung was die Datei-Viewer in Teams angeht und springt in nicht nachvollziehbarer Art und Weise zum Web-Client, wenn man eine Datei ansehen will (dies ist abhängig davon, wo die Datei ge-

speichert ist. Auf dem Desktop wird für Dateien in Box scheinbar der Box-Viewer genutzt, der dann auch funktioniert).

Damit sind wir aber bei einem Kernproblem von Cloud-Lösungen, das sehr ernst genommen werden muss. Die Lösungen, die ich heute in der Cloud bekomme, sind extrem gut, frei von Altlasten und liefern ein bisher unbekanntes Niveau an Effizienz. Slack ist hier ein gutes Beispiel. Auch weil Slack eine komplett offene Lösung ist und fast beliebig mit anderen Cloud-Lösungen kombiniert werden kann (Alsana, Box, ...). Das Grundprinzip solcher Cloud-Lösungen besteht also daraus, dass ich die Dienste auswähle, die zu mir passen und diese dann mit Schnittstellen integriere. Darin liegt aber ein erhebliches wirtschaftliches Problem. Addiere ich die Kosten pro Arbeitsplatz solcher Kombinations-Lösungen auf, so komme ich schnell auf Lizenzkosten zwischen 50 und 100 Euro pro Arbeitsplatz und Monat. Und dabei habe ich Produkte wie Salesforce noch gar nicht berücksichtigt. Ich habe zwar geringere Betriebskosten, aber gerade durch die Kombination von Produkten und die Pflege von Schnittstellen ist dieses Szenario nicht frei von Betriebs- und auch Betreuungskosten.

Und damit wären wir dann bei Microsoft. Microsoft hat mit Office 365 ein Produkt geschaffen, das wirtschaftlich nur schwer zu ignorieren ist. Die Einzelkomponenten sind dabei häufig schlechter als die direkten Konkurrenten, die nur diese eine Funktion bieten (Ausnahme Office). Die Grundfrage bei Office 365 ist schlicht: nehme ich Funktionsnachteile aufgrund der Kostenvorteile in Kauf? Und wie groß dürfen die Nachteile werden, damit ich sie noch akzeptiere? Teams ist dabei auf einem sehr guten Weg. Es ist klar eines der besseren Microsoft-Produkte. Die Integration der Externen muss noch gelöst werden und die Tatsache, dass ich Dateien in den Workspace kopieren kann ist für mich ein absolutes No-Go (dazu gleich mehr). Aber Hand aufs Herz: was passiert im deutschen Markt, wenn Microsoft endlich tatsächlich als Provider auftritt und das mit einem attraktiven Preis untermauert? Zumindest im SMB-Markt dürfte das gravierende Folgen haben.

Damit kommen wir zur Frage des idealen Funktionsumfangs auf der grünen Wiese. Im Prinzip gefällt mir die Kombination aus Slack, Sprache und Video gut und ich denke, dass dies der richtige Weg ist. Der Teufel liegt hier im Detail. Diese Produkte werden sehr schnell sehr unübersichtlich. Funktionen wie die Konfiguration der individuellen Notifikationen, eine individuelle Gestaltung der Kanäle und Labels oder die dynamische Suche und Ansicht nach

Die Zeit nach ISDN ist die Zukunft von UC: wie konzipiert man eine zukunftssichere Kommunikations-Lösung?

Hash-Tags werden dann entscheidend für die Akzeptanz (was allerdings eine konsistente Nutzung von Hash-Tags voraussetzt, aber das ist ja kein neues Problem). Auch würde ich mir funktional wünschen, dass ich Externe per Email in einen Channel integrieren kann. Dies geht bisher nach meinem Kenntnisstand nur beim Abgeben eines Kommentars (Teams), die Antwort bleibt im Chat-Tool.

Ich möchte an dieser Stelle aber eine Sichtweise zu diesem Thema klar abgrenzen: den Umgang mit Dateien im Rahmen von Kollaboration. Meine Sichtweise ist dabei ganz klar: Jede Lösung, die mit Kopien von Dateien arbeitet, scheidet von vorn herein aus. Ich unterstelle, dass ein Unternehmen, das Wert auf eine gute Kollaborations-Lösung legt, eine separate Lösung für Datei-Kollaboration hat. Die ist sowie so zur Integration mobiler Teilnehmer erforderlich. Den Marktstandard setzt hier im Moment aus meiner Sicht Box, dir wir auch bei ComConsult Research als Dateisystem einsetzen. Aber auch Google, Dropbox und Microsoft müssen beachtet werden. Für mich persönlich ist Box weiterhin das Maß der Dinge und setzt den Funktions-

Standard in diesem Bereich. Slack integriert Box in sehr guter Form. Mit der Integration von Teams in der Desktop-Version könnte ich fast leben, dazu müsste ich jetzt die Integration Externer sehen, um das abschließend bewerten zu können. Bei einem Channel für Externe müssen die Rechte der dabei betroffenen Dateien konform mit den Rechten im Dateisystem sein (zumindest wenn ich keine Kopie zulasse, das dürfte der Grund sein, warum die Anbieter mit Kopien arbeiten, es macht das Rechtssystem einfacher).

Um dies klar zu sagen und auch keine Zweifel aufkommen zu lassen:

- Datei-Kollaboration gehört dann und nur dann in ein UC-Kollaborations-Tools, wenn es ein entsprechendes Datei-Kollaborations-Tool geeignet integrieren kann. Eine autonome Speicherung, sprich eine Kopie, sollte aus meiner Sicht in jedem Fall vermieden werden.
- Dies hat viele Komponenten, unter anderem wie ich eine Datei ansehe oder öffne/bearbeite und wie sich Änderungen konsistent im System verbreiten.

Auch die Qualität und Performance der Synchronisation ist ein wichtiges Auswahlkriterium. Tatsächlich ist die Liste der Kriterien relativ lang, die Auswahl eines solchen Tools ist komplex und in jedem Fall sollte nicht davon ausgegangen werden, dass diese Tools sowieso alle gleich sind.

Gibt es ein Fazit an dieser Stelle? Bewusst nicht. Dieses Geleit dient dazu, eine Diskussion zum UC-Forum im November vorzubereiten. Es darf aber keinen Zweifel an der Notwendigkeit einer Kommunikations-Vision geben. Eines ist dabei für mich absolut sicher: die Reduzierung auf Sprache ist eine teure Sackgasse. Sie hat genau das zur Konsequenz, was wir bei Cisco zum Beispiel als Anbieter sehen: eine Kombination verschiedener Dienste mit unterschiedlichen Benutzerschnittstellen. Das ist teuer, komplex zu betreiben und wird in keinem Fall auf breite Akzeptanz stoßen. Reine Sprache ist ein toter Dienst, ein Teil unserer Geschichte, vergleichbar mit dem Analog-Telefon. Ruhe in Frieden.

Ihr
Dr. Jürgen Suppan

ComConsult UC-Forum 2017

20.11. - 22.11.2017 in Königswinter

Die ComConsult Akademie veranstaltet vom 20.11. bis 22.11.17 ihren Kongress "ComConsult UC-Forum 2017" in Königswinter.

Das diesjährige UC-Forum analysiert die herausragenden Trends für Unified Communications und Collaboration, VoIP sowie Videokonferenzen und gibt Empfehlungen für Projekte, Technologie-Auswahl und Investitionen in zukünftige Kommunikationslösungen. Das weiterhin dominante Thema ist „All-IP“, die Abschaltung der ISDN- und PSTN-Infrastruktur durch nationale wie internationale Provider und die sich daraus ergebenden Probleme.

Im Rahmen des Forums werden Herausforderungen rund um „All-IP“ identifiziert und Lösungsansätze aufgezeigt, angefangen bei der Frage wie es mit Fax Diensten weitergeht bis hin zu alternativen Anschlüssen für Gefahrenmeldeanlagen. Dabei darf nicht übersehen werden, dass der Markt sich in einem dramatischen Wandel befindet. Traditionelle Hersteller kämpfen ums Überleben (oder zumindest die Produktqualität!), andere machen sich mit ihren Kollaborationsplattformen auf zu neuen Ufern. Die zunehmende Bedeutung von cloudbasierten UC-Produkten und die

Verschiebung von Kommunikationsdiensten von Voice- zu Cloud-Providern werden zu weiteren Verwerfungen im Markt führen. Neue Cloud Angebote – auch von etablierten Lösungsanbietern, wie Alcatel, Cisco oder Mittel – sprechen eine eindeutige Sprache.

Aber auch die Situation rund um Microsoft Office 365 und Skype for Business bewegt aktuell die Gemüter. Dabei wird oft die Frage aufgeworfen wo die Microsoft Lösung im Vergleich z.B. mit Cisco steht.

Dies geht einher mit einer Welle neuer Dienste und einer Neugestaltung des Mobilfunks. Gleichzeitig rücken Technologien wie Session Border Controller das SIP Protokoll wieder in den Mittelpunkt. Sie entscheiden mehr oder weniger über die Zukunftsfähigkeit moderner UC-Lösungen.

Wir analysieren dementsprechend auf dem UC-Forum 2017 für Sie:

- Wie positionieren sich Microsoft und Cisco, wer hat im Moment die bessere Lösung?
- Die TR Notruf 2.0 ist da. Was sind die wesentlichen Neuerungen?
- Mit SIP Connect und ETSI TISPAN gibt es endlich akzeptierte Peering Stan-

dards. Was bieten sie und wo werden sie eingefordert?

- Enterprise Lösungen aus der Sicht des Clients. Wohin entwickeln sich Technik und Funktionen?
- UCC auf dem Weg in die Cloud – was ist möglich und was zu beachten?
- ISDN und PSTN Abschaltung aus Sicht von Providern und Anwendern. Wo liegen die Herausforderungen?
- Fax Dienste sind tot und die mit ihnen verbundenen Arbeitsprozesse müssen sich ändern aber wie sehen die Alternativen aus?

Als zusätzliche Sonderthemen haben wir für das diesjährige Forum adressiert:

- IT-Compliance und die neue Datenschutzgrundverordnung
- Enterprise-Projekterfahrungen bei einem weltweiten Rollout von Office 365 und Skype for Business
- Qualitätssicherung durch VoIP Quality Monitoring und Cloud Readiness Assessments

Seien Sie dabei und erhalten Sie die aktuellsten Trendanalysen und Informationen von ComConsult Research mit Top-Referenten, Analysen, Projektberichten und Praxiserfahrungen.

Programmübersicht ComConsult UC-Forum 2017

Montag 20.11.2017 - UCC auf dem Weg in die Cloud

9:30 Uhr

Keynote

- Cloud und nochmals Cloud • Die ISDN Abschaltung ist da
Markus Geller, ComConsult Research GmbH

10:00 Uhr

Erfolgreiche Umsetzung der Cloud-Strategie für UCC

- Definition der Cloud-Strategie für UCC
- Welche Voraussetzungen müssen für die Umsetzung der Cloud-Strategie geschaffen sein • Migrationsplanung und -umsetzung
- Beispiele für die Nutzung von Cloud-Diensten
Markus Emde, ComConsult Beratung und Planung GmbH

10:45 Uhr

Cloud Collaboration und die Integration von Web- und Videokonferenzen - UC aus dem Mobilfunknetz

- Cloud Lösungen und die Möglichkeiten der 3rd Party Integration
- Netzwerk und Sicherheit
- Mezzanine Produkt Suite
Thomas Brüning, Oblong Industries

11:15 Uhr Kaffeepause

11:45 Uhr

Herausforderungen Fehlersuche und Problemlösung bei Sprache, Video und Bildschirmübertragungen

- Customer Experience Management bei Echtzeitkommunikation von Sprache und Video in Cloud- und Hybridumgebungen
- Assessment/ Testing/ Assessor
Andreas Wächter, Integrated Research Germany GmbH

12:30 Uhr

Ein Client für Contact Center und andere Fälle

- Suitepad bzw. Macnetix im Hotelumfeld
- ASCOM myco 2 • TUI Meinschiff App • Contact Center Frontends
- Integrationsmöglichkeiten mit Collaboration-Lösungen
Lars Dietrichkeit, innovaphone AG

13:00 Uhr Mittagspause

14:30 Uhr

Client der Zukunft – Update 2018

- Cisco Spark • Avaya Zang/Equinox
- Unify Circuit • Alcatel Rainbow
- Microsoft Office 365 • Innovaphone
Markus Geller, ComConsult Research GmbH

15:15 Uhr

Cloud Collaboration und Integration von Konferenzen und Drittlösungen

- Lösungen für Cloud Collaboration
- Architektur für Unternehmen und Netzbetreiber
- Mobility, Telefonie, Konferenzen, Video und persistente „social collaboration“
- Contact Center, CRM und Groupware Integration
- Global verfügbare Cloud Services als Alternative zum eigenen Betrieb
Jürgen Engelhard, Mitel Deutschland GmbH

15:45 Uhr Kaffeepause

16:15 Uhr

Where Everthing Connects (CPaaS)

- Von der Infrastruktur agnostischen Integration von Geschäftsprozessen in Plattformen bis zur Einbindung von kundenspezifische Applikationen • Welche Technologie macht dies möglich?
- Kannibalisieren wir uns selbst?
Rene Princz-Schelter, ALE Deutschland GmbH

16:45 Uhr

DSGVO – Was passiert im Mai 2018

- Die neue EU- Datenschutz Grundverordnung im Überblick
- Was ändert sich für die Unternehmen?
Ulrich Emmert, esb Rechtsanwälte

ab 18:00 Uhr Happy Hour

Dienstag 21.11.2017 - Cloud ist nicht alles. Was sonst noch wichtig ist!

9:00 Uhr

Assessment von Microsoft Office 365 - Anforderungen und Konsequenzen für die IT

- Grundlagen: Lizenzmodelle, Anbindung an die Microsoft Cloud, Integration des Active Directory
- Anforderungen an die Netzinfrastruktur: WAN-Anbindung, Tools zur Überprüfung der Netzqualität, Netzdesigns zur Anbindung von Niederlassungen, Tuning Möglichkeiten
- Erfahrungen aus Kundenprojekten
Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

10:00 Uhr

Datenschutz, Datensicherheit und Datenhoheit bei Cloud Collaboration Tools

- Intro: EU DS-GVO/GDPR und die Auswirkung auf Real Time Chat Communication Plattformen in der Cloud
- Lösungen am Markt & Cisco Spark Feature Übersicht
- Cisco Spark Hybrid Data Security – eine technische Lösung auf eine juristische Frage? • Key Federation im Detail – für sichere Zusammenarbeit zwischen Firmen • Ein vorläufiges Fazit
Sebastian Bonk, avodaq AG

10:45 Uhr Kaffeepause

11:15 Uhr

Secure productive Enterprise - So sieht moderne Zusammenarbeit heute aus – einfach, offen, sicher, mobil!

- Was für Anforderungen stellt die moderne Arbeitswelt an Unternehmen und Arbeitnehmer?
- Modernes Arbeiten mit der Microsoft Plattform inklusive Live Demonstration
- Datenschutz und Datensicherheit gewährleisten – Security im Kontext Zusammenarbeit und wie Microsoft Technologie Ihrem Unternehmen hilft GDPR konform zu werden
Dipl. Betriebsw. Jörg Petter, Microsoft Deutschland GmbH

11:45 Uhr

Cisco vs. Microsoft – Was leisten die UC-Portfolios der beiden Hersteller?

- Typische Ausgangssituationen und Zielszenarien
- Vergleich und Bewertung der UCC-Lösungsportfolios
- Welche Use-Cases werden durch die Hersteller adressiert?
- Was ist jeweils das bessere Deployment-Szenario?
Dipl.-Ing. Dominik Zöller, freier Experte

12:30 Uhr Mittagspause

14:00 Uhr

Realisierung von SIP Trunking in der Projektpraxis

- Projekt-Rahmen • Standardisierung: SIPConnect, ETSI TISPA, ATIS NNI
- Betrachtete Provider • Realisierungs-Varianten
- Evaluierte Kriterien • Kosten • Bewertungs-Ergebnisse
Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

15:00 Uhr

Avaya BREEZE - Kommunikation und Zusammenarbeit im digitalen Zeitalter mit Fallbeispielen aus der Praxis

- Breeze als Beschleuniger für smarte digitale Lösungen für die Automatisierung • Turnkey und maßgeschneiderte Nutzererfahrung
Thomas, Römer, Avaya Deutschland GmbH

15:30 Uhr Kaffeepause

16:00 Uhr

Collaboration mit WebRTC (Live Chat)

- Kundenbeispiel Sparkasse Niederrhein
- Geschäftsstellen im ländlichen Bereich
- TextChat / VideoChat
Raphael Bossek, estos GmbH
Mario Wellmanns, Sparkasse am Niederrhein

16:30 Uhr

UCC und IPv6: Neues Protokoll, neue Probleme?

- Was ändert sich mit IPv6?
- Welche Tücken gibt es bei Endgeräten und Software?
- Wie verhindert man Blackholes, in denen UCC-Pakete verschwinden?
- Wie migriert man unternehmensintern sanft von IPv4 nach IPv6?
Markus Schaub, ComConsult Studytv

Programmübersicht ComConsult UC-Forum 2017

Mittwoch 22.11.2017 - Abschaltung ISDN 2018

9:00 Uhr

Sonderanschlungen in der Praxis

- Empfehlungen für
 - BMA, EMA, ÜMA • POS
 - Gebäudeleitechnik (Aufzugnotruf)
- VdS Empfehlungen

Markus Emde, ComConsult Beratung und Planung GmbH

9:45 Uhr

All-IP aus Carrier- und Kundensicht

- Neues Carriernetz und neue Services – was ändert sich?
- Neue Chancen für das Design von Sprach- und Datennetzen
- Praxistipps und Projekterfahrungen

Dipl.-Ing. Wilfried Meer, T-Systems International GmbH

10:30 Uhr Kaffeepause

11:00 Uhr

Notruf in Unternehmensnetzen

- AKNN Empfehlung für Provider (Notruf; Leistungsmerkmale)
- TR Notruf 2.0

Dipl.-Ing. Markus Bornheim, Avaya Deutschland GmbH

11:45 Uhr

Die Private Telefonie Cloud der TK

- Warum Session Border Controller (SBCs)?
- ISDN-Backup mit „Trigger“ u. SIP-Trunks
- Herausforderungen bei der Implementierung
- Entwicklungsstrategie All IP

Dipl.-Ing. Rolf Nagelfeld, Techniker Krankenkasse

12:30 Uhr Mittagspause

14:00 Uhr

Migration zu SIP Trunking

- ISDN über SIP – die Evolution von reinem SIP-Trunking

Reinhard Otto, Colt Technology Services GmbH

14:45 Uhr

SBC Design

- Anschaltung
- Designbeispiele
- Funktionen

Markus Emde, ComConsult Beratung und Planung GmbH

15:15 Uhr Kaffeepause

15:45 Uhr

Fax Ablösung

- T.30 Standard (Was ist T.38; Alternative T.37)
- Rechtssichere Alternativen (Zertifikatsbasierte Lösungen)

*Markus Geller, ComConsult Research GmbH
Dr. Rolf Fiedler, Ferrari electronic AG*

Der Veranstalter behält sich Änderungen im Programm vor

Folgende Firmen nehmen an der begleitenden Ausstellung teil

In der parallel stattfindenden Ausstellung haben führende Hersteller und Dienstleister der Branche und die Kongressteilnehmer die Möglichkeit zum interaktiven Kontakt und Informationsaustausch.



Anmeldung an kundenservice@comconsult-research.de

ComConsult UC-Forum 2017

Ich buche den Kongress
ComConsult UC-Forum 2017

vom 20.11. - 22.11.17 in Königswinter zum Preis von 2.390,- € netto

Vorname _____ Nachname _____

Bitte buchen Sie mir ein Hotelzimmer

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

 Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

eMail _____ Unterschrift _____

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

Fortsetzung von Seite 1



Dipl.-Ing. Hartmut Kell kann bis heute 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 hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Als erstes ist die Konstruktion des Röhrchens zu betrachten, welches die Glasfaser unmittelbar umgibt und welches die Faser vom Rest des Kabels mechanisch weitestgehend entkoppelt. Hier gibt es im Wesentlichen Typen, bei denen die Fasern bzw. Adern lose im Röhrchen untergebracht wurden (Hohlader, Bündelader) oder die Typen, bei denen die Glasfaser relativ kompakt bzw. fest von einem Röhrchen „eingepackt“ sind (Vollader, Kompaktader), dazu siehe auch Abbildung 1.

Bei der Kabelseele betrachtet man die verschiedenen Möglichkeiten, ein oder mehrere Röhrchen in einem Kabel zu integrieren. Dies ist notwendig, da in den meisten Fällen nur 12 bzw. 24 Fasern pro Röhrchen eingezogen werden und demzufolge bei mehr als 24 Fasern mehr als 1 Röhrchen in einem Kabel vorhanden sind.

Das ganze Innere des Kabels wird durch den Außenmantel geschützt, dieser hat somit unmittelbaren Kontakt mit der Verlegeumgebung und seine Eigenschaften müssen passend sein.

Hohlader

Die Hohlader ist prädestiniert für den Einsatz in Umgebungen mit starken Temperaturschwankungen. Dies hat folgenden Grund: Alle Adern mit den jeweils darin enthaltenen Fasern werden üblicherweise helixförmig um ein zentrales Stützelement verseilt. Diese Helix und die radiale Beweglichkeit der Faser innerhalb der Ader erlaubt bei Zug oder Stauchung des Kabels (z.B. verursacht durch Temperaturschwankungen aber auch Kabeleinzug) eine ausgleichende Bewegung des Lichtwellenleiters innerhalb der Ader, ohne dass eine sofortige Dehnung der Faser selbst entsteht. Es sind Kabeldehnungen im Bereich von 0,5% bis 1% möglich,

ohne dass eine Dämpfungserhöhung in der Faser entsteht. (siehe Abbildung 2)

Bei der Planung von Lichtwellenleiterverkabelungen im Außenbereich, wo der Einsatzschwerpunkt der Hohlader liegt, werden zunehmend Kabel verwendet mit hoher Faseranzahl, in der Regel mit mindestens 24 Fasern pro Kabel. Dies ist eine unübliche Größe für Hohladerkonstruktionen (der Außendurchmesser des Kabels wird zu groß und das Kabel wird zu schwer) und demzufolge ist die Hohlader bei den meisten Planungen als mögliche Alternative verschwunden, hier hat sich in den letzten Jahren die Bündelader in den Vordergrund gestellt.

Bündelader

Die Bündelader ist in den meisten Punkten identisch zur Hohlader, besitzt aber bei hoher Faseranzahl einen geringeren Außendurchmesser. Alleine der Aderdurchmesser von ca. 1,4 mm bei ei-

ner einfasrigen Hohlader im Vergleich zu einer 12-Faser-Bündelader mit einem Durchmesser von ca. 3,5 mm macht dies deutlich.

Die Faseranzahl pro Kabel wird bei den meisten Herstellern in 4er-Schritten angeboten, alle anderen Typen können zwar hergestellt werden, gehören aber nicht zum Standardrepertoire eines Kabelherstellers.

Eine Anpassung an die üblichen Größen von nichtmodularen Rangierfeldern führt zur weiteren Empfehlung, die Glasfaserkabel nach Möglichkeit in 12er-Schritten zu dimensionieren. Leere Kupplungsausbrüche können vermieden werden und die Verkabelung bleibt übersichtlicher. Aufgrund von umfangreichen Erfahrungen bei Erweiterungen oder gar von Sanierungen von Netzen konnte festgestellt werden, dass „Zwischengrößen“ wie z.B. 6 oder 10 Fasern pro Kabel unübersichtlich im Betrieb sind und die eingesparten

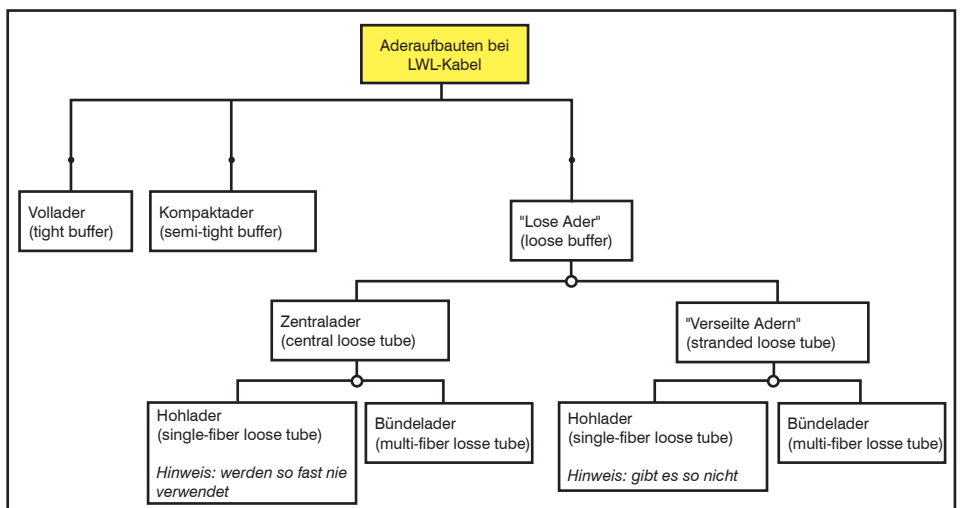


Abbildung 1: Aderaufbau bei LWL-Kabel

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

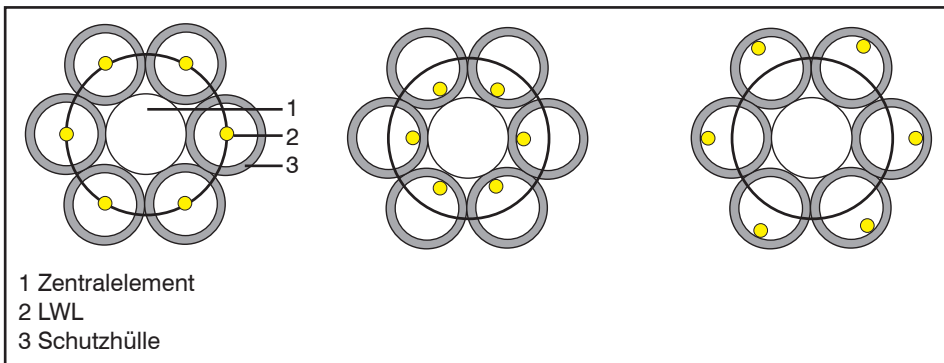


Abbildung 2: Verselung der Hohladern und „Stresswirkungen“

Quelle: Siemens

Kosten in keinem Verhältnis zu den damit verbundenen Unübersichtlichkeiten stehen. Eine Teilspleißung von vorhandenen Fasern mit dem Ziel, zunächst Kosten zu sparen und dann gegebenenfalls die restlichen Fasern nachzuspleißen, hat sich ebenfalls nicht bewährt; zu groß ist der Aufwand in einem laufenden Netzwerk.

Fest- oder Vollader

Bei der Fest- oder Vollader wird auf die Glasfaser eine feste Schutzhülle aus Kunststoff aufgebracht, diese Ader ist damit deutlich dünner als eine Hohladern. Elastische Dehnungen des Kabels wirken sich aufgrund der fehlenden Bewegungsmöglichkeiten der Faser innerhalb der Ader negativ auf die Dämpfungsqualität aus. Auch ein optionaler Wassereintritt würde wegen des fehlenden Schutzgels zur „Erblindung“ der Faser führen. Insbesondere bei Verlegung von Lichtwellenleiter im Außenbereich sind hier die Risiken zu groß, so dass die Fest-/Vollader überwiegenden Einsatz im Inhouse-Bereich findet. Einige Hersteller wie z.B. Leonie bieten z.B. auch Außenkabel in Festadern aufbau an, mit dem Verweis im Datenblatt, dass dies nur in geeigneten Schutzrohren verlegt werden darf.

Die meisten auf dem Markt angebotenen Fest-/Volladern besitzen einen dickeren Außendurchmesser, das liegt an der „Einbettung“ jeder Ader in einen eigenen Kevlar-mantel, der es ermöglicht, jede Faser/Ader ohne Spleißvorgang direkt an einen Stecker anzubringen. Diese Möglichkeit, ein Kabel „auseinander zu brechen“ führt zur Bezeichnung Break-Out-Kabel. (siehe Abbildung 3)

Zum Vergleich der Außendurchmesser vier Beispiele eines Herstellers:

- Kabel mit 12 Festadern (verseilte Einzelkabel): Außendurchmesser 14,5 mm
- Kabel mit 12 Festadern (kein Einzelkevlar): Außendurchmesser 7 mm
- Kabel mit 12 Hohladern: Außendurchmesser 15,7 mm

- Kabel mit 12 Fasern in einer Bündelader: Außendurchmesser 13,5 mm; hier ist jedoch ein Nagetierschutz berücksichtigt und der Durchmesser bleibt auch bis 60 Fasern bei 13,5 mm!

Da die Festadern dünner, leichter und biegsamer ist, wird sie häufig als Anschlusskabel oder bei fertig konfektionierten Stücken für improvisierte Verkabelungen (z.B. bei Notstrecken) eingesetzt. Wird eine Faserzahl von mehr als 12 Stück verlangt, so wird man eher die kostengünstigere und deutlich dünnere Bündelader einsetzen.

Nachteilig bei der Direktmontage einer Festadern ist, dass der Prozess zum Absetzen der Faser (d.h. Befreiung der Faser vom Primärcoating) insbesondere bei größeren Längen (20 cm und mehr) relativ mühselig ist. Deshalb wird in vielen Fällen, in denen eine Direktmontage gefordert wird, statt der Volladern die Kompaktadern eingesetzt.

Kompaktadern

Um den Nachteilen in punkto Absetzbarkeit zu begegnen, wurde die Kompaktadern (auch semilose Ader genannt) entwickelt. Im Gegensatz zur Fest-/Volladern liegt die Faser ähnlich einer Hohladern mit einem radialen Spiel von 50 µm bis 100 µm leicht distanziert in der Sekundärbe-

schichtung (siehe Abbildung 3). Diese Konstruktion eignet sich für direkte Steckermontage und Spleißtechnik, da sie sich leicht bis zu 1,5 m absetzen lässt. Ein weiterer Vorteil gegenüber der Festadern liegt in der mechanischen Entkopplung der Faser und des Sekundärcoatings, daraus resultiert eine größere Unempfindlichkeit gegen Längs- und Querkkräfte.

Kompaktadern gibt es wahlweise mit einer Gel-Gleichschicht oder trocken. Die Funktion des Gels dient dabei primär zur Reduzierung des Reibungskoeffizienten und Stabilisierung der definierten Faserüberlänge, weniger zum Schutz gegen Wassereintritt. Auch dieser Typ ist nicht für den Außenbereich prädestiniert.

In Installationskreisen ist der gelgefüllte Typ wegen seiner schwierigen Handhabung und Säuberung unbeliebt, ein Herausfließen des Gels nach erfolgter Installation ist bei normalen Betriebstemperaturen nicht möglich. Grundsätzlich ist bei der Planung zu prüfen, ob die Umgebung ein gelgefülltes Kabel verlangt, eine typische Büro-Verkabelung wird dies wohl eher nicht notwendig machen.

Weiterer Aufbau der Kabelseele

Die Erfahrung zeigt, dass sich in vielen Leistungsverzeichnissen bzw. Ausschreibungen die Beschreibung der Lichtwellenleiter-Kabels nur auf den Aderaufbau beschränkt, die verschiedenen Varianten zur Gestaltung der Kabelseele werden zum Teil nur unzureichend spezifiziert. Neben den Adern besteht die Kabelseele aus Stützelementen und Zugentlastungselementen.

Zunächst ist zu unterscheiden zwischen der Zentraladernkonstruktion und verseilten Kabelkonstruktion. Bei der Zentraladernkonstruktion befindet sich in der Mitte des Kabels lediglich eine einzelne Ader mit maximal 24 Fasern (Bündeladertyp). Bei der verseilten Konstruktion wer-

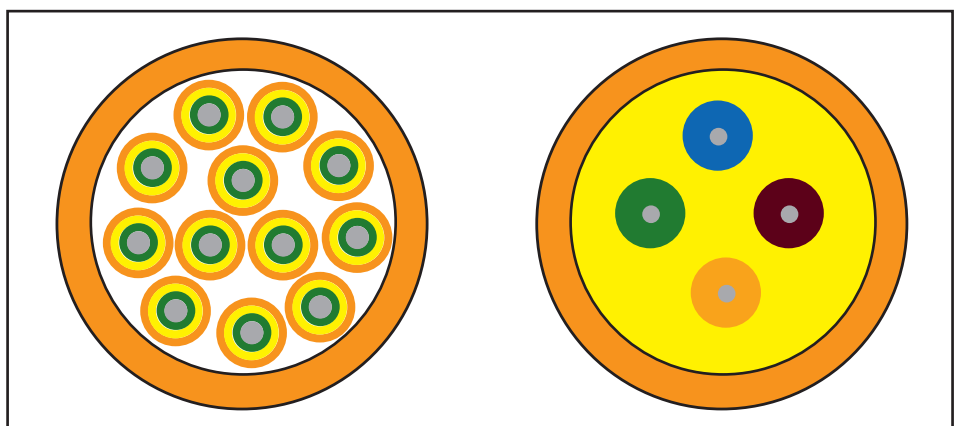


Abbildung 3: Gegenüberstellung Festadern mit/ohne Einzelkevlar

Quelle: Leonie

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

den mehrere „Röhrchen“ um ein zentrales Stützelement herum angeordnet, bei sehr hoher Faseranzahl kann das in mehreren übereinanderliegenden Lagen erfolgen. Der Begriff Lagenkabel bezeichnet dabei nicht diese „Übereinanderlegung“, sondern dass die Elemente um das Stützelement herum Einzelelemente sind. Werden mehrere Bündel (bestehend jeweils aus mehreren Adern und einem Stützelement) wiederum um ein zentrales „Hauptstützelement“ verseilt, so spricht man von Lichtwellenleiter-Bündelkabel, dabei können die Elemente auch Hohladern, Festadern oder Kompaktadern sein, es müssen nicht zwangsläufig Bündeladern sein. (siehe Abbildung 4)

Der Vorteil der Zentralader liegt einmal in seinem geringen Außendurchmesser, hier wieder ein Vergleich von zwei ansonsten gleichwertigen Typen:

Hersteller A

Kabel mit 24 Fasern als Zentraladerkonstruktion: Außendurchmesser 10 mm
Kabel mit 24 Fasern in verseiltem Aufbau: Außendurchmesser 12,5 mm

Hersteller B

Kabel mit 12 Fasern als Zentraladerkonstruktion: Außendurchmesser 8,5 mm
Kabel mit 12 Fasern in verseiltem Aufbau: Außendurchmesser 15 mm

Hersteller C

Kabel mit 24 Fasern als Zentraladerkonstruktion: Außendurchmesser 7,8 mm
Kabel mit 24 Fasern in verseiltem Aufbau: Außendurchmesser 12 mm

Bei der Bewertung ist zu beachten, dass die Bündeladerkonstruktionen bei gleichbleibendem Außendurchmesser z.T. das 5- bis 6-fache an Fasern aufnehmen können. Ob die Reduzierung des Durchmessers bei einer Faseranzahl von maximal 24 Fasern einen wirklichen Vorteil bei der Kabelverlegung bringt, ist jedoch zu bezweifeln.

Zum anderen erhöht die Einbringung des, zumeist aus Kunststoff bestehenden Stützelementes bei der Lagenverseilung die Brandlast, auch hier Vergleichswerte (alle als flammwidrige Bündelader-Ausführung):

Hersteller A

Kabel mit 24 Fasern als Zentraladerkonstruktion: Brandlast 1,3 MJ/m
Kabel mit 24 Fasern in verseiltem Aufbau: Brandlast 2,4 MJ/m

Hersteller B

Kabel mit 12 Fasern als Zentraladerkonstruktion: Brandlast 1,1 MJ/m
Kabel mit 12 Fasern in verseiltem Aufbau: Brandlast 3,5 MJ/m

Hersteller C

Kabel mit 24 Fasern als Zentraladerkonstruktion: Brandlast 1,09 MJ/m
Kabel mit 24 Fasern in verseiltem Aufbau: Brandlast 2,20 MJ/m

Als Nachteil der Zentraladerkonstruktion ist in jedem Falle die geringere Zugfestigkeit zu nennen. Durch die fehlende Helixform der Verseilung besitzt die einzelne Faser keine Faserüberlänge, die im Falle von Stauchungen oder Dehnungen des Kabels eine Dehnung der Fasern vermeiden kann. Besonders das zusätzliche zentral liegende Stützelement - zumeist aus glasfaserverstärktem Kunststoff GFK - verbessert die Zugfestigkeit besonders (siehe Produktabelle).

Füllung der Kabelseele als Schutz gegen Wassereintritt

Wie bereits dargelegt, besteht bei vielen Kabeltypen die Möglichkeit, diese mit oder ohne Gelfüllung einzusetzen, dabei wurde bisher die Gelfüllung in erster Linie unter dem Aspekt der Reduzierung des Reibungskoeffizienten betrachtet. In den meisten Fällen soll das Gel als Schutz gegen Wassereintritt wirken, es ist also ein typisches Element von bei Außenkabeln.

Die Füllung der Verseilhohlräume (also zwischen den Adern) mit einem Petrolatgel (Öl-Basis) soll verhindern, dass sich Wasser von außen nach innen (Querswasserdichtigkeit) oder entlang des Kabels (Längswasserdichtigkeit) ausbreiten kann. Eine Kunststoffsperrschicht (meist aus Polyamid) zwischen Kabelmantel und dem Gel verhindert, dass die Füllung durch den Kabelmantel abwandern. Ergänzt wird die Füllung der Verseilhohlräume in vielen Fällen durch eine Gel-Füllung der Hohl- bzw. Bündeladern selbst (dazu siehe vorherige Erläuterungen). Die Füllung hat keinerlei Einfluss auf die Übertragungseigenschaften der Fasern. Diese Lösung bietet einen hohen Schutz, wird aber wie bereits angesprochen von den Installationsfirmen wegen des hohen Reinigungsaufwandes ungern eingesetzt.

Als Alternative zur Füllung der Verseilhohlräume gibt es im Markt weitere Lösungen:

- Pudermaterial zur Absorption der Feuchtigkeit: Diese Lösung ist wegen der Verschmutzungsgefahr in Spleißboxen oder Muffen ungeeignet.
- Quellvlies (oder Quellgarn): Um die Verseilung herum befindet sich ein Vlies welches bei Wassereintritt aufquillt und sowohl das Wasser absorbiert als auch die Leckstelle abdichtet.

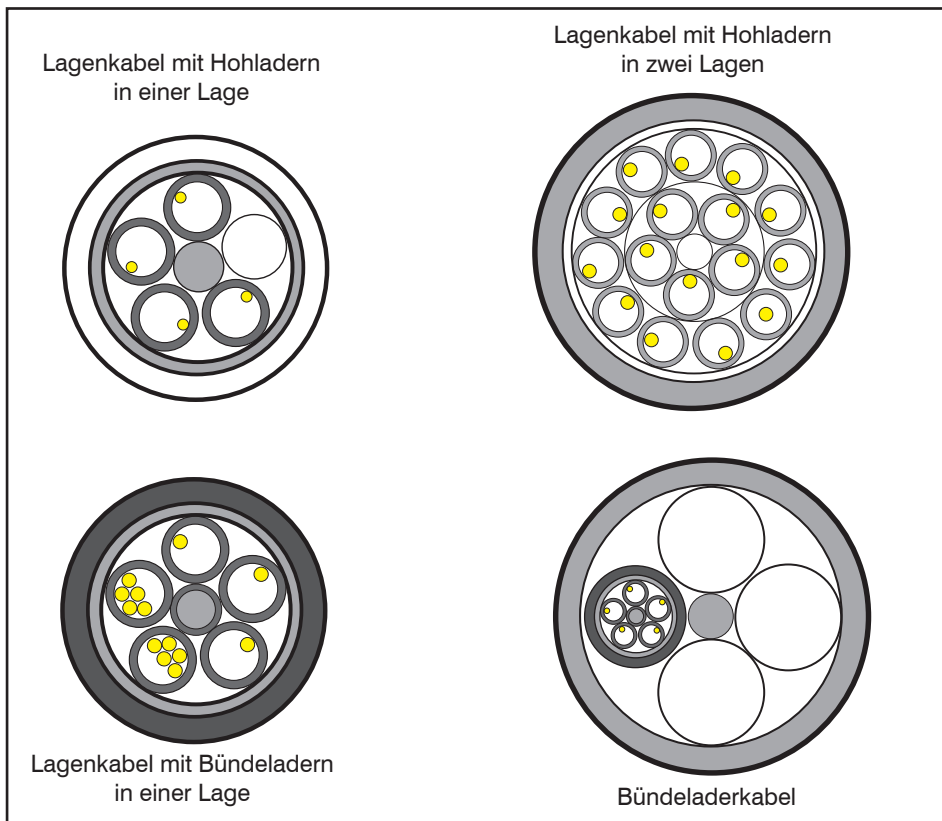


Abbildung 4: Verschiedene Arten von Kabelseele

Quelle: Siemens

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

• **Dry-Sealing:** Diese Methode wurde vom Kabelhersteller Acome entwickelt, hierbei wird ein „trockenes“ Gel in Form von Polyacrylsäuresalzen auf Glasgernelemente ins Kabel eingebracht und das Material verwandelt sich erst bei Wassereintritt in flüssiges Gel. Damit behält das Kabel seine Montagefreundlichkeit im trockenen Zustand und ist trotzdem geschützt (Zeitgewinn nach Herstellerangabe ca. 50% zu „normalen“ Gellösungen).

Bei der Verlegung von Kabeln im Innenbereich sollte auf die Gelfüllung der verseilten Hohlräume verzichtet werden, die Aderfüllung kann wie beschrieben aus Gründen der besseren Gleitfähigkeit weiterhin Sinn machen. Umstritten ist, ob bei senkrechter Verlegung bzw. Befestigung eines Kabels mit gelgefüllten Bündeladern die Gefahr besteht, dass die Füllung nach der senkrechten Montage im Laufe der Zeit abfließt (Beispiel: Sekundärkabel in einem Hochhaus); dem Autor liegen diesbezüglich keinerlei Negativ-Berichte vor.

Mantelmaterialien

Der Kabelmantel muss die Kabelseele vor mehreren Gefahren schützen, dazu sind mechanische, thermische, chemische Gefahren und die Feuchtigkeit zu zählen. Es stehen mehrere Materialienarten zur Verfügung:

- Polyvinylchlorid PVC
- Fluorpolymer (FP bzw. FEP)
- Polyethylen (PE)
- Polyurethan (PUR)
- verschiedene Typen von halogenfreien und/oder flammwidrigen Werkstoffen, allgemein geführt unter Flame Retardant Non Corrosive (FRNC) oder Low Smoke Zero Halogen (LSOH oder LSZH).

Beide Begriffe FRNC und LSZH werden zum Teil sehr willkürlich durcheinandergebracht, stehen aber für verschiedene Eigenschaften:

FR: Ein Kabel mit dieser Eigenschaft ist schwierig zu entzünden. Dabei spielt aber nicht nur das Material eine Rolle, sondern auch der Aufbau.

NC: Kabelmaterial und Adern enthalten keine im Brandfall korrosiven Materialien, das heißt aber nicht, dass sie rauchfrei sein müssen.

LS: Kabelmaterial und Adern enthalten keine im Brandfall stark rauchenden Materialien, das heißt aber nicht, dass sie rauchfrei sind oder schwer entflammbar.

ZH: Diese Kabel enthalten keine korrosiven Halogene, das heißt aber nicht, dass nicht andere „nichthalogene“ Materialien

im Brandfall zu korrosiven Gasen oder Rauch führen können.

Die genaue Betrachtung der Bezeichnungen macht deutlich, dass ein FRNC-Kabel des Herstellers A nicht unbedingt vergleichbar ist mit einem LSZH-Kabel des Herstellers B, dies ist ein wichtiger Unterschied, der bei der Planung berücksichtigt werden muss.

PVC bietet neben der guten Handhabung (weiches Kabelmaterial) den Vorteil, dass es flammhemmend ist. Bei der Erwärmung des Materials oberhalb von 200 °C entsteht neben Salzsäuregas und hochgiftigen Dioxinen auch eine hohe Rauchentwicklung. Diese Gefahren haben dazu geführt, dass PVC innerhalb Europas nicht mehr akzeptiert wird. Falls bei der Planung jedoch aus anderen Gründen auf dieses Material besteht, so wird die Suche bei deutschen/europäischen Kabelherstellern schwierig, die PVC-haltigen Kabeltypen wurden zumeist aus dem Sortiment entfernt. Eine Entsorgung von PVC-haltigen Kabeln ist ggf. nur unter sehr hohem Kostenaufwand möglich, das sollte bei der Sanierung von Altverkabelungen frühzeitig geprüft werden.

FEP wird wegen seiner Hitzebeständigkeit (Temperaturbereich bis 200 °C) vor allem in den USA als Ersatzstoff für PVC verwendet. Da dieses Material ebenfalls halogenhaltig ist, bleibt die Dioxin-Gefahr, und ein Einsatz dieses teuren Materials kommt in Deutschland zumeist nicht in Frage.

PUR zeichnet sich insbesondere durch hohe Abriebsfähigkeit und Ölbeständigkeit aus, eine Eigenschaft, die zwar selten im Backbone- oder Büro-Bereich benötigt wird, aber im Produktionsbereich inner-

halb von Maschinen- oder Schaltanlagen gefordert werden kann.

Brandeigenschaften

In Europa werden speziell für die Datentechnik im Inhouse-Bereich entwickelte halogenfreie und schwerentflammbare Kabel eingesetzt. Es sind im Markt zwei unterschiedliche Typen verfügbar, die jedoch beide unter dem Begriff **FRNC/LSOH** angeboten werden können. Da die Typen nicht gleichwertig sind, sollte bei der Planung der funktionelle Unterschied bekannt sein.

Basis Etylen-Vinyl-Acetat (EVA)

Kabel mit diesem Material (auch unter der Bezeichnung Copolymer geführt) erfüllen nicht nur die Brandtests mit einzelnen Kabeln sondern auch Bündelbrandtests.

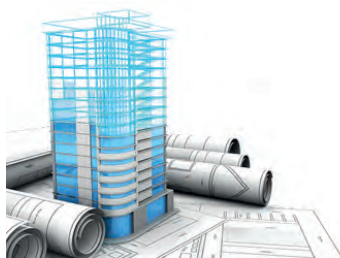
Basis Etylen-Ethyl-Acetat (EEA)

Kabel mit diesem Material erfüllen nur die Brandtests mit einzelnen Kabeln (Einzelbrandtest), keine Bündelbrandtests, dieses ist jedoch günstiger.

Es ist darauf hinzuweisen, dass einige Tests nur die Fähigkeit des Kabels beschreiben, einen Brand nicht fortzuleiten, ob das Kabel selbstverlöschend ist, wird dagegen nicht zwangsläufig geprüft. Weiter muss im Rahmen der Planung objektiv geprüft werden, ob man bei einer Glasfaserverkabelung mit so großen Kabelmengen rechnen wird, dass der Vorteil von EVA tatsächlich zum Tragen kommt, bei einer Fiber-To-The-Desk-Lösung wird dies sicher von Wichtigkeit sein, bei einzelnen Primär- und Sekundärleitungen wohl kaum.

Bei Unklarheit sollte in der Planungs- oder Ausschreibungsphase gegebenenfalls eine

Sonderveranstaltung



IT-Infrastrukturen für das Gebäude der Zukunft 17.10.2017 in Bonn

Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die gewerkübergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können. Diese Veranstaltung wendet sich

an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerkeübergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

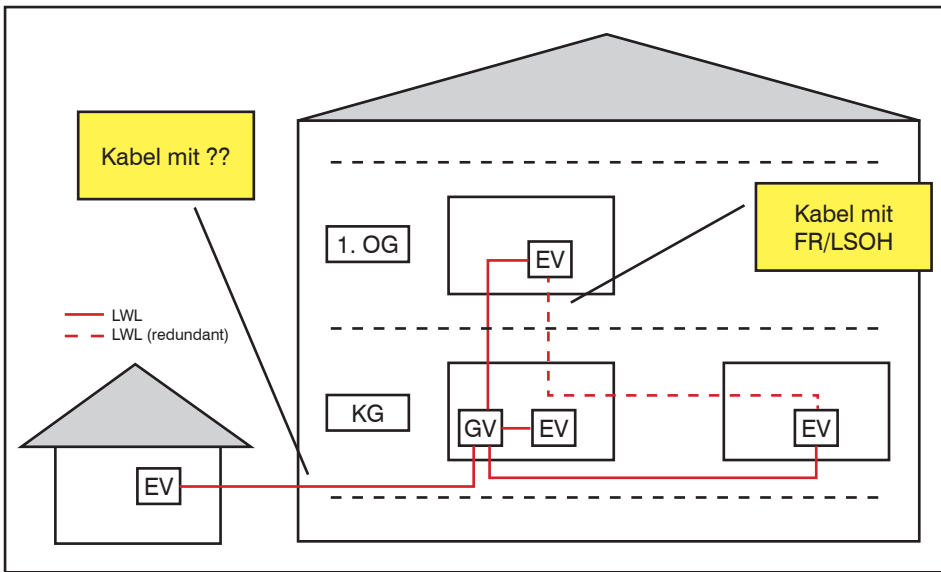


Abbildung 5: Schemadarstellung Primärverkabelung über Außenbereich

Prüfung der Brandeigenschaften erfolgen. Es ist zu beachten, dass eine Unterscheidung der beiden Materialien nicht anhand der DIN/VDE-0888-Kurzbezeichnung möglich ist, diese verwendet nur den Buchstaben „H“ für beide Varianten.

Ein klassisches, auch heute weiterhin sehr häufig eingesetztes Material, stellt **PE** dar. Dieses Material zeichnet sich durch seine hohe UV-Beständigkeit und Resistenz gegen Wassereintritt aus (z.B. werden die meisten hochwertigen Teichfolien aus PE hergestellt), PE ist prädestiniert als Mantelmaterial im Außenbereich. Der Einsatz von PE-Kabel wurde in den letzten Jahren in Fachkreisen in Frage gestellt, da bei größeren Kabel-Längen im Inhouse-Bereich, z.B. vom Gebäudeeintrittspunkt bis zum Verteiler dieses Kabel als potentielle Brandgefahr eingestuft wird. Im Falle eines Brandes besitzt PE keinen Schutz gegen Feuer, brennt relativ schnell und ist nicht selbstverlöschend.

Abbildung 5 verdeutlicht das daraus resultierende Problem: Im Inhouse-Bereich, also zumeist bei der Sekundärverkabelung, bieten sich Materialien an, die unter dem Aspekt des Brandschutzes besonders gut geeignet sind. Im Außenbereich versucht man zwischen den Gebäuden Kabel aus PE zu verwenden, insbesondere wenn eine direkte oder indirekte Erdverlegung unumgänglich ist. Was ist aber zu tun, wenn sich der GV nicht direkt am Eintrittspunkt des Außenkabels befindet, wenn das Kabel noch auf eine lange Strecke durch das Gebäude zu verlegen ist?

In den meisten Installationen, selbst im sensiblen Bereich wie öffentlichen Gebäuden, wird PE als bevorzugtes Mantelma-

terial zur gebäudeübergreifenden Verbindung vorgesehen, konkrete Vorschriften oder gesetzliche Vorgaben, die das verbieten, sind dem Autor nicht bekannt. Für den Fall, dass man auf PE im Gebäude verzichten will, gibt es drei Alternativen:

Alternative 1

Man verwendet so genannte „aufteilbare“ Kabel (DIN-Bezeichnung „AT“; nicht zu verwechseln mit den aufteilbaren Break-Out-Kabeln), die sowohl einen außenliegenden PE-Mantel haben, als auch darunterliegend einen Mantel aus anderem Material (in der Vergangenheit meist PVC, heute natürlich halogenfrei). Der PE-Mantel wird nach Gebäudeeintritt entfernt, das weiter verlegte Kabel liegt dann in PE-freier Version vor. Diese Technik wird heute kaum eingesetzt.

Alternative 2

Das PE-Außenkabel wird unmittelbar nach Gebäudeeintritt geschnitten und mit Hilfe einer Muffe an ein (z.B. schwer entflammables halogenfreies) Innenkabel gespleißt. Der notwendige Einsatz einer Muffe führt zu erhöhten Kosten, diese Alternative wird ebenfalls kaum eingesetzt.

Alternative 3

Einsatz von so genannten Universalkabeln. Dieser Kabeltyp wird häufig verwendet, häufig sind die Nachteile bzw. Risiken aber unbekannt. Das Kabelmaterial ist halogenfrei und flammwidrig (Einzelbrandtest) und bietet gleichzeitig einen „Grundschutz“ gegen Wassereintritt, es ist sowohl für den Innen- als auch für den Außeneinsatz geeignet. Viele Hersteller weisen jedoch darauf hin, dass von einer direkten Erdverlegung abgeraten wird, für diese Einsatzumgebung bietet man dann z.B. bei Le-

oni einen Typen mit zusätzlichem Metallschutz an. Bei den meisten Planungen ist jedoch unklar, ob man einen einigermaßen „wasserfreien“ Kabelweg im Außenbereich hat oder garantieren kann. Deshalb bleibt weiterhin im Gelände das herkömmliche PE-Außenkabel die sichere Variante.

Für den Fall, dass ein Kabel in einem dauernd mit Wasser gefüllten Kabelweg zu liegen kommt, muss der Einsatz von metallgeschützten Kabeln in Erwägung gezogen werden, inklusive der damit verbundenen Problematik einer galvanischen Verbindung von Gebäuden (Potentialverschleppung, Sicherstellung von Überspannungsschutz). Ein reines PE-Kabel bietet in derartigen Umgebungen letztendlich keinen zuverlässigen Schutz.

Aktuell wird derzeit darüber diskutiert, ob die seit dem 1. Juli 2017 verpflichtende Einhaltung der EN50575 auch eine Bedeutung für die Planung hat. Diese verpflichtende Einhaltung gilt zunächst nur für die Kabelhersteller und sie ermöglicht eine bessere vergleichende Beurteilung der Brandeigenschaften der Kabel. Dazu wurde eine Art von Code eingeführt, anhand dessen man diese Eigenschaften erkennen und vergleichend bewerten kann. Die Kabelindustrie bzw. deren Verband leitet in ihren Veröffentlichungen daraus Empfehlungen ab, welcher Kabeltyp wo sinnvoll einzusetzen ist. Beispielsweise wird in Fluchtwegen in Hochschulen empfohlen, nur Kabel vorzusehen, die der Euroklasse B2ca/s1/d1/a1 einzusetzen. Eine Einhaltung dieser Empfehlung ist nach aktuellem Stand keine Vorschrift. Nach Ansicht des Autors sollte das Leib und Wohl der Menschen so hohe Bedeutung haben, dass für den Fall eines Brandes präventiv das Beste getan werden wird, was technisch und in vertretbarem Aufwand machbar ist, deshalb ist eine Berücksichtigung der Empfehlungen letztendlich sinnvoll. Nachteilig ist, dass bei aktuellem Stand die Mehrkosten dieser zertifizierten Kabel doch sehr hoch sind (teilweise 30% teurer und mehr) und eine diesbezügliche Entscheidung nicht leicht macht; möglicherweise wird bei größeren produzierten Kabelmengen dieser höhere Materialpreis kurz- und mittelfristig noch deutlich fallen.

Nagetierschutz

Das Thema Nagetierschutz wird kontrovers diskutiert. Auf der einen Seite gibt es die Meinung, dass es letztendlich einen sicheren metallfreien Nagetierschutz nicht gibt. Auf der anderen Seite ist gerade die Metallfreiheit und die somit ausschließbaren galvanischen und elektromagnetischen Störmöglichkeiten ein besonderer Vorteil der Glasfaser mit metallfreiem Nagetierschutz. Ein weiteres Argument gegen me-

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

tallhaltige Wellmantel (statt z.B. Stahl- drahtarmierungen) stellt die Gefahr von bleibenden Dehnungen des Kabels nach Einzug dar, dies kann die bertragungseigenschaften des Lichtwellenleiters beeintrachtigen.

Um die erste Behauptung empirisch unterlegen zu knnen, msste es ein normiertes Prfverfahren geben. Dies ist nicht der Fall. Damit bleibt die Definition und Interpretation von „Nagetierschutz“ jedem selbst berlassen. In der Praxis hat sich jedoch gezeigt, dass der Nagetierbefra ein geringeres Risiko darstellt als zum Beispiel der berhmt Bagger oder gar ein Blitzschlag. Dies mag in bestimmten Umgebungen (z.B. Kabelverlegung in Hafennahe) aber auch anders sein. Wegen dieses fr die meisten Umgebungen doch geringen Nagetier-Risikos werden im Auenbereich zumeist Kabel mit metallfreiem Nagetierschutz verlegt, es gibt verschiedene metallfreie Nagetierschutzlsungen, die jedoch keine bemerkenswerten, objektiv nachprf- baren Unterschiede aufweisen. Bei der Planung empfiehlt sich aber im Auenbereich mindestens ein metallfreier Nagetierschutz.

Im Produktionsbereich werden zwischen den Verteilern immer hufiger bewahrte Kabel verlegt, zum einen wegen des hheren Nagetierrisikos und zum anderen, um dem Kabel eine hhere mechanische Robustheit gegenber den „harten“ Umweltbedingungen zu geben, man denke z.B. an die Nachverkabelung von armdicken Starkstromkabeln. Bei der Auswahl geeigneter Kabel wird man feststellen, dass nagetiergeschtzte Innenkabel eine Raritat sind, es werden zumeist gelfreie Auenkabel vorge- sehen (hier gut geeignet: Universalkabel).

Marktbersicht oder was sind die besten Kabel

Im Rahmen eines konkreten Projektes wurden konkrete Anforderungen an die Materialeigenschaften spezifiziert und an diverse Hersteller mit der Bitte um Nennung von dazu passenden Produkten und deren technischen Eigenschaften weitergereicht. Die im Artikel beigelegten Tabellen geben einen Teil der Ergebnisse wieder. Die Tabelle macht aber insbesondere folgendes deutlich:

- Es gibt nicht das beste Kabel oder den besten Hersteller.

- Es gibt sehr groe qualitative Unterschiede und der genaue Vergleich der „eigenen“ Anforderungen mit den angebotenen Kabeltypen sollte unbedingt vorgenommen werden.

- Einige Hersteller haben marktunbliche Derivate in ihrem Produktportfolio, welche herausragende Eigenschaften haben, die aber sehr untypisch fr diesen Kabeltyp sind, es lohnt sich als auch bei speziellen Anforderungen, gezielte Anfragen an die Hersteller zu richten.

Unbedingt zu empfehlen ist die genaue Spezifikation von konkreten und zum Einsatz passenden Anforderungen (z.B. konkrete Vorgabe der Zugfestigkeit in Newton). Die Definition eines Typs nur in Form von VDE0888-Abkrzungen (z.B. I-D(ZN) H) ist zu wenig, zu gro ist die Gefahr von extrem stark schwankenden Angebotspreisen oder gar einen ungeeigneten Typ angeboten zu bekommen. Die Spezifikation von sehr hohen Anforderungen sollte wohlbedacht vorgenommen werden, hufig stehen diese Anforderungen nicht im richtigen Verhaltnis zu dem tatsachlich bentigten Material und verteuern die Produkte extrem.

Auenkabel*	Huber+Suhner	Huber+Suhner	Leoni	Leoni	Nexans	Nexans	Nexans
Typ	W(ZNG)Y	BWSN(ZNG)V	KL-A-DQ(ZN)B2Y	KL-A-DQ(ZN)B2Y	LANmark-OF UG PE Black	LANmark-OF MG PE Black	LANmark-OF MicroBundle PE
verfgbare Faseranzahl	2 bis 24	24, 48, 72, 96, 144	2 bis 24	24 bis 144	2, 6, 12, 24	24, 36, 48, 144	12, 24, 36, 48, 144
Adertyp	Zentralader	Verseilt	Zentralader	Verseilt	Zentralader	Verseilt	Verseilt
Durchmesser [mm]	8,5	9,6	7,1	11,5	6,9	7,9	12,4
Zugfestigkeit wahrend Installation [N]	2000	9000	1750	4000	1800	2200	2200
Querdrukfestigkeit dauerhaft [N/cm]	120	600	150	300	200	100	400
Temperaturbereich [°C]	bei Verlegung	-10 bis 50 Grad	-10 bis 50 Grad	-5 bis 40 Grad	-10 bis 50 Grad	0 bis 50 Grad	0 bis 40 Grad
	im Betrieb	-40 bis 70 Grad	-40 bis 70 Grad	-25 bis 60 Grad	-40 bis 60 Grad	-30 bis 60 Grad	-30 bis 70 Grad
Mantelmaterial	PE	PE	PE	PE	PE	PE	PE
Metallfreier Nagetierschutz	Glass-Roving	Glass-Roving	Aramidgarn	Aramidgarn	Aramidgarn	Aramidgarn	Ja
Langs- und Querwasserschutz	Gelfrei	Gelfrei	Gel	Gel	Gel	Gel	Gel und Quellgarn
Erdverleger	Ja	Ja	Ja	Ja	Ja, in Sandbett mglich	Ja, in Sandbett mglich	Ja

Auenkabel*	Nexans	Eku-Kabel	Eku-Kabel	Eku-Kabel	Eku-Kabel
Typ	LANmark-OF MD PE/PE	A-DQ(ZN)B2Y	A-DQ(ZN)B2Y	I/A-DQ(ZN)BH (Maxibndel)	I/A-DQ(ZN)BH (Minibndel)
verfgbare Faseranzahl	24, 48, 72, 96	4, 6, 8, 12, 16, 24	24, 36, 48, 72, 144 (und mehr)	4, 6, 8, 12, 16, 24	24, 36, 48, 60, 72, 96, 144
Adertyp	Verseilt	Zentralader	Verseilt	Zentralader	Verseilt
Durchmesser [mm]	15,9	max. 8,6 mm	12,5 bis 16,8	7,8	10,2 bis 16,8
Zugfestigkeit wahrend Installation [N]	6000	1500 oder 2500	5000	1500	5000
Querdrukfestigkeit dauerhaft [N/cm]	600	??	??	??	??
Temperaturbereich [°C]	bei Verlegung	0 bis 40 Grad	-5 bis 40 Grad	-5 bis 40 Grad	-5 bis 50 Grad
	im Betrieb	-30 bis 70 Grad	-30 bis 60 Grad	-30 bis 60 Grad	-20 bis 60 Grad
Mantelmaterial	PE	PE	PE	LSZH	LSZH
Metallfreier Nagetierschutz	Ja	Glasgarn	Glasgarn	Glasgarn	Glasgarn
Langs- und Querwasserschutz	Gel und Quellgarn	Gel	Gelfrei	Gelfllung in der Ader	Gelfllung in der Ader
Erdverleger	Ja	Ja	Ja	Ja	Ja

* Angaben ohne Gewahr

Lichtwellenleiterkabel: Planung, Auswahl, Besonderheiten und Produktbeispiele

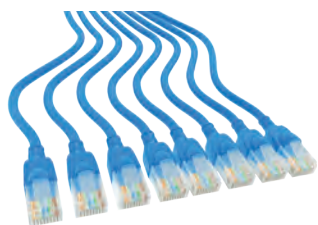
Innenkabel*	Huber+ Suhner	Huber+ Suhner	Leoni	Leoni	Nexans	Nexans	Nexans	Eku-Kabel	Eku-Kabel	
Typ	Q(ZNG)H	BWSN(ZNG)H	KL-U-DQ(ZN)BH	KL-U-DQ(ZN)BH	LANmark-OF microbundle LSZH	LANmark-OF microbundle LSZH	LANmark-OF microbundle PE	I/A-DQ(ZN)BH (Maxibündel)	I/A-DQ(ZN)BH (Minibündel)	
verfügbare Faseranzahl	2 bis 24	24 bis 144	bis 24	24, 48, 96, 144	4 bis 12	24 bis 96	12 bis 144	4, 6, 8, 12, 16, 24	24, 36, 48, 60, 72, 96, 144	
Adertyp	Zentralader	Verseilt	Zentralader	Verseilt	Zentralader	Verseilt	Verseilt	Zentralader	Verseilt	
Durchmesser [mm]	7,0	9,6 bis 13,5 mm	7,7	11,4 bis 17	6	7,2	12,4	7,8	10,2 bis 16,8	
Zugfestigkeit während Installation [N]	2000	9000	2500	4000	2200	2000	2200	1500	5000	
Querdrukfestigkeit dauerhaft [N/cm]	200	300	300	300	200	100	400	??	??	
Temperaturbereich [°C]	bei Verlegung	-10 bis 50 Grad	-10 bis 50 Grad	-5 bis 50 Grad	-5 bis 50 Grad	0 bis 40 Grad	0 bis 40 Grad	0 bis 40 Grad	-5 bis 50 Grad	-5 bis 50 Grad
	im Betrieb	-40 bis 70 Grad	-40 bis 70 Grad	-25 bis 60 Grad	-40 bis 60 Grad	-20 bis 60 Grad	-30 bis 60 Grad	-30 bis 70 Grad	-20 bis 60 Grad	-20 bis 60 Grad
Mantelmaterial	LSFH	LSFH	Halogenfrei und flammwidrig	Halogenfrei und flammwidrig	LSZH	LSZH	nein: PE	LSZH	LSZH	
Metallfreier Nagetierschutz	Glasroving	Glasroving	Aramid/ Glasroving	Glasroving	Ja	Ja	Ja	Glasgarn	Glasgarn	
Längs- und Querwasserschutz	Nein	Nein	Gelfüllung in der Ader	Gelfüllung in Ader und Verseilung	Gel (reduziert)	Nein?	Gel (reduziert)	Gelfüllung in der Ader	Gelfüllung in der Ader	
Erdverleger	Nein	Nein	in Sandbett möglich	in Sandbett möglich	Nein	Nein	Ja	Ja	Ja	

* Angaben ohne Gewähr

BreakOut*	Huber+ Suhner	Huber+ Suhner	Huber+ Suhner	Leoni	Leoni	Nexans	Eku-Kabel
Typ	Duplex Rund	Duplex Figure 0	OptiPack	KL-U-VQ(ZN)H	KL-I-V(ZN)H	LANmark-OF-Tight Buffer Universal	I-V(ZN)HH (Breakout)
verfügbare Faseranzahl	2,0	2,0	12, 24	6, 12, 24	2, 4, 6, 8, 10, 12	2 bis 24	2, 4, 8, 12, 24
Adertyp	Vollader	Kompakt, trocken	Vollader	Festader	Vollader	??	Kompaktader, trocken
Durchmesser [mm]	2,1	ca. 3 x 6	3 bis 3,6	5,9 bis 9,4	4,2 bis 7	5,3 bis 7,8	7 bis 15,1
Zugfestigkeit während Installation [N]	200	800	500	800	800	700 bis 1500	700 bis 1200
Querdrukfestigkeit dauerhaft [N/cm]	500	700	100	30	50	100	??
Temperaturbereich [°C]	bei Verlegung	-10 bis 50 Grad	-10 bis 50 Grad	-5 bis 50 Grad	-5 bis 50 Grad	0 bis 40 Grad	-5 bis 50 Grad
	im Betrieb	-20 bis 70 Grad	-20 bis 70 Grad	-20 bis 70 Grad	-20 bis 70 Grad	-10 bis 70 Grad	-25 bis 70 Grad
Mantelmaterial	LSFH	LSFH	LSFH	halogenfreier/ flammwiedriger Compund	halogenfreier/ flammwiedriger Compund	LSZH	LSZH

* Angaben ohne Gewähr

Seminar



Verkabelungssysteme für Lokale Netze 11.12. - 12.12.2017 in Bonn


Dieses Seminar erklärt praxisnah und herstellernerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen.



Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Neben der Erläuterung der aktuellen Normen wird die praktische Handhabung der Normungsvorgaben erklärt, wo macht eine Beachtung Sinn, wo nicht, wo ist es nicht ausreichend. Konkrete Durchführungen von Planungen in kleinen Übungsgruppen vertiefen die gewonnenen Erkenntnisse.

Referent: Dipl.-Ing. Hartmut Kell

Preis: 1.430,- € netto

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

Aktueller Kongress

ComConsult Technologie-Tage 2017

06.11. - 07.11.2017 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 06.11. bis 07.11.2017 ihren Kongress "ComConsult Technologie-Tage 2017" in Düsseldorf.

Die ComConsult Technologie-Tage 2017 wenden sich an Entscheider in Unternehmen und analysieren die Herausforderungen, denen sich IT-Infrastrukturen in den nächsten Jahren stellen müssen. Top-Experten der Branche beleuchten die Markt- und Technologie-Situation der nächsten Jahre und geben Empfehlungen für ein zukunftsorientiertes und sicheres IT-Fundament. Dieser Kongress evaluiert, welche Technologie-Bausteine aus welchen Bereichen im Moment wichtig sind und für die Planung und den Betrieb bekannt sein sollten.

Strategien für sichere Investitionen in IT-Infrastrukturen und Architekturen

Würde man heute ein Rechenzentrum oder ein Gebäude komplett neu ausstatten oder bauen, würde es sich deutlich von der Situation vor 5 Jahren unterscheiden. Skalierbarkeit und Wirtschaftlichkeit führen zu deutlich veränderten Schwerpunkten: der Wunsch, bestehende Kapazitäten schnell und preiswert in kürzester Zeit anpassen zu können, erfordert geeignete Architekturen über Technologie-Grenzen hinweg. Die Abgrenzung zur Cloud ist dabei ebenso eine treibende Kraft wie eine Chance. Zum einen haben Cloud-Rechenzentren Technologien und Architekturen marktreif und allgemein nutzbar gemacht, die es so vorher nicht gab. Zum anderen wird eine teilweise Integration von Cloud-Leistungen für die meisten Betreiber auf 5 Jahre gesehen unvermeidbar sein. Die Schlüsselfrage ist:



wie können Zukunfts-sichere Architekturen entwickelt werden, auf deren Basis mit hoher Sicherheit und Wirtschaftlichkeit investiert werden kann?

Fundamente im Technologie-Mix 2020

Die unvermeidbare Anpassung der IT-Architekturen positioniert die Basis-Technologien für Rechenzentren und das Gebäude der Zukunft neu. Zum einen gibt es Schwerpunktverlagerungen in Richtung Funk-Technologien, zum anderen erfordern moderne RZ-Architekturen eine Trennung von Netzwerk-Basis (Underlay) und Netzwerk-Nutzung (Overlay). In Summe führt dies zu einer veränderten Technologie-Auswahl für die nächsten Jahre. Gleichzeitig wird immer deutlicher, dass die Cloud als Leistungs-Baustein in einem Gesamtkonzept nicht fehlen darf. Cloud-Lösungen werden immer weniger als Gefahr für die Unternehmens-IT gesehen und bekommen immer mehr den Charakter

von extrem wichtigen Ergänzungs-Bausteinen zu einem wirtschaftlichen und flexiblen Gesamtbild. Als Ergänzung müssen sie aber sauber in die bestehende Landschaft integriert werden. Dies erfordert angemessene und wohl überlegte Technologie-Entscheidungen nicht nur auf der Seite der Cloud.

Sicherheits-Strategie 2020

Das Kernproblem aller Sicherheits-Lösungen ist die schnelle Anpassung an einen veränderten Bedarf. Skalierbarkeit im Technologie-Mix wird parallel zu einer Herausforderung für Sicherheit. Sowohl die Gefahren als auch die Lasten verändern sich in so hohen Geschwindigkeiten, dass eine statische Sicherheits-Lösung auf Dauer nicht den erforderlichen Grad an Sicherheit liefern wird. Auch im Sicherheits-Bereich brauchen wir ebenfalls eine erhebliche Skalierbarkeit, die im Rahmen eines Gesamtkonzepts flexibel mit dem Bedarf wachsen kann. Dabei spielen juristische Compliance-Fragen eine immer größere Rolle. Die bekannten Ransomware-Angriffe haben nachdrücklich gezeigt, dass sowohl eine geeignete technische als auch eine den juristischen Normen entsprechende Compliance-Lösung gefordert ist. In Kombination mit der Integration der Cloud und der Komplexität, die aus Entwicklungen wie Smart-Buildings entsteht, muss Sicherheit einmal wieder neu positioniert werden.

Hier setzen die ComConsult Technologie-Tage 2017 an: wir analysieren, wie Unternehmen und Behörden erfolgreich diese Herausforderungen bestehen können. Wir evaluieren, wie ein zukunftssicheres Technologie-Fundament aussehen kann.


Anmeldung an kundenservice@comconsult-research.de

ComConsult Technologie-Tage 2017

Ich buche den Kongress
ComConsult Technologie-Tage 2017

06.11. - 07.11.2017 in Düsseldorf
zum Preis von 1.990,- € 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 Technologie-Tage

Montag 06.11.17

Infrastruktur-Architekturen der Zukunft

9:30 Uhr

Keynote: Security by Design – Informationssicherheit als integraler Bestandteil der IT

- Cyber-Angriffe: Bedrohungen und mögliche Sicherheitsmaßnahmen
- Konsequenzen von Virtualisierung, SDN, SDDC, HCI, Container und Co. auf die Informationssicherheit
- Informationssicherheit in und aus der Cloud
- Smart Building, Smart Home, Smart Vehicle, Smart Factory, Smart ...: Warum die Sicherheit hier an Grenzen stößt?
- Umdenken ist erforderlich: Notwendigkeit von Security by Design

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 Uhr

IT-Infrastrukturen im Gebäude der Zukunft:

Bedarf, Potenziale und Gefahren

- Das Smart Building und die Auswirkung auf Infrastrukturen
- Beacon Technologien im Gebäude der Zukunft
- Das neue Gewerk IT-Security als Teil des Smart Buildings
- Vor- und Nachteil von Cloud-Diensten für Sensortechnik und BIM

Dipl.-Inform. Thomas Steil, ComConsult Beratung und Planung GmbH

11:15 Uhr Kaffeepause

11:45 Uhr

Azure kontra AWS: wer hat die bessere Cloud?

- Wie unterscheiden sich die Netzkomponenten und Designansätze von Microsoft und Amazon?
- Worauf ist bei der Auswahl der richtigen Cloud-Lösung zu achten?
- Kann man die Preise beider Anbieter miteinander vergleichen?
- Welche nativen Sicherheitsmechanismen bieten die Cloudprovider?
- Welche Verbindungsvarianten für Hybrid-Cloud-Lösungen existieren?

Markus Schaub, ComConsult Study.tv

12:30 Uhr Mittagspause

14:00 Uhr

High Performance Computing auf dem Weg zur unverzichtbaren Normalität für alle

- Technologiebausteine
- Anwendungen
- Planung

Dr. Markus Ermes, ComConsult Beratung und Planung GmbH

14:45 Uhr

Microsoft Office 365: Erfolgreiche Nutzung und Anforderungen an IT-Infrastrukturen

- Grundlagenentscheidungen: Nutzung der Office-365-Suite: Wer – Was – Wie; Lizenzmodelle; Anbindung an die Microsoft Cloud: Single Tenant vs. Multiple Tenants; Integration des Active Directory; Single Sign On
- Anforderungen an die IT-Infrastruktur: WAN-Anbindung: Bandbreite, Laufzeit, Übertragungsqualität; Tools zur Überprüfung der Netzqualität; Netzdesigns zur Anbindung von Niederlassungen; User Experience; Tuning Möglichkeiten
- Erfahrungen auf Kundenprojekten

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

15:30 Uhr Kaffeepause

16:00 Uhr

Sicherer und effizienter Einsatz von IOS im Unternehmen, was ändert sich durch iOS11?

- DEP, VPP, MDM
- Anwender-Features mit Produktivitäts-Potential
- Fallstricke der neuen iOS11-Version
- Was wird besser mit iOS11

Mark Zimmermann, Freier Experte

16:45 Uhr

Cybersecurity: aktuelle Rechtsfragen

- Datenschutzgrundverordnung - radikale Verschärfung des Datenschutzes
- Aktuelle Entwicklungen im Bereich der betrieblichen IT-Sicherheit
- Haftung der Unternehmensleitung bei Verstößen gegen die Informationssicherheit
- Eckpunkte einer Absicherung nur Umsetzung von IT/Compliance

Dr. Jan Byok, Bird & Bird LLP

Dienstag 07.11.17

Technologien der Zukunft

9:00 Uhr

Overlays im Campus-Netz

- Kommt das Overlay nun auch ins Campus-Netz?
- Grundsätzlichen Design-Annahmen und -Ideen für den Einsatz von Overlay-Strukturen?
- Beispielbetrachtung: Campus Fabric, SPBm und weitere

Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

9:45 Uhr

Software Defined Storage: Wird das traditionelle SAN überflüssig?

- Technologieübersicht - Virtualisierung bestehender Speichersysteme vs. Software Defined
- Storage Plattform auf Basis von Direct Attached Storage
- Skalierbarkeit, Management und Leistungsgrenzen
- Anwendungsszenarien

Dr. Stefan Muthmann, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

11:00 Uhr

Das Fax ist tot, aber was tritt an seine Stelle?

- Modemtechnologie in Zeiten von IP: T.30 G.711 inband Übertragung; T.37 asymmetrisches Verfahren über IP; T.38 symmetrisch Variante über IP
- Aufbau einer T.30 und einer T.38 Übertragung: Wo liegen die Probleme? (Endgerätesituation; Gateways; Was machen die SIP-Trunk / VoIP-Provider?)
- Alternative Verfahren: Was ist EDI?; Was sind digitale Signaturen? (Software Anbieter im Vergleich); Vorteile und Verfahren

Markus Geller, ComConsult Research GmbH

11:45 Uhr

WLAN, Mobilfunk und andere Funktechniken - gegenseitige Ergänzung oder Störfaktor?

- Die Grenzen des WLAN und neue Ideen zu deren Überwindung
- WLAN Offload und Konsequenzen für Betreiber
- Muss man Funkdienste gegeneinander abschirmen?
- Freiheit von Störungen sicherstellen: Funkfrequenzkataster
- Gesundheitsrisiko Funk? Muss man am Ende den Menschen abschirmen?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 Uhr Mittagspause

14:00 Uhr

5G: Basis für Mobilität, Disruption und Agilität

- Anforderungen moderner Anwendungsbereiche z.B. AR, VR, IoT, autonomes Fahren
- Entwicklung der Mobilfunktechnologie von LTE über LTE Advanced zu 5G
- Neue Konzepte für Small Cells, mögliche Konflikte zu WLANs, Fog Computing
- Ergebnisse aus den Feldversuchen von AT&T, Verizon, Nokia, CCI und anderen
- Die Standardisierung beginnt 2018. Was bringt die erste Welle?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:45 Uhr

Sind die Tage der Netzneutralität gezählt?

- Was ist Netzneutralität?
- Sind die Tage der Netzneutralität gezählt?
- Auswirkungen auf Verbraucher
- Auswirkungen auf Unternehmen
- Funktioniert die Priorisierung?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 Uhr

Herausforderung Informationssicherheit für das Gebäude der Zukunft

- Schadsoftware, Krypto-Trojaner, zielgerichtete Angriffe, Desinformation und (Distributed) Denial of Service: Bedrohungen der IT im Gebäude der Zukunft
- Welche Informationssicherheitsstandards sind für Smart Buildings relevant?
- Absicherungen von Smart Buildings mit IEC 62443
- Zonenkonzepte, mandantenfähige Infrastrukturen und Netzzugangskontrolle: Brauchen wir das wirklich?
- Absicherung von Funknetzen, Anbindung von Smartphones und Tablets: Alles wie gehabt?
- Wo sich Internetanbindung und DMZs im Smart Building vom Rest der Welt unterscheiden
- Ohne Cloud kein Smart Building: Sichere Cloud-Dienste und sichere Cloud-Nutzung für Nutzer und Betreiber
- Security by Design: Standardisierte Bausteine als Basis

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

Fortsetzung von Seite 1



M.Sc. Daniela Gies ist als Beraterin bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft beschäftigt sie sich besonders mit Sicherheitskonzeptionen nach ISO 27001 und BSI IT-Grundschutz und deren Umsetzung.



Dipl.-Inform. Thomas Steil ist bei der ComConsult Beratung und Planung GmbH für die konzeptionelle Planung in den Bereichen Netze und IT-Infrastruktur zuständig. Neben seiner Tätigkeit als Berater und Projektleiter ist er Autor diverser deutscher und englischsprachiger Artikel.

In der Praxis bedeutet dies erst einmal, dass unzählige Sensoren, Aktoren und IT-Anwendungen miteinander kommunizieren. Das reicht von Heizung, Klima, Beleuchtung, Zugangskontrolle, Überwachung bis zur Versorgung des Arbeitsplatzes. Da die Kaffeemaschine in einem modernen Bürogebäude mit der Lohnbuchhaltung kommuniziert, um den getrunkenen Kaffee direkt vom nächsten Gehalt abzuziehen und der Teppich plötzlich einem Gast den Weg zum richtigen Besprechungsraum leuchtet und damit zusätzlich die Funktion einer Beleuchtung oder Digital Signage Lösung erfüllt, steht der IT-Planer plötzlich vor der Frage, ob er die IP-Adresse des Teppichs logisch im Netz der Beleuchtung platzieren sollte und welche Firewall-Regeln zwischen der Kaffee-Maschine und der zentralen SAP-Datenbank einzurichten sind. Klingt absurd, ist aber Realität.

Wenn diese Fragen erst zum Zeitpunkt der Inbetriebnahme geklärt werden, ist bei der Planung im Vorfeld sicher schon viel schiefgelaufen. Die Wahrscheinlichkeit hierfür ist hoch, denn noch immer planen die verschiedenen Gewerke isoliert voneinander, obwohl sie im Endeffekt alle auf dieselbe Ressource, IT-Infrastruktur, angewiesen sind. Dies gilt für das Energieleitsystem, die Beleuchtung, die Medientechnik, die Arbeitsplätze und Besprechungsräume, das Besucherleitsystem, die Parkraumverwaltung, die Telefonie, die Videoüberwachung, die Zugangskontrolle, die Steuerung der Aufzüge, Wartungszugänge und viele weitere Systeme und Funktionen im Gebäude.

Hinzu kommt noch der ganz entscheidende Aspekt der IT-Sicherheit. Szenarien, die noch vor ein paar Jahren als Science-Fiction abgetan wurden, sind heute bereits bittere Realität. Zu Zeiten von Hackerangriffen, wie auf den Bundestag [1] oder durch Sicherheitsexperten auf einen fahrenden Jeep [2] und Ransomware kann auch ein modernes Gebäude ein lukratives Ziel von Angriffen werden. Blamabel, wenn durch die Lautsprecheranlage der neueste Megahit ertönt und die Beleuchtung im Takt blinkt. Unvorstellbar was passieren würde, wenn ein Angreifer die Türen elektronisch verriegeln und gleichzeitig einen Feueralarm auslöst [3].

Daher ist die IT-Sicherheit eines der zentralen Themen bei der Planung eines modernen Gebäudes. Die damit verbundenen Fragestellungen erstrecken sich auf die gesamte aktive und passive Infrastruktur und die verwendeten Übertragungstechniken.

Stand der Technik

In einem modernen Gebäude gibt es aktuell eine Vielzahl von Netzwerkbereichen, die eigene Hardware, proprietäre Protokolle und eigene Steckerverbindungen nutzen. Dabei kann die Zahl der verwendeten Protokolle in den Bereichen Gebäudeautomation, Fördertechnik, Zutrittskontrolle, Beleuchtung, Parkanlage usw. ohne weiteres einen hohen zweistelligen Wert erreichen. Dazu kommen dann noch die Kommunikationsbeziehungen der Bereiche untereinander, die abgesehen von der technischen Machbarkeit

auch Fragen der Sicherheit aufwerfen. Es ist zwar bequem, wenn der Mitarbeiter den Kaffee mit seiner persönlichen Karte bezahlen kann und ihm der Betrag direkt vom Lohn abgezogen wird. Aber will man wirklich, dass, wie eingangs erwähnt, die Kaffeemaschine dazu mit der Lohnbuchhaltung, einem kritischen Bereich mit hohen Sicherheitsanforderungen, direkt kommuniziert? Die Technik lässt dies zu und der Wunsch nach Bequemlichkeit lässt die Anforderungen entstehen, die dann von moderner IT-Infrastruktur ermöglicht werden sollen.

Bei der Auswahl der Firewalls beispielsweise sind die unterschiedlichen Protokolle der Gebäudetechnik zu berücksichtigen. Was bringt eine Firewall, die nur einige Bereiche schützen kann, wenn andere, kritische Netzbereiche nicht geschützt werden können?

Sicherheitsanforderungen an das Netz

Im Rahmen der sicherheitstechnischen Konzeptionierung eines Netzes für die Gebäudetechnik sollten bedarfsgerecht verschiedene Sicherheitsniveaus zum Beispiel Standard und hoch betrachtet werden, wobei weitestgehend hoher Schutzbedarf der Systeme hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit bestehen wird. Aufgrund der unterschiedlichen Kritikalität hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit werden daher an die unterschiedlichen Anbindungen auch unterschiedliche Anforderungen gestellt, um dem gegebenen Schutzbedarf zu entsprechen.

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

In das Sicherheitskonzept müssen die spezifischen Anforderungen und Vorgaben der Gebäudetechnik mit aufgenommen werden. Dabei ist es wesentlich, die spezifischen Anforderungen zu ermitteln, beispielsweise aufgrund der eingesetzten Komponenten. Insbesondere die Kommunikationsbeziehungen der eingesetzten Netz- und Anwendungsprotokolle sowie der Zugriffsmöglichkeiten über Außenbindungen sollten darin enthalten sein. Soweit technisch möglich, sind natürlich sichere Protokolle einzusetzen. Aber dies kann schnell unmöglich werden, wenn Hardwarekomponenten in das Gebäudetznetz integriert werden, die nur einem veralteten oder unsicheren Standard entsprechen und keine Möglichkeit zum Update bieten. Sollte es daher nicht möglich sein, sind solche Komponenten netztechnisch so weit wie möglich zu separieren. Wenn ein System kompromittiert wird, so soll der Schaden einen möglichst kleinen Bereich betreffen und die Auswirkungen minimal bleiben. Das Konzept muss kontinuierlich gepflegt und regelmäßig aktualisiert werden. Insbesondere müssen die Vorgaben allen verantwortlichen Mitarbeitern bekannt sein. Dass dies nicht immer einfach zu realisieren ist, sollte jedem bekannt vorkommen. Eine erstellte Dokumentation wird selten gepflegt, da das Wissen mit den Mitarbeitern mitwächst und die Zeit für die Pflege mutmaßlich nicht ausreicht. Der veraltete Zustand fällt meist erst neuen Mitarbeitern auf, die dann vor einem Berg nutzlosem Papier stehen und kein Wissen mehr daraus erlangen können. Es muss also ein Prozess geschaffen werden, der die Pflege der Dokumente mit möglichst geringem Arbeitsaufwand ermöglicht und somit die Mitarbeiter motiviert, dies auch zu tun. Dieses Konzept sollte aber auch die Anforderungen an das Netz der Gebäudetechnik, zum Beispiel hinsichtlich der zu trennenden Netzbereiche und Nutzergruppen sowie der grundsätzlichen Absicherung von Zugriffen und der Netzzugangskontrolle enthalten.

Dabei kommt der Dimensionierung der Netz- und Sicherheitskomponenten und Übertragungsstrecken sowie den Redundanz- und Redundanzmechanismen für die Kommunikationswege eine entscheidende Rolle zu. Denn IoT-Geräte und -Sensoren senden oftmals häufig kleine Datenmengen mit einer hohen Frequenz. Vibrationssensoren, die 1000 Messwerte pro Sekunde ins Netz pumpen, sorgen schnell dafür, dass die Netzauslastung steigt, obwohl die Netto-Datenmenge gering ist. Hier bieten Hersteller mittlerweile Produkte wie Switches und Router an, die diese Messwerte selbstständig aggregieren und dann nur einen Mittelwert pro Sekunde ins Netz schicken.

Darüber hinaus sollte die sichere Administration und Überwachung sowie die systemübergreifende Protokollierung Teil dieses Konzepts oder untergeordneter Konzepte sein.

Grundlegende Voraussetzung für einen dauerhaft sicheren Betrieb ist die Klassifizierung der Daten und Systeme entsprechend der Sicherheitsniveaus hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit.

Schützenswerte Daten müssen immer über sichere Protokolle übertragen werden, falls über eingeschränkt vertrauenswürdige Netze kommuniziert wird. Wenn sichere Protokolle nicht genutzt werden können, muss zumindest über zusätzliche Mechanismen angemessen verschlüsselt und authentisiert werden.

Wenn man sich diese Minimalanforderungen ansieht, erkennt man, dass jede Netzimplementierung auf einer geeigneten, vollständigen und nachvollziehbaren Planung basieren muss. Diese Planung muss bei Erweiterungen fortgeschrieben werden. Da sind wir wieder bei der Dokumentation! Gerade wenn, wie bei „smarten“ Gebäuden nicht auf best practices zurückgegriffen werden kann, ist die Dokumentation unabdingbar.

Die Spezifikation von Netzarchitektur und Netzdesign muss dabei alle Netzbereiche der Gebäudetechnik umfassen. Das bedeutet, dass die Netzarchitektur für die Außenbindungen, inklusive Remote Wartung und Firewall-Architekturen sowie die Übergänge zum allgemeinen Netz berücksichtigt werden müssen. Darüber hinaus sind DMZ-Design, Festlegungen an welchen Stellen des Netzes welche Si-

cherheitskomponenten zu platzieren sind und welche Sicherheitsfunktionen diese realisieren müssen, zu spezifizieren. Zusätzlich ist die Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur auch im Netzbereich der Gebäudetechnik zu spezifizieren. Hierbei sind insbesondere die Zonierung sowie die Übergangspunkte der Netze sowie gegebenenfalls gemeinsam genutzte Netzbereiche festzulegen.

In der Notfallplanung und den abgeleiteten Konzepten sind insbesondere die Gebäudetechnik und die zugrundeliegende Netzarchitektur und Netzdesign zu berücksichtigen. Dies muss regelmäßig überprüft werden.

Für die Gebäudetechnik sollte ein Netz mit eigener Hardware vorhanden sein, d. h. es werden dedizierte Komponenten für das Netz Gebäudetechnik realisiert. Das treibt natürlich den Preis und die Betriebskosten nach oben, ist aber nicht zu vermeiden, wenn man Wert auf die Sicherheit des Gebäudes legt. Jegliche Kommunikation von anderen Netzen, wie dem internen Netz der Nutzer oder auch dem Internet mit dem Netz der Gebäudetechnik muss dann über eine Firewall abgesichert und der Zugriff entkoppelt werden.

Sollte die Gebäudetechnik auf das WLAN des Gebäudes angewiesen sein, ist dies mit Mitteln der logischen Trennung, wie zum Beispiel VLANs, vom übrigen WLAN zu trennen.

Das Netz Gebäudetechnik ist entsprechend den unterschiedlichen Funktionsgruppen, beispielsweise Fördertechnik,

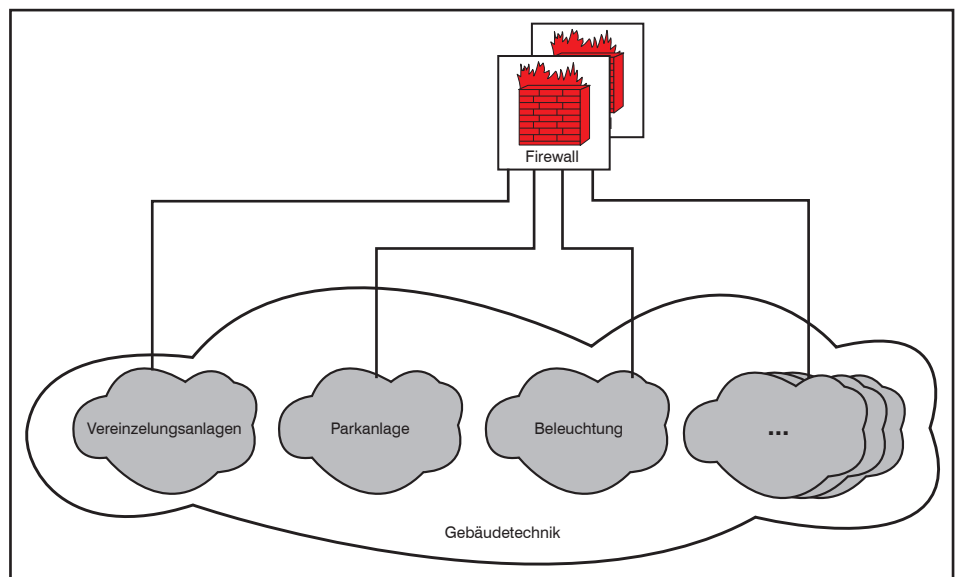


Abbildung 1: Segmentierung des Netzes Gebäudetechnik entsprechend den Funktionsgruppen

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

Parkanlage und Beleuchtung in logische Teilnetze zu trennen, siehe beispielhaft Abbildung 1. Die logischen Teilnetze werden im Folgenden auch Segmente genannt. Diese Segmente sollten so klein wie möglich realisiert werden, um im Fall eines erfolgreichen Angriffs auf eine Komponente den Schaden einzugrenzen und einen Zugriff auf andere Bereiche zu erschweren. Dabei ist die Kommunikation zwischen diesen Segmenten über eine Firewall geeignet abzusichern.

Auch sollte dokumentiert werden, wenn ein Segment ein hohes Sicherheitsniveau hat oder eine erhöhte Schwachstelle darstellt und daher gesondert abgesichert werden muss.

Clients und Server sind in unterschiedlichen Segmenten zu platzieren. Die Kommunikation zwischen diesen Segmenten muss mindestens durch eine Firewall kontrolliert werden.

Systeme, die eine Platzierung von Clients und Servern in einem gemeinsamen Sicherheitssegment erfordern, sind als Ausnahmen explizit system- bzw. anwendungsspezifisch zu regeln.

Die Segmentierung des Netzes Gebäudetechnik ist im Netzkonzept zu erfassen und zu pflegen. Es beschreibt, welche Segmente initial angelegt werden und welche Vorgaben es für die Schaffung weiterer Segmente und ihrer Positionierung gibt. Darüber hinaus muss in dem Segmentierungskonzept die Netzzugangskontrolle für Sicherheitssegmente mit Clients sowie die Positionierung von Endgeräten (dual-homed systems), die mehrere Segmente bedienen, festgelegt werden. Dabei sollten soweit möglich für diese Systeme spezifische Segmente angelegt werden.

Server, die grundlegende Dienste für mehrere Segmente bereitstellen, werden in einem dedizierten Segment positioniert und die Kommunikation durch eine Firewall kontrolliert. Dies betrifft auch allgemeine Netzdienste der Gebäudetechnik, z.B. NTP oder Verzeichnisdienste.

Absicherung der Anbindung und Zugriffe

Es ist eine zweistufige Firewall-Architektur für die Anbindung an das Internet zu realisieren. Zwischen den beiden Firewall-Stu-

fen, die physisch getrennt werden, sind Sicherheits-Proxies oder Application Layer Gateways (ALG) zu realisieren, die über Transferetze dual-homed zur äußeren Firewall und zur internen Firewall angebunden werden (Entkopplung der Kommunikation). Außer den Firewalls und Sicherheits-Proxies dürfen keine weiteren Systeme in diesen Transferetzen integriert werden. Es darf kein Transportnetz konfiguriert werden, das beide Firewall-Stufen direkt miteinander verbindet. Diese Struktur wird im Folgenden auch P-A-P-Struktur (Paketfilter, Application Layer Gateway, Paketfilter) genannt und ist in Abbildung 2 dargestellt.

Von nicht oder nur eingeschränkt vertrauenswürdigen Netzen darf nicht direkt via IP auf Systeme im internen Netz zugegriffen werden. In der zweistufigen Firewall-Architektur muss jeglicher eingehende und ausgehende Datenverkehr durch die äußere bzw. die innere Firewall kontrolliert und gefiltert werden. Der Sicherheits-Proxy muss, soweit technisch möglich, jeden Datenverkehr entkoppeln und die Firewalls müssen die Datenflüsse in das interne Netz auf die benötigten Protokolle und Kommunikationspartner einschränken. So sollten in Richtung eines Segmentes, in dem keine Komponente via BAC-Net kommuniziert, keine solche Kommunikation zugelassen werden.

Internet-Anbindung und Anbindung von Cloud-Diensten

Da immer mehr Komponenten eines modernen Gebäudes auf Cloud-Dienste außerhalb des eigentlichen Gebäudes angewiesen sind, ist die Internetanbindung vollständig redundant zu gestalten, um den Verfügbarkeit zu gewährleisten. Dazu sind mindestens zwei Anbindungen an unterschiedliche Internetdiensteanbieter nötig. Diese Anbindungen sind dabei möglichst wegedundant innerhalb und außerhalb der eigenen Zuständigkeit zu realisieren. Durch die Vermeidung dieses Single Point of Failure (SPoF) kann man die Chance geringhalten, dass ein Bagger aus Versehen beide Internetleitungen kappt.

Die physische Sicherheit der Internetanbindung ist aber nur ein Baustein eines sicheren Gebäudes, denn die Internet-Anbindung ist zusätzlich mit einem Schutz vor (D)DoS-Angriffen zu versehen. Für Massenangriffe kann dies durch eine spezielle Infrastruktur des Internet Service Providers oder eines Dienstleisters erfolgen. Zur gezielten (D)DoS-Abwehr ist per Bandbreitenmanagement die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und Protokollen aufzuteilen.

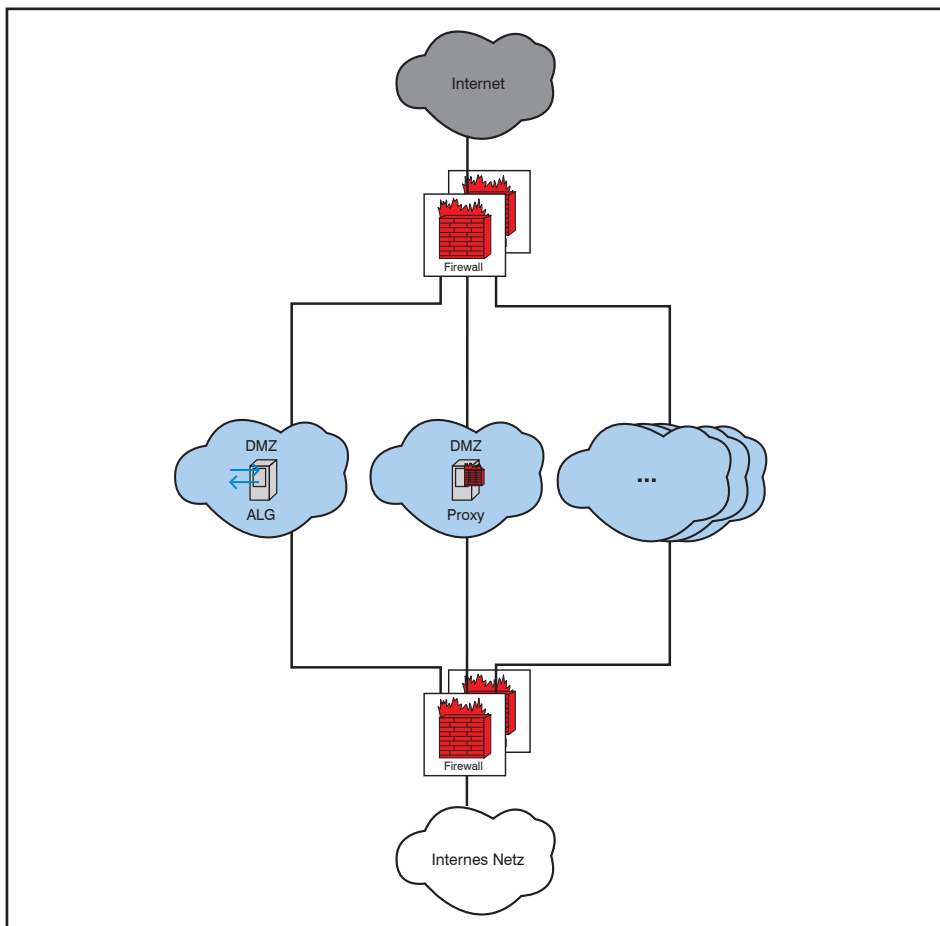


Abbildung 2: Beispielhafte P-A-P Struktur

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

Für jeden Dienst der Gebäudetechnik, der aus dem Internet erreichbar ist, muss eine DMZ eingerichtet werden. Für die Realisierung der DMZ muss unter Berücksichtigung der allgemeinen Konzepte und Anforderungsspezifikationen ein Konzept zur DMZ-Segmentierung erstellt werden.

Jede eingehende und ausgehende Kommunikation von internen Komponenten mit dem Internet muss in einer dedizierten DMZ über einen Sprung-Server entkoppelt und Zugriffe hinreichend authentisiert werden. Sollte die Verbindung nicht vertrauenswürdig sein, sollten immer auch VPN-Techniken zur Verschlüsselung zum Einsatz kommen.

Der Schutzbedarf der Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit ist zu bestimmen. Abhängig von der Kritikalität der Verfügbarkeit des Cloud-Dienstes oder des Schutzbedarfs hinsichtlich Vertraulichkeit oder Integrität der übertragenen Daten sind für diese Cloud-spezifische Anforderungen zu definieren.

Einige Cloud-Dienste setzen lokal in den Gebäuden ein Gateway ein, das einerseits die Verbindung über das Internet aufbaut und andererseits Dienste im Netz der Gebäudetechnik steuert. Beim Einsatz eines solchen Gateways ist jegliche Kommunikation des Gateways nach außen durch eine Firewall abzusichern. Die Kommunikation des Gateways Richtung Netz der Gebäudetechnik ist ebenfalls durch eine Firewall abzusichern und die Zugriffe müssen über einen Sprungserver entkoppelt werden. Ist eine Entkopplung des Zugriffes nicht möglich, so ist eine dedizierte Sicherheitsbetrachtung durchzuführen.

Remote-Zugriffe für Wartungs- und Administrationsaufgaben

Für Systeme in bestimmten Netzsegmenten ist ein Remote-Zugriff für Wartungs- und Administrationsaufgaben notwendig. Diese Netzsegmente sind in der Planung zu bestimmen. Die Anbindung erfolgt über das Internet, siehe auch Abbildung 3. Diese Zugriffe müssen mindestens mittels einer zweifaktor-Authentisierung und über verschlüsselte und authentisierte Tunnel abgesichert erfolgen. Sofern technisch möglich, sind direkte Durchgriffe in das Netz Gebäudetechnik zu verhindern und über einen Sprungserver zu entkoppeln und die Kommunikation über eine eigene Firewall zu kontrollieren. Die Zugriffsrechte und -möglichkeiten sind, insbesondere wenn eine Entkopplung nicht möglich ist, soweit wie möglich einzuschränken.

Abbildung 3 zeigt schematisch die Anbindung eines Dienstleisters für administrative sowie Wartungszugriffe. Solche

Zugriffe sind nur durch hinreichend vertrauenswürdige Dienstleister zuzulassen.

Für die Authentisierung von Zugriffen sind dem Schutzbedarf entsprechende Authentisierungsmethoden einzusetzen.

Nutzer müssen eindeutig identifiziert und authentisiert werden. Über nicht vertrauenswürdige Netze (Nutzer-Authentisierung) ist eine Multifaktor-Authentisierung erforderlich. Darüber hinaus kann bei hohem Schutzbedarf der entsprechenden Systeme für Zugriffe über nicht vertrauenswürdige Netze eine vorherige Genehmigung der Anmeldung gefordert werden.

Ebenso sind Software-Prozesse und Geräte (Maschinen-Authentisierung) eindeutig zu identifizieren und authentisieren.

Entsprechend des Schutzbedarfs der Systeme ist beim Einsatz von Passwörtern zur Authentisierung die Stärke der Passwörter (hinsichtlich Lebensdauer und Komplexität) festzulegen. Gegebenenfalls sind weitere Maßnahmen, wie der Einsatz von PKI-Zertifikaten, vorzuziehen.

Erfolgreiche Authentisierungsversuche sind festzuhalten und nachzuverfolgen, um Anomalien feststellen zu können.

Der Zugang von Endgeräten zu den Funktionsbereichen (Segmenten) des Netzes der Gebäudetechnik ist zu kontrollieren und zu authentisieren.

Geeignete Auswahl der Cloud-Dienste

Grundvoraussetzung an einen Anbieter eines Cloud-Dienstes ist der Nachweis eines effektiven, vollumfänglichen und nachhaltigen Managements der Informationssicherheit (Information Security Management System, ISMS). Ein solcher Nachweis kann über die Zertifizierung des Anbieters hinsichtlich der genutzten Dienste nach ISO 27001, ISO 27001 auf Basis von IT-Grundschutz oder einem vergleichbaren etablierten Standard erfolgen.

Darüber hinaus sollte der Anbieter über eine Zertifizierung nach ISO 27017 „Code of practice for information security controls based on ISO/IEC 27002 for cloud services“ verfügen. Alternativ kann eine

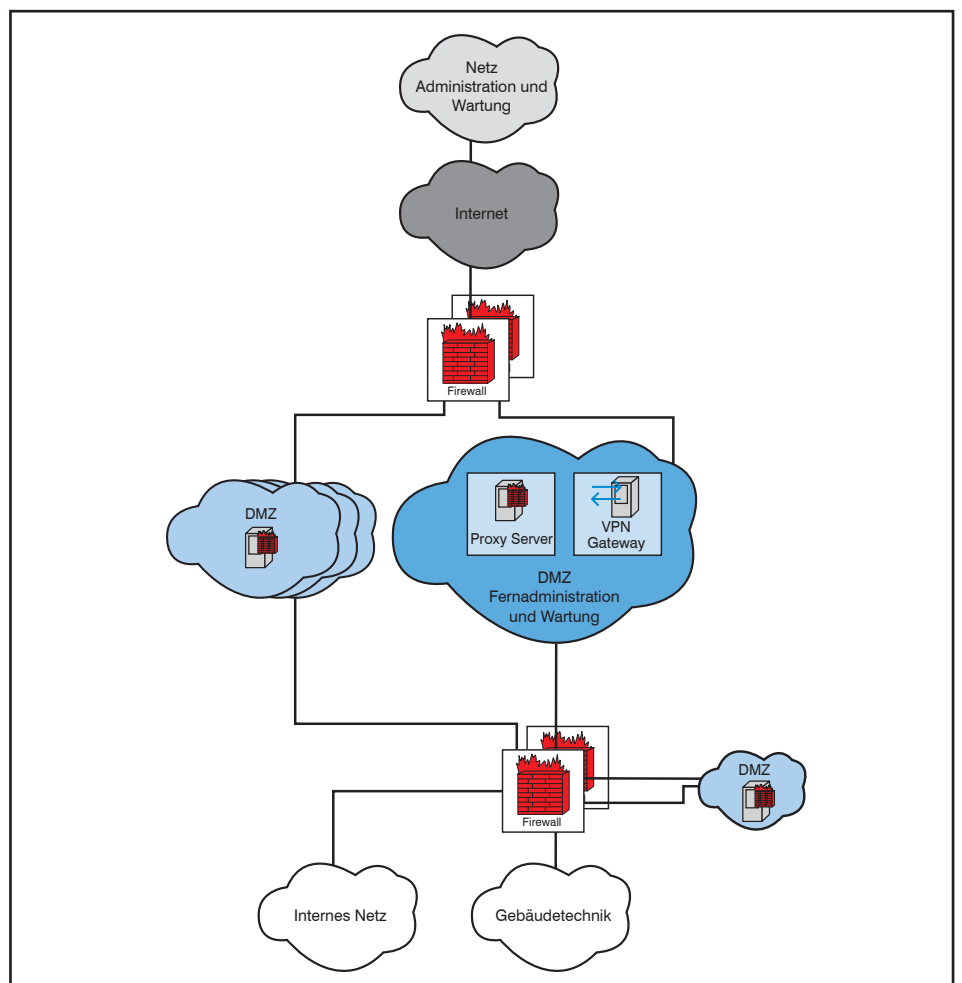


Abbildung 3: Remote-Zugriffe für Wartung und Administration

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

vergleichbare Cloud-spezifische Zertifizierung durch den Cloud-Anbieter nachgewiesen werden, z.B. gemäß Cloud Security Alliance (CSA).

Zusätzlich sollte bei einem hohen Schutzbedarf eines Cloud-Dienstes (wie dem Cloud Sever) die Einhaltung der Anforderungen aus dem „Anforderungskatalog Cloud Computing (C5) - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“ des BSI durch den Dienstleister, zum Beispiel durch einen Wirtschaftsprüferbericht, nachgewiesen werden.

Bei der Auswahl des Cloud-Anbieters sind abhängig von der Art des Cloud-Dienstes und den zugehörigen Anforderungen ggf. weitere Standards zu berücksichtigen. Werden zum Beispiel personenbezogene Daten in der Cloud verarbeitet, ist ISO 27018 „Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors“ anzuwenden.

Nutzt ein Cloud-Anbieter für die Bereitstellung des Cloud-Dienstes wiederum Cloud-Dienste eines anderen Cloud-Anbieters, muss die so entstehende Kette hinsichtlich der Forderung von den oben genannten Nachweisen und Zertifizierungen vollständig berücksichtigt werden.

Dieses Vorgehen ist weit verbreitet, da viele Cloud-Dienstleister Softwareentwickler sind, die Rechenleistung und Speicherkapazität wiederum als Cloud-Dienstleistung einkaufen.

Webanwendungen und Webservices müssen nach Stand der Technik (z.B. entsprechend OWASP) entwickelt, getestet und betrieben werden. Insbesondere müssen Webanwendungen und Webservices über eine 3-Tier-Architektur realisiert werden.

Auf jeden eingesetzten Cloud-Dienst sind die Bausteine und die damit verbundenen Maßnahmen der BSI IT-Grundschutz-Kataloge [4] B 1.17 Cloud-Nutzung sowie B 1.11 Outsourcing relevant und insofern anzuwenden. Für die Absicherung der Verbindungen des Cloud-Dienstes über entsprechende APIs ist der Baustein B 5.24 Web-Services anzuwenden. Im Rahmen der Grundschutzmodernisierung [5] entstehen Aktualisierungen und weitergehende Bausteine und Maßnahmen, die für Bereich Smart Building relevant sind.

Protokollvielfalt in Smart Buildings

Die am häufigsten anzutreffenden Protokolle sind WLAN, ZigBee, Z-Wave, BACnet und neuerdings auch immer öfter EnOcean. Im Folgenden stellen wir kurz einige

eingesetzte Protokolle unter dem Aspekt Sicherheit vor.

Funk-basierte Kommunikation ist immer mittels sicherer Protokolle zu übertragen oder mittels geeigneter kryptographischer Verfahren abzusichern. Sofern dies nicht möglich ist, weil beispielsweise die genutzten Protokolle, wie Bluetooth Low Energy (BLE), keine Verschlüsselung unterstützen, muss je nach Anwendungsfall entschieden werden.

Bereits in der Planungsphase ist ein Funkfrequenz-Kataster zu erstellen, in dem ein Verzeichnis aller genutzten, auf Funktechnik basierenden Applikationen enthalten ist und für die verschiedenen Frequenzen der Primärnutzer festgelegt wird. Zudem ist das Potential für Konflikte und gegebenenfalls folgende Störungen der Kommunikation zu untersuchen, siehe auch Abbildung 4. Weiterhin ist zu beachten, welche Störungen der Funkfrequenz von außen bzw. von innen zu Beeinträchtigungen oder gar Ausfällen der Kommunikation führen können und wie diese aussehen würden. Hierzu ist in der Planung eine Risikoanalyse durchzuführen.

Die WLAN-Infrastruktur sollte Controllerbasiert aufgebaut und vom restlichen Netz durch eine Firewall getrennt werden und nur in Ausnahmefällen sollte die WLAN-Infrastruktur Bestandteil der Gebäudetechnik sein. Besser ist ein physisch separiertes Teilnetz der Gebäudetechnik einzuplanen. Dies treibt die Kosten aber nach oben. Daher sollten die Kosten von Firewall und separater WLAN-Hardware einer genauen Risikobetrachtung unterzogen werden.

Die WLAN-Kommunikation der Gebäudetechnik muss jedoch als eigener Mandant im WLAN realisiert werden. Gegebenenfalls sind für das WLAN der Gebäudetechnik mehrere Mandanten für einzelne zu separierende Funktionsbereiche zu realisieren. Am WLAN-Controller wird die Mandanten-Kommunikation nur in dafür vorgesehenen Segmente übertragen, sodass die Kommunikation vom restlichen Netz logisch getrennt ist. Selbstverständlich muss die WLAN-Kommunikation nach Stand der Technik (WPA2) mittels kryptographisch Verfahren abgesichert und Zugriffe authentisiert werden.

Beim Einsatz von ZigBee ist dringend davon abzuraten, ZigBee Home Automation 1.2 oder eine früheren Version einzusetzen, da hier ein öffentlich bekanntes Schlüssel-paar (Fallback Key) von den Komponenten unterstützt werden muss [6]. Das Protokoll sollte nur in dafür vorgesehenen, dedizierten Segmenten eingesetzt werden und diese Segmente sollten vom restlichen Netz getrennt werden.

Komponenten mit ZWave-Funktechnologie dürfen nur genutzt werden, wenn es sich um zertifizierte Produkte handelt, um Störungen des Funknetzes zu vermeiden. Die Kommunikation sollte nur in dafür vorgesehene, dedizierte Segmente überführt werden, so dass die Kommunikation vom restlichen Netz getrennt ist.

BACnet ist seit vielen Jahren ein fester Bestandteil von Gebäuden und hat sich bewährt. Man sollte bei der Verwendung jedoch berücksichtigen, dass die Kommunikation unterschiedlicher Komponenten unter BACnet aufgrund herstellereigener

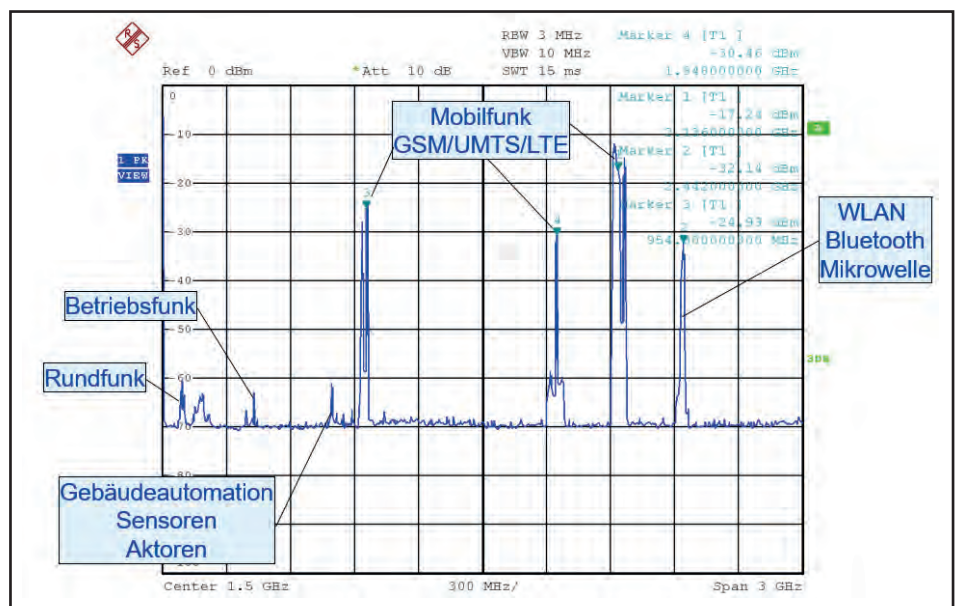


Abbildung 4: Funkdienste im Gebäude

Sicherheitsanforderungen an Netzarchitektur und Netzdesign eines Gebäudes der Zukunft

Implementierungen stets auf Kompatibilität zu testen und hinsichtlich der Sicherheitseinstellungen zu überprüfen sind. Vorzugsweise sind Tests mittels physischen Komponenten an einem Prototypen vorzunehmen.

Bei der Verwendung von EnOcean ist zu beachten, dass die in Europa verwendete Frequenz von 868,3 MHz (gemäß R&TTE-Spezifikation EN 300220) frequenztechnisch sehr dicht am LTE Upstream der Deutschen Telekom liegt (852–862 MHz). Dies kann dazu führen, dass die Signale überlagert werden und die Zuverlässigkeit stark abnimmt. Dabei kann es vorkommen, dass der Benutzer selbst die Störquelle in Form eines Mobiltelefons bei sich trägt. Da funktionieren alle Schalter bei der Abnahme problemlos, da der Tester ein Vodafone Handy bei sich trägt. Im normalen Betrieb können Personen mit Telekom Mobilfunkvertrag dann plötzlich die Lichtschalter nicht mehr richtig bedienen.

Dies ist eines der Beispiele dafür, warum die Erstellung und Pflege eines Frequenzkatasters nötig und sinnvoll ist, selbst wenn es in diesem Beispielfall nur die Fehlersuche erleichtert hat.

Fazit und Ausblick

Aktuell ist IT-Sicherheit über viele Gewerke verteilt und jeder kocht seinen eigenen Kaffee. Einen ersten Anhaltspunkt können hier die Maßnahmen des BSI liefern. Relevant sind dabei die Maßnahmen des Bausteins B1.11 Outsourcing, B1.17 Cloud Nutzung und B2.24 Web-Services. Aber auch diese sind für ein modernes Gebäude unzureichend.

Daher MUSS Sicherheit der Gebäudetechnik in Zukunft eine eigene, integrative Planungsaufgabe werden. Wer Sicherheit den Planern der konventionellen Gebäudetechnik-Gewerke überlässt, kann sicher sein, dass das Gebäude in naher Zukunft ein beliebtes Ziel von Cyber-Angriffen wird. Nicht weil die Planer inkompetent sind, sondern weil Sicherheit in der Planung auch Kompetenzen erfordert, die häufig nicht gegeben sind. Der Planer der IT-Sicherheit für ein Gebäude muss in der Lage sein, den einzelnen Gewerken konkrete und zwingende Vorgaben zu machen. Ist das nicht gegeben, wird ein Smart Building nicht funktionieren und eine große Menge an Schwachstellen aufweisen. Diese Form der Vorschriften hat der Artikel in Ansätzen geliefert. Allerdings kann dies nur als grobe Richtlinie dienen und ist für jedes Gebäude gezielt auszuarbeiten.

Die einzige Lösung, die auf Dauer funktionieren wird, ist die Schaffung eines

„neuen“ Basis-Gewerks IT-Infrastrukturen. Und dieses Basis-Gewerk legt die erforderlichen Infrastrukturen für Video-Überwachung, Zugangstechnik, Brandmeldetechnik, Heizung-Klima-Lüftung, Arbeitsplatz-Versorgung, und was die Zukunft noch alles bringen mag, fest.

Ebenso brauchen wir verbindliche Richtlinien, die IoT-Geräte erfüllen müssen. Das kann man aber nur erreichen, wenn man den Einsatz von Geräten, die diese Richtlinien nicht erfüllen, kategorisch ausschließt. Am Schluss darf nicht das günstigste Produkt, sondern das sicherste die Wahl des Bauherrn oder Betreibers sein.

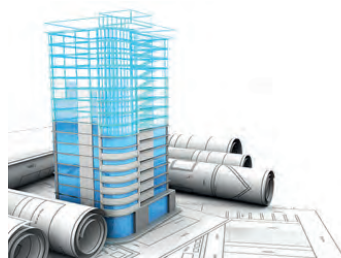
Zu einer Zertifizierung oder Ähnlichem von IoT-Geräten gibt es verschiedene Bestrebungen, unter anderem von der europäischen IT-Sicherheitsbehörde ENISA [7][8]. Die Anerkennung der Bedeutung der IT-Sicherheit auf europäischer Ebene wird auch durch das kürzlich erschienene Strategiepapier zur Cybersicherheit „Building strong cybersecurity for the EU“ [9] sichtbar. Diese sind allerdings kaum bekannt und werden aktuell nicht als relevant für Ausschreibungen erachtet.

Diese Bemühungen kommen spät und es lässt sich nur hoffen, dass die Bemühungen schnell Ergebnisse zeigen, bevor eine Vielzahl von Gebäuden fertig gestellt und mit unsicherer Technik ausgestattet sind. Denn nur selten lassen sich die einzelnen Komponenten eines modernen Gebäudes im Nachhinein durch Softwareupdates sicherer machen.

Verweise

- [1] Siehe: <http://www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause>
- [2] Siehe: <https://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html>
- [3] Siehe: „Informationssicherheit im Mikrokosmos von Smart Buildings“, Netzwerkinsider August 2017, <http://www.comconsult.com/informationssicherheit-im-mikrokosmos-von-smart-buildings/>
- [4] Siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
- [5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/itgrundschutz_modernisierung_node.html
- [6] Siehe: <https://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html>
- [7] <https://www.enisa.europa.eu/>
- [8] <https://www.heise.de/newsticker/meldung/EU-IT-Sicherheitsbehoerde-ENISA-will-deutlichen-Kompetenzzuwachs-3687230.html>
- [9] <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN>

Sonderveranstaltung



IT-Infrastrukturen für das Gebäude der Zukunft 17.10.2017 in Bonn

Diese Sonderveranstaltung diskutiert mit Ihnen:

- welchen Infrastruktur-Bedarf das Gebäude der Zukunft erzeugt
- wie eine effiziente, flexible und Gewerke-übergreifende Infrastruktur-Planung erfolgt
- wie Mehrwert-Dienste in einzelnen Gewerken auf diese Basis-Schicht von Infrastruktur aufsetzen

Diese Veranstaltung wendet sich an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerke-übergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.

Preis: 1.090,-- € netto



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktuelle Sonderveranstaltung

IT-Infrastrukturen für das Gebäude der Zukunft

17.10.17 in Bonn

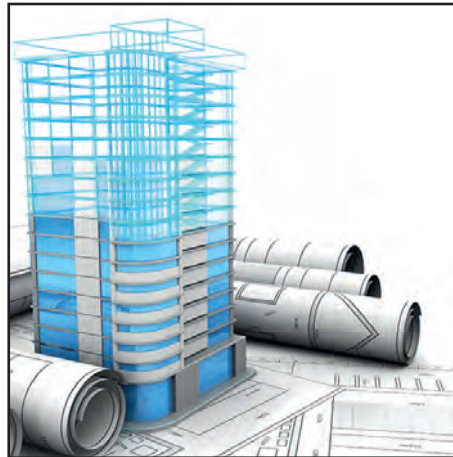
Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die Gewerk-übergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können.

Diese Infrastrukturen umfassen:

- eine Anwendungs-unabhängige Verkabelung
- eine Anwendungs-unabhängige Vorbereitung für unterschiedliche Funknetze
- flächendeckende Funknetze
- eine flächendeckende Gleichstrom-Versorgung auf der Basis Power-over-Ethernet

Diese Sonderveranstaltung diskutiert:

- welchen Infrastruktur-Bedarf das Gebäude der Zukunft erzeugt
- wie eine effiziente, flexible und Gewerke-übergreifende Infrastruktur-Planung erfolgt
- wie Mehrwert-Dienste in einzelnen Gewerken auf diese Basis-Schicht von Infrastruktur aufsetzen



Wir gehen dabei auf eine Reihe von Spezialfragen ein, die helfen, den Aspekt der langfristigen Investitionssicherung abzudecken:

- wie sieht der Arbeitsplatz der Zukunft aus und welche Infrastruktur erfordert er?
- welchen Stellenwert hat eine WLAN-Infrastruktur im Gebäude der Zukunft und wie dicht wird sie geplant?

- was bedeutet Smart Building und wie kann es sauber auf eine Basis-Infrastruktur aufgesetzt werden?
- wie sieht die Anwendungs-neutrale Verkabelung eines Gebäudes aus? Bis wohin sollte sie gebracht werden und ab wann startet der Gewerke-spezifische Teil?
- wo steht Power-over-Ethernet technisch, was ist in den nächsten Jahren zu erwarten und wie kann es Gewerke-übergreifend und flexibel genutzt werden?
- wie effizient können Mehrwertdienste wie Beacon-Technologien integriert werden?
- welche Rolle wird Mobilfunk mit 5G spielen? Inwieweit muss es mit den anderen geplanten Funktechnologien als Einheit gesehen werden?

Diese Veranstaltung wendet sich an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerke-übergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.

Sichern Sie sich noch einen der letzten Restplätze!

Anmeldung an kundenservice@comconsult-research.de

IT-Infrastrukturen für das Gebäude der Zukunft

Ich buche das Seminar
IT-Infrastrukturen für das Gebäude der Zukunft

17.10.2017 in Bonn
zum Preis von € 1.090,- netto

Bitte buchen Sie mir ein Hotelzimmer

Vorname


Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

 Buchen Sie über unsere Web-Seite
www.comconsultakademie.de

eMail

Unterschrift

 Programmübersicht IT-Infrastrukturen für das Gebäude der Zukunft

Dienstag 17.10.2017**9:30 Uhr****Keynote: SMART Commercial Building - Die Digitalisierung verändert die Anforderungen an unsere Gebäude**

- Trends und Beispiele
- Digitalisierungsbausteine Hardware/Software
- Use Cases für die Bauherren/Investoren
- Vorgehensweise (Anforderungsmanagement)
- Entscheidervorlage Digitalisierung
- Neues Leistungsbild Digitalisierung „Digital Transformation Manager“

*Dipl.-Ing. Klaus Dederichs,
Drees & Sommer GmbH*

10:15 Uhr**Intelligenz im Gebäude: Sensoren, Beacons, Cloud - macht das Sinn?**

- Aktuelle Situation bei modernen Gebäuden - Protokolle und Hardware
- Indoor Navigation und Asset Tracking (Technologien dafür z.B.: Beacons)
- Soll man ausgewählte Daten sammeln oder alles, was man bekommen kann?
- Schutzbedarf der Daten
- Gefahr der Scheinkorrelation (Storks deliver Babies von Matthews (2000))
- Beispiele für sinnvolle Datenkorrelationen --> Heatmaps
- Cloud-Dienste und Mehrwert
- Fazit und Ausblick: MetaCloud --> eine zentrale Anlaufstelle für den Betrieb, eine API für die App

*Dipl.-Inform. Thomas Steil,
ComConsult Beratung und Planung GmbH*

11:00 Uhr Kaffeepause**11:30 Uhr****Der Arbeitsplatz der Zukunft – Anforderungen an die Infrastruktur**

- Kabeltechnik
- Netzwerktechnik
- Endgerätetechnik
- Applikation
- Edge Data Center bringen die Rechenleistung näher zum Nutzer

*Dipl.-Ing. Thomas Simon,
ComConsult Beratung und Planung GmbH*

12:15 Uhr**WLAN und andere Funktechniken**

- Stand der Technik bei WLAN
- Wie viele Access Points werden benötigt und wie verkabelt man sie?
- „WLAN-Verteiler“ werden marktfähig, sind sie für das Smart Building geeignet und lassen sich dadurch Kabel sparen?
- Jedem sein eigenes WLAN oder zentrale WLAN-Infrastruktur für alle Mieter?
- Welche Rolle spielen Mobilfunk und andere Funkdienste in Gebäuden?
- Braucht man Abschirmungen gegen Funkwellen von außen?
- Wie lassen sich gegenseitige Störungen zwischen Funkdiensten in einem Smart-Building vermeiden?

*Dr. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH*

13:00 Uhr Mittagspause**14:00 Uhr****Verkabelung als Gewerke-übergreifende Basis für die Gebäude-IT**

- Kann es eine Gewerke-übergreifende Universal-Verkabelung für ein Gebäude geben? Wenn ja, wo ist die Schnittstelle zu den Gewerken und was umfasst der Gewerke-übergreifende Teil?
- Wie unterscheidet sich die EN 50173-6 von den bisherigen Verkabelungsnormen?
- Wie viele Unterverteiler werden benötigt, um eine saubere Basis für alle Gewerke zu legen?
- Was bringt die Berücksichtigung der Norm an Vorteilen?
- Was sind die Besonderheiten einer anwendungsneutralen Verkabelung bei Nutzung durch die Gebäudeleittechnik?
- Welche grundsätzlichen technischen und organisatorischen Entscheidungen müssen getroffen werden?
- Warum lassen sich die bekannten Verkabelungs-Technologien und Materialien nicht immer 1:1 für Netze der Gebäudeleittechnik verwenden?
- Warum kann man aus den Erfahrungen beim Aufbau von lokalen Netzen im Industrie-Umfeld lernen?

*Dipl.-Ing. Hartmut Kell,
ComConsult Beratung und Planung GmbH*

14:45 Uhr**Power-over-Ethernet: Gewerke übergreifende Stromversorgung im Gebäude der Zukunft**

- Was leistet PoE nach dem heutigen Stand der Technik?
- Neue Einsatzgebiete erobern den Markt. Welche Herausforderungen sind damit verbunden und wie können wir sie gewinnbringend nutzen?
- Welche planerischen Maßnahmen ergeben sich aus dem flächendeckenden und Gewerke übergreifenden Einsatz von PoE?
- Hohe Datenraten vs. PoE. Was nicht passt, wird passend gemacht
- IEEE 802.3bt: Die Revolution für den Arbeitsplatz der Zukunft?

*Dipl.-Ing. Stephan Bien,
ComConsult Beratung und Planung GmbH*

15:30 Uhr Kaffeepause**16:00 Uhr****Herausforderung Informationssicherheit für das Gebäude der Zukunft**

- Schadsoftware, Krypto-Trojaner, zielgerichtete Angriffe, Desinformation und (Distributed) Denial of Service: Bedrohungen der IT im Gebäude der Zukunft
- Welche Informationssicherheitsstandards sind für Smart Buildings relevant?
- Absicherungen von Smart Buildings mit IEC 62443
- Zonenkonzepte und Netzzugangskontrolle: Brauchen wir das wirklich? • Mandantenfähige Infrastrukturen für Nutzer und Betreiber von Smart Buildings
- Absicherung von Funknetzen, inkl. WLAN, 5G und Co., Anbindung von Smartphones und Tablets: Alles wie gehabt?
- Wo sich Internetanbindung und DMZs im Smart Building vom Rest der Welt unterscheiden
- Ohne Cloud kein Smart Building: Sichere Cloud-Dienste und sichere Cloud-Nutzung für Nutzer und Betreiber
- Security by Design: Skalierbare Sicherheitsarchitekturen

*Dipl.-Inform. Daniel Prinzen,
ComConsult Beratung und Planung GmbH*

Standpunkt

Verschlüsselung in der Cloud: Licht am Ende des Tunnels

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.

„Eine solide Verschlüsselung der Daten ist das A und O bei der Nutzung von Cloud-basierten Diensten.“

Sollte Ihnen dieser Anfang des Artikels irgendwie bekannt vorkommen, ist es kein Wunder, denn vor ziemlich genau vier Jahren hatte ich mich im September 2013 mit dem Thema Verschlüsselung in der Cloud schon einmal auseinandergesetzt, letztendlich mit der pessimistischen Feststellung, dass die Public Cloud für Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und/oder Integrität eigentlich nicht in Frage kommt [1].

Inzwischen habe sich aber an einigen Stellen entscheidende Dinge getan!

Gut, zum sicheren Transport von Daten zur und von der Cloud ist zunächst nicht viel zu sagen. Das sind bewährte Techniken der Bauart TLS und Co. Für die Authentisierung und für die Berechtigung haben wir auch Lösungen. Die sichere Speicherung von Daten in einer Public Cloud unter Verwendung eines eigenen Schlüsselmaterials ist auch nichts Exotisches mehr. Beispielsweise finden wir in der Microsoft Cloud als treffende Bezeichnung für den entsprechenden Service in Anlehnung an BYOD den Begriff BYOK (Bring Your Own Key).

Das eigentlich Interessante muss also an einer anderen Ecke verborgen sein. Erinnern wir uns an einen aus Sicherheitsperspektive unangenehmen Sachverhalt: Sobald wir Rechenleistung aus der Cloud per Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oder Software as a Service (SaaS) beziehen und damit Daten in der Cloud verarbeiten, benötigen wir die Daten in der Cloud im Klartext und haben damit zwangsläufig einen Verschlüsselungsendpunkt in der Cloud. Damit ist auch die grundsätzliche Möglichkeit der Kompromittierung der Daten in der Cloud gegeben und sind wir wieder bei der Feststellung von oben, dass die Public Cloud für Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit



und/oder Integrität eigentlich nicht in Frage kommt.

Nun war schon 2013 eine wesentliche Technik bekannt, die dieses Dilemma lösen könnte: die Homomorphe Verschlüsselung. Dabei werden verschlüsselte Daten in die Cloud geschickt. Die Cloud verarbeitet die Daten ohne sie zu entschlüsseln und schickt das Ergebnis zurück. Die Mathematik eines Homomorphen Verschlüsselungsverfahrens sorgt dann dafür, dass nach Entschlüsselung der Daten durch den Nutzer tatsächlich das korrekte Rechenergebnis beim Nutzer des Cloud-Dienstes vorliegt. Eigentlich genial, denn wir hätten in der (Public) Cloud keinen Verschlüsselungsendpunkt mehr. Leider ist dies immer noch recht akademischer Natur, da die Verfahren (noch) nicht effizient genug realisiert werden können. Inzwischen konnte zwar für neuronale Netze tatsächlich nachgewiesen werden, dass hier effiziente Homomorphe Verschlüsselungsverfahren möglich sind (was für KI-basierte Berechnungen im Big-Data-Umfeld wichtig ist), von einer umfassenden Praxistauglichkeit sind wir aber noch recht weit entfernt [2].

Die Frage ist nun, ob es inzwischen Alternativen gibt, die mit anderen Techniken eine Privatsphäre in der Public Cloud ermöglichen können, und die Antwort ist tatsächlich: Ja!

Der Einsatz verschlüsselter Sandboxes zur Absicherung von Daten auf einem Smartphone oder Tablet ist eine inzwischen seit Jahren bewährte Lösung. Die Idee ist nun, solche Sandboxes für Daten und Code auf Prozessorebene in einem Computer so zu

realisieren, dass nur der Besitzer des entsprechenden Schlüsselmaterials auf Daten und Code zugreifen kann. Eine Sandbox kann so insbesondere sogar vor unberechtigten Zugriffen über das Betriebssystem geschützt werden. Ein Angreifer, der einen Rechner hackt, hat dann trotzdem keinen Zugriff auf die Sandbox. Mit solchen Techniken könnten Cloud-Dienste so abgesichert werden, dass die Datenverarbeitung in der Cloud abläuft und der Cloud-Betreiber oder ein Angreifer trotzdem keine Möglichkeit hat auf die Daten im Klartext zuzugreifen.

Einen solchen Ansatz haben nun Intel und AMD in ihren CPUs realisiert.

Mit Intel Software Guard Extensions (SGX) liegt eine Technik vor, mit der eine Applikation einen gesicherten Bereich (eine sogenannte Enclave) anfordern kann, in dem Daten gesichert gelagert und verarbeitet werden. Dies setzt natürlich voraus, dass die Software diese Funktionen auch nutzt, d.h. bestehende Software muss angepasst werden, um z.B. dafür zu sorgen, dass in einer Cloud die (Micro-)Services, die von den Cloud-Kunden aufgerufen werden, auch in einer entsprechenden Kunden-Enclave laufen. Interessant ist auch die Frage, wie auf Ebene eines Virtualisierungshosts diese Technik genutzt werden könnte, um VMs vor unberechtigten Zugriffen zu schützen.

Da die Funktionen komplett in Hardware realisiert sind, bleiben einem Angreifer nun nicht mehr viele Möglichkeiten. Ein Angriff könnte zunächst auf Ebene der Hardware selbst geschehen, was aber einen entsprechenden Zugriff erfordert. Da Intel SGX jedoch ein komplexes System darstellt (und komplexe Systeme, ob Hard- oder Software, sind nun einmal kaum fehlerfrei realisierbar) wird damit zu rechnen sein, dass sich in Intel SGX Schwachstellen verbergen, die nur darauf warten ausgenutzt zu werden [3].

AMD geht für die Epyc-Prozessoren mit der Secure Memory Encryption (SME) einen etwas anderen Weg und adressiert dabei deutlich sichtbar auch Cloud Provider. Die Verschlüsselung erfolgt pro Speicher-Page und wird über spezielle Bits aktiviert. Damit ist auch hier eine Verschlüsselung pro Applikation möglich und das Betriebssystem oder andere Prozesse können den Speicherbereich nicht lesen. Selbst DMA-fähige Hardware erhält

Verschlüsselung in der Cloud: Licht am Ende des Tunnels

auf diese Weise keinen Zugriff. Natürlich hat dies einen geringen Overhead, der sich in einer leicht erhöhten Latenz zeigt. SME wird auch eine der interessantesten neuen Elemente in Linux 4.14 sein [4].

Richtig interessant wird SME, wenn man diese Funktion mit Secure Encrypted Virtualization (SEV) auf die Server-Virtualisierung überträgt. Bei SEV verschlüsselt die CPU die Arbeitsspeicherebereiche, die von Virtual Machines (VMs) verwendet werden, mit einem für die VM individuellen Schlüssel. Damit ist es weder für einen Administrator noch für einen Angreifer, dem es gelungen ist, aus einer VM aus- und in eine andere VM oder in den Hypervisor einzubrechen, möglich auf den unverschlüsselten Speicherbereich zuzugreifen. Für IaaS

hätten wir so beispielsweise eine Möglichkeit, VMs auf eine sichere Weise auch in einer Public Cloud zu nutzen.

Insgesamt ist damit endlich ein Licht am Ende des Tunnels für den Aufbau sicherer (Public-)Cloud-Infrastrukturen deutlich sichtbar geworden! Wir werden diese Techniken daher genau im Auge behalten und im Netzwerk-Insider und auf den kommenden Foren der ComConsult hierzu berichten.

Verweise

[1] „Das Dilemma der Verschlüsselung in der Cloud“ aus "Der Netzwerk Insider" vom September 2013, verfügbar unter <https://www.comconsult-research.de/das-dilemma-verschlusselung/>

[2] Zur Anwendung in neuronalen Netzen siehe <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/CryptonetsTechReport.pdf>. Ein allgemeines Status-Update kann unter <https://www.networkworld.com/article/3196121/security/how-to-make-fully-homomorphic-encryption-practical-and-usable.html> gefunden werden.

[3] Für eine Analyse der Sicherheit von Intel SGX siehe: <https://www.blackhat.com/docs/us-16/materials/us-16-Aumasson-SGX-Secure-Enclaves-In-Practice-Security-And-Crypto-Review.pdf>

[4] Siehe <https://www.heise.de/ct/artikel/Die-Neuerungen-von-Linux-4-14-3831941.html>

ComConsult RZ-Tage

Netzwerk-Architekturen der Zukunft im RZ 11.12.17 in Köln

Integration von Cloud-Lösungen in die RZ-Infrastruktur 12.12.17 in Köln

Die ComConsult Akademie veranstaltet am 11.12. und am 12.12.2017 ihre Sonderveranstaltungen "ComConsult RZ-Tage – Netzwerk-Architekturen der Zukunft im RZ" und "ComConsult RZ-Tage – Integration von Cloud-Lösungen in die RZ-Infrastruktur" in Köln.

Das Mega-Thema für alle Rechenzentren ist "One-Stop-Provisioning": wie können die Infrastrukturen für neue Anwendungen durch Parametrierung mittels Orchestrierungs-Konsole schnell zur Verfügung gestellt werden? Projektzeiten sollen so aus dem Bereich von Jahren auf wenige Wochen verkürzt werden.

Dies erfordert:

- Infrastrukturen müssen ausreichende Kapazität haben, die Architektur muss auf eine schnelle Erweiterung ausgelegt sein
- Netzwerk-, Server- und Speicher-Kapazitäten müssen bei Bedarf exklusiv einer Anwendung zugewiesen werden können

- Eine Anwendung soll nur die ihr zugeordneten Ressourcen sehen und nicht auf die Ressourcen anderer Anwendungen zugreifen können
- RZ-Leistungen müssen gezielt um Funktionen aus der Cloud ergänzt werden, die dann wiederum in eine Gesamtarchitektur integriert werden
- Dies führt zu gravierenden Änderungen in der Planung und Bereitstellung von Infrastrukturen.

Wir analysieren auf dieser Top-Veranstaltung zentrale Fragen, die die Zukunft vieler Rechenzentren bestimmen werden. Die Anzahl der Teilnehmer ist aus logistischen Gründen begrenzt, wir empfehlen deshalb dringend eine frühzeitige Buchung. Die Tage sind einzeln und zusammen zum Paketpreis buchbar.

Der erste Tag beschäftigt sich mit folgenden Fragen:

- Geht Layer 2 komplett in den Hypervisor?

- Underlay + Overlay: was ist das, warum brauchen wir das?
- Welche Rolle wird OSPF in Zukunft haben: ist es bedroht?
- Warum reicht OSPF alleine nicht aus?
- Ist BGP die Antwort?
- Welche Controlplane brauchen wir für das Overlay?
- Zentral oder dezentral?

Den zweiten Tag widmen wir diesen Fragestellungen:

- Warum Ergänzungs-Lösungen einen Mehrwert bringen
- AWS kontra Azure: Modell-Projekt
- Office 365: Anforderungen an die IT
- Sicherheit trotz Cloud

Wenn Sie beide Veranstaltungen der "ComConsult RZ-Tage" buchen, bieten wir Ihnen einen Rabatt von 390,- € an.

Sie zahlen für beide dann nur 1.790,- € statt regulär 2.180,- €.


Anmeldung an kundenservice@comconsult-research.de

ComConsult RZ-Tage

Ich buche die Veranstaltung(en)
ComConsult RZ-Tage

- 11.12.2017 in Köln - 1.090,- € netto
- 12.12.2017 in Köln - 1.090,- € netto
- 11.12.2017 in Köln - 1.790,- € 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 RZ-Tage

Montag 11.12.2017 - Netzwerk-Architekturen der Zukunft im RZ

- 9:30 Uhr**
Neue Hardware: Voraussetzung für neue Lösungen in RZ-Netzen
- Anforderungen an moderne Rechenzentren: Skalierbarkeit, Flexibilität, Universalität
 - Evolution der Hardware: CPU, GPU, Speicher
 - Hardware Protokoll-Unterstützung der aktuellen 100 GbE Switch ASICs mit 25/50 GbE Unterverteilung
 - Möglichkeiten, Entwicklung und Verfügbarkeit von 200/400 GbE und Silicon Photonics
- Dr. Franz-Joachim Kauffels, Technologie-Analyst*
- 10:30 Uhr Kaffeepause**
- 11:00 Uhr**
Ist Layer 2 im DC noch zeitgemäß? Netzdesigns im Vergleich
- Neue Anwendungen erfordern ein neues Netzwerkdesign (Probleme des Spanningtree Protokolls, LACP – eine beschränkte Alternative)
 - Layer 2 Design oder auch Switchfabric (TRILL; SPB, MC-LAG, SDN Einbindung)
 - Layer 3 Design – Einführung (Hyper Scale DC von Microsoft und Facebook, Use Cases, Design Vorgaben)
 - Layer 4 Design – Was ist das? (Multipath TCP, QUICK)
- Markus Geller, ComConsult Research GmbH*
- 12:00 Uhr Mittagspause**
- 13:00 Uhr**
EGP statt IGP: das Ende von OSPF? Wo ist die investitionssichere Zukunft? Welches Routing Protokoll im DC?
- Wie funktioniert modernes IP Routing? (Link State, Distance Vector, Path Vector)
 - Topologie bekannt und nun?
 - Welche Auswirkungen ergeben sich aus der Kenntnis der Topologie?
 - BGP statt OSPF: Die Gründe (Grenzen des Area Designs, Update Verhalten, Virtuelle Links)
 - BGP Gestaltung und Aufbau (Pfad Auswahl im DC, SDN Controller)
 - iBGP vs. eBGP (ECMP, BFD)
- Markus Geller, ComConsult Research GmbH*
- Spine-Leaf, Scale-Out: Alles klar? (Skalierung, Multi Vendor Support)
- Markus Geller, ComConsult Research GmbH*
- 14:00 Uhr**
Von der Server-Virtualisierung zur Private Cloud: Die Bedeutung des Software-defined Datacenters
- Server-Virtualisierung
 - Storage-Virtualisierung
 - Overlays und Software-defined Networking (SDN)
 - Integration von Sicherheitskonzepten (Mikrosegmentierung)
- Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH*
- 15:00 Uhr Kaffeepause**
- 15:15 Uhr**
Overlays und das Problem mit dem Control-Layer
- Motivation: Warum Overlays?
 - Anforderungen an moderne RZ-Netzdesigns
 - Einflussfaktoren: Storage-Anbindung, Cloud-Anbindung, Redundanz
 - Vorteile und Nachteile typischer Designs
 - Hypervisor vs. Netzwerkkomponente: Wo enden die Overlays?
 - Übersicht gängiger Overlay-Technologien
 - Welche Tunnelprotokolle stehen zur Verfügung?
 - MPLS / PBB / TRILL / VXLAN / NVGRE / Geneve
 - Wo liegen die Unterschiede und wie sieht deren Zukunft aus?
 - Das Problem mit dem Control-Layer
 - Brauchen wir eine übergreifende Control-Plane?
 - Controllerbasierende vs. Data-Plane-basierende Lösungen
 - IS-IS, SDN, Multiprotokoll BGP
 - Auf dem Weg zur einheitlichen Control Plane?
 - Lösungen im Vergleich:
 - SPBM (802.1Qaq), NSX und VXLAN, EVPN VXLAN
 - Eigenschaften, Protokolle, Leistungsmerkmale
 - Anwendungsfälle
- Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH*
- ab 18:00 Uhr Happy Hour**

Dienstag 12.12.2017 - Integration von Cloud-Lösungen in die RZ-Infrastruktur

- 9:30 Uhr**
Nutzung von Public Clouds zur Unterstützung von Geschäftsprozessen
- Ziele und Erwartungen
 - Was leisten Cloud-Dienste heute? Wo steht der Markt?
 - Ausgewählte Einsatzszenarien
- N.N.*
- 11:00 Uhr**
AWS vs Azure: warum Cloud? Welche Cloud? Dienste, Preise, Konzepte in der Analyse
- Komponenten der Cloud: Dienste, Server, Regionen, Netzwerke
 - Anbindung des RZ an die Clouds von Microsoft und Amazon: VPN, Direct Connect, ExpressRoute, Statisch oder BGP
 - Netzwerkgestaltung in und mit der Cloud
 - Projekterfahrungen aus Migration von ComConsult-Study.tv in die Cloud
- Markus Schaub, ComConsult-Study.tv*
- 11:30 Uhr Kaffeepause**
- 11:45 Uhr**
Microsoft Office 365: Erfolgreiche Nutzung und Anforderungen an die IT
- Software aus der Cloud
 - Ziele und Erwartungen
 - Warum Cloud-Anwendungen „anders“ sind
 - Beispiele
 - Assessment von Office 365:
 - Nutzung der Office-365-Suite: Wer – Was – Wie
 - Lizenzmodelle
 - Anbindung an die Microsoft Cloud: Single Tenant vs. Multiple Tenants
 - Integration des Active Directory
 - Single Sign On
 - Anforderungen an die IT-Infrastruktur
 - WAN-Anbindung: Bandbreite, Laufzeit, Übertragungsqualität
 - Tools zur Prüfung der Netzqualität
 - Netzdesigns zur Anbindung von Niederlassungen
- User Experience
 - Tuning-Möglichkeiten
 - Erfahrungen aus Kundenprojekten
- Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH*
- 13:15 Uhr Mittagspause**
- 14:15 Uhr**
Informationssicherheit in und aus der Cloud
- Herausforderung sicheres Cloud Computing
 - Integration Private Cloud und Provider Cloud
 - IAM und Data Loss Prevention für die sichere Nutzung von Cloud-Diensten
 - Verschlüsselung von Daten in der Cloud: Möglichkeiten und Grenzen
 - Standardisierte und zertifizierte Cloud-Sicherheit
 - Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
 - Rolle der Cloud bei der Abwehr von zielgerichteten Angriffen und von Distributed Denial of Service (DDoS)
- Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*
- 15:45 Uhr**
IT-Recht und die Cloud
- Vertragsrecht in der Cloud
 - Grundlagen und typologische Einordnung
 - Do´s und Don´ts in Cloudverträgen
 - Datenschutz in der Cloud
 - Datenschutzrechtliche Ausgangslage (neues Recht vs. altes Recht)
 - Gestaltungstipps für sicheres Cloud Computing
 - Informationssicherheit in der Cloud
 - Sicherheitslage in der Cloud
 - Rechtliche Anforderungen an die IT-Sicherheit beim Cloud Computing
- Dr. Jan Byok, Bird & Bird LLP*
- 16:30 Uhr Ende der Veranstaltung**

Aktuelle Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 18.10. - 19.10.2017 in Bonn

Die ComConsult Akademie veranstaltet vom 18.10. bis 19.10.2017 ihre Sonderveranstaltung "Wireless und Mobility" in Bonn.

Das IoT, autonome Mobilität und neue Arbeitsplatzmodelle verändern die Anforderungen an flächendeckende Wireless Infrastrukturen dramatisch. Neue WLAN-Techniken und 5G Mobilkommunikation führen zu einem neuen Universum für die Versorgung von menschlichen und maschinellen Teilnehmern. Die Sonderveranstaltung widmet sich mit herausragenden Referenten diesem hoch dynamischen Problemkreis.

Die Positionierung von Wireless-Netzwerken ist in einem starken Wandel von einer Ergänzungs- hin zu einer Haupt-Kommunikationsstruktur. Die Auslöser dieser Entwicklung kommen aus verschiedenen Bereichen ausgehend von IoT, Gebäude-Automatisierung bis hin zu flexiblen und mobilen Arbeitsplätzen.

Dementsprechend ändern sich die Standards und die Planungsansätze. Und gleichzeitig müssen wir Wireless immer mehr als Spektrum sich ergänzender Technologien sehen. Von Bluetooth über ZigBee zum WLAN und von da zum Mobilfunk.

Das Ergebnis: eine Zukunfts-taugliche Wireless-Infrastruktur erfordert eine ab-



gestimmte Gesamtplanung, die zudem auf den zukünftigen Bedarf ausgelegt ist.

Hier setzt unsere Sonderveranstaltung an.

Wir analysieren und diskutieren mit Ihnen:

- Mit welchen Verkehrsvolumina müssen wir rechnen? Was ändert sich? Wie können wir den Zukunftsbedarf erfassen und beherrschen?
- Wie wird sich die Zahl zu vernetzender Endpunkte verändern? Welche Anwendungen werden damit verbunden sein?
- In welchem Umfang ist das traditionelle WLAN darauf vorbereitet? Was kann getan werden, um seine Zukunfts-

Tauglichkeit zu verbessern?

- Wie kann WLAN in Zukunft gegenüber dem Mobilfunk abgegrenzt werden? Oder gibt es einen integrierten Planungsansatz?
- Welche Konsequenzen bringt Gebäudeautomatisierung mit Anwendungen wie Beacons und zusätzlichen Netzwerktopologien wie ZigBee oder Bluetooth mit sich?
- Gibt es eine Chance für eine flächendeckende Wireless-Infrastruktur mit einem Technologie-Mix für ein Gebäude?
- Welche neuen Perspektiven bieten neue Technologien wie die Übertragung im Millimeterbereich? Brauchen wir derartige Mikrozellen?

Die Zellen-Technologien sind aber nur die eine Seite der Medaille. Wichtige Themen zur Infrastruktur sind also mindestens:

- Struktur und Betrieb angemessener Backbones
- Sicherheit als Gesamtkonzept für Wireless
- Taktische und rechtliche Sicherheit
- Wirkung der Technologien auf Menschen

Die ComConsult Sonderveranstaltung „Wireless und Mobility“ ermöglicht Ihnen die Diskussion all dieser Themen mit hochkarätigen, erfahrenen Spezialisten. Sichern Sie sich rechtzeitig Ihren Platz!

Anmeldung an kundenservice@comconsult-research.de


Wireless und Mobility

Ich buche die Sonderveranstaltung
Wireless und Mobility

18.10. - 19.10.2017 in Bonn
zum Preis von 1.990,- €

inklusive Report "Wireless-Systeme
der nächsten Generation"
zum Teilnehmer Sonderpreis von 298,- €

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 Wireless und Mobility

Mittwoch 18.10.17

9:30 Uhr

Wireless: Basis für Disruption und Agilität

- Mobilität als Grundlage neuer Arbeitsplatzmodelle
- Disruption und Agilität als wesentliche Triebkräfte
- Neue Anwendungen und Anforderungen an Multi-Gigabit WLANs
- IoT und die enge Verbindung zu Mobilfunktechnologie (5G)
- Strukturelle Aspekte unterstützender Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 Uhr

WLANs zwischen Altlasten und Hoffnung

- IEEE 802.11ac in den verschiedenen Geschmacksrichtungen
- Ist mit 10 Gbit/s auf 2,4 und 5 GHz Schluss oder geht zukünftig noch mehr?
- WLAN im 60-GHz-Band: Es gibt Standards, aber kaum Anwendungen
- Was sagt die IEEE zur Mobilfunk-Integration?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:30 Uhr Kaffeepause

12:00 Uhr

Netz-Architekturen für (High Speed) WLANs

- Welche Anforderungen bestehen an die Netzarchitektur für den Aufbau von WLANs? • Der WLAN-Controller: Flaschenhals oder Mittel der Wahl?
- Alternativen zum WLAN Controller: Was bieten die Hersteller?
- IEEE 802.3bz: Seit dem 27.09.2016 gibt es „Breitreifen“ für Access Points

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

13:00 Uhr Mittagspause

14:30 Uhr

WLAN-Zellplanung auf dem Prüfstand

- Welchen Stellenwert hat die WLAN-Zellplanung bei der Konzeptionierung einer WLAN-Infrastruktur?
- Welche Parameter sind bei einer professionellen WLAN-Zellplanung zu berücksichtigen?
- Ausleuchtungsmessung vs. Simulation
- Häufige Fehler, die Sie unbedingt vermeiden sollten. Dos and Don'ts

Dipl.-Ing. Stephan Bien, ComConsult Beratung und Planung GmbH

15:15 Uhr

Kritisches Infrastrukturelement:

PoE für höhere Geschwindigkeiten

- Was leistet PoE nach dem heutigen Stand der Technik?
- Neue Einsatzgebiete erobern den Markt. Welche Herausforderungen sind damit verbunden und wie können wir sie gewinnbringend nutzen?
- Welche planerischen Maßnahmen ergeben sich aus dem flächendeckenden und Gewerke übergreifenden Einsatz von PoE? • Hohe Datenraten vs. PoE. Was nicht passt, wird passend gemacht
- IEEE 802.3bt: Die Revolution für den Arbeitsplatz der Zukunft?

Dipl.-Ing. Stephan Bien, ComConsult Beratung und Planung GmbH

16:00 Uhr Mittagspause

16:30 Uhr

Sicherheit im WLAN:

Es gibt immer noch Herausforderungen!

- Warum traditionelle Hotspots so gefährlich sind
- Sichere Hotspots mit Hotspot 2.0: Wie funktioniert EAP-SIM in der Praxis?
- Lücken in IEEE 802.11i / WPA2
- Fallstricke bei der kombinierten Maschinen- und Nutzerauthentisierung mit IEEE 802.1X
- Neue Entwicklungen bei EAP: TEAP und Co.
- Was kommt nach WPA2?
- WLAN Security im IoT braucht neue Konzepte: DPP, Passpoint, ...

Dipl.-Inform. Daniel Prinzen, ComConsult Beratung und Planung GmbH

17:15 Uhr

Genauere Lokalisierung mobiler Endgeräte mit WLAN oder Bluetooth LE Beacons

- Unterscheidung zwischen Lokalisierung mittels WLAN und BLE Beacons
- WLAN: Welche Genauigkeit lässt sich bei der Lokalisierung von WLAN Endgeräten erreichen? • WLAN: Cisco Hyperlocation – Angle-of-Arrival Auswertung von Datenframes erlaubt eine Steigerung der Genauigkeit auf 1-3m
- BLE: Cisco Virtual Beacon Solution – weniger Hardware Beacons und wie Machine Learning den RF-Fingerprint ersetzt.

Christian Gauer, Cisco Systems GmbH

Donnerstag 19.10.17

9:00 Uhr

Intelligenz im Gebäude: Sensoren, Beacons, Cloud - macht das Sinn?

- Aktuelle Situation bei modernen Gebäuden - Protokolle und Hardware
- Indoor Navigation und Asset Tracking (Technologien dafür z.B.: Beacons)
- Datensammlung und Schutzbedarf der Daten
- Scheinkorrelation und Beispiele für sinnvolle Datenkorrelationen --> Heatmaps • Cloud Dienste und Mehrwert
- Fazit und Ausblick: MetaCloud --> eine zentrale Anlaufstelle für den Betrieb, eine API für die App

Dipl.-Inform. Thomas Steil, ComConsult Beratung und Planung GmbH

9:45 Uhr

Mobile Netzwerke sind mehr als nur WLAN –

Lokationsabhängige Interaktionen mit Anwendern durch Einsatz von Beacons und Apps

- Eine Infrastruktur, ein Management für WLAN und BLE Beacons
- Verschiedene Wege zur eigenen Unternehmens App mit Lokationsdiensten - von einfach bis komplex
- Neue Services für Anwender durch den Einsatz von Beacons live gezeigt
- Asset Tracking als integrierter Bestandteil einer Beaconlösung
- Branchenbezogene Beispiele: Gesundheitswesen, Retail, Unternehmensnetze

Reinhard Lichte, HPE Aruba Germany

10:30 Uhr Kaffeepause

11:00 Uhr

WLAN als Teil eines Software Defined Enterprise Networks

- Einheitliches Management und Zugangskontrolle für LAN und WLAN
- Automatische Kontrollmechanismen bis auf Applikationsebene
- On-Premise vs. Cloud
- Wireless IDS/IPS
- Wie sieht die Zukunft aus?

Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

11:45 Uhr

WLAN und Mobilfunk als Gesundheitsrisiko?!

- Begriffe erklärt: SAR-Wert und Leistungsflussdichte
- Wovor schützt uns der Gesetzgeber?
- Gefahren der Funkwellen jenseits amtlicher Grenzwerte
- Messtechnik und Nachweis
- Empfehlungen zum Schutz der Mitarbeiter

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:15 Uhr Mittagspause

13:45 Uhr

Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen

- Grundlagen der deutschen Störerhaftung
- Neueste Entwicklungen im Bereich der Störerhaftung
- Zukunft der deutschen Störerhaftung
- Praxistipps zum Betrieb privater WLAN-Infrastrukturen

Dr. Jan Byok, Bird & Bird LLP

14:30 Uhr

Von LTE Advanced zu 5G

- Mobilfunk: Stütze der nächsten digitalen Revolution
- Koexistenz von LTE / 5G und WLANs
- 5G: Konzepte, Technologien, Feldversuche, Standardisierung
- Die Eckpfeiler des ITU-Standards für 5G vs. Pre-Standard-Lösungen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

15:30 Uhr Ende der Veranstaltung

Report- Neuerscheinung (2. Auflage) zur Sonderveranstaltung

Wireless-Systeme der nächsten Generation

Anwendungen, Systeme, Anforderungen

von Dr. Franz-Joachim Kauffels

Mit Ihrer Seminarbuchung der Sonderveranstaltung "Wireless und Mobility" können Sie die Neuauflage (August 2017) des Reports "Wireless-Systeme der nächsten Generation" zum vergünstigten Paketpreis erwerben.

Dieser Report ist ein unverzichtbares Hilfsmittel für alle, die sich mit der Schaffung von Wireless Versorgungsstrukturen für die Anforderungen der digitalen Zukunft zu rüsten. Die Studie hilft, die neuen drahtlosen Übertragungstechniken und ihre Wechselwirkungen besser einzuschätzen und die passende Infrastruktur vorzubereiten.

Die Neuauflage befasst sich zusätzlich ausführlich mit der kommenden 5G-Technologie, möglichen Varianten, Anwendungsfeldern und Implikationen. Durch 5G bleibt letztlich kein Stein mehr auf dem anderen. Zusätzlich gibt es ein neues Kapitel, welches den aktuellen Erkenntnisstand hinsichtlich möglicher Wechselwirkungen der vielen neuen Funkssysteme auf den menschlichen Organismus darstellt.

Der Report ist dadurch von fünf auf sieben Kapitel angewachsen.

Im ersten Kapitel betrachten wir die Entwicklung von Anwendungen und Anforderungen. Das zweite Kapitel ist der aktuell neu verfügbaren WLAN-Technik, primär IEEE 802.11ac ab „Wave 2“ gewidmet. Kapitel drei beleuchtet die Entwicklung kleinerer Funkzellen und Mikrozellen im Millimeterwellen-Bereich (50 bis 60 GHz-Bänder).



2. aktualisierte und deutlich erweiterte Auflage August 2017

Hier können leicht Multigigabit-Leistungen erreicht werden, aber eben verbunden mit recht geringen Ausdehnung der Zellen. IEEE 802.ad „WiGig ®“ ist der erste Repräsentant dieser Systemklasse.

Die Zukunft wird allerdings durch die Entwicklung der Mobilfunksysteme deutlich stärker geprägt als durch die der WLANs. Ausgehend von LTE gibt es eine Reihe von Weiterentwicklungen in neuen Releases, einschließlich der Möglichkeit des Vordringens von Providern in lizenzfreie Bereiche, die bislang den WLANs vorbehalten waren. Kapitel vier stellt diese Entwicklungen dar. Es wird klar, dass hier die Messlatte für die mobile Kommunikation deutlich höher gelegt wird.

Neben LTE auf dem Weg zu 5G wird es neue WLAN-Techniken mit deutlich mehr Leistung und höherer Qualität geben, wie IEEE 802.11ax und IEEE 802.11ay. In Kapitel 5 beleuchten wir, was das in Zukunft für die unterstützenden Infrastrukturen, besonders in Unternehmen, bedeutet. Mittelfristig ist mit einer notwendigen Versorgungsleistung für WLAN-Zellen von mindestens 10 Gbit/s. zu rechnen.

5G ist nicht nur einfach eine weitere Mobilfunktechnologie, sondern spannt ein völlig neues Universum der Mobilkommunikation und ihrer Möglichkeiten auf. Natürlich wird es auch eine „verbesserte“ Handy-Kommunikation geben, aber die eigentliche Herausforderung ist die Versorgung von Milliarden neuer Mobilstationen im Rahmen von IoT. Ein autonomes Auto erzeugt bis zu 60 GByte Daten pro Stunde, ein Wärmehähler vielleicht 1000 Bit/Monat. Tauchen Sie mit diesem Report in die Welt der Anwendungen, Möglichkeiten und technischen Lösungen dafür ein. Übrigens: die Standardisierung wird in wichtigen Teilen von 2020 auf 2018 vorgezogen. Seit es Funkssysteme mit größerer Ausbreitung gibt, machen sich viele Menschen Sorgen um die möglichen Schäden für ihre Gesundheit. In letzter Zeit ist es vermehrt zu einer Ballung und Verdichtung solcher Systeme gekommen, die bei Manchen sogar Angst oder andere psychologische Wirkungen hervorgerufen hat, die sie in Leben und Arbeit negativ beeinflusst haben. Der Report blickt auf den aktuellen Stand der Forschung und gibt Anhaltspunkte zur weiteren Recherche.

Bestellung an kundenservice@comconsult-research.de

Wireless-Systeme der nächsten Generation – Anwendungen, Systeme, Anforderungen

Ich bestelle den Report

Wireless-Systeme der nächsten Generation

zum Preis von 349,- € netto zzgl. Versandkosten

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ,Ort

eMail

Unterschrift



Bestellen Sie über unsere Web-Seite

www.comconsult-akademie.de

Dank Apple wird Augmented Reality ein massentauglicher Gamechanger

Dank Apple wird Augmented Reality ein massentauglicher Gamechanger



Mark Zimmermann weist mehrere Jahre Erfahrung in den Bereichen Mobile Sicherheit, Mobile Lösungserstellung, Digitalisierung und Wearables auf. 2009 hat er ein Team zur mobilen Lösungsentwicklung für einen der großen Energieversorger Deutschlands aufgebaut. Dieses Team hat über die Zeit sowohl Endkunden-Apps als auch Apps für den internen Einsatz agil gemeinsam mit dem Fachbereich entwickelt. Für eine dieser Lösungen wurde im Jahr 2013 der Best-Practice-Award 2013 des Bensberger Kreises vergeben. Er versteht es, mobile Themen aus den unterschiedlichen Herausforderungen darzustellen. Hierzu ist er auf nationaler Ebene mit Vorträgen und als freier Autor für Fachpublikationen tätig.

Als Steve Jobs das erste iPhone vorgestellt hatte, wurde er von verschiedenen etablierten (Handy-) Herstellern belächelt. Keiner ahnte, wie die Auswirkungen dieses Gerätes aussehen würden.

Es folgten immer „fettere“ Jahre der Gewinne, in denen die Smartphone-Branche jährlich um 50 Prozent zulegte. Im Jahr 2016 endeten diese Zuwachsraten jedoch. 2016 verkaufte Apple noch 74,8 Millionen iPhones und in 2017 waren es dann (immerhin) 78,2 Millionen. Dies lässt die Schlussfolgerung zu: drei Jahre nach dem letzten Kassenschlager (iPhone 6), wächst auch Apple im einstelligen Prozentbereich und folgt damit den anderen Marktteilnehmern.

Auf der Seite des iPads sieht es hingegen anders aus. Die Verkaufszahlen des iPads haben sich nach über drei Jahren erstmals im dritten Quartal 2017 stabilisiert. Der Abwärtstrend wurde, anscheinend mit Ausblick auf die Möglichkeiten mit iOS 11, gebremst. Hier zeigt sich, dass Apple scheinbar den Wunsch und den Bedarf der Bestands- und Unternehmenskunden erkannt hat und mit steuernden Maßnahmen einen positiven Einfluss bewirken konnte.

Dies ist signifikant für die Entwicklungen am Markt, denn hier findet ein Fokuswechsel vom Neukunden auf Bestandskunden statt. Bestehende Kunden müssen für die Plattform weiter begeistert werden, Neukunden müssen diese Begeisterung entfacht bekommen. Anreize, ein neues Gerät zu kaufen, sind nun nicht nur hardwarenahe Möglichkeiten wie eine „High Speed“-Datenübertragung oder ein „Dual-Kamera“-System. Auch Softwareneuheiten wie „Augmented Reality“ stehen im Vordergrund bei einer Endgeräte/Plattform Auswahl.

Augmented Reality (AR) als Produktivitätsfaktor

Apple ist nie der Erste, aber wenn Apple etwas anfasst - dann richtig. Auch wenn viele es anders vermuten, aber es war noch nie das Ziel von Apple, der Erste am Markt zu sein. Der iPod war nicht der erste MP3-Player, das iPhone nicht das erste Smartphone, das iPad nicht das erste Tablet.

Auch im Umfeld von AR ist dies nicht anders. Es gab bisher viele Lösungen am Markt. Diese basierten teilweise auf besonderer Hardware (z.B. Projekt Tango von Google) oder benötigten Markerbildern bzw. QRcodes für die Platzierung von Objekten im Raum.

Mit iOS 11 gibt Apple nun den Entwicklern ein Framework an die Hand, mit dem die bestehenden Lösungen über Nacht bedeutungslos geworden sind. Mit iOS 11 entstand die größte AR-fähige Plattform der Welt (Stand 2017) mit einer einfachen Entwicklungsumgebung.

Einfach für Entwickler

ARKit ist nicht nur mächtig, es fokussiert sich auch komplett auf die Entwicklergemeinschaft. Apple bietet die API nicht nur in Xcode, zur Positionierung von Objekten per SceneKit (3D) bzw. SpriteKit (2D) an, sondern auch direkt als Unity3D- sowie Unreal-Plugin. Die beiden Game-Engines sind sowohl für die Spiele-Entwicklung als auch für geschäftlich genutzte 3D-Anwendungen eine feste Größe mit jeweils einer eigenen breiten Entwicklergemeinschaft.

Neben der Entwicklergemeinschaft überraschen ARKit-Anwendungen durch die Genauigkeit, mit der virtuelle Objekte auf ebenen Flächen positioniert werden können. Digitale 3D-Abbilder lassen sich mit

ARKit in realen Umgebungen mit 60 fps platzieren. Dabei greift ARKit unter anderem auf das ebenfalls mit iOS 11 eingeführte Framework Metal 2 zurück. Bereits vor einiger Zeit löste Apple das in die Jahre gekommene OpenGL Framework durch eine schlanke und performante Implementierung mit Namen Metal 1 ab. Metal 2 verspricht noch einmal das 10-fache an Performance.

ARKit ist enorm umfangreich und bleibt trotzdem für Entwickler ein leichtgewichtiges Framework, vor allem im Vergleich zu bisher am Markt vorhandenen (Open-Source-) Alternativen.

Räume verstehen und Objekte platzieren

Die bereits erwähnten QRcodes und Markerbilder halfen bisherigen Lösungen, eine Position zu erkennen und die Orientierung der Fläche im Raum im Verhältnis zum iPhone zu bestimmen. ARKit erledigt dies nebenbei. Dabei erfasst ARKit die im Raum befindlichen Flächen (inkl. deren Begrenzung) und erkennt die Höhenunterschiede zwischen den Flächen. So werden Flächen auf Tischen und Böden korrekt in Relation gesetzt. Entwickler erhalten direkt Zugriff auf eine 3D Landschaft, in der sich Objekte positionieren lassen. Das iOS Gerät ist dabei die „virtuelle Kamera“. Dies wird auch als „visual inertial odometry“ bezeichnet. Das Drehen des iPhones dreht für die jeweilige App „lediglich“ die virtuelle Kamera.

Damit die digitalen Bilder in der realen Umgebung auch in der richtigen Größe dort auftauchen, nutzt Apple die Hardware seiner Geräte voll aus. Hierzu gehören die integrierte Kamera sowie die Lage- und Bewegungssensoren. Bei dem iPhone 7 Plus kommt auch die Dual-Kamera mit zum Zug, um die Entfernung von

Dank Apple wird Augmented Reality ein massentauglicher Gamechanger

Objekten noch genauer zu berechnen. Schwenkt der Anwender mit dem iPhone oder iPad kurz "aus dem Bild", dreht er sich um die eigene Achse oder geht einige Schritte und blickt zurück, hat sich das positionierte Objekt nicht fortbewegt.

Die Genauigkeit ist beeindruckend. Auf iOS-Geräten mit mindestens einer A9-CPU (iPhone SE, iPhone ab 6s, iPad ab 2017 bzw. Pro-Modelle) können sich Objekte fest positionieren lassen. Diese behalten auch dann ihren Platz, wenn der Anwender mit dem Gerät den Raum verlässt. Zwar verdecken reale Wände und Objekte nicht das 3D-Abbild, aber die Genauigkeit ist trotzdem verblüffend.

So präsentierte Craig Federighi, Senior Vice President Software Engineering bei Apple, in einer rund zweiminütigen Demonstration auf der WWDC 2017, wie sich eine virtuelle Tasse Kaffee, eine virtuelle Lampe und eine virtuelle Vase auf einem realen Tisch positionieren lassen und führte vor, wie lebensnah beispielsweise der virtuelle Schattenwurf ausfällt.

Die am 12. September vorgestellten iPhone Modelle mit der neuen A11 Bionic-CPU, einem neuen Lage- und Beschleunigungssensor und speziell kalibrierter 12 MP Kamera, bieten eine noch genauere Präzision. (siehe Abbildung 1)

Die Demo war mehr als beeindruckend, denn sie macht deutlich, dass ARKit sich nicht nur um die Positionierung von Objekten im Raum kümmert. Apple nimmt dem Entwickler nicht nur die Notwendigkeit ab, selbst ein Verständnis der Umgebung (Umgebung erkennen und verstehen zur realistischen Positionierung) zu implementieren, ARKit unterstützt auch



Abbildung 1: Die virtuelle Tasse wird, je nach Beleuchtungssituation, angepasst dargestellt

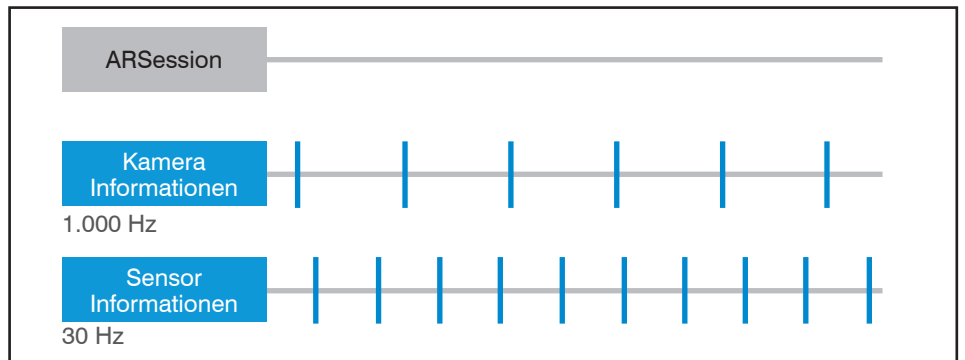


Abbildung 2: Das Zusammenspiel von Kamera (Optik) und (interner) Sensorik reicht aus, um Objekte im richtigen Größenverhältnis, an einer festen Stelle, mit korrekter Auswertung der Beleuchtungssituation darzustellen.

bei der Auswertung von Helligkeit und Farbtemperatur.

Die vorherrschende Beleuchtung wird ebenfalls als Beleuchtungsinformation auf Basis der Umgebungslichtberechnung (Standardwert: 1000 Lumen) ausgewertet. Ein virtuelles Objekt wird damit weder zu hell noch zu dunkel dargestellt. Auch Veränderungen der Lichtverhältnisse zur Laufzeit werden korrekt einbezogen. (siehe Abbildung 2)

Flächen lassen sich mit ARKit nur auf Tischen, Böden und Ähnlichem erkennen. An Wänden fehlt diese Funktion noch. Trotzdem können diese ebenfalls für die Positionierung genutzt werden. ARKit verwendet hier so genannte Featurepoints. Das sind im Grunde „Auffälligkeiten“ in der Umgebung. An horizontalen Flächen werden diese zu Ebenen zusammengefasst, an Wänden, Schrägen oder Decken stehen die Featurepoints einzeln zur Verfügung. Auch hier kann eine Interaktion mit virtuellen Objekten erfolgen.

Apple hört im Übrigen nicht mit der reinen Positionierung auf. Die Objekte können animiert werden und sogar als Audio-Quelle fungieren. Der Ton wird daraufhin positionsgenau angespielt. Dabei berücksichtigt das Framework auch die akustische Filterung durch digitale Objekte, die zwischen der Audioquelle und der virtuellen Kamera liegen. Hier spielen die iOS-Frameworks jedoch eine übergeordnete Rolle, da ARKit lediglich die „Bühne für das Schauspiel“ ist.

Zusätzliche Möglichkeiten mit dem iPhone X

Mit dem iPhone X werden die bereits genannten Sensoren nicht nur verbessert, es gibt auch einen neuen zusätzlichen Sensor. Der True-Depth-Sensor, auf der Vorderseite des iPhone X, wird nicht nur für die beworbene Gesichtserkennung zum Entsperren

des Gerätes - als Ersatz für TouchID - verwendet.

Entwickler können auf einem iPhone X diesen Sensor zu einer stabilen und flüssigen Gesichtsauswertung nutzen. Dabei stehen dem Entwickler nicht nur die Tiefeninformation (AVDepthData), sondern auch eine Erkennung der Gesichtsmetriken und des Gesichtsausdrucks in Echtzeit zur Verfügung.

Diese Daten stehen mit 60Hz zur Auswertung bereit, sobald ein Gesicht erkannt wird. Ab jetzt steht das Gesicht dem Entwickler als so genannter ARFaceAnchor zur Verfügung. Also solcher beschreibt die API nicht nur aktuelle Position und Orientierung des Gesichtes, es stehen auch 3D Informationen zur Topologie (ARFaceGeometry) und des Gesichtsausdrucks zur Verfügung.

Dabei steht keine reale Gesichtsmasse direkt zur Verfügung. Vielmehr entspricht die Topologie einem generischen Gesichtsmodell, um die Dimensionen, die Form und den aktuellen Ausdruck des detektierten Gesichtes abzurufen. Dies erlaubt es Entwicklern, nicht nur Selfi-Effekte wie z.B. MakeUp, Tattoos usw. zu simulieren, es erlaubt auch das Erfassen von „Emotionen“ in Echtzeit.

Die so genannten blendShapes stellen ein abstrahiertes Modell des aktuellen Gesichtsausdrucks zur Verfügung. Entwickler erhalten so Zugriff auf die Bewegung einzelner Gesichtselemente (Auge, Mund, ...) des Anwenders. Diese Informationen können verwendet werden, um 2D- oder 3D-Inhalte wie einen Charakter oder einen Avatar zu beleben, aber auch, um die Gesichtsausdrücke mit besagten „Emotionen“ in Echtzeit zu verbinden.

Hier ist vor allem im dienstlichen Einsatz Vorsicht geboten. Aufgrund der Fürsorgepflicht von Unternehmen für Mitarbeiter, ist ein kritisches Auge auf derartige Aus-

Dank Apple wird Augmented Reality ein massentauglicher Gamechanger

wertungen in Apps zu achten. Stellen Sie sich eine Customer Relationship Management App vor, die zum Verwalten von Kundenbeziehungen aktiv genutzt wird. Mit diesen ARKit Auswertungen könnte diese App (theoretisch) den Gefühlszustand des Mitarbeiters - zur Laufzeit - erfassen, analysieren und sogar zu einer Leistungsbeurteilung heranziehen.

Effizient für Unternehmen

Die gezeigten Möglichkeiten, bereits wenige Tage nach der Ankündigung zur WWDC 2017, waren beeindruckend. AR wurde über Nacht massentauglich. Entwickler aus aller Welt zeigten positionierte 3D Objekte, nicht nur auf Tischen und Fußböden, auch an Wänden und in der freien Natur. Teure Hardware wie die HoloLens wird damit unnötig.

Alleine die Tatsache, dass Entwickler binnen Tagen schon sehr ansehnliche Demos erstellt haben, verdeutlicht, wie komfortabel sich die Schnittstelle nutzen lässt. Die folgenden Beispiele geben dabei einen Eindruck der technischen Machbarkeit dieser Technologie.

Beispiel 1: Beratung für Möbel- und Einrichtungshäuser

Jeder hatte schon mal diese Fragen: "Passt das Sofa in mein Wohnzimmer?", "Welche Stühle passen zu welchem Tisch am besten?" oder auch "Wie bekomme ich die ganzen Schränke und Elektrogeräte in meiner "Wunsch"-Küche unter?"

Als Verkaufsinstrument unterstützt ARKit das Vertriebspersonal dabei, ein Produkt in allen Farbvariationen in Originalgröße vor dem Kunden zu präsentieren. Privatleute können ihr Zuhause mit Einrichtungsgegenständen in AR ausstatten und so einen Fehlkauf verhindern.

Wie Apple schon auf der Keynote zur WWDC 2017 verlauten ließ, arbeitet der Möbelhersteller IKEA bereits an einer entsprechenden Virtualisierung seines Kataloges. Das Ergebnis des schwedischen Möbelriesen nennt sich "Ikea Place" und hält genau das ein, was man sich von einer Augmented-Reality-App verspricht. Sie bekommen so nicht nur ein Gefühl dafür, ob ein Möbelstück gut aussieht. Sie erkennen auch, wie es sich in dem Rest des Raumes integriert.

In Zukunft sind Sie in der Lage, die geplante Küche direkt in Ihrer Wohnung zu sehen. Sie sehen die Anschläge der Türen (in welche Richtung sie sich öffnen), die Armaturen des Waschbeckens, den Herd und alles andere. Das Ganze wird im 1:1-Maßstab eingeblendet.

Beispiel 2: Visualisierungen für Architekten, Garten- und Landschaftspfleger
ARKit kann auch große Objekte, z.B. Häuser einblenden. Visualisierungen können so auf einer Baustelle überlagert dargestellt werden und unterstützen bei der Positionierung von Leitungen, Finden von verlegten Anschlüssen oder bei der Vorschau von Materialien im Endausbau.

Stellen Sie sich vor, Sie betreten eine Wiese, auf der Ihr Traumhaus entstehen soll. Der Architekt hat eine entsprechende App dabei und Sie können in das neue Heim virtuell hineingehen. Sie planen Steckdosen, Tapetenfarbe, Fenstergrößen, einfach alles. Und wenn es in den ersten Stock hochgehen soll, kann der Architekt diesen zu Ihnen "herunter" holen, denn virtuelle Treppen lassen sich nur schwer besteigen.

Beispiel 3: Museen und Ausstellungen
Die bisherigen Beispiele zeigen Objekte in ihrer Originalgröße. In Museen und Ausstellungen können ARKit Apps genutzt werden um historische Schlachten auf dem Tisch nachzustellen oder um Überreste von Burgen und Städten virtuell darzustellen. Jeder noch so kleine Winkel kann "gesichtet" und durch Sprachausgabe und Infotafel "erklärt" werden.

Beispiel 4: Endkundensupport

Mit iOS 11 haben Entwickler auch Zugriff auf die Tiefeninformation der zweiten Kamera (iPhone 7 Plus). Muss ein Anwender eine Waschmaschine anschließen und ist sich nicht sicher, wie die notwendigen Handgriffe sind, kann er sich diese vom Support direkt zeigen lassen. Dank der Tiefeninformation können "Montagehinweise" direkt im Raum, in der richtigen Tiefe, eingeblendet werden.

Auch beim Thema Customer Support wird Augmented Reality neue Möglichkeiten schaffen. Fällt beispielsweise eine Waschmaschine beim Privatkunden oder eine Produktionsanlage im Unternehmen aus, können Lösungsansätze im direkten Umfeld der Maschine eingeblendet werden, so dass Servicetechniker oder die Kunden selbst Unterstützung erhalten.

Die Möglichkeit, einen Experten per Remote-Support dem Kunden zuzuschalten, werden so zum Greifen nah.

Aber auch in der Industrie revolutioniert AR den Umgang mit Anleitungen. So können Bedienungsanleitungen direkt als Überlagerung an Geräten angezeigt werden.

Beispiel 5: Werkzeugkasten in der Hosentasche

Auf Grund der genauen Erfassung kann

ARKit auch als Möglichkeit zur Abstandsmessung verwendet werden. Techniker kommen so in die Lage physikalische Abmessungen per App komfortabel zu erfassen.

Beispiel 6: Assistenzsystem zur Navigation

Navigationen, sowohl draußen als auch in Innenräumen wie Lagerhallen und Bürogebäuden, lassen sich mit visueller Unterstützung anreichern. Anwender erhalten so keine abstrakte Karte. Vielmehr erhält dieser einen korrekt dargestellten Weg direkt in der physikalischen, die er interpretieren muss. Es zeigen Pfeile den korrekten Pfad direkt in der eigenen Umgebung an.

Die Augmented-Reality-App-Schlacht beginnt

Die technische Meisterleistung von ARKit blieb nicht lange ohne Folgen. Mit dem SDK ARCore reagierte Google auf Apples Vorstoß innerhalb weniger Monate. Bis dahin war die AR-Plattform von Google, mit Namen Tango, an spezielle Sensoren und Kameras gebunden. Diese waren kaum bis gar nicht käuflich erwerblich. Eine Unterstützung auf handelsüblichen Geräten gab es nicht. Dies versucht Google nun mit ARCore zu liefern.

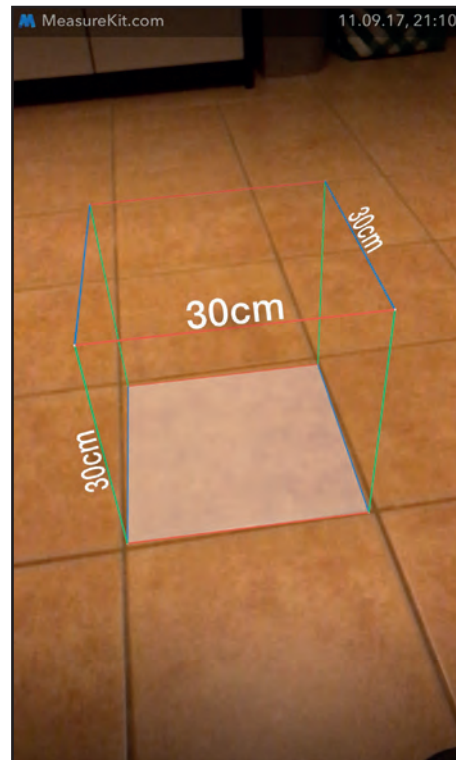


Abbildung 3: Die MeasureKit-App von www.MeasureKit.com zeigt beeindruckend, welche Werkzeuge (Zollstock, Wasserwaage, Winkelmesser und viele mehr) mit ARKit möglich sind

Dank Apple wird Augmented Reality ein massentauglicher Gamechanger

Softwareseitig setzt ARCore auf Java/OpenGL, Unity bzw. Unreal. Dabei bietet das Framework eine Bewegungsverfolgung, die Erfassung und Analyse der Umgebung und der Lichtverhältnisse.

Was sich auf den ersten Blick wie die Möglichkeiten von ARKit anhört, ist bei genauerer Betrachtung nur eine Schnittmenge davon. Abgesehen von (Beta bedingten) Herausforderungen, dass ARCore erkannte Flächen verliert und 3D Objekte im Verhältnis zur virtuellen Kamera „unnatürlich“ darstellt, gibt es tiefgreifende architekturelle Unterschiede.

ARKit setzt nicht auf OpenGL, sondern auf die Apple eigene Optimierung Metal 2. So schafft eine selbst erstellte OpenGL ES 2.0 Demo-App bis zu 2.200 Sprites bei 60 fps auf einem iPhone 6+. Metal 1 hingegen konnte bis zu 6.600 Sprites im gleichen Setup darstellen. Die gleiche Anzahl von Sprites unter OpenGL ES 2.0 reduziert die Darstellung auf 22,5 fps. Da ARKit auf Metal 2 aufsetzen, das für sich noch einmal eine Optimierung um den Faktor 10 veranschlagt, ist die Performance gegenüber OpenGL entsprechend. Zusätzlich ist die Programmiersprache Swift für den Compiler entsprechend optimiert.

Ferner abstrahiert Apple vieles vom Entwickler weg, womit sich ein Android Entwickler konfrontiert sieht. So ist das Platzen von Audio Quellen an SceneKit

Objekten in Swift einfach, in ARCore eine echte (haareraufende) Herausforderung.

Auch die Unterstützung in der Entwicklungsumgebung kommt noch zu kurz. XCODE ist in der Lage, Objekte im DAE (Digital Asset Exchange) zu importieren. Namensaktie 3D Werkzeuge können dieses Dateiformat erzeugen. Für ARCore muss dem Entwickler ein OpenGL Objekt zur Verfügung gestellt werden. Diese Unterstützung fehlt (noch) im Android Studio. Die von Google angepriesenen Tools um 3D Objekte zu erzeugen (Blocks: <https://vr.google.co/blocks> bzw. Tilt Brush: <https://www.tiltbrush.com>) stellen Hilfsmittel zur 3D Erzeugung dar. Eine Konvertierung von bestehenden 3D Objekten habe ich nicht gefunden.

Allgemein muss festgehalten werden, dass vieles noch nicht ausführlich dokumentiert wurde und es noch einige Stolpersteine im Framework gibt, die mit dem aktuellen Beta Stand zu tun haben. Ich bin mir sicher, das Google hier noch (besser) nachlegen wird.

Die aktuelle Version, die Entwicklern als Beta zur Verfügung steht, unterstützt aktuell jedoch nur das Google eigene Pixel-Modell und das aktuellste Samsung Galaxy S8. In Zukunft sollen aber weitere Geräte entsprechende Unterstützung erhalten. Hersteller wie beispielsweise Samsung, Huawei, LG und Asus arbeiten mit Google hier eng zusammen. Am Ende

der Preview-Phase sollen über 100 Millionen Geräte unterstützt werden. Im Vergleich zu der Installationsbasis für iOS ist diese Zahl jedoch immer noch verschwindend gering.

Auf kurzfristige (Apple) und mittlere (Google) Sicht haben die Konzerne aus den Vereinigten Staaten die Möglichkeit, die AR-Technologie für den Mainstream in Smartphones und Tablets zu integrieren. Anbieter wie Facebook stehen hingegen vor dem Problem, nicht die vollständige Kontrolle über die AR-Erfahrung der Anwender zu haben - weil ihnen der tiefe Zugriff auf die (Consumer-)Hardware fehlen.

Fazit

Nach 10 Jahren iOS und Android sind die Kosten für einen Plattformwechsel zwar signifikant, aber nicht unüberwindbar. Allerdings trifft es Apple in diesem Zuge am geringsten, denn ein Wechsel zwischen Samsung, HTC, Sony oder Huawei ist nach Kostenrechnung einfacher als zwischen iOS und Android. Der Schachzug, auch ältere Geräte mit AR zu beglücken, dürfte Apple in die Karten spielen und gleichzeitig einen Zukunftsmarkt adressieren. Analysten schätzen den weltweiten Markt für Augmented Reality bis ins Jahr 2020 auf über 10 Mrd. \$.

Ich freue mich Ihnen in meinem Seminar weitere Besonderheiten und Neuigkeiten aus der iOS-Welt mitteilen zu können.

iOS im Unternehmen

22.11.2017 in Bonn

Die Teilnehmer erhalten zunächst einen Überblick über die neuen Möglichkeiten und Produktivitätspotentiale von iOS 11 aus Sicht eines Mitarbeiters. Im Anschluss folgt der Blick aus Sicht der Unternehmens-IT. Der Lebenszyklus der iOS-Geräte, von der Beschaffung, der Verteilung, der Verwaltung bis zur Rückführung wird näher beleuchtet. Der Schwerpunkt hier liegt auf den Möglichkeiten von MDM-Systemen in Verbindung mit den Be-

reitstellungsprogrammen DEP und VPP aus dem Hause Apple. Abschließend erhalten die Seminarteilnehmer einen Blick unter die Haube. Die Frameworks von iOS verhelfen Unternehmens-Apps zu einem nicht zu verachtenden Effizienzgewinn, gerade im Vergleich zu anderen mobilen Geräteplattformen.

Praktische Beispiele aus dem realen Leben im Umgang mit mobilen Lösungen runden

das Informationsspektrum ab.

Folgende Themenschwerpunkte werden behandelt


- Grundlagen zu iOS
- Herausforderungen und Möglichkeiten für die Entwicklung effizienter Apps
- Praktische Beispiele für und praktischer Bezug zu bestehenden Produktivitäts-Tools

Anmeldung an kundenservice@comconsult-research.de

Ich buche das Seminar **iOS im Unternehmen**

22.11.2017 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 _____

ComConsult Veranstaltungskalender

**Kommunikation über Private WAN und Internet,
16.10. - 17.10.2017 in Frankfurt**

Garantietermin

Dieses Seminar vermittelt die Erfahrungen aus den jüngsten Projekten mit dem Fokus Konzeption und Ausschreibung von WANs. Teilnehmer dieses Seminars profitieren von langjährigen Erfahrungen der Vortragenden im WAN-Bereich, kombiniert mit dem großen Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen. Ferner werden Erfahrungen bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb in diesem Seminar vermittelt.

Preis: 1.590,-- €*

**IP-Telefonie und Unified Communications erfolgreich planen und umsetzen,
16.10. - 18.10.2017 in Frankfurt**

Garantietermin

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: 1.890,-- €*

**Sonderveranstaltung: IT-Infrastrukturen für das Gebäude der Zukunft,
17.10.2017 in Bonn**

Garantietermin

Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die Gewerke-übergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können. Diese Veranstaltung wendet sich an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerke-übergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.

Preis: 1.090,-- €*

**IT-Verträge: B2B – verhandeln, verändern, durchsetzen, sanieren,
18.10.2017 in Bonn**

Garantietermin

Lernen Sie als Nichtjurist wie Sie einen guten Vertrag für den Kauf oder Verkauf eines Produktes oder einer Dienstleistung umsetzen können. Beherrschen Sie die unbedingt notwendigen Teile eines Vertrags. Vermeiden Sie typische Fehler und bereiten Sie sich angemessen auf Krisen vor.

Preis: 1.090,-- €*

Sonderveranstaltung: Wireless und Mobility, 18.10. - 19.10.2017 in Bonn

Garantietermin

Das IoT, autonome Mobilität und neue Arbeitsplatzmodelle verändern die Anforderungen an flächendeckende Wireless Infrastrukturen dramatisch. Neue WLAN-Techniken und 5G Mobilkommunikation führen zu einem neuen Universum für die Versorgung von menschlichen und maschinellen Teilnehmern. Die Sonderveranstaltung widmet sich mit herausragenden Referenten diesem hoch dynamischen Problembereich.

Preis: 1.990,-- €*

IT-Projektmanagement Kompaktseminar, 07.11. - 09.11.2017 in Aachen

Rabattaktion

Seminar über Projektmanagement in der IT. Es wird speziell auf die Anforderungen und Herausforderungen von IT-Projekten eingegangen. Lernen Sie wie Sie Projekte sauber aufsetzen und überwachen und mit welchen Methoden und Hilfsmitteln Sie die Termin-einhaltung sicherstellen können.

Preis: 1.890,-- €*

Troubleshooting für Netzwerk-Anwendungen, 07.11. - 09.11.2017 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,-- €*

Crashkurs IT-Recht für Nichtjuristen, 08.11.2017 in Düsseldorf

Basis-Kenntnisse im IT-Recht sind ein Muss für jeden Projektleiter oder Entscheider. Dieser Crash-Kurs bringt Sie in einem Tag auf den Stand des notwendigen Wissens: Vertragsrecht, Datenschutz, Lizenzrecht, Compliance, IT-Sicherheit und Haftung.

Preis: 1.090,-- €*

RZ-Kopplung: Georedundanz für Rechenzentren, 08.11.2017 in Düsseldorf

Die gestiegene Bedeutung von zentralen IT-Systemen für Unternehmen und gesetzliche Vorgaben erfordern geo-redundante Standorte von Rechenzentren. Für die Bereitstellung und den Betrieb der Rechenzentrums-Kopplung wird besonderes Know-how und strategische Planung benötigt. In diesem Seminar werden die aktuellsten Technologien und Anforderungen vorgestellt und ein optimales Gesamtkonzept beschrieben.

Preis: 1.090,-- €*

SIP – Basis-Technologie der IP-Telefonie, 08.11. - 10.11.2017 in Stuttgart

Ziel der Schulung ist die Erläuterung von SIP als Schlüsseltechnologie für eine offene, leistungsfähige und kostenoptimale Kommunikationslösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Herstellerlösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: 1.890,-- €*

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger

19.02. - 23.02.18 in Aachen
14.05. - 18.05.18 in Aachen

TCP/IP-Netze erfolgreich betreiben

12.03. - 14.03.18 in Berlin
04.06. - 06.06.18 in Bonn

Internetworking

13.11. - 16.11.17 in Aachen
09.04. - 12.04.18 in Aachen
18.06. - 21.06.18 in Aachen

Paketpreis für ein 5-tägiges, ein 4-tägiges, ein 3-tägiges Intensiv-Seminar € 6.000,--* (Einzelpreise: € 2.490,--*, € 2.290,--*, 1.890,--*)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen

24.04. - 27.04.18 in Aachen

Trouble Shooting für Netzwerk-Anwendungen

07.11. - 10.11.17 in Aachen
15.05. - 18.05.18 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen

16.10. - 18.10.17 in Frankfurt
12.03. - 14.03.18 in Bonn
14.05. - 16.05.18 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie

08.11. - 10.11.17 in Stuttgart
11.04. - 13.04.18 in Düsseldorf
04.06. - 06.06.18 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications

27.11. - 29.11.17 in Berlin
23.04. - 25.04.18 in Bonn

Optionales Einsteiger-Seminar:

IP-Wissen für TK-Mitarbeiter

19.02. - 20.02.18 in Bonn
03.05. - 04.05.18 in Köln

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,--* statt € 5.670,--*

Optionales Einsteigerseminar: Aufpreis € 1.190,--* statt € 1.590,--*

* alle ausgewiesenen Preise sind netto-Preise

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: kundenservice@comconsult-research.de
<http://www.comconsult-research.de>

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

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research