ComConsult Research

Der Netzwerk Insider

Oktober 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Authentifizierung und Single Sign On in Cloud-Umgebungen

von Dipl.-Math. Cornelius Höchel-Winter

Die Flut an Cloud-Angeboten nimmt täglich zu und es ist heutzutage nicht nur im privaten Umfeld kaum vorstellbar ohne Software oder Infrastruktur-Produkte aus der Cloud auszukommen. Die Nutzung von Software im Allgemeinen muss aber einfach und intuitiv sein, und dies gilt im Besonderen für Aspekte, die vom Benutzer als eher lästige Randerscheinungen wahrgenommen werden. Hierzu zählt an erster Stelle der Anmeldevorgang.

Hinzu kommt, dass kaum ein Anwender dazu in der Lage ist, sich ohne zusätzliche Hilfsmittel eine Vielzahl verschiedener

Passwörter in der nötigen Komplexität zu merken – und das gängige Hilfsmittel hierfür ist nach wie vor der Zettel in der oberen Schreibtischschublade.

Die Lösung hierfür heißt Single Sign On, das heißt der Aufbau oder die Nutzung einer Authentisierungs- und Autorisierungsarchitektur, bei der sich der Benutzer nur ein einziges Mal anmeldet (authentisiert) und die dann im Hintergrund und transparent für den Benutzer dafür sorgt, dass er die Anwendungen, die für ihn freigegeben sind, so nutzen kann wie sie für ihn freigegeben sind.

weiter auf Seite 6

Zweitthema

Strukturierte Verkabelung für Technische Gebäudeanlagen

von Dipl.-Ing. Hartmut Kell

Vor über 20 Jahren wurde in der EN 50173 die „Anwendungsneutrale Kommunikationskabelanlage“ in ihrer ersten Version spezifiziert, trotz anfänglicher Skepsis und durchaus vieler Optimierungspunkte hat sie sich durchgesetzt, ein Gebäude mit Büroarbeitsplätzen ist ohne informationstechnische Verkabelung und damit ohne Anwendung der EN 50173 nicht mehr vorstellbar.

Die Nutzbarkeit und Akzeptanz dieser ersten Version führte dazu, dass auch eine Standardisierung der IT-Verkabelung in Gebäuden ohne Büroarbeitsplätze sukzessive erfolgte. Ob Rechenzentrum oder Industriegebäude, für alles gibt es eine europäische oder nationale Verkabelungsnorm. Ganz zum Schluss erst aber wurde in den Normungsgremien die Notwendigkeit gesehen auch eine anwendungsneutrale Kommunikationsverkabelung für Geräte zu definieren, die selbstverständlich in jedem Gebäude zu finden ist, die aber bisher klassisch mit Netzwerk oder ähnlichem nichts zu tun hatte und damit mit eigenen Strukturen, Materialien und Techniken versorgt wurde. Bei der Planung von Gebäuden wird diese Form der Technik mit dem Begriff der „Technischen Gebäudeanlage“ oder abgekürzt TGA beschrieben und es war abzusehen, dass auch in diesem speziellen Umfeld eine andere Art der Kommunikationsverkabelung mehr und mehr Einzug halten wird. Der nachfolgende Artikel geht auf diese Art der Verkabelung ein und analysiert die im Jahr 2014 verabschiedete Norm, die aus Sicht des Autors auch nach 2 Jahren noch nicht im Bewusstsein der Fachplaner angekommen ist.

weiter auf Seite 21

Geleit

Herausforderung Agilität

auf Seite 2

Standpunkt

„Alle Räder stehen still, wenn dein starker Arm es will“ oder das unterschätzte Angriffspotential von DDoS

auf Seite 16

Aktuelle Kongresse

ComConsult Technologie-Tage 2016 UC-Forum 2016

auf Seite 4/5 und Seite 14/15

Aktuelle Sonderveranstaltung

Wireless und Mobility

auf Seite 17/18

Zum Geleit

Herausforderung Agilität

Wer kennt sie nicht, die Erzählungen über Projekte, die Wochen oder Monate auf einen Server oder mehr Netzwerk-Kapazität warten mussten. Aber diese Zeiten sind vorbei. Wenn es ein einzelnes herausragendes Kriterium gibt, an dem sich die IT-Infrastruktur-Planung in Zukunft orientieren muss, dann ist es die schnelle Bereitstellung von Kapazitäten. Und der Begriff Agilität beschreibt genau dies, also eine IT-Infrastruktur, die agil und flexibel ist.

Warum ist dies das dominante Kriterium für eine Zukunfts-orientierte IT? Dafür gibt es mehrere Gründe.

Der sicher dominierende Grund ist, dass viele Branchen und Unternehmen sich in einer Wettbewerbs-Situation befinden, die es nicht mehr erlaubt, Projektzeiten von 12 bis 24 Monaten für eine zentrale Lösung zu haben. Die Liste der Unternehmen, die in den letzten 10 Jahren gescheitert sind, weil sie sich nicht schnell genug anpassen konnten, ist lang. Und dies wird sich in den kommenden Jahren weiter verschärfen. Fortschritte auf der Technologieseite (zum Beispiel im Bereich Artificial Intelligence), die Notwendigkeit einer neuen und verbesserten Kunden-Ansprache und ein zunehmender internationaler Konkurrenzdruck erzeugen einen exponentiell wachsenden Druck auf einzelne Branchen. Nicht alle werden davon betroffen sein, aber wen es trifft, den trifft es hart. Die IT-Abteilung ist dabei in der Regel gar nicht der Kern des Problems. Ein Unternehmen muss sich in seiner Gesamtheit an die veränderten Marktgegebenheiten anpassen. Und dabei gibt es viele interne Widerstände. Diese führen aber auch dazu, dass häufig ein Sündenbock gesucht wird. Und IT ist prädestiniert dafür.

Der zweite und sehr ernst zu nehmende Grund ist die veränderte Architektur von Anwendungen. Die betrifft zwar nicht alle Anwendungen, aber sicher mehr als 90%. Anwendungs-Architekturen sind heute stark parallelisiert und erlauben damit eine schnelle Anpassung an wechselnde Last-Anforderungen. Dies passt wiederum sehr gut zu modernen Virtualisierungs-Architekturen, die Lastanpassung über die Anzahl paralleler virtueller Maschinen umsetzen. Und es gibt eindrucksvolle Beispiele dazu, wie gut solche Architekturen skalieren.

Der dritte Grund liegt in einem Umdenken in Benutzer-Schnittstellen. Vor allem Web-Applikationen, die auf eine bestimmte Art der Bedienung ausgelegt sind, haben Benutzerschnittstellen in eine bestimme Richtung verschoben. Ein Beispiel sind Dashboards in ERP-Anwendungen, die flexibel angepasst werden können und aus denen heraus ein schneller Drill-Down in die Details möglich ist. Diese Art der Anwendung sehen wir heute in der gesamten Breite von CRM bis hin zur Buchhaltung.

Der vierte Grund ist die Weiterentwicklung von Artificial Intelligence AI. Hier werden wir aller Voraussicht nach in den nächsten drei bis fünf Jahren eine signifikante Änderung beobachten. Neben IBM mit dem schon alten Bekannten Watson sind auch Google und Microsoft aggressiv an den Markt gegangen. AI wird vor allem die Interaktion mit Benutzern verändern, indem das System quasi ahnt was der Benutzer will und die entsprechende Funktionalität anwendet oder bereit stellt. Das ist nicht neu und alle neueren Buchhaltungssysteme wenden eine einfache Regel-basierte Form davon an (mit einer dramatischen Reduzierung der notwendigen Zeit bei der Eingabe und einer Reduzierung der Fehlerquote), aber es nimmt an Geschwindigkeit zu. Tatsächlich kann dieser vierte Bereich dazu führen, dass Unternehmen viel schneller als erwartet wesentliche Anwendungen neu programmieren müssen, wollen sie nicht zurück fallen.

Wo liegt jetzt aber das Problem für die IT-Abteilung? Nun, zum einen ist nicht jede Infrastruktur-Lösung skalierbar. Wir haben in der Vergangenheit häufig auf den besseren und schnelleren neuen großen Server gesetzt. Das dies nun keine Rolle mehr spielt, da nur die Zahl der parallelen virtuellen Server entscheidet, erfordert ein Umdenken. Damit ist auch ein Umdenken in den Betriebsprozessen verbunden, da sich die Zahl der Betreuungspunkte erhöht und formal ein Problem im Operating entsteht, wenn Applikationen nicht mehr statisch den Betriebsmitteln zugeordnet werden. Das ist aber nicht das zentrale Problem. Das zentrale Problem ist, dass isolierte Lösungen keinen Sinn machen. Wenn ich Kapazität skalieren will, dann muss das für die Gesamtheit aus Server, Speicher, Netzwerk, Sicherheit gelten. Kombiniert man das mit dem Anspruch von Verfügbarkeit und im Extremfall von Georedundanz, dann wird die Aufgabe komplex (auch weil dies über ggf über Abteilungs-Grenzen hinaus geht). Und damit ist man dann je nach Unternehmensgröße bei der Diskussion von Automatisierung. Für kleinere Unternehmen kann dies mit den bestehenden Möglichkeiten der einzelnen Plattformen abgedeckt werden, aber für größere Lösungen wird ein umfassender Ansatz erforderlich. Den liefert im Moment nur OpenStack. Und wie schon häufiger an dieser Stelle erwähnt, ist OpenStack kein Trivialprojekt und dementsprechend teuer.

Dabei drängt sich natürlich der Gedanke an die Cloud auf. Und tatsächlich werden wir genau diesen Aspekt auf unseren Technologietagen vertiefen. Wir sind davon überzeugt, dass es eine sinnvolle Strategie für ein Rechenzentrum für eine erfolgreiche Zukunft gibt. Dabei muss niemand vor der Cloud Angst haben. Aber die Forderung nach Agilität ist völlig unabhängig von einer Cloud-Diskussion zu sehen. Es gibt genügend Anwendungen, die nie in der Cloud landen werden. Und trotzdem muss auch für diese Anwendungen eine agile und flexible Lösung gefunden werden.

Ist der schwarze Peter dabei bei den Basis-Infrastrukturen? Nur wenn sich die Betreiber dumm anstellen. Die Bereitstellung von Rechenleistung, von Speicher, von Netzwerk und Sicherheit muss heute im Stundenbereich möglich sein. Auch wenn die Anforderung völlig unerwartet kommt. Die Betreiber haben schlicht keine andere Wahl und müssen dieses leisten. Wer dies nicht kann, der wird nicht überleben. Tatsächlich wird sich damit aber das Problem verschieben. Der Programmierer der Applikation oder der Datenbank-Planer wird in der Praxis große Probleme haben, neue Funktionalität im Stundenrhythmus anzubieten. Aber hier muss man die Kirche im Dorf lassen. Wir sind historisch gesehen zum Beispiel daran gewöhnt auf neue Funktionen im Banken und Versicherungsbereich Monate und Jahre zu warten. Wenn wir hier eine Lösung schaf-

fen, die diese Zeit auf Wochen reduziert, dann ist das in vielen Bereichen völlig ausreichend. Viel wird aber von dem kompletten Entwicklungssystem, sprich der Gesamtplattform abhängen.

Aber bevor das in der Diskussion untergeht, noch einmal die zentrale Anforderung an Basis-IT-Infrastrukturen: die Bereitstellung neuer Kapazität muss in mehr als 90% aller Fälle in wenigen Stunden möglich sein. Real bedeutet das, dass die Kapazität schon vorhanden sein muss und die Bereitstellungszeit aus der Konfiguration und Übergabe bestehen muss. Dies wiederum bedeutet, dass in eine höhere Kapazität investiert werden muss als eigentlich im Moment gebraucht wird. Aber bei einer geeigneten Technologieauswahl ist dies nicht unbedingt ein wirtschaftlicher Nachteil. Der Weggang vom Einzelsystemdenken hin zu einem Denken in einem wirtschaftlich optimalen modularen System führt auch zu signifikanten Einsparungen. Es ist eben deutlich preiswerter in einen Verbund von E5-Servern zu investieren als in die E7-Spitzenleistung zu gehen.

Zum Abschluss soll an dieser Stelle noch einmal betont werden, dass wir von ComConsult Research in dem Merkmal der Agilität das wichtigste Kriterium einer zukunftsorientierten IT sehen. Agilität sollte vor allen anderen Diskussionen kommen. Ohne Agilität geht in Zukunft gar nichts mehr.

In diesem Sinne

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Technologie-Tage 2016 07.11.-08.11.16 in Köln

Die ComConsult Technologie-Tage 2016 wenden sich an Führungskräfte und Entscheider und analysieren wie unsere IT in Zukunft aussehen wird. Die Kernthemen sind: Strategien für das Rechenzentrum der Zukunft, Skalierbarkeit im Technologie-Mix 2020, Kommunikations-Strategie 2020, Sicherheits-Strategie 2020.

Moderator: Dr. Jürgen Suppan - Preis: 1.990,- € netto

Besuchen Sie auch das Kongress-Portal zu diesem Kongress

Auf dem Portal stellen wir Ihnen Hintergrundinformationen rund um die Themen der Veranstaltung zur Verfügung.

Einige Beiträge sind spezielle Angebote, auf die ausschließlich Kongressteilnehmer Zugriff haben. Melden Sie sich hierfür mit Ihren Zugangsdaten an.

Nutzen Sie die Gelegenheit, hier bereits im Vorfeld der Veranstaltung Kommentare und Fragen zu den einzelnen Beiträgen abgeben zu können und mit den Referenten über die Themen zu diskutieren.

Folgende Artikel stehen Ihnen z.B. auf dem Portal zur Verfügung:

Data Analytics im Rechenzentrum
Das Fax stirbt 2018 – T.38 ein Verfahren ohne Zukunftssicherheit
Distributed Virtual Routing (DVR)
Die Zukunft des SIP Protokolls

Informieren Sie sich jetzt!

www.comconsult-research.de/kongresse/ttage-2016/

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktueller Kongress

ComConsult Technologie-Tage 2016 07.11.-08.11.16 in Köln

Die ComConsult Akademie veranstaltet vom 07.11. bis 08.11.16 ihre "ComConsult Technologie-Tage 2016" in Köln.

Dieses Jahr haben wir folgende zentrale Themenbereiche in den Vordergrund gestellt:

1. Strategien für das Rechenzentrum der Zukunft

Würde man heute ein Rechenzentrum 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 kann ein Rechenzentrum zu einer fundierten technischen und wirtschaftlichen Identität kommen, die die Vorteile der Cloud erfolgreich integriert, aber die Kernleistung weiterhin lokal erbringt.

2. Kommunikations-Strategie 2020 im Mittelpunkt

Betrachtet man den Technologie-Mix aus Server, Speicher, Endgerät und Kommunikation, dann sind die ersten drei genannten Technologie-Bereiche relativ stabil im Sinne einer kontinuierlichen und ggf. etwas verlangsamten Evolution. Die aktuellen Analysen von ComConsult Research sehen aber einen dringenden Bedarf zur Positionierung der Kommunikations-Strategie für die nächsten 3 bis 5 Jahre. Dafür gibt es im Kern zwei Auslöser: All-IP und 5G auf der einen und mobile Endgeräte und Sensoren im Rahmen von IoT auf der anderen Seite. Diese beiden Auslöser werden insbesondere auf der Wireless-Seite eine neue Situation schaffen. Parallel dazu gibt es durch das Zusammenwachsen von WAN und Internet eine neue Form von "Corporate Network".

3. Skalierbarkeit in einem Technologie-Mix

Wenn wir über Strategien für die Zukunft sprechen, muss Skalierbarkeit in jedem Fall im Mittelpunkt stehen. Trotz einer verlangsamten Technologie-Entwicklung bei Servern und Speichern führt der Planungs-Aspekt Skalierbarkeit zu veränderten Produktentscheidungen, bei Speicher-Systemen gar zu veränderten Architekturen. In jedem Technologiebereich wird Skalierbarkeit zum dominanten Planungs-Kriterium. Die Frage ist, welche Ausprägung von Technologien hier einen wesentlichen Zugewinn bringen und wie diese zum Kern einer Zukunfts-Strategie beitragen können. Da wir gleichzeitig eine weiter zunehmende Abhängigkeit zwischen unseren Kern-Technologien haben, muss Skalierbarkeit auch Technologie-übergreifend gesehen werden. Schnell wachsende Kapazitäten bei Servern und Speichern erfordern zwangsläufig eine Anpassung auf der Kommunikationsseite. Skalierbarkeit in einem Technologie-Mix ist deshalb eine zentrale Herausforderung.

4. 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.

Anmeldung an kundenservice@comconsult-research.de

ComConsult Technologie-Tage

Ich buche den Kongress
ComConsult Technologie-Tage 2016

☐ 07.11.-08.11.16 in Köln - € 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 2016

Montag 07.11.2016

9:30 - 10:30 Uhr
Keynote: Rechenzentrum kontra Cloud: Bausteine einer Zukunfts-Strategie für Rechenzentren
- Anforderungen an das Rechenzentrum der Zukunft
- Technologie-Situation der Basis-Technologien und Ausblick
- Abhängigkeiten zwischen Technologien und deren Handhabung
- Leistungs-Übersicht und Bewertung der Cloud
- Vor- und Nachteile: wer kann was besser, wo liegen die Nachteile
- Strategie für das erfolgreiche Rechenzentrum der Zukunft

Dr. Jürgen Suppan, ComConsult Research GmbH

10:30 - 11:15 Uhr
5G: Rückgrat der nächsten industriellen Revolution
- 5G: Anwendungsbereiche, Technologien und Bedeutung für Unternehmen
- Status von Komponenten, Szenarien und Standardisierung US und EU
- Starten statt Warten: LTE als Übergangstechnologie
- Aktuelle Entwicklungen von LTE Tel. 13 - 15 in 3GPP
- Anforderungen an unterstützende Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

11:15 - 11:45 Uhr Kaffeepause

11:45 - 12:30 Uhr
Das Software-Defined Data Center - Der Paradigmenwechsel in der IT
- Begriffsbestimmung: Was bedeutet Software-Defined?
- Virtualisierung plus SDN = Private Cloud?
- Technische und organisatorische Anforderungen und Erwartungen:
  - Virtualisierung von Sicherheitsfunktionen
  - Integration von Cloud- und Fog-Computing
  - Unterstützung für Anwendungen
  - organisatorische Anpassungen in der IT

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

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45
Wie Container das RZ verändern
- Was sind Container und wie funktionieren sie?
- Wie unterscheiden sich Container von klassischen Virtualisierungstechniken?
- Netzwerkschnittstellen von Containern
- Interaktion zwischen Containern und Microprozessen
- Container und DevOps: ein Herz und eine Seele?

Markus Schaub, ComConsult-Study.tv

14:45 - 15:30
Netzzugang zur Cloud
- Zugriff auf Public und Private Cloud
- Warum die Verbindung zum Internet immer wichtiger wird
- Braucht man noch ein Wide Area Network (WAN)?
- Software Defined WAN
- Wie die Umstellung auf Internet Protocol Version 6 (IPv6) sanfter als befürchtet erfolgen kann

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 16:45 Uhr
Das Ende von PSTN & ISDN
- Welche Änderungen ergeben sich aus der Umstellung?
- Was bieten die Provider?
- Welche Problem sind noch nicht eindeutig gelöst?
- Warum das Thema Session Border Controller wichtig ist

Markus Geller, ComConsult Research GmbH

16:45 - 17:00 Uhr
Zusammenfassung des Tages, Fragen Diskussion

17:00 - 18:00 Uhr
Den Schwarm führen: Organisations- und Führungsprinzipien für Innovation und Veränderung

Dipl.-Kfm. Lars Sudmann, Speaker & Trainer

Happy Hour ab 18:00 Uhr

Dienstag 08.11.2016 - vormittag

9:00 - 9:45 Uhr
Neubau von Rechenzentren
- Digitalisierung und die Auswirkungen für Rechenzentren
- Neue Trends im Rechenzentrumsumfeld
- Bauliche und technische Anforderungen/Security und Verfügbarkeit
- SPOC (Single Point of Contact)
- Energieoptimierungstrends
- Abwärmenutzung, Rechenzentren als dezentrales Kraftwerk

Klaus Dederichs, Drees & Sommer

9:45 - 10:30 Uhr
IoT-Sicherheit - aus Fehlern lernen und damit langfristig Erfolg sichern
- Plattform-Evolution zum Internet der Dinge
- Langfristiges Ziel: Vertrauen und Zuverlässigkeit
- Stand der Sicherheit an Beispielen: Babymonitoring, Industriesteuerungen, Automotive
- IoT der zweiten Generation - wie bekommt man die Risiken in den Griff?

Prof. Dr. Marko Schuba, Fachhochschule Aachen

10:30 - 11:15 Uhr
Funk – das Medium der Zukunft! Ist Ethernet tot?
- Wo steht Wireless LAN heute, wo geht es hin?
- Welchen Bedarf haben Anwendungen heute und in Zukunft?
- Welche Auswirkungen hat das auf Sicherheit?
- Welche Auswirkungen hat das auf die WLAN-Planung?
- Wie investieren Unternehmen zukunftssicher in Funktechnik?
- Weder WLAN noch Ethernet, ist Mobilfunk eine Alternative?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:15 - 11:45 Uhr Kaffeepause

11:45 - 12:30 Uhr
EU Datenschutz-Grundverordnung - Datenschutz in neuer Dimension
- Gesetzgebungsgeschichte und Ziele der EU-Datenschutz-Grundverordnung
- Überblick zu den wichtigsten Regelungen für die Praxis (u. a. Extraterritorialer Anwendungsbereich, Erlaubnistatbestände, Auftragsverarbeitung, Drittstaatentransfers)
- Änderungen im Vergleich zum BDSG – was ändert sich, was bleibt gleich?
- Aufsicht, Sanktion und Haftung

Dr. Jan Byok, Bird & Bird LLP

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Der Arbeitsplatz der Zukunft - (k)eine Frage der Endgeräte
- Was sind die bestimmenden Faktoren für den Arbeitsplatz der Zukunft?
- Welche Rolle spielen Endgeräte, Applikationen und Dienste für den Arbeitsplatz?
- Welche Dienste und Applikationen sind relevant für den Arbeitsplatz der Zukunft?
- Sind Standardisierungsbemühungen sinnvoll und erfolgversprechend?
- Welche Arbeitsplatzkonzepte adressiert der Markt heute schon?

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

14:45 - 15:30 Uhr
Informationssicherheit in und aus der Cloud
- Herausforderung sicheres Cloud Computing in Public Cloud, (virtual) Private Cloud und Hybrid Cloud
- Standardisierte und zertifizierte Cloud-Sicherheit
- Data Loss Prevention in der Cloud
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Rolle der Cloud bei der Abwehr von Distributed Denial of Service (DDoS)
- Abwehr zielgerichteter Angriffe durch Cloud-Dienste

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 - 16:15 Uhr
Herausforderungen an die Informationssicherheit in der Industrie 4.0
- Standards zur Sicherheit von IT im Industriebereich und die besondere Bedeutung von IEC 62443
- Warum die Industrie 4.0 nicht ohne Zonenkonzepte auskommt und welche Herausforderungen hier für Sicherheits-Gateways bestehen
- Warum eine starke Öffnung zum Internet notwendig ist und was sich an traditionellen Sicherheitskonzepten ändern muss
- Mit welchen Problemen durch die Industrie 4.0 für die sichere Administration und Überwachung der industriellen IT zu rechnen sind
- Virtuelle Fabrik: Nutzung von Cloud-Diensten in der Industrie 4.0
- Kann das gut gehen: Intelligente Maschinen entscheiden für Menschen?
- Masse statt Klasse: Fließender Übergang zum Internet of Things

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Schwerpunktthema

Authentifizierung und Single Sign On in Cloud-Umgebungen

Fortsetzung von Seite 1

Dipl.-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Nun ist Single Sign On (SSO) bei weitem nichts Neues und keineswegs auf die Cloud fokussiert. Gerade in Windows-Domänen haben Datenbank-Server oder andere Systeme mit eigenen Benutzer- und Rechtedaten in der Regel schon „immer“ ein Single Sign On unterstützt. (siehe Abbildung 1)

Aber gerade bei der Integration von mehreren Cloud-Produkten im Unternehmen spielt Single Sign On eine wichtige Rolle. Denn Cloud-Anwendung haben spezielle Eigenschaften, die letztlich dem Anspruch geschuldet sind, ohne besondere Anforderungen an die Umgebung, in der sie gestartet werden, zu funktionieren (anywhere, anytime, any device):

Separate Benutzerbasis: „Any Device“ wird typischerweise dadurch erreicht, dass auf Web-Technologien und Zugriff via Browser gesetzt wird. In der Regel startet der Zugang zu einer Cloud-Anwendung über eine einfache Login-Seite, wo man Benutzername und Passwort eingeben muss. Diese auf den ersten Blick recht einfache Zugangsmethode impliziert jedoch, dass jeder Cloud-Provider und damit fast jede Cloud-Anwendung mit einer eigenen Benutzerdatenbank und oft zusätzlich mit einem eigenen Rechtekonzept daherkommen.

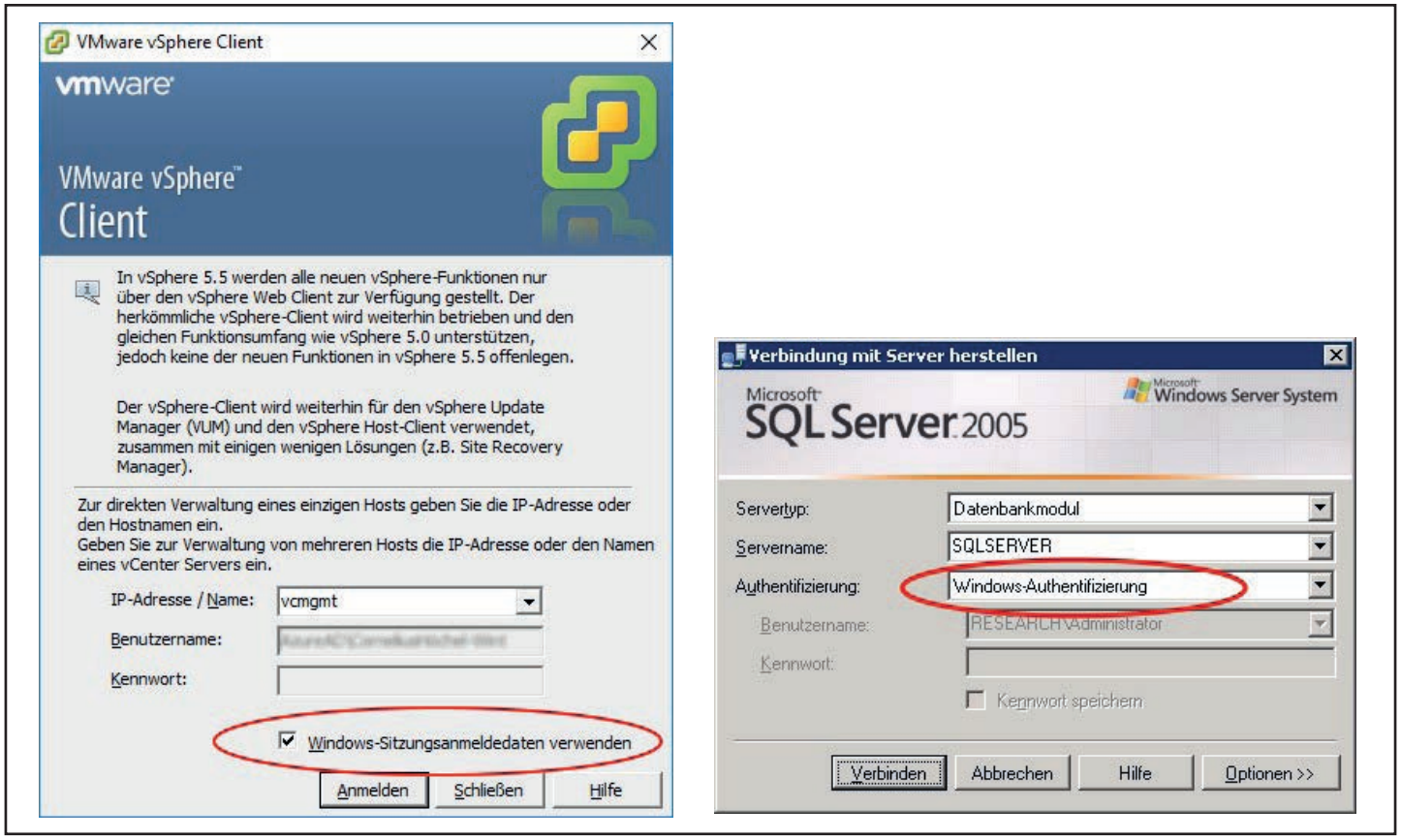

Abbildung 1: Integrierte SSO-Funktionalität in einer Windows-Domäne am Beispiel des vSphere Clients und des Verwaltungstools für Microsoft SQLServer.

Authentifizierung und Single Sign On in Cloud-Umgebungen

Hohe Sicherheitsanforderungen: „Anywhere“ bedeutet, dass die Anwendungen über das Internet mehr oder weniger öffentlich erreichbar sind und damit natürlich hohen Sicherheitsanforderungen unterliegen: Jeder Zugriff muss authentifiziert werden und gerade für die Zugangspasswörter muss eine ausreichende Komplexität gefordert werden.

Daraus ergeben sich auf mehreren Seiten nicht zu unterschätzende Probleme:

1. Die Benutzer selbst müssen sich eine Vielzahl von Benutzernamen-Passwort-Kombinationen merken, die Passwörter sollen möglichst komplex sein und die Idee, für alle Zugänge dasselbe Passwort zu nutzen, ist einerseits aus Sicherheitsüberlegungen eigentlich abzulehnen (lässt sich aber gerade in der Cloud nicht unterbinden) und scheitert andererseits ganz oft an der Realität: Die Provider haben einfach unterschiedliche Vorgaben für Passwörter. Die einen akzeptieren kein Leerzeichen, die andern keinen Schrägstrich, bei wiederum anderen wird der Komplexitätsindikator erst ab 16 Zeichen grün, während die andere Cloud nur maximal 12 Zeichen akzeptiert. Und dann kommen noch diverse Vorgaben für die maximale und minimale Nutzungszeit von Passwörtern hinzu.

   Hier öffnet sich schnell ein riesiges Sicherheitsproblem, da die Benutzer anfangen, sich ihre Passwörter aufzuschreiben, nach Ablauf von Passwörtern nur an der letzten Stelle einen Zähler zu erhöhen etc. pp.

   Wenn sich dann auch noch die Benutzernamen bei verschiedenen Produkten unterscheiden, ist die Akzeptanz bei den Mitarbeitern schnell völlig am Ende. Und der direkt beim Passwort notierte Benutzername führt jedes Sicherheitskonzept ad absurdem.

   Und Nein: Passwort-Safes sind keine geeignete Lösung für die Mehrzahl der Endbenutzer. Unserer Erfahrung nach kommen damit nur IT-affine Benutzer zurecht.

2. Aber auch für die Benutzeradministration explodieren plötzlich die Probleme. Nicht allein deswegen, weil die Benutzer nach mehrfachen Falscheingaben jetzt nicht nur im lokalen Active Directory gesperrt und wieder freigeschaltet werden müssen, sondern eben bei vier, fünf, sechs verschiedenen Cloud-Providern.

   Ein großer Teil zusätzlicher Arbeit entsteht dadurch, dass bei den verschiedenen Providern Benutzerkonten für neue Mitarbeiter angelegt und – ganz wichtig – für ausgeschiedene Mitarbeiter gelöscht oder gesperrt werden. Vergessen Sie nicht, wir sprechen hier über Cloud-Anwendungen! Das heißt, der ausgeschiedene Mitarbeiter hat in der Regel auch außerhalb des Unternehmens Zugriff auf die Anwendung.

3. Speicherdienste in der Cloud, aber auch komplexere Cloud-Anwendungen wie CRM oder Finanz- oder Buchhaltungsdienste nutzen – genauso wie übrigens ihre lokalen Pendants – anwendungsspezifische Rechtekonzepte. Lokale Anwendungen sind aber oft enger in das lokale Betriebssystem integriert als das mit Cloud-Anwendungen möglich ist und haben damit die Möglichkeit beispielsweise lokale Sicherheitsgruppen für ihr eigenes Rechtekonzept zu nutzen. Das macht vieles einfacher.

   Bei der Einführung von Cloud-Anwendungen mit eigenem Rechtekonzept muss dieses selbstverständlich an die Unternehmensanforderungen angepasst werden. Das eigentliche Problem besteht aber wiederum darin, dieses anwendungsspezifische Konzept – oder diese unterschiedlichen Konzepte bei verschiedenen Cloud-Diensten – immer wieder aktuell zu halten.

   Ein typisches Beispiel: Speicherdienste wie Box, Dropbox oder andere bietet den unbestritten großen Vorteil, zum Beispiel projektspezifische Daten auf Verzeichnis- oder sogar Dateiebene für externe Mitarbeiter freizugeben. Wer sorgt aber dafür, dass diese Freigaben auch wieder zurückgenommen werden, wenn sie nicht mehr benötigt werden?

Es ist offensichtlich, dass diese Probleme nicht durch schärfere Passwort-Policies und Mehrfaktor-Authentifizierung entschärft werden können – eher im Gegenteil.

Microsoft zeigt mit der Einführung einer PIN-basierenden Anmeldeoption mit einem Microsoft-Account bei Windows 10 übrigens durchaus überzeugend, dass Einfachheit und Sicherheit sich nicht zwangsläufig widersprechen:

- Für die regelmäßige Anmeldung am Arbeitsplatz-PC wird eine einfache und verglichen zum Passwort deutlich kürzere PIN genutzt. Da diese PIN gerätespezifisch festgelegt ist und daher nur am eigenen PC verwendet werden kann, ist das Missbrauchsrisiko deutlich geringer als das des Passworts, das von überall auf der Welt genutzt werden kann.

- Für das Passwort selbst, das weiterhin für alle verbundene Microsoft-Dienste gilt, kann so eine hohe Komplexität, gegebenenfalls sogar eine Zwei-Faktor-Authentifizierung gefordert werden.

Protokolle

Es gibt eine ganze Reihe standardisierter und auch proprietärer Protokolle zur verteilten Benutzerauthentifizierung.

Die zugrundeliegende Architektur ist dabei meist sehr ähnlich. Unterschieden werden drei Rollen:

- der Benutzer, der einen bestimmten Dienst nutzen will,
- der Dienstanbieter, der den gewünschten Dienst zur Verfügung stellt,

- ein Authentifizierungsdienst, der den Benutzer identifizieren kann und dem der Dienstanbieter vertraut.

Die prinzipielle Funktionsweise folgt folgendem Schema (siehe auch Abbildung 2):

Der Benutzer will einen bestimmten Dienst nutzen, z. B. eine Flugreise buchen. Dazu wendet er sich an den Dienstanbieter, in unserem Beispiel ein Reisebüro. Das Reisebüro fordert ihn auf, sich auszuweisen. Falls der Benutzer noch keinen gültigen, vom Reisebüro akzeptieren Ausweis besitzt, wendet er sich an eine Authentifizierungsstelle, dem das Reisebüro vertraut, im Beispiel das Einwohnermeldeamt. Dort authentisiert er sich mit geeigneten Mittel und erhält von dem Amt einen Ausweis, mit dem er sich beim Reisebüro ausweisen kann.

Der Dienstanbieter wird jetzt in der Regel die ihm vorgelegten und vom Authentifizierungsdienst beglaubigten Daten selbstständig prüfen und eigenständig entscheiden, welche Daten für ihn von Belang sind und welche Rechte er daraufhin dem Benutzer zugesteht. Im Beispiel könnte das Reisebüro beispielsweise zusätzlich zur prinzipiellen Identitätsbestätigung auch das Geburtsdatum des Kunden beachten.

Die Idee hinter diesem Konzept ist, dass der Identitätsnachweis, den die Authentifizierungsstelle dem Benutzer ausstellt, in einem gewissen Sinne „universell“, d. h. gegen unterschiedliche Dienstanbieter genutzt werden kann. Erst diese universelle Nutzbarkeit dieser „Bescheinigung“ macht solche Verfahren SSO-fähig, da in der Folge die Authentifizierung bei anderen Dienstanbietern automatisiert und damit transparent für den Benutzer selbst erfolgen kann.

Darüber hinaus werden keine Passwörter oder ähnliche sicherheitsrelevante Informationen zu den Dienstanbietern geschickt und es erfolgt auch keine (erneute) Kommunikation zwischen Dienstanbieter und Authentifizierungsstelle. Das heißt, die Bild skizzierte Vertrauensbeziehung zwischen Dienstanbieter und Authentifizierungsstelle wird bereits im Vorfeld aufgebaut – entweder direkt durch ein geeignetes Schlüsselaustausch-Verfahren oder indirekt über öffentliche Zertifikate (z. B. X.509).

Diese Aufteilung der Informationsflüsse bei der Authentifizierung ist der wesentliche Unterschied zu Authentifizierungsverfahren wie IEEE 802.1X oder ähnliche, die RADIUS oder TACACS nutzen. Bei diesen Verfahren (siehe Abbildung

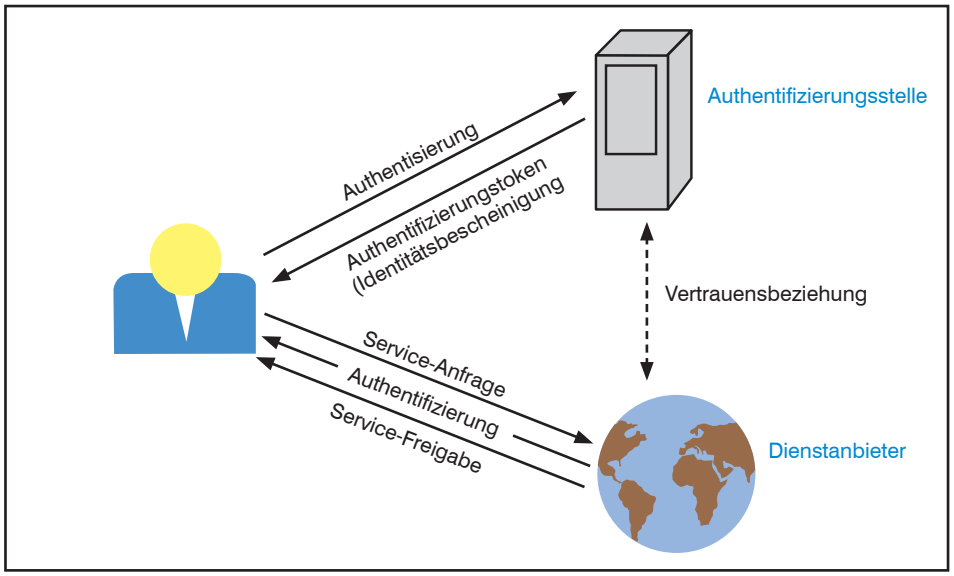

Abbildung 2: Schematische Darstellung einer verteilten Authentifizierung

3) sitzt nämlich der Dienstanbieter („Authenticator“ im VPN-Gateway, Zugangs-Switch etc.) in Form eines Türstehers mitten im Verkehrsfluss zwischen Benutzer und Authentifizierungsdienst.

Solche „Inline“-Verfahren werden hauptsächlich als zentralisierte Authentifizierungsverfahren innerhalb eines LANs verwendet, da der Dienstanbieter Zugriff auf die Authentisierungsdaten des Benutzers hat. Auch wenn man diesen Datenstrom Ende zu Ende verschlüsseln kann, ergeben sich daraus diverse Sicherheitsrisiken, die man sich bei dem verteilten Modell oben ersparen kann.

Darüber hinaus eignen sich solche Verfahren nicht für ein Single-Sign-On, da unterschiedliche Dienstanbieter jeweils eine neue Authentifizierung bei Benutzer anfordern müssen. Der Benutzer besitzt in diesem Modell einfach keinen universell einsetzbaren Identitätsnachweis.

Hauptproblem bei allen Modellen ist, dass offensichtlich alle drei beteiligten Instanzen das genutzte Protokoll verstehen, das heißt zumindest in den sie selbst betreffenden Teilen implementiert haben müssen. Auf diesen Aspekt werden wir im Folgenden noch eingehen.

Kerberos

Im Windows-Umfeld wird zur Authentifizierung und Autorisierung Kerberos genutzt. Kerberos ist ein seit langem bekanntes, offenes Protokoll zur Authentifizierung. Kerberos wurde bereits in den 1980er Jahre am MIT entwickelt, die aktuelle Version ist in RFC 4120 veröffentlicht. Microsoft nutzt das Protokoll seit Windows 2000 in allen Serverbetriebssystemen, außerdem ist Kerberos das standardmäßige Authentifizierungsprotokoll bei allen Windows-Clients, nachdem sie einer Domäne beigetreten sind.

Die Authentifizierungsstelle heißt bei Kerberos „Key Distribution Center“ und ist unterteilt in zwei Komponenten, dem „Authentication Server“ und dem „Ticket Granting Service“. Beide Funktionen laufen üblicherweise auf demselben Server und haben in jedem Fall Zugriff auf eine gemeinsame Datenbasis, in der für jeden autorisierten Benutzer und jeden an-

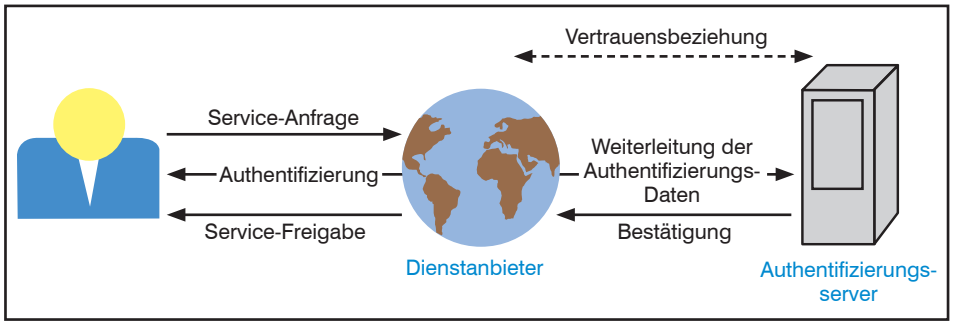

Abbildung 3: Inline-Authentifizierung am Beispiel von IEEE 802.1X

Authentifizierung und Single Sign On in Cloud-Umgebungen

gebundenen Service (Dienstanbieter) ein eigener, geheimer Schlüssel liegt. Diese Schlüssel werden zur Verschlüsselung mittels symmetrischer Verfahren genutzt und werden niemals über das Netzwerk ausgetauscht.

Als zentrale Datenbasis wird in der Regel das Active Directory genutzt, Kerberos selbst lässt aber auch andere Verzeichnisdienste wie z. B. LDAP zu.

Kerberos arbeitet mit sogenannten Tickets. Tickets sind verschlüsselte Informationen, die dem Client ausgestellt und übergeben werden, die der Client selbst aber nicht entschlüsseln kann. Kerberos unterscheidet zwischen

- dem Ticket Granting Ticket (TGT), das bei der ersten Authentifizierung des Benutzers beim Authentication Server ausgestellt wird und dem Benutzer zur Authentisierung beim Ticket Granting Service dient und
- den Service Tickets, die vom Ticket Granting Service (TGS) ausgestellt werden und dem Benutzer zur Authentisierung beim jeweiligen Service dienen.

Im Einzelnen funktioniert das Verfahren wie folgt (siehe auch Abbildung 4):

1. Der Benutzer meldet sich an der Domäne an (z. B. mit Benutzername und Passwort oder wie auch immer). Aus diesen Logindaten leiten beide Seiten (Client und Authentication Server) denselben geheimen Schlüssel des Benutzers ab.
2. Der Authentication Server schickt zwei Nachrichten an den Client:
   a. Nachricht (2) mit einem neuen „TGS-Sitzungsschlüssel“ für den Client, verschlüsselt mit dem geheimen Schlüssel des Benutzers.
   b. Nachricht (3) mit einer Reihe von Informationen über den anfragenden Client wie Benutzername, Netzwerkadresse und außerdem mit einer Gültigkeitsdauer und dem TGS-Sitzungsschlüssel aus Nachricht (1), verschlüsselt mit dem geheimen Schlüssel des TGS. Dies ist das sogenannte Ticket Granting Ticket (TGT).

Nachricht (1) kann der Client entschlüsseln und hat so einen einzigartigen Schlüssel zur verschlüsselten Kommunikation mit dem TGS, der ihn gleichzeitig zusammen mit dem TGT als der behauptete Benutzer authentifiziert.

Will der Benutzer jetzt einen bestimmten Service nutzen, wird dieses Verfahren auf eine analoge Art und Weise zuerst mit dem Ticket Granting Service und dann mit dem Service-Anbieter wiederholt:

1. Der Client schickt zwei Nachrichten an den TGS:
   a. Eine unveränderte Kopie des TGT (= Nachricht (3)) zusammen mit der Information, welchen Dienst er nutzen will.
   b. Seinen eigenen Benutzernamen zusammen mit einem Zeitstempel, verschlüsselt mit dem TGS-Sitzungsschlüssel aus Nachricht (2).
2. Damit kann der Client vom TGS authentifiziert werden und erhält im Erfolgsfall zwei Nachrichten zurück:
   a. Nachricht (5) mit einem neuen Service-Sitzungsschlüssel für den Client, verschlüsselt mit dem TGS-Sitzungsschlüssel, den der TGS dem TGT (3/4) entnommen hat.
   b. Nachricht (6) als sogenanntes Service Ticket. Dieses Ticket enthält ähnliche Informationen wie das TGT über den anfragenden Client zusätzlich jedoch den neuen Service-Sitzungsschlüssel zur Kommunikation zwischen Client und Service-Anbieter, verschlüsselt mit dem geheimen Schlüssel des Service.
3. Wie oben kann der Client Nachricht (3) entschlüsseln und erhält so einen einzigartigen Schlüssel zur verschlüsselten Kommunikation mit dem Service-Anbie-

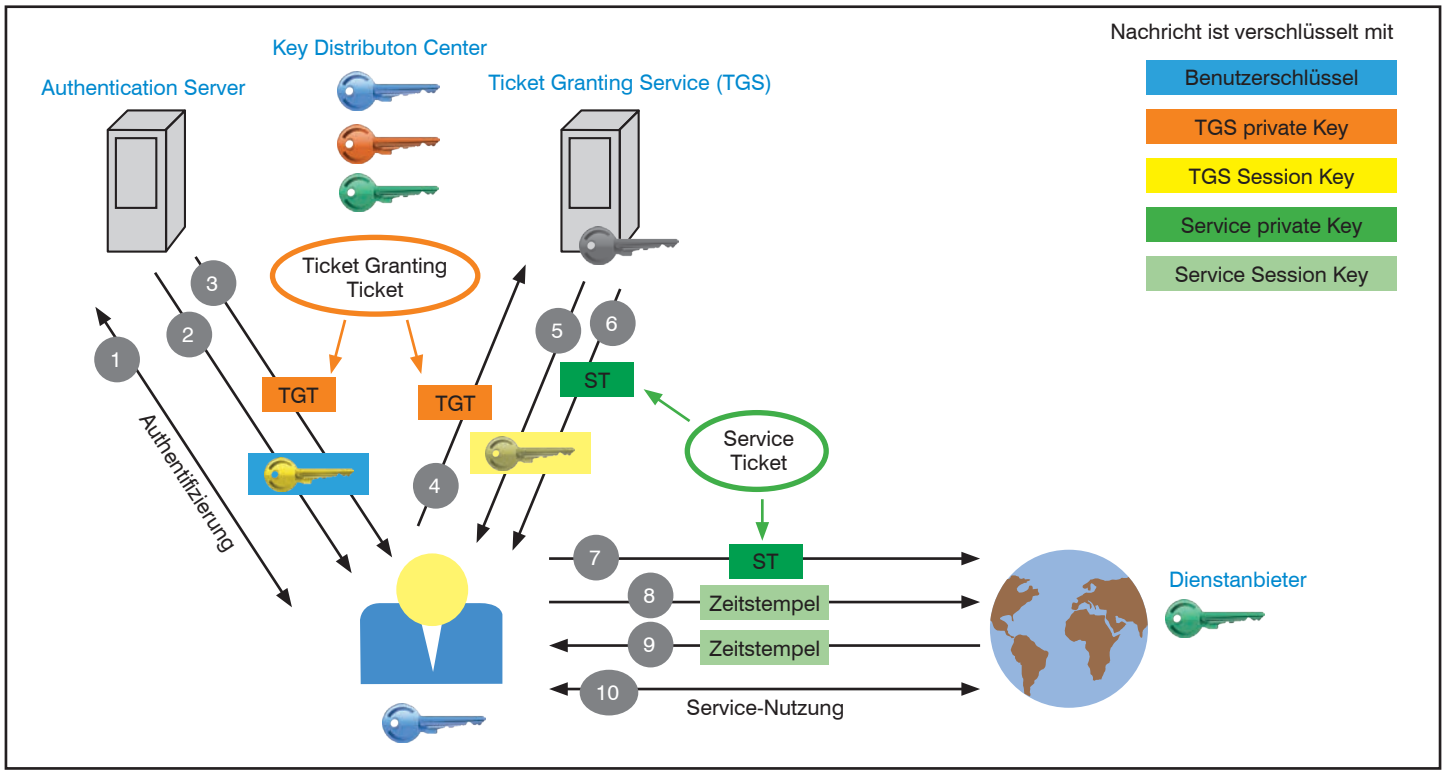

Abbildung 4: Kerberos Funktionalität

ter. Jetzt schickt der Client zwei Nachrichten an den Service:

a. Eine unveränderte Kopie des Service Tickets, das ja mit dem geheimen Schlüssel des Service verschlüsselt ist.

b. Eine weitere Nachricht (8) mit seinen Benutzernamen und einem Zeitstempel, verschlüsselt mit dem Service-Sitzungsschlüssel aus Nachricht (5).

4. Damit kann der Client auch vom Service-Anbieter authentifiziert werden und erhält im Erfolgsfall eine Bestätigungsnachricht (9) zurück, die mit dem gemeinsamen Service-Sitzungsschlüssel aus dem Service Ticket (6/7) verschlüsselt ist. Diese Nachricht enthält den Zeitstempel aus Nachricht (8), womit auch der Client den Service-Anbieter authentifizieren kann und damit mit Service-Anfragen beginnen kann.

Zusammenfassend kann man zu Kerberos sagen:

1. Kerberos ist ein weit implementierter und seit langem bekannter Authentifizierungsdienst, der auch und gerade über unsichere Netze SSO-Funktionalität zur Verfügung stellt.

2. Der große Nachteil von Kerberos ist, dass ein eigenes Protokoll zum Austausch der Nachrichten genutzt wird (standardmäßig über UDP oder TCP Port 88). Das bedeutet, dass sowohl auf der Client- als auch auf der Service-Seite Kerberos direkt in der Software implementiert sein muss. Bild 1 zeigt zwei Beispiele, wo selbst die Benutzeroberflächen angepasst wurden. Für Cloud-Anwendungen ist Kerberos daher weitgehend unbrauchbar.

SAML

SAML steht für Security Assertion Markup Language und ist ein offener Standard zur Authentifizierung von Usern, Federation zwischen Dienstanbietern und Single-Sign-On-Szenarien. Schon an dieser Aufzählung können Sie erkennen, dass SAML ein sehr umfangreiches Framework ist, weshalb ich im Folgenden die Authentifizierung und SSO-Funktionalität von SAML in den Vordergrund stellen werde.

SAML wird vom Security Services Technical Committee (SSTC) der OASIS (Organization for the Advancement of Structured Information Standards) entwickelt. Die erste Version V1.0 wurde im November 2002 veröffentlicht, die aktuelle Version V2.0 stammt vom März 2005 und wird derzeit immer noch weiterentwickelt.

Im Gegensatz zu Kerberos basiert SAML auf XML und passt damit deutlich besser in die Cloud und zu HTML- und SOAP-basierenden Anwendungen.

Die Kernelemente von SAML sind sogenannte Assertions, zu Deutsch Erklärungen. Diese Assertions sind XML-Dokumente, in denen sowohl die Anfragen als auch die Antworten transportiert werden. Abbildung 5 zeigt ein typisches Assertion als Antwort auf eine Authentifizierungsanfrage.

Die Antwort umfasst:
- den Aussteller (Issuer) dieser Erklärung,
- das Datum, wann diese Erklärung erstellt wurde,
- warum diese Erklärung erstellt wurde (InResponseTo),
- wohin die Erklärung weitergeleitet werden soll (Destination),
- den Status der Überprüfung (samlp:StatusCode, hier: Success),
- wie die Überprüfung durchgeführt wurde (AuthnContext, hier: Password),
- ein paar zusätzliche Attribute wie zum Bei-

```
<samlp:Response ID="_a4958bfd-e107-4e67-b06d-0d85ade2e76a"
        Version="2.0"
        IssueInstant="2013-03-18T07:38:15.144Z"
        Destination=https://contoso.com/identity/inboundsso.aspx
        InResponseTo="id758d0ef385634593a77bdf7e632984b6"
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        https://login.microsoftonline.com/82869.../</Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    ...
  </ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <Assertion ID="_bf9c623d-cc20-407a-9a59-c2d0aee84d12"
        IssueInstant="2013-03-18T07:38:15.144Z" Version="2.0"
        xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>https://login.microsoftonline.com/82869.../</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      ...
    </ds:Signature>
    <Subject>
      <NameID>Uz2Pqz1X7pxe4XLWxV9KJQ+n59d573SepSAkuYKSde8=</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <SubjectConfirmationData
                InResponseTo="id758d0ef385634593a77bdf7e632984b6"
                NotOnOrAfter="2013-03-18T07:43:15.144Z"
                Recipient="https://contoso.com/identity/inboundsso.aspx" />
      </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2013-03-18T07:38:15.128Z"
                NotOnOrAfter="2013-03-18T08:48:15.128Z">
      <AudienceRestriction>
        <Audience>https://www.contoso.com</Audience>
      </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
      <Attribute
        Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
        <AttributeValue>testuser@contoso.com</AttributeValue>
      </Attribute>
      <Attribute
        Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>3F2504E0-4F89-11D3-9A0C</AttributeValue>
      </Attribute>
      ...
    </AttributeStatement>
    <AuthnStatement AuthnInstant="2013-03-18T07:33:56.000Z"
        SessionIndex="_bf9c623d-cc20-407a-9a59-c2d0aee84d12">
      <AuthnContext>
        <AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
      </AuthnContext>
    </AuthnStatement>
  </Assertion>
</samlp:Response>
```

Abbildung 5: SAML Response Assertion

spiel den Benutzernamen des Users und
- unter welchen Bedingungen (Anschnitt Conditions) die Erklärung benutzt werden soll (Im Beispiel ist ein Gültigkeitszeitrahmen von gut einer Stunde und der Ziel-Provider angegeben).

Außerdem ist das Dokument signiert (Abschnitt ds:Signature) und kann so vom Empfänger auf seine Glaubwürdigkeit überprüft werden. Zusätzlich kann seit SAML 2.0 das komplette Dokument oder Teile davon verschlüsselt werden.

Hieran erkennt man die prinzipielle Struktur von SAML:

1. Es gibt wiederum drei miteinander kommunizierende Parteien: den Benutzer, einen „Identity Provider“, der den Benutzer authentifizieren kann, und einen „Service Provider“, den der Benutzer kontaktiert und der die Identität und gegebenenfalls weitere Details über den Benutzer wissen möchte. Daher wird der Identity Provider als ausstellende Stelle auch als „SAML Asserting Party“ bezeichnet und der Service Provider als auswertende Stelle als „SAML Relying Party“.

2. Der Service Provider erstellt eine Anfrage (in Form eines XML-Dokuments) und der Identity Provider antwortet seinerseits mit einem XML-Dokument (Assertion), das die gewünschten Informationen enthält, und unterzeichnet dieses Dokument.

   Diese Assertion können, wie oben gezeigt, eingesetzt werden, um eine zentrale Authentifizierung und SSO zu implementieren, aber auch einfach zur Autorisierung, indem Benutzerrechte und Gruppenzugehörigkeiten abgefragt werden.

   Darüber hinaus ist auch ein Informationsaustausch zwischen verschiedenen Identity Providern möglich, um beispielsweise neue Benutzerkonten anzulegen, Benutzer zu sperren und ähnliches. Hierzu wird lediglich einer der Identity Providern als Service Provider betrachtet, der einen entsprechenden Dienst (z. B. „Benutzer anlegen“) anbietet.

3. Wo und wie die Benutzerdaten gespeichert sind, ist für das Konzept unerheblich. Unterstützt werden die üblichen Verzeichnisdienste wie LDAP und AD, aber auch verteilte Konzepte sind realisierbar, indem eine Anfrage einfach weitergeleitet wird.

4. Wie die Tickets bei Kerberos werden Assertions nicht direkt zwischen Service und Identity Provider ausgetauscht, sondern immer über den Benutzer geleitet. SAML nutzt hierfür beispielsweise den Mechanismus HTTP-Redirect (siehe unten „Bindings“).

5. Der Service Provider (= die Anwendung) bleibt bei seiner Entscheidung, wie er mit der Service-Anfrage des Benutzers umgehen soll, letztendlich autark. Das heißt, trotz einer SAML-Antwort entscheidet er selbst, welche Informationen des Assertions er wie oder gegebenenfalls überhaupt beachtet. So kann beispielsweise ein Provider einen kürzeren oder längeren Gültigkeitszeitrahmen akzeptieren als im Assertion vermerkt, oder er kann trotz Authentifizierung bestimmte Benutzer aus lizenzrechtlichen Gründen ablehnen.

Das Gesamtkonzept von SAML ist dabei durchaus komplex und unterscheidet weitere abstrakte Designelemente wie Protocols, Bindings und Profiles.

Protocols sind festgelegte Frage-Antwort-Abfolgen für festgelegte Aufgaben. Der Standard definiert sechs solcher Protokolle:

- Authentication Request Protocol (für Authentifikation und SSO),
- Single Logout Protocol (führt für einen Benutzer einen simultanen Logout bei allen verbundenen Service Providern aus),
- Assertion Query and Request Protocol (dient der Suche nach bereits bekannten Assertions),
- Artifact Resolution Protocol (dient dazu Referenzen statt vollständige Informationen zu übermitteln),
- Name Identifier Management Protocol (hiermit können Identifier eines Benutzers verändern werden),
- Name Identifier Mapping Protocol (hiermit können unterschiedliche Identifier (z. B. Benutzernamen) bei verschiedenen Providern einander zugeordnet werden).

Bindings beschreiben die unterschiedliche Transportmöglichkeiten für Assertions. In der Regel werden die XML-Dokumente über HTTP base64-encoded oder über SOAP transportiert. Beschrieben sind:

- HTTP Redirect Binding (die Daten stehen direkt im URL als GET-String),
- HTTP POST Binding (die Daten werden im Feld einer HTML-Form übergeben),
- HTTP Artifact Binding (dient der Auflösung von Referenzen, hier findet ausnahmsweise eine direkte Kommunikation zwischen den Providern statt),
- SAML SOAP Binding (die Daten werden als SOAP-Message im HTML-Body übertragen),
- Reverse SOAP (PAOS) Binding,
- SAML URI Binding (um bekannte Assertions abzurufen).

Profiles spezifizieren, wie welche Assertions, Protokolle und Bindings für konkrete Anwendungsfälle genutzt werden sollen. Hiermit soll insbesondere die Interoperabilität von SAML verbessert werden. Das wichtigste Profil ist das „Web Browser SSO Profile“.

Fazit zu SAML: Das Protokoll kann die Identität, Eigenschaften und Rechte von Benutzern von einer zentralen Instanz an Service Provider (in der Regel eine Web-Anwendung) sicher weitergeben, ohne dass die Anwendung Zugriff auf das Benutzerverzeichnis hat. Da die Kommunikation zwischen Identity und Service Provider über XML-Dokumente läuft, lässt sich SAML sehr gut in typische Cloud-Szenarien einbinden.

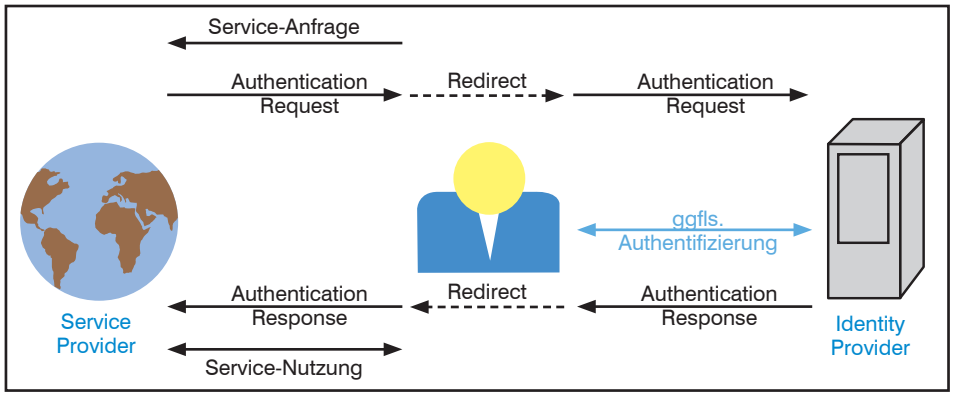

Abbildung 6: SAML Funktionskonzept

Weitere Alternativen

Weitere prominente Alternativen zu SAML sind: OpenID, OAuth und OpenID Connect.

OpenID ist ein offener Standard der OpenID Foundation und richtet sich in erster Linie an private Endanwender. Es gibt eine ganze Reihe von Providern, die kostenfreie OpenID-Konten anbieten, und eine große Zahl von Web-Sites, wo man sich mit seiner OpenID anmelden kann.

Das Verfahren ist sehr ähnlich wie eine Authentifizierung mit SAML, es werden jedoch nur sehr wenige Attribute des Benutzers übergeben und die Architektur ist ein gutes Stück einfacher. So wird der zugehörende Identity Provider beispielsweise einfach aus der Domäne der angegebenen OpenID geschlossen.

OAuth steht für Open Authorization, die aktuelle Version ist in RFC 6749 veröffentlicht. Wie der Name sagt, ist OAuth im engeren Sinn kein Authentifizierungsprotokoll, sondern dient der Autorisierung des Zugriffs auf eine Web-Anwendung.

Die große Bedeutung von OAuth ist seine API-Unterstützung und für REST-Webservices. Mittels OAuth kann ein Benutzer eine Anwendung autorisieren, in seinem Namen Aktionen auszuführen. Während dieser Autorisierung durch den Benutzer erhält dieser einen Access Token, mit dessen Hilfe die Anwendung ohne weiter Authentifizierung agieren kann. Dies ist insbesondere für den Datenaustausch bei REST-Services hilfreich.

Der Nachteil von OAuth ist wie gesagt, dass es keine Authentifizierung unterstützt. Diese Lücke schließt **OpenID Connect**. OpenID Connect ist die neuste Version von OpenID, integriert jedoch OAuth und erweitert so OAuth praktisch zum Authentifizierungsprotokoll.

Identity Management in und mit der Cloud

Wie eingangs erwähnt, ist es ein immanentes Merkmal von Cloud-Anwendungen, dass sie eine eigene Benutzerbasis und -verwaltung umfassen. Gleichzeitig wird es für alle Unternehmen, die mehr als ein oder zwei Cloud-Anwendungen nutzen, ungeheuer wichtig, Single Sign On nutzen zu können. Die sich aus unabhängigen Benutzerverwaltungen und mehreren Benutzerkonten pro Mitarbeiter ergebenden Nachteile und Sicherheitsrisiken wurden diskutiert und sind zu gravierend als dass man sie einfach ignorieren könnte.

Daher ist auch der Druck auf die Cloud-Provider groß, SSO-Funktionalität zur Verfügung zu stellen – und mit den vorgestellten Protokollen ist die Technik hierfür vorhanden.

Darüber hinaus wird es immer wichtiger, Anwendungen in der Cloud miteinander und Anwendungen aus der Cloud in Unternehmensabläufe nahtlos zu integrieren. Aber spätestens, wenn Sie unterschiedliche Cloud-Anwendungen verbinden wollen, müssen Sie dazu in der Lage sein, Authentisierungsdaten von der einen Cloud zur anderen zu transportieren. Nehmen Sie zum Beispiel eine CRM- oder eine Buchhaltungsanwendung, die objektspezifische Dokumente wie Briefe, Angebote oder Rechnungen direkt aus der Anwendung heraus bei einem Storage-Provider wie Box.com ablegen möchten. Natürlich muss hierbei gewährleistet sein, dass der Besitzer des Dokuments eindeutig dem Nutzer der CRM-Anwendung zugeordnet werden kann, und umgekehrt. Das heißt, aus Sicht der CRM-Anwendung gehört das Dokument zu einem bestimmten CRM-Datensatz, aus Sicht der Storage-Anwendung gehört das Dokument dem User, der dem CRM-User auf der Storage-Seite zugeordnet ist.

Kurz gesagt, ohne SSO-Funktionalität gibt es keine Funktionsintegration.

Gleichzeitig ergibt sich für die Provider hieraus ein neues Geschäftsmodell, sei es als eigenständiges Produkt oder einfach nur zur Kundenbindung: Eine eigene Benutzerverwaltung haben sie eh, mindestens eine SSO-Lösung müssen sie auch bereitstellen. Warum nicht gleich die Identity-Provider-Komponente mit installieren und alles machen. Denn wer die Benutzerdaten verwaltet, hat ein Bein mehr in der Tür zum Kunden als derjenige, auf dessen Dienste „nur“ via SSO zugegriffen wird. Microsoft geht beispielsweise mit Azure so weit, dass sie für Web-Anwendungen SSO anbieten, die selbst gar keine SSO-Lösung unterstützen. Der Trick dahinter ist, dass Azure hier so wie einige Passwort-Safes arbeitet: Man hinterlegt bei Azure die URL der Login-Seite und das Passwort und Azure füllt die Anmeldeform automatisch aus – na ja, besser als der Zettel unter der Tastatur.

Single Sign On ist für die Provider also ein zweischneidiges Schwert – und so zeigen sie sich auch am Markt. SSO-Provider möchten sie gerne alle spielen: Google, Facebook, Salesforce, Microsoft, IBM, Dell, Oracle, SAP, die Telekom und viele andere. Wenn man aber ein bestimmtes SSO-Protokoll anfragt oder für das eigene Produkt SSO-Funktionalität aktivieren möchte, wird es schnell etwas aufwändiger.

Typische Problemfelder, mit denen man sich auseinandersetzen muss, sind:

- Bei manchen Providern können nur alle oder keine Benutzerkonten auf SSO umgestellt werden.
- Bei einzelnen Providern geht mit SSO die Möglichkeit verloren, sich direkt mit Benutzername und Passwort anzumelden.

- Will man den Benutzern die Möglichkeit erhalten, sich auf beide Möglichkeiten (mit und ohne SSO) anmelden zu können (manche Smartphone-Apps kommen mit SSO nicht so gut zurecht), muss man natürlich damit leben, dass die Passwörter irgendwann ablaufen und die Anwendung trotz SSO-Nutzung unbedingt ein neues Passwort will.

- Bei manchen Providern funktioniert SSO nur, wenn die Benutzernamen auf beiden Seiten gleich lauten.

Die ist übrigens ein Punkt, den wir so wie so dringend empfehlen. Es erleichtert die Zuordnung der verschiedenen Benutzerkonten nicht nur dem SSO-Protokoll sondern auch der eigenen Rechteverwaltung und Fehlersuche.

Da viele Produkte als Benutzername eine E-Mail-Adresse fordern und praktisch alle diese Form unterstützen, ist es angeraten, alle Benutzername in dieser Form anzulegen.

Trotzdem kann man feststellen, dass Single Sign On auch für Cloud-Anwendungen mittlerweile weit verbreitet ist und von der großen Mehrzahl der Anwendungen unterstützt wird. Für welchen Identity Management Provider Sie sich entscheidet, hängt von vielen individuellen Faktoren ab. Eine generelle Empfehlung kann man an dieser Stelle seriös nicht geben. Einige Gesichtspunkte bei der Auswahl sind:

- Sie sollten natürlich ihrem Identity Provider vertrauen.

- Business Continuity spielt sicherlich in diesem Bereich eine große Rolle. Sie sollten verhindern, einen Single Point of Failure aufzubauen. Hinterfragen Sie diesen Punkt bei den Providern Ihrer Wahl.

- Es gibt Provider, die sich speziell auf dieses Geschäftsfeld konzentriert haben (z. B. PingIdentity, okta, oneLogin).

- Microsoft hat in Umgebungen mit Office 365 und Windows 10 sicherlich eine Sonderstellung, da bei Office 365 auch Azure AD enthalten ist und Sie mit Azure AD Ihr lokales Active Directory synchronisieren können.

Fazit

Kommen wir zum Schluss noch einmal zu den eingangs skizzierten Problemen von Cloud-Anwendungen zurück:

- der Umgang mit Passwörtern von Endanwendern,

- die Administration von mehreren Benutzerverzeichnissen,

- die Rechteverwaltung bei autonomen Anwendungen.

Der erste Punkt ist zweifellos das größte Problem. Akzeptanz bei den Endbenutzern und ein einfacher, aber sicherer Umgang mit den Zugangsdaten ist durch nichts zu ersetzen. Hier helfen Single-Sign-On-Verfahren, genau hierfür sind sie entwickelt. In Windows-Umgebungen kann man via Synchronisation von Azure AD mit dem lokalen Active Directory (oder alternativ direkt mit Microsoft Accounts) sogar die Windows-Anmeldung integrieren. Der Benutzer kann so alle unterstützten Cloud-Dienste direkt ohne weitere Authentifizierung nutzen wie er es von lokalen Anwendungen gewohnt ist.

Um auch die Benutzeradministration zu entlasten, ist SSO nur ein erster Schritt. Insbesondere wenn man Cloud-Konten automatisiert erzeugen und löschen will, braucht man ein übergreifendes Identity-Management – und leider auf der Gegenseite auch Cloud-Anwendungen, die das unterstützen. Das machen bei weiterem nicht alle!

Aber auch schon die Aufgabe, verschiedene Benutzerverzeichnisse in den Basisdaten synchron zu halten, kann sich als aufwändig herausstellen. Bei einigen Produkten gibt es immerhin API-Schnittstellen oder Reporting-Funktionen, die einem wenigsten den jeweiligen Ist-Stand liefern. Der Rest bleibt der Kreativität ihrer Administratoren überlassen.

Ganz weit weg von einer übergreifenden Lösung sind wir beim Thema Rechteverwaltung und Gruppenzugehörigkeit. Viele Cloud-Produkte kennen gar keine frei definierbaren Gruppen, die man übernehmen oder synchronisieren könnte, sondern nur fest vorgegebene Rollen. Inwieweit man solche Zuordnungen programm- oder skriptgesteuert vornehmen kann, muss man im Einzelfall klären. Im Grunde hilft aber nur eine saubere Dokumentation des Rechtekonzepts – und die eben angesprochene Kreativität ihrer Administratoren.

Eine Single-Sign-On-Lösung ist also wichtig, in manchen Szenarien schon aus Sicherheitsgründen sogar unumgänglich, im administrativen Bereich werden damit allerdings bei weitem nicht alle Probleme gelöst.

Wie sind Ihre Erfahrungen? Über Rückmeldungen würden wir uns freuen:
www.comconsult-research.de/authentifizierung-singlesignon

Aktueller Kongress

ComConsult UC-Forum 2016
21.11. - 23.11.16 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 21.11. bis 23.11.16 ihr "ComConsult UC-Forum" in Düsseldorf.

Der VoIP und UC-Markt ist in einer Umbruchsphase wie wir sie in den letzten 5 Jahren nicht erlebt haben. Die weltweiten Ankündigungen zum Thema Ablösung der PSTN Infrastrukturen sowie die neue Dynamik im Cloud Markt durch den Eintritt der VoIP und UC Entwickler als Provider von UCaaS und cPaaS Lösungen zeigt, dass bisherige Denkweisen und Betriebskonzepte überprüft werden müssen.

Gerade die Umbrüche im öffentlichen Telekommunikationsnetz führen zu technologischen Neuausrichtungen. Dienste wie Fax, Modem und Analoganschlüsse sind in einer IP basierten Kommunikationswelt nicht mehr fortzuführen, wie aber können sie ersetzt werden? UC erfährt durch WebRTC eine komplette Umorientierung, gerade im Hinblick auf eine einheitliche,

webbasierte Basistechnologie, die endlich unabhängig ist von Betriebssystemen oder Entwicklungsumgebungen. Was aber bedeutet dies für unsere Unternehmen? Wird jetzt alles einfacher oder gibt es doch noch Einschränkungen?

Aber auch das Thema Betrieb von VoIP und UC Anwendungen steht vor neuen Herausforderungen. Durch den Markteintritt der Hersteller von Kommunikationslösungen in die Welt der Cloud werden klassische On Premise Modelle immer mehr in Frage gestellt. Jedoch muss auch hier hinterfragt werden, für wen sich ein CAPEX orientierter Ansatz lohnt und für wen die OPEX Variante der richtige Weg ist.

Diese und viele weitere Aspekte sind Schwerpunkt unseres diesjährigen UC-Forums. Seien Sie dabei, unsere Top Referenten erläutern Ihnen die wichtigsten Trends und Entwicklungen die für eine zukunftsfähige Unternehmens-IT unabdingbar sind.

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 2016

Montag 21.11.2016 - UC 2016 – Cloud und Co.

9:30 - 10:15 Uhr
Keynote
- Wo steht der Markt für UC, Video und Collaboration?
- Was wurde eigentlich aus WebRTC?
- Welche Fragen wirft All-IP auf?
- Gibt es ein Leben ohne die Cloud?
- Welche Trends gestalten den Arbeitsplatz der Zukunft?

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

10:15 - 11:00 Uhr
UC goes http:
WebRTC Anwendungen im Vergleich
- Kommunikation ist mehr als telefonieren
- Warum ist Web Technik hierfür ideal
- Wie schlagen sich die Lösungen etablierter Hersteller: Cisco Spark, Unify Circuit, Alcatel Lucent Enterprise Rainbow, ...

Markus Geller, ComConsult Research GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Monitoring für Enterprise VoIP-Dienste
- Warum nicht Wireshark?
- Qualität von VoIP - Woran hakt es?
- Testing vs. Monitoring - ein integrierter Ansatz
- Übersprechen, Fax-Abbrüche - Troubleshooting-Beispiele aus der Praxis

Dr. Michael Wallbaum, VOIPFUTURE GmbH

12:15 - 12:45 Uhr
Wie reif ist Skype for Business als TK-Ersatz
- Wofür braucht man noch TK-Anlagen wenn es Skype-for-Business gibt?
- Wo liegen die Stärken und Schwächen von S4B?
- Wie stellt sich Microsoft die Video-Integration von morgen vor?
- Was ist die Vision hinter „Surface Hub“?
- Ist Skype-for-Business untrennbar mit Office365 verbunden?

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

12:45 - 13:00 Uhr
Tour Guide zur Ausstellung
- Welche Aussteller sind im Forum vertreten?
- Welche Trends lassen sich an der Ausstellung ablesen?
- Was sind die persönlichen Highlights?

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

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:15 Uhr
Arbeitsplatz-Optimierung - Office Delve und Office Graph als Fitness App für das Berufsleben
- Finden Sie heraus, wie effizient Sie kommunizieren, um Ihre Leistungsfähigkeit zu steigern
- Das intelligente Werkzeug erkennt, mit wem und woran Sie arbeiten und verbindet Sie mit neuen relevanten Informationen und Kontakten
- Erkennen Sie, womit andere sich momentan beschäftigen, mit wem sie zusammenarbeiten und wo ihre Kompetenzen liegen
- Office Delve zeigt auf, womit Sie Ihren Arbeitstag verbringen (E-Mails, Besprechungen, …) und ermöglicht Ihnen eine bessere Zeiteinteilung
- Sie erfahren, mit wem Sie wie viel Zeit verbringen und wer mehr Aufmerksamkeit benötigt

Christian Sailer, Microsoft Deutschland GmbH

15:15 - 15:45 Uhra
Blick hinter die Kulissen: innovaphone Cloud
- Architekturkomponenten: PBX, Session Border Controller, Reverse Proxy, PSTN Anbindung (ISDN/SIP/Federation)
- Redundanzmöglichkeiten
- Multiservicefunktionen: Videokommunikation, Desktopsharing, WebRTC Toolbox
- Ende zu Ende Sicherheit durch DTLS Verschlüsselung

Lars Dietrichkeit, innovaphone AG

15:45 - 16:15 Uhr Kaffeepause

16:15 - 16:45 Uhr
Liefert die Cloud die bessere UC-Lösung?
- Wie sehen die UC-Angebote in der Cloud aus?
- Werden alle Funktionsbereiche abgedeckt?
- Welche Anforderungen entstehen an die Verbindung zur Cloud?
- Wie wird Video umgesetzt?
- Ist die Cloud als UC-Lösung wirklich preiswerter?
- Wie können Drittprodukte integriert werden, geht das überhaupt?
- Wie sieht der Betrieb aus, ist er mehr oder weniger aufwendig als eine lokale UC-Lösung?

Markus Geller, ComConsult Research GmbH

16:45 - 17:45 Uhr
Podiumsdiskussion: UC aus der Public Cloud, Pro‘s und Con‘s
Mit Herstellern auf dem Podium

ab 18:00 Uhr Happy Hour

Programmübersicht ComConsult UC-Forum 2016

Dienstag 22.11.2016 - All-IP

9:00 - 9:45 Uhr
SIPconnect 2.0: Neuer Standard für SIP Trunking
- SIPconnect 1.1 • SIPconnect 2.0
- Architektur • Voice-LM
- Video-Unterstützung
- IPv6 • Notruf

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

9:45 - 10:30 Uhr
All-IP Migration aus Carrier- und Kundensicht
- Warum überhaupt All-IP?
- Neue Carrier-Infrastuktur, neue SIP- und VPN-Services: Was ändert sich und wann?
- Chancen durch All-IP: Neue Designansätze bei Sprach- und Datennetzen

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

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:30 Uhr
Nicht alles ist Sprache... - was passiert mit den Sonderanschaltungen beim Umstieg auf All-IP
- Was sind Sonderanschaltungen?
- Was passiert da?
- Was sind die Folgen bei der Abschaltung von ISDN
- Vergleich Gateways vs. IP-Migration
- Wie sieht ein Migrationspfad aus?
- Wie ändert sich der Betrieb?

Henry Lakatos, D.I.E. Projekt GmbH

11:30 - 12:00 Uhr
Einsatzszenarien eines Avaya SBC für Enterprise – weit über SIP-Trunking hinaus!
Relevanz eines SBC an der Demarkationslinie zum Unternehmen
- 5 Gründe für einen Avaya SBCE im Unternehmen (Mehr als nur eine Firewall!, Remote-User, WebRTC, Multimedia, Recording)
- Wie sieht eine SIP Connect Zertifizierung aus?

Thomas Römer, Avaya Deutschland GmbH

12:00 - 12:30 Uhr
All-IP in Filialszenarien
- Was unterscheidet All-IP in Filialszenarien von anderen Szenarien?
- Was ist bei Filialszenarien zu beachten? Wo liegen die Fallstricke?
- Wie sehen Architekturen aus und mit welcher Technik setzt man sie um?

Markus Emde, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:30 Uhr
Cisco Collaboration Cloud
- Neue Modelle der Zusammenarbeit unter Berücksichtigung von veränderten betrieblichen Anforderungen
- Integration von interaktiven Hilfsmitteln und Endgeräten in eine gesamtseitliche SaaS Lösung
- Einbindung von Anwendungen über offene APIs
- Wie adressiert die Lösung die Sicherheitsanforderungen und den Schutz der Privatsphäre

Tobias Neumann, Cisco Systems GmbH

14:30 - 15:15 Uhr
Datenschutz bei der Umstellung auf All-IP
- Verschlüsselungsanforderungen und Netztrennung
- SIP-Trunking und Verschlüsselung
- Anforderungen durch das IT-Sicherheitsgesetz und die Cyber-Security-Richtlinie der EU
- Anforderungen durch die EU-Datenschutzverordnung ab Mai 2018

Ulrich Emmert, esb Rechtsanwälte

15:15 - 15:45 Uhr Kaffeepause

15:45 - 16:45 Uhr
Enterprise Session Border Controller: Evaluierung
- Einsatzbereiche: UNI, NNI, E-SBC
- Funktionsbereiche
- ALE, Avaya, Cisco, Mitel, Unify

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

Mittwoch 23.11.2016 - Zusatztag „Arbeitsplatz der Zukunft“

9:00 - 9:45 Uhr
Einführung zum RfQ „Arbeitsplatz der Zukunft“
- Welche Anforderungen stellen sich an den Arbeitsplatz der Zukunft?
- Welche Szenarien und Use Cases wurden im RfQ angefragt?
- Welche Hersteller und Lieferanten beteiligen sich an der Live-Demo?

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

9:45 - 12:00 Uhr (integrierte Kaffeepause)
Live-Demos zum RfQ „Arbeitsplatz der Zukunft“
Referenten der teilnehmenden Hersteller und Lieferanten
- Führung zu den Live-Demo-Stationen der Aussteller
- Präsentation von Use-Cases
- Anschauen und Ausprobieren von realen Arbeitsplatzszenarien

12:00 - 12:45 Uhr
Wieviel Social Collaboration braucht ein Unternehmen?
- Wie relevant ist Social Collaboration für Unternehmen?
- Wann sollte man mit Social Collaboration starten?
- Wie führt man Social Collaboration ins Unternehmen ein?

Dr. Thomas Kreye, CEO, Just Software AG

12:45 - 13:45 Uhr Mittagspause

13:45 - 15:00 Uhr
Diskussionsrunde „Arbeitsplatz der Zukunft“
- Offene Diskussionsrunde mit Ausstellern und Teilnehmern
- Anregungen und Kritik zu den gezeigten Arbeitsplatzkonzepten
- Erfüllen die gezeigten Arbeitsplätze die Teilnehmererwartungen?
- Erfahrungsaustausch

15:00 - 15:45 Uhr
Arbeitsplatztransformation und Change-Management
- Wie führt man neue Technologien am Arbeitsplatz ein?
- Wie wichtig ist Change Management für die Arbeitsplatztransformation?
- Welche CM-Maßnahmen haben sich in der Praxis bewährt?

Johanna Ahrens, avodaq AG

15:45 - 16:00 Uhr
Wrap-up des Tages

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

Anmeldung an kundenservice@comconsult-research.de

ComConsult UC-Forum 2016

Ich buche den Kongress
ComConsult UC-Forum 2016

☐ Kongress mit Zusatztag
21.11. - 23.11.16 in Düsseldorf - € 2.390,--

☐ Kongress ohne Zusatztag
21.11. - 22.11.16 in Düsseldorf - € 1.990,--

☐ Zusatztag am 23.11.16 - € 990,--

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

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

Standpunkt

„Alle Räder stehen still, wenn dein starker Arm es will“ oder das unterschätzte Angriffspotential von DDoS

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.

Ursprünglich stammt das Zitat „Alle Räder stehen still, wenn dein starker Arm es will“ aus einem Lied von 1863 für den „Allgemeinen Deutschen Arbeiterverein“ und appellierte an die Kraft eines Arbeitskampfs, die sich aus gemeinsam handelnden einzelnen Individuen ergibt. Übertragen auf die Informationstechnik könnte man auf der einen Seite vielleicht an Schwarmintelligenz denken, wie sie im Moment im Rahmen der Industrie 4.0 intensiv erforscht wird. Auf der anderen Seite wird man aber schnell an Distributed Denial of Service (DDoS) erinnert.

Der Angreifer nutzt bei einer DDoS-Attacke simultan viele Endgeräte (Slaves), um über ein Netzwerk das Opfer mit Nachrichten in kumulierter Kapazität der Slaves zu fluten, bis die angegriffenen Dienste nicht mehr verfügbar sind. Es ist klar, dass sich hierzu mit einer entsprechenden Schadsoftware präparierte PCs besonders gut eignen, die vom Angreifer über die Schadsoftware ferngesteuert werden. Das Ergebnis sind sogenannte Botnets, die auch als Dienstleistung / Handelsware in den dunklen Stellen des Internet seit geraumer Zeit (teilweise sogar ziemlich preiswert) angeboten werden. DDoS im Internet erfreut sich einer ungebremsten Attraktivität, da es aufgrund des leichten Zugangs, der Möglichkeit sich als Angreifer effektiv zu verbergen und der vergleichbar geringen notwendigen Bandbreite ausgesprochen einfach ist, einen Internet-Zugang lahmzulegen.

Besonders kritisch ist dies angesichts der Tatsache, dass eine hohe Verfügbarkeit des Internet-Zugangs für immer mehr Institutionen von entscheidender Bedeutung ist. Es gibt Fälle, in denen eine Nichtverfügbarkeit im Bereich von wenigen Sekunden ausreicht, um signifikanten Schaden zu verursachen. Mögen solche Fälle jetzt noch selten sein, spätestens mit der Industrie 4.0 und dem Internet of Things (IoT) wird die Anforderung einer hohen Verfügbarkeit die Regel sein. Machen wir uns nichts vor: Das Internet ist wie die Luft zum Atmen geworden

und mit DDoS kann diese Luft ausgesprochen dünn werden.

Daher ist eigentlich klar, dass Maßnahmen gegen DDoS Bestandteil (fast) jeder IT sein sollten. Die Frage ist also: Was können wir gegen DDoS überhaupt tun? Denn Maßnahmen gegen DDoS in der eigenen Infrastruktur sind oft nicht wirkungsvoll genug, da es bereits in dem Moment, in dem die DDoS-Attacke den eigenen Internet-Zugang erreicht, eigentlich schon zu spät sein kann. Sinnvoller sind daher Lösungen, bei denen der eingehende Netzverkehr zunächst über ein sogenanntes Scrubbing Center bei einem Dienstleister (typischerweise in der Cloud geleitet wird, siehe z.B. Cloudflare). Im Scrubbing Center kann DDoS-Verkehr erkannt sowie herausgefiltert („abgebürstet“, daher die Bezeichnung) werden und erst dann wird der gereinigte Verkehr in die eigene Infrastruktur geleitet. Nach diesem Prinzip funktioniert auch Google Project Shield.

Das Scrubbing Center ist also eine Art Prügelknabe, der statt der eigenen Internet-Anbindung in den Ring geschickt wird. Dass so etwas funktioniert, setzt voraus, dass das Scrubbing Center selbst die Schläge einer DDoS-Attacke weitestgehend wegstecken kann, was primär durch eine hohe Kapazität der Internetanbindung des Scrubbing Center und durch zielgerichtete intelligente Filter, die Verkehrsmuster von DDoS-Angriffen erkennen können, erreicht wird. Damit sind wir leider auf dem Fußboden der Realität, denn auch ein Scrubbing Center kann nur mit Wasser kochen: Es kann konzeptionelle Schwächen der Protokolle im Internet nicht beseitigen und es muss wie wir alle mit dem Preis der Freiheit des Internets leben.

Dieses Problem wird an Meldungen der letzten Tage deutlich: Zunächst war im September dieses Jahres ein prominenter Security Blogger zielgerichtet Opfer von einer DDoS-Attacke geworden, die vom Dienstleister Akamai zunächst erfolgreich abgewehrt wurde[1]. Dann hatte Akamai jedoch bei einer erneuten DDoS-Attacke kapituliert, was bei einer Rekordangriffsintensität von ca. 620 GBit/s auch nicht verwundert. Hier werden Grenzen der DDoS-Abwehr deutlich: Während bei DDoS die Kapazität einer DDoS-Attacke mit der Anzahl der Slaves recht einfach skaliert, hat ein Scrubbing Center das Problem schnell und dynamisch Kapazität und Rechenleistung für einen überwachten Internet-Zugang bereitzustellen. Auf Seiten des Scrubbing Center ist hier wesentlich mehr Intelligenz und auch Kapazität erforderlich als auf Angreiferseite. Der Angreifer ist also eigentlich immer im Vorteil. Nebenbei, kurz nach dem beschriebenen Vorfall wurde ein neuer Rekord gemeldet: Wir haben inzwischen DDoS-Angriffe der Terabit-Klasse![2] Es wird vermutet, dass es sich hierbei um ein Botnet aus IP-Kameras handelt. Die dunkle Seite des Internet heißt das IoT also herzlich willkommen und begrüßt die dazugekommene Vielzahl an frei verfügbaren verwundbaren Endgeräten.

Wenn nun die Abwehr von DDoS die beschriebenen Grenzen hat, lohnt sich der Aufwand für Abwehrmaßnamen trotzdem? Ja, denn einerseits rüsten die Anti-DDoS-Anbieter nach und andererseits sind die meisten Angriffe von deutlich geringerer Intensität und können problemlos von abgewehrt werden. Das ist natürlich nicht besonders zufriedenstellend und es wäre schöner, DDoS technisch unmöglich machen zu können (z.B. durch eine Art Zwang zur Absicherung von Endgeräten). Nur wäre das Ergebnis ein überwachtes reglementiertes Netz, das kein Internet mehr wäre.

[1] Siehe **http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/**

[2] Siehe **https://www.heise.de/security/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html**

Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 12.12.-13.12.16 in Köln

Die ComConsult Akademie veranstaltet vom 12.12. bis 13.12.16 ihre Sonderveranstaltung "Wireless und Mobility" in Köln.

Die permanente Steigerung der Anzahl mobiler Endgeräte mit immer mehr Leistung ist ein längst nicht mehr aufzuhaltender Trend. Provider sind schon seit einiger Zeit dabei, die Mobilfunknetze deutlich aufzurüsten. Dies betrifft auch Betreiber privater wireless Infrastrukturen. Sie werden kaum Videos oder Spiele in großem Umfang unterstützen müssen. Man kann aber davon ausgehen, dass die hohe Leistung der mobilen Endgeräte auch für die Realisierung eines verbesserten Benutzer-Erlebnisses bei bestehenden und neuen Anwendungen genutzt wird. Die vielen unterschiedlichen Ansätze für Augmented Reality sprechen z.B. eine deutliche Sprache. Ist eine Technologie, wie in diesem Falle die mobile Anbindung intelligenter Endgeräte verfügbar und erfolgreich, kommen im Laufe der Zeit sozusagen „natürlich“ neue Anwendungen hinzu.

Mega-Treiber: Cloud, Video und IoT

Moderne Arbeitsplatzmodelle gehen von vollständig mobilen Endgeräten aus. Es darf auf die Dauer keine spürbaren qualitativen Unterschiede bei der Benutzung Cloud-basierter oder sonstiger Dienste und Kollaborationstechniken in Abhängigkeit vom Ort oder dem grade vorliegenden Mobilitätsgrad geben.

Es besteht die quasi unabwendbare Tendenz, drahtlose Netze zur Lieferung immer reicherer Inhalte an immer mehr Endgeräte zu benutzen. Dies erzeugt einen erheblichen Druck auf die Ressource, über die wir liefern: die Kapazität des (drahtlosen) Netzes und der dahinter liegenden Infrastruktur.

Ein weiterer Mega-Treiber ist das IoT, die automatische Kommunikation von Maschinen, Sensoren und Aktoren untereinander. Viele IoT-Konzepte könnten ohne drahtlose Verbindungen nicht implementiert werden. Das erzeugt eine völlig neue Dimension von Anforderungen, Leistungsprofilen und Spezial-Technologien.

Private flächendeckende WLAN-Versorgungsstrukturen nach IEEE 802.11ac: mehr Fragen als Antworten!

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

Man kann behaupten, dass Wave2 und Wave3 die ersten wirklich für den professionellen Einsatz gedachten Varianten von IEEE 802.11ac sind. Was bedeutet das in der Praxis? Welche Steuerungsmöglichkeiten bieten uns die einschlägigen Hersteller an?

Eine wesentliche Frage ist: wie werden die neuen Systeme in die Gesamt-Architektur integriert? Die oftmals propagierte „gesteigerte Benutzererfahrung“ ist ja gut und schön, aber welche Anforderungen stellt sie an die betriebliche Logik der Infrastrukturen?

Nach wie vor sollte doch der sichere und wirtschaftliche Betrieb der privaten drahtlosen Infrastrukturen im Vordergrund stehen. Provider erwarten die Möglichkeit, ihre Strukturen aus der Cloud mittels SDN/NFV zu steuern und z.B. Instanzen virtueller Small Cells dynamisch auf der physikalischen Infrastruktur zu schaffen. Sind derartige Funktionen für „normale“ private Betreiber wirklich erforderlich? Wie können Sicherheitskonzepte elegant und wirkungsvoll umgesetzt werden?

Es gab in den letzten Monaten eine Menge von Mergern zwischen Infrastruktur-Anbietern und WLAN-Spezialisten. Cisco hat sich Meraki einverleibt, Aruba gehört jetzt zu HP Enterprise, Brocade funkt jetzt mit Ruckus und auch Extreme/Enterasys haben sich noch einen kleinen WLAN-Spezialisten organisiert. Die Erwartung ist, dass dadurch Synergien zwischen den WLAN-Lösungen und der notwendigen Switching-Infrastruktur entstehen. Wie sieht das aber genau aus? Welche Vorteile ergeben sich möglicherweise für den Betreiber?

Mobilfunk: letztlich das Ende der privaten WLANs?

Schließlich: wie geht es weiter mit dem Mobilfunk? Ausgehend von LTE entwickeln sich nicht nur die nächsten Releases mit deutlich erhöhter Funktionalität bis hin zu 5G, sondern parallel dazu auch Begehrlichkeiten hinsichtlich der bislang den WLANs vorbehaltenen lizenzfreien Frequenzbereiche. Um nämlich die hochgesteckten Ziele von 5G erreichen zu können, brauchen die Provider alle Frequenzen, die nicht bei „3“ auf dem Baum sind, von stillgelegten TV-Kanälen bis hin zu gelegentlichen Lücken in systematischen Funkdiensten. Die Zukunft gehört dem dynamisch etablierten virtuellen Spektrum. Treffen aber konventionelle WLANs mit LTE oder 5G-Signalen zusammen, werden sie höchst wahrscheinlich den Kürzeren ziehen. Oder kann man vorbeugen?

Schon vor über fünf Jahren wurde der Standard IEEE 802.11ad für die Multi-Gigabit-Kommunikation im 60 GHz Millimeterwellen-Bereich definiert. Auch Small Cells werden zunehmend im Millimeterwellenbereich aufgesetzt. Wie sind derartige Trends für private Betreiber zu werten?

Die Entwicklung internationaler Mobilfunkstandards ist deutlich aufwändiger als z.B. eine neue Ethernet-Norm. Die meis-

ten Kunden bekommen heute LTE nach Release.10. Rel. 10 bis ca. Rel .12 heißen auch „LTE Advanced“. Schon in diesen Versionen wird das Konzept aufgegriffen, die Leistung von LTE durch die Hinzunahme von passenden Zellenkonzepten zu erhöhen. Unter Voraussetzung eines guten Interferenz-Managements steigt die mögliche Leistung eines LTE-Versorgungsbereiches (einer Basis-Station) deutlich mit der Anzahl von kleinen Zellen (Small Cells). Richtig spannend wird es mit den Versionen ab Rel. 13 und 5G.
Wie könnte sich das auswirken? Normalerweise wird ein LTE Netz von einem Provider betrieben und auch WLAN oder auf anderer Technik beruhende Small Cells werden auch von ihm kontrolliert.

Gravierende Auswirkungen auf die unterstützende Infrastruktur

Die Anforderungen an die mobile Versorgung steigen stark und man wird darauf Antworten finden müssen. Es wird sicher nicht zu weniger, sondern eher zu mehr WLAN-Zellen kommen. Das wird glücklicherweise durch die entsprechenden Ethernet-Technologien für die Integration der vielen APs unterstützt.

Allgemein werden heute WLAN-Access Points mit 1 GbE und PoE versorgt. Im letzten Jahr wurden neue Ethernet Datenraten definiert, nämlich 2,5 und 5 GbE, die für die Versorgung anspruchsvollerer Access Points nach 802.11ac noch über ältere Kabel gedacht sind. Betrachtet man aber die jetzt schon in Entwicklung befindlichen Nachfolgestandards IEEE 802.11 ad (schon längst fertig), ax und ay, sieht man schnell, dass 5 GbE viel zu kurz greifen. Provider nutzen optische Infrastrukturen, alleine wegen der Latenzen. Ist das auch der Weg für ambitionierte private Betreiber?

Sie sehen: viele Entwicklungen, viele Technologien, Fragen über Fragen. Auf unserer einzigartigen Sonderveranstaltung hören Sie, was erfahrene Top-Spezialisten, Planer, Hersteller und Berater empfehlen. Nutzen Sie die Gelegenheit auch zur ausführlichen Diskussion, bevor die Wireless Welle Sie überflutet.

Die Referenten


Dr. Jan Byok


Dipl.-Ing. Stefan Bien


Dr. Johannes Dams


Dipl.-Ing. Olaf Hagemann


Dr. Simon Hoff


Dr. Franz-Joachim Kauffels


Reinhard Lichte


Dipl.-Ing. Markus Nispel


Dipl.-Ing. Michael Schneiders


Dr. Joachim Wetzlar


Dipl.-Ing. Dominik Zöller

Anmeldung an kundenservice@comonsult-research.de

Sonderveranstaltung Wireless und Mobility

Ich buche die Sonderveranstaltung
Wireless und Mobility

☐ 12.12.-13.12.16 in Köln
zum Preis von € 1.990,--

☐ inklusive Report "Wireless-Systeme der nächsten Generation"
zum Teilnehmer Sonderpreis von 174,- €

☐ 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 Sonderveranstaltung Wireless und Mobility

Montag 12.12.2016

9:30 - 10:30 Uhr
Wireless World: Anforderungen der Digitalen Zukunft
- Implikationen der wachsenden Cloud-Nutzung
- 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 - 11:30 Uhr
Stand der Technik bei WLAN
- 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 - 12:00 Uhr Kaffeepause

12:00 - 13:00 Uhr
WLAN, ein Medium für alle Anwendungen?
- Mobilität und Einfachheit sind Triebfedern für die WLAN-Vernetzung
- Hohe Verfügbarkeit, Reaktivität und Bitrate: Geht das überhaupt mit WLAN?
- Wie bekommt man die optimale Ausleuchtung in Büros und Hallen am besten hin?
- Welche Frequenzen sollen für welche Anwendungen genutzt werden?
- An allen Ecken funkt es: Lassen sich Störungen überhaupt vermeiden?
- „Fremde" Funkanwendungen sickern unbemerkt ein! Wie geht man damit um?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:30 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 und Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 17:00 Uhr
All-IP: ein einheitlicher Access für jegliche Sprachkommunikation. Sind DECT und VoWLAN tot?
- Die Rolle von LTE und 5G im All-IP-Netz
- Mobilfunk in Enterprise-Kommunikationslösungen
- VoLTE und 5G als Ersatz für VoWLAN und (IP-)DECT

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

17:00 - 18:00 Uhr
Von LTE Advanced zu 5G
- Mobilfunk: Stütze der nächsten digitalen Revolution
- Techniken von LTE Advanced
- Koexistenz von LTE / 5G und WLANs
- 5G: Konzepte, Technologien, Feldversuche, Standardisierung

Dr. Franz-Joachim Kauffels, Technologie-Analyst

ab 18:00 Uhr Happy Hour

Dienstag 13.12.2016

9:00 - 10:30 Uhr
Wireless / Mobile / Cloud Security: Ganzheitliche Konzepte sind gefragt
- Sicherheit im WLAN: Ein alter Hut?
- Warum es trotz Hotspot 2.0 kaum sichere Hotspots gibt
- Absicherung von iOS und Android
- Sichere Integration mobiler Endgeräte
- Schlüsselelement sichere Cloud-Dienste
- Rolle von MDM und WLAN Management aus der Cloud

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Auf dem Weg zum All Wireless Office
- WLAN als normales Office Connect muss wie Strom, Wasser, Klima als Infrastruktur leistungsstark zur Verfügung stehen
- Nutzung der WLAN Infrastruktur von allen User- und Gerätetypen
- WLAN und dann ... – Analytics, Locationbased Serivces. Beispiel: der intelligente Meetingraum
- WLAN als Offload von Mobilnetzen in empfangsschwachen Officebereichen
- On-premise, private Cloud oder Public Cloud Lösungen – eine Portfolio für alles

Reinhard Lichte, Aruba - a Hewlett Packard Enterprise Company

11:45 - 12:30 Uhr
Moderne flächendeckende Enterprise WLANs
- Neue Anforderungen durch Cloud und Hybrid Enterprise
- Rolle von SDN/NFV bei der WLAN-Steuerung
- Integriertes Produktspektrum für Zellen und Infrastruktur
- Anwendungsbeispiele

Dipl.-Ing. Markus Nispel, Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 15:00 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

15:00 - 16:00 Uhr
Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen
- Grundlagen der deutschen Störerhaftung nach ständiger BGH-Rechtsprechung (Neueste Entwicklungen im Bereich der Störerhaftung)
- Gesetzesänderung des TMG aus Sommer 2016
- EuGH Urteil aus Herbst 2016 (Zukunft der deutschen Störerhaftung, Gestaltungstipps für Betreiber privater WLAN-Infrastrukturen)

Dr. Jan Byok, Bird & Bird LLP

16:00 Uhr der Veranstaltung

Report-Neuerscheinung

Wireless-Systeme der nächsten Generation:

Anwendungen, Systeme, Anforderungen

In den nächsten Tagen erscheint ein neuer Technologie-Report von Dr. Fanz-Joachim Kauffels bei der ComConsult Research GmbH.

In diesem Report geht es unter anderem um folgende Fragen:

- Ist es weitsichtig, die Infrastruktur an einer einzigen WLAN-Generation zu orientieren?
- Welche Anforderungen ergeben sich, wenn wir nicht nur auf die Systeme schauen, die man jetzt im Laden kaufen kann, sondern auch auf die, die in den nächsten fünf Jahren mit Sicherheit kommen werden?

Blickt man auf die Anforderungen der jetzt in Entwicklung befindlichen Systeme wie IEEE 802.11ax und 11ay, sieht man sofort, dass diese mit 2,5 oder 5 GbE absolut nicht auskommen. Ein sehr wesentlicher Schritt bei diesen Versionen ist, dass das DCF-Verfahren wohl endlich abgelöst wird, was der Autor aber erst glaubt, wenn er es sieht. Dadurch wird hier schon eine vollwertige 10 GbE Infrastruktur mit entsprechender Verkabelung notwendig. Aber auch schon für IEEE 802.11ac Wave 2 oder 3 wird es Access Points mit 10 GbE-Ports Richtung Infrastruktur geben. Ein in 2016 noch fehlender Baustein ist Power over 10 GBASE-T, aber auch hier gibt es eine Reihe von Alternativen und Prototypen, die mit Sicherheit sehr bald zu guten standardisierten Lösungen führen werden.

Die Angst mancher Betreiber vor zu hohen Kosten einer 10 GbE Infrastruktur ist nicht begründet. 10 GbE ist angesichts der Verfügbarkeit von 25/50/100 GbE Switching-Lösungen schon jetzt eine Technologie der zweiten Reihe. Es gibt 10/40 GbE Switch-Chips in rauen Mengen, ein Switch-Port tendiert jetzt schon hinsichtlich der Kosten in Richtung zweistelliger US$-Bereich und wird sich in nächster Zeit alle rund 18 Monate halbieren. Möchte man dann z.B. 2020 auf eine vollständige 10 GbE-Infrastruktur für die WLANs hochrüsten, kosten die Switches höchstens so viel wie heute 1 GbE-Switches. Sind dann aber Kabel und ältere Switches ungeeignet und von zu schlechter Qualität, wird es ärgerlich und teuer!

Der Report hat abgesehen von einer Einleitung fünf Kapitel. Im ersten Kapitel betrachten wir die Entwicklung der Anwendungen und die sich daraus ergebenden Anforderungen genauer. Das zweite Kapitel ist der aktuell neu verfügbaren WLAN-Technik, primär 802.11ac ab „Wave 2“, gewidmet. Kapitel drei beleuchtet die Entwicklung kleinerer Funkzellen, Mikrozellen oder Arbeitsplatz-Zellen im Millimeterwellen-Bereich (50 – 60 GHz-Bänder). Mit vergleichsweise geringem Aufwand können hier Multi-Gigabit Datenraten erzielt werden, aber eben mit einer recht begrenzten Ausdehnung der Zelle. Der bereits länger bestehende Standard IEEE 802.11ad wurde durch WiGig® zu neuem Leben erweckt. Was die Zukunft der drahtlosen Übertragung in der Zukunft ganz bedeutend prägen wird, ist die Entwicklung von LTE und LTE Advanced hin zu 5G Mobilfunk, die wir im vierten Kapitel darstellen. Hier wird die Messlatte für private Versorgungsinfrastrukturen immer höher gesetzt. Gleichzeitig könnte es vermehrt zu Konflikten kommen, wenn die Provider auch mit LTE in die bisher den lizenzfreien WLAN-Systemen vorbehaltenen Frequenzbereiche eindringen möchten. Diese Diskussion ist längst noch nicht ausgestanden. Das fünfte Kapitel stößt dann in den Bereich der in absehbarer Zukunft neu hinzu kommenden Techniken und Verfahren, auch im Hinblick auf die Koexistenz mit 5G, vor. Hierbei werden auch die sich jeweils im Rahmen der Technologien ergebenden Anforderungen an die Infrastruktur diskutiert.

Sparen Sie 50% als Teilnehmer an der Sonderveranstaltung Wireless und Mobility

Bestellung an kundenservice@comonsult-research.de

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-research.de

Zweitthema

Strukturierte Verkabelung für Technische Gebäudeanlagen

Fortsetzung von Seite 1

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

Sinn der strukturierten Verkabelung

Errichter von Gebäuden wie z.B. Architekten müssen sich bei Bürogebäuden damit auseinandersetzen, wie die einzelnen Arbeitsplätze mit einer IT-Verkabelung auszustatten sind. Dies ist Standard jeder Planung neuer Gebäude und wird durch den Nutzer als bereitgestellte Infrastruktur, ähnlich der Stromversorgung, zwingend vorausgesetzt. Die auf diese passive Infrastruktur aufsetzende Kommunikationstechnik ist in den mit Abstand allermeisten Fällen eine Netzwerk/IP-basierende Technologie. Theoretisch könnte dieses Netzwerk auf Basis von unterschiedlichen Zugangstechnologien realisiert werden, doch faktisch ist dies Stand heute ausschließlich Ethernet nach IEEE802.3. Damit verliert die Anwendungsneutralität der Verkabelung an Bedeutung, in der Norm wird sie aber weiterhin als Anforderung aufrechterhalten. Dieses Ethernet ist letztendlich auch dafür verantwortlich, dass die EN 50173 im Laufe der 20 Jahre immer wieder angepasst werden musste, keine bzw. kaum eine andere leitungsgebundene Übertragungstechnik hat so großen Einfluss auf die Anpassungen und Erweiterungen genommen. Wurden neue Funktionen beim Ethernet-Zugangsverfahren entwickelt, so erfolgte zunächst die Prüfung, ob dies mit der vorhandenen Verkabelung möglich ist und mit welchen Konsequenzen. War es nicht möglich, wurde eine Überarbeitung der EN 50173 notwendig, sehr häufig mit einer Dauer der Normungsanpassung von mehreren Jahren (man erinnere sich an die gefühlte endlose Standardisierung der Klasse E).

Welche Konsequenzen hat dies für die Betrachtung einer anwendungsneutralen Kommunikationsverkabelung *„zur Unterstützung von Nutzer-unspezifischen Diensten..., von denen viele die Verwendung von ferngespeisten Geräten erfordern“* (Zitat aus der EN 50173-6)? Für den Fall, dass bei der Planung eines neuen Gebäudes eine TGA-Verkabelung für diese Nutzungsformen geplant wird, muss sich diese nach der höchsten Anforderungsklasse zum aktuellen Stand der verfügbaren Übertragungstechniken richten, und das ist weiterhin die Ethernet-Technologie. Warum? Zur Vermeidung von Neuverkabelung und unter Beachtung der allgemein üblichen Prognose, dass auch bei diesen „ferngespeisten“ Geräten im Laufe der Zeit Ethernet als Kommunikationstechnik zum Einsatz kommen wird, sollte die Verkabelung entsprechend eingerichtet sein, sprich sie sollte strukturiert und anwendungsneutral sein (man denke an die aktuelle Diskussion zum Thema Industrie 4.0).

Erste Anforderungsspezifikationen

Geht man davon aus, dass die Kommunikationsverkabelung zwischen den Verteilern weiterhin im Wesentlichen geprägt wird durch große Distanzen und höhere Datenraten, so kommt in erster Linie Lichtwellenleiter als Medium in Frage. Bei der physikalischen Anbindung der „TGA-Endgeräte“ an das Netzwerk dagegen dürfte bevorzugt gefordert werden,

- eine Datenrate von nicht weniger als 100 Mbit/s sicherzustellen
- eine Stromversorgung über die Datenleitung mit Hilfe von Power-over-Ethernet sicherzustellen.

Daraus resultiert Twisted Pair (in Deutschland als „symmetrische Verkabelung“ geführt) als bevorzugtes Übertragungsmedium, doch muss diese „Endgeräte“-Verkabelung auch

- so aufgebaut werden wie bisher (selbe Topologie bzw. Hierarchie)?
- mehr als 100 Mbit/s übertragen können?
- mehr als 100 MHz übertragen können?
- überall den RJ45-Steckverbinder bereitstellen?

Die Beantwortung dieser Fragen lässt sich nur sehr wenig auf Grundlage von Erfahrungen durchführen, dazu steht die Einführung der Netzwerk-Technik in diesen TGA-Bereichen noch viel zu sehr am Anfang. Wünschenswert wären also möglichst herstellerneutrale Standards oder Richtlinien, die Hilfe bei der Planung leisten könnten. Gibt es diese Richtlinien/Standards, sind diese ausreichend bzw. vollständig zur Durchführung der Planung bzw. was muss der Planer möglicherweise noch ergänzen?

Normenübersicht

Herstellerneutrale Verkabelungsnormen existieren seit 1995, als weltweit gültige Normen (ISO/IEC 11801 plus weitere), als Europäische Normen (EN 50173) und als Deutsche Normen (DIN/EN 50173), welche weitestgehend eine Übersetzung EN 50173 mit geringfügigen nationalen Änderungen darstellt. Einen besonderen Fall stellen die amerikanische Normen der EIA/TIA dar, sie sind zwar kaum als Planungsrichtlinie in Deutschland zu nutzen, bilden aber sehr häufig bei neuen Technologien die ersten herstellerunabhängigen Richtlinien, welche anschließend in großen Teilen in den oben genannten internationalen und nationalen Normen einfließen. Bleiben wir aber bei den national wichtigen Normen, auch hier gibt es nicht die EINE Norm, in der alles enthalten ist, stattdessen gibt es neben der zentralen Normenreihe EN 50173 weitere bedeutende Normen. Als Beispiele sind zu nennen die EN 50346 in Zusammenhang mit den Messungen der Verkabelung, die EN 50288 in Zusammenhang mit der Spezifikation der Twis-

ted-Pair-Kabel oder die IEC 60603 in Zusammenhang mit der Spezifikation der Steckertechnologie bei Twisted-Pair.

Im vorliegenden Artikel liegt der Fokus auf der EN 50173-6 (Anwendungsneutrale Verkabelung für verteilte Gebäudedienste), deren letzte Überarbeitung im Mai 2014 erfolgt ist. Es wird notwendig sein, die wesentlichen Unterschiede

- zur EN 50173-1 (September 2011),
- zur EN 50173-2 (Anwendungsneutrale Verkabelung in Bürogebäuden; September 2011)
- und zur EN 50173-3 (Anwendungsneutrale Verkabelung in industriell genutzten Gebäuden; September 2011)

zu zeigen, denn nur die Berücksichtigung und Kenntnis der Basisnorm EN 50173-1 ist nicht ausreichend.

Die genannten ergänzenden Normen erläutern in der Einleitung den jeweiligen Anwendungsbereich:

EN 50173-2: Die Richtlinie beschreibt die IT-Verkabelung für Anwender in Büroumgebungen, die auf eine anwendungsneutrale Infrastruktur statt proprietärer Lösungen setzen.

EN 50173-3: Die Richtlinie beschreibt die IT-Verkabelung für Anwender mit industriell genutzten Kommunikationsanlagen, die auf eine anwendungsneutrale Infrastruktur statt proprietärer Lösungen setzen und die einen Schwerpunkt beim Zugangsverfahren Ethernet erwarten. Ziel ist die durchgängige Einbindung dieser Lösungen in vorhandene Unternehmensnetze/ -infrastrukturen der Bürobereiche. Wichtig ist die Abgrenzung: Sie betrachtet keine Kabelanlagen im Industrie-Bereich, die an den „Schnittpunkt“ der EN 50173-3 angeschlossen werden, z.B. Profinet-Verkabelungen.

EN 50173-6: Die Richtlinie beschreibt Kommunikationskabelanlagen für „nutzer-unspezifische Kommunikationsdienste“, welche auf ferngespeiste Geräte Zugriff haben wie z.B.

- Telekommunikation,
- Energiemanagement,
- Steuerung Umgebungsbedingungen,
- Zugangskontrolle,
- Alarmierung.

Interessant ist, dass der definierte Anwendungsbereich auch medizinische Bereiche umfasst, wie z.B. Schwesternrufanlage, Patientenüberwachung oder ähnliche. Im Prinzip würde dies bedeuten, dass kein modernes Krankenhaus mehr geplant werden dürfte ohne Beachtung der EN 50173-6. Ziel ist die Ablösung einer bedarfsorientierten Verkabelung und damit Vereinheitlichung der gesamten IT-Infrastruktur eines Gebäudes und, darauf wird besonders hingewiesen, die Verringerung der Verkabelung und damit eine Brandlastreduzierung. Auch in der EN 50173-6 werden nicht die Kabelanlagen betrachtet, die an den „Schnittpunkt“ der EN 50173-6 oder -3 angeschlossen werden (also z.B. keine Berücksichtigung von Spezialverkabelungen einer Evakuierungsanlage).

Beide dienen grundsätzlich den Errichtern von Gebäuden (z.B. Architekten) als Planungshilfen für eine IT-Verkabelung bevor die spezifischen Anforderungen der eingesetzten Übertragungstechniken bekannt sind, somit stellen sie im Grunde genommen ein „Muss“ für alle Gebäudeplaner dar. Aus Sicht des Autors ist gerade die EN 50173-6 aber noch nicht wirklich im Planungsdenken vieler Gebäudeplaner „angekommen“.

Grundnorm und Bürogebäudenorm

Alle drei Normen (-2, -3, -6) sind ohne gleichzeitige Beachtung der EN 50173-1 nicht anwendbar, denn sie weisen zumeist nur die Unterschiede zur Basisnorm EN 50173-1 aus. Geht es z.B. darum, in welchen Güteklassen die Materialien der symmetrischen Verkabelung (TP-Verkabelung) einzuteilen sind, so wird auf die Basisnorm verwiesen und es gelten exakt die gleichen Spezifikationen. In einem entscheidenden Punkt unterscheiden sich alle Normen, dies ist die empfohlene Topologie.

Die sternförmige „Rumpf-Topologie“ der Basisnorm EN 51073-1 sieht wie folgt aus: Mit Hilfe der Elemente Standortverteiler (SV), Gebäudeverteiler (GV) und Etagenverteiler (EV) wird eine 2-stufige Topologie realisiert. Die 2 Stufen sind:

- Primärverkabelung
- Sekundärverkabelung

Vor der Verabschiedung der EN 50173-2 wurde die Basisnorm noch in der bekannteren 3-stufigen Form geführt, in der es auch noch eine Tertiärverkabelung gab, die in den Teilnehmeranschlusseinheiten (TA) bzw. informationstechnischen Anschlüssen endete. Da diese dritte Stufe in Abhängigkeit der Nutzungsform des Gebäudes nicht immer identisch sein kann, wurde diese dritte Ebene aus der Basisnorm herausgenommen und in unterschiedlichen Formen in den Ergänzungsnormen für Bürogebäude, Industriegebäude und für verteilte Gebäudedienste spezifiziert. (siehe Abbildung 1)

Für jede Hierarchieebene können unterschiedliche Medien geplant werden mit unterschiedlichen Güteklassen, bei Kupfer werden die Begriffe „Kategorie“ (z.B. Kategorie 7) und „Klasse“ (z.B. Klasse E) verwendet, bei Lichtwellenleiter die Begriffe „OM“, „OS“, „OP“, „OH“ für die Fasertypen und „OF“ für die Streckenklasse (es gibt bis heute keine Güteklassen in diesen Normen für LWL-Stecker!).

In der Annahme, dass den meisten Lesern die Topologie der EN 50173-2 (Bürogebäude) bekannt ist, konzentrieren wir uns auf die beiden Alternativen, der EN 50173-3 und -6. Schauen wir uns zunächst die Topologie der „Industrieverkabelung“ einmal an, was fällt auf:

Industrieverkabelung

Die Ebene Primär- und Sekundärverkabelung wurde übernommen, dies vereinfacht die Anbindung von Industrieverkabelungen/-topologien an bereits vorhandene Topologien. Explizit wird darauf hingewiesen, dass auch Bus- und Ringtopologien unterstützt werden und damit vielfältige Möglichkeiten zur Bildung von redundanten Strukturen möglich sind.

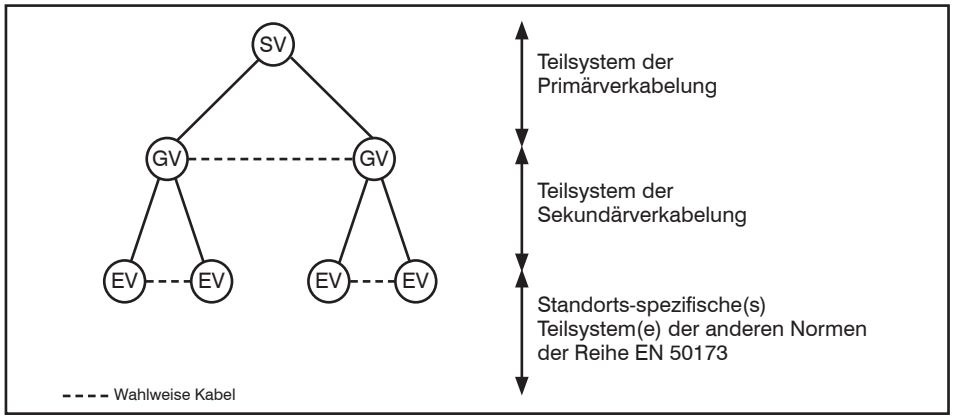

Abbildung 1: Sterntopologie nach EN 50173-1

Strukturierte Verkabelung für Technische Gebäudeanlagen

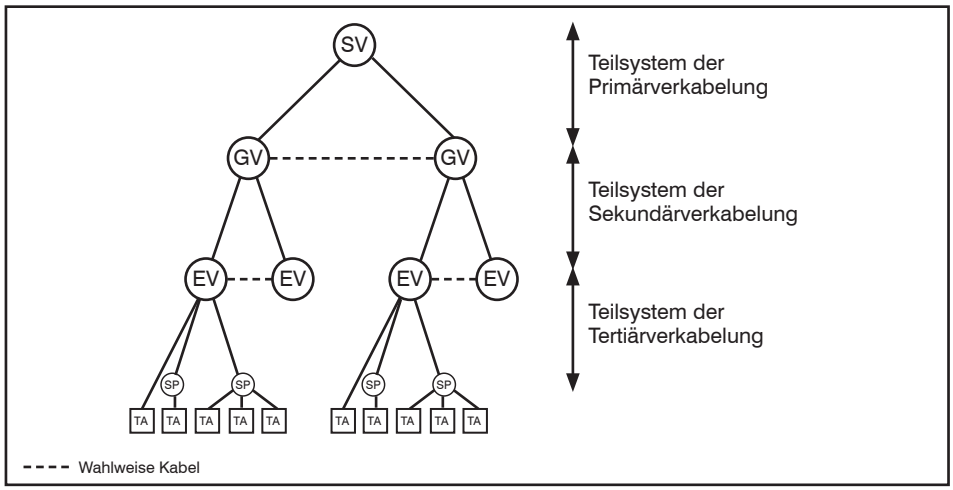

Abbildung 2: Sterntopologie nach EN 50173-2

Unterhalb des Etagenverteilers wird eine neue Ebene eingeführt, welche die dritte Ebene in Ergänzung zur EN 50173-1 (siehe Bild) und die Alternative zur dritten Ebene der EN 50173-2 (siehe Bild) darstellt. Diese neue Ebene heißt nicht Tertiärverkabelung (wie in der EN 51073-2), sondern Etagenverkabelung und stellt eine Ebene zur Verbindung des Etagenverteilers mit dem neu definierten Zwischenverteiler (ZV) dar. Aus Sicht des Autors ist der Begriff „Etagenverkabelung“ etwas unglücklich gewählt, denn häufig wird im üblichen Sprachjargon bei der Planung die Tertiärverkabelung auch „Etagenverkabelung“ genannt. Normativ ist die Etagenverkabelung der EN 50173-3 aber etwas anderes als die Verkabelung zur Anbindung von Endgeräten. (siehe Abbildungen 2 und 3)

Die Anbindung der „Industrie-Endgeräte“ erfolgt mit Hilfe einer neuen, zusätzlichen vierten Ebene unterhalb der Etagenverkabelung, sie dient zur Verbindung der Teilnehmeranschlüsse (= Dosen im allgemeinen Sprechjargon) mit dem Verteiler. Unter dem Etagenverteiler und dem Teilnehmeranschluss kann man sich ja noch etwas vorstellen, doch der Zwischenverteiler? Wozu dient das?

Zur Erläuterung ein Beispiel: Man stelle sich eine Maschine oder Anlage in einer industriell genutzten Halle vor, welche mehrere Datenanschlüsse benötigt. Vorhandener Platz oder andere Umgebungsbedingungen lassen keinen klassischen Etagenverteiler (inkl. 19“-Technik ö.ä.) zu, sondern nur einen speziellen „Zwischenverteiler“. Ein typischer Zwischenverteiler könnte eine Einheit

- mit Hutschiene,
- plus speziellen Hutschienen-Switches,
- plus Hut-Schienen-Anschlussmodulen

sein, von dem ausgehend dann die Datenkabel zur Teilnehmeranschlussbuchse verlegt werden. An die Teilnehmeranschlussbuchse kann dann eine Maschine direkt angeschlossen werden (z.B. mit Ethernet) oder aber auch eine „Automationsinsel“, die mit Hilfe einer eigenen Übertragungstechnik intern kommuniziert und die lediglich den Anschluss „nach draußen“ benötigt. (siehe Abbildung 4)

Nach den Erfahrungen des Autors ist dies ein typisches Szenario: Die häufig werksübergreifende IT-Abteilung stellt mit dem Zwischenverteiler einen definierten Übergabepunkt bereit, an den sich die Netze anschließen können, die nicht im Zuständigkeitsbereich der IT-Abteilung befinden, z.B. ein Profinet, eine Feldbus-Technologie o.ä.. Der Vorteil dieser Topologie besteht also u.a. darin, dass eine „saubere“ organisatorische Trennung beibehalten wird, indem der IT-Anlagenverteiler nicht direkt in dem IT-Etagenverteiler vorgesehen wird, sondern separat bleibt. Eine Durchmischung von möglicherweise unterschiedlichen organisatorischen Kompetenzen und Zuständigkeiten kann vermieden werden.

Verkabelung für Gebäudeanlagen

Die Hierarchie der EN 50173-6 ist etwas komplizierter, auch hier wird die Ebene der Primärverkabelung aus der Basisnorm übernommen, unterhalb des Gebäudeverteilers jedoch wurden alle Teilelemente insbesondere die Verteilerelemente neu definiert. Es wurde

1) eine andere Sekundärverkabelung definiert (Verbindung von Gebäudeverteiler und Diensteverteiler (DV) → Etagenverteiler ist im Unterschied zur EN 50173-2 und -3 nicht notwendig),

2) eine neue Ebene unterhalb der Sekundärverkabelung definiert, welche in 2 Varianten abgebildet werden kann (Typ A und Typ B).

Es ist davon auszugehen, dass Gebäude, welche mit einer völlig normkonformen Kommunikationsverkabelung ausgestattet werden sollen, in Zukunft dann neben dem Standard-Etagenverteiler auch Diensteverteiler, Dienstekonzentrationspunkte (DKP) und Diensteanschlüsse (DA) haben werden. Dies bedeutet nicht zwangsläufig, dass ein Diensteverteiler in einem anderen Raum oder an einem anderen Punkt platziert werden muss als der Etagenverteiler, aus normativer Sicht ist ein Verteiler nicht gleich einem Raum (Zitat: „*Verteiler = Begriff zur Bezeichnung der Funktionen einer Zusammenstellung von Komponenten (z.B. Rangierfelder, Rangierschnüre) für die Verbindung von Kabeln*“).

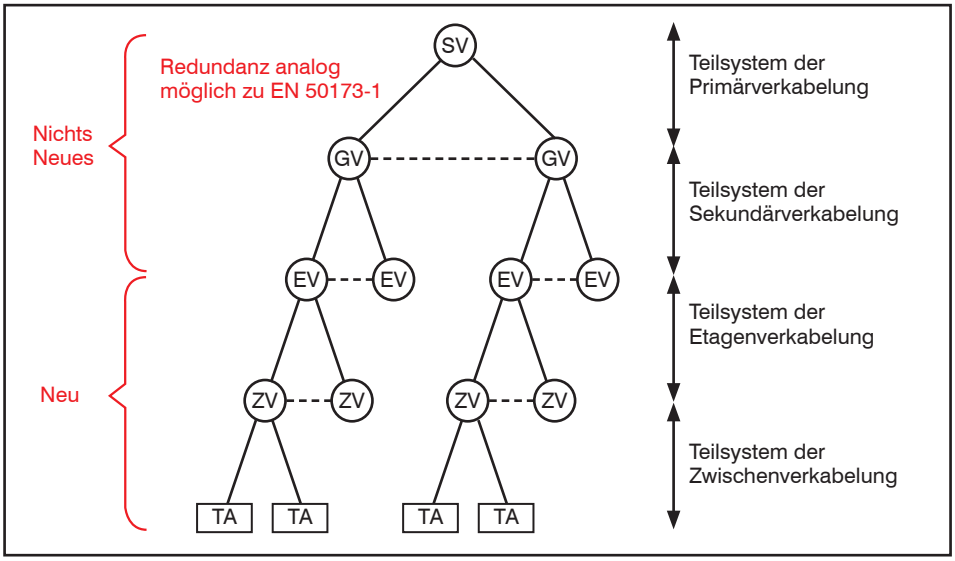

Abbildung 3: Sterntopologie nach EN 50173-3 (Industrie-Verkabelung)

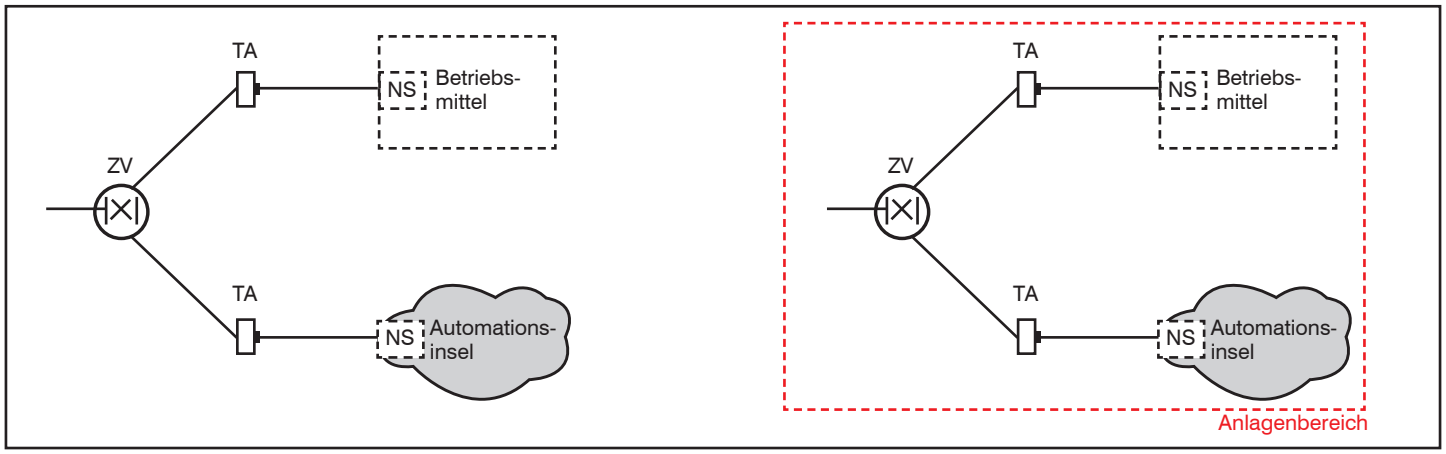

Abbildung 4: Zwischenverkabelung (links: außerhalb der Anlage, rechts in der Anlage)

Versucht man eine Analogie zur bekannten klassischen Verkabelung herzustellen, so kann sinngemäß angenommen werden,

- dass der Diensteverteiler ähnlich dem Etagenverteiler ist,
- dass der Dienstekonzentrationspunkt ähnlich dem Sammelpunkt ist,
- dass der Diensteanschluss ähnlich dem Teilnehmeranschluss ist. (siehe Abbildung 5)

Der Unterschied zwischen Typ A und Typ B (siehe Abbildung 5) besteht im Wesentlichen darin, dass bei Typ B der Diensteanschluss nicht definiert wird und damit „Endanschlüsse“ nicht Gegenstand der Norm sind. Doch wozu ist das Ganze gut, gerade diese Unterteilung? Dazu zwei Beispiele.

Im ersten Beispiel betrachten wir die WLAN-Verkabelung (siehe Abbildung 7), also die Verkabelung zur Anbindung der Access Points. Bisher werden diese WLAN-Anschlüsse unter der Tertiärverkabelung geführt und der Teilnehmeranschluss TA stellt das abschließende Element dar. Doch ist das tatsächlich ein Element der Tertiärverkabelung, gelten für dieses Element dann alle Anforderungen, die man an einen Tertiäranschluss stellt? Da dieses Kabel zur Verbindung eines Switches und eines weiteren elektronischen Verteilelementes dient (in diesem Sinne ist ein Access Point zu sehen), könnte man die Strecke auch als Backbone-Verkabelung definieren. Diese „Unschärfe“ lässt sich mit Hilfe der EN 50173-6 beseitigen, denn hier wird dediziert auf den Aufbau von Funkzellen eingegangen (informativer Anhang B). Wie in Abbildung 7 erkennbar, stellt der Diens-teanschluss DA den Datenanschluss zur Realisierung der Funkzelle dar und damit gilt die Topologie nach Variante B. Zur Planung der Funkzellengröße macht die Norm verschiedene Vorschläge in Bezug auf den Radius der Funkzelle. Aber Achtung: Es ist noch nicht der Standard IEEE802.11ac oder ad berücksichtigt. Die Norm empfiehlt eine Klasse EA für die Realisierung der Diensteverteilungsverkabelung, was im Übrigen aber ohnehin bei den meisten Planungen als Standard vorgesehen wird.

Welchen Einsatzfall muss man sich für Variante B vorstellen? Es ist mit Sicherheit damit zu rechnen, dass Kommunikationsanlagen zum Einsatz kommen werden, die nicht anwendungsneutral sind, nicht auf IP/Ethernet-Basis arbeiten und demzufolge ggf. eine völlig andere Art der Verkabelung erfordern. Sind diese Anlagen(-teile) über weite Flächen oder Gebäudeteile verteilt, so kann es Sinn machen, diese Teile mit Hilfe einer anwendungsneutralen Verkabelung miteinander zu verbinden. In diesem Falle wäre der Anlagentyp B zu wählen. (siehe Abbildung 8)

Der Diensteverteiler bildet in allen beiden Varianten ein wesentliches Planungselement und muss entsprechend frühzeitig bei der Planung eines neuen Gebäudes berücksichtigt werden. In der Norm wird empfohlen, dass ein DV auf 1.000 qm vorzusehen ist und nach Möglichkeit mindestens einer pro Etage. Exakt die gleichen Empfehlungen gelten in der Büronorm EN 50173-2 für die Planung der Etagenverteiler. Lässt das wiederum den Schluss zu, beide Funktionalitäten in einem Raum abzubilden oder wäre es doch besser, einen

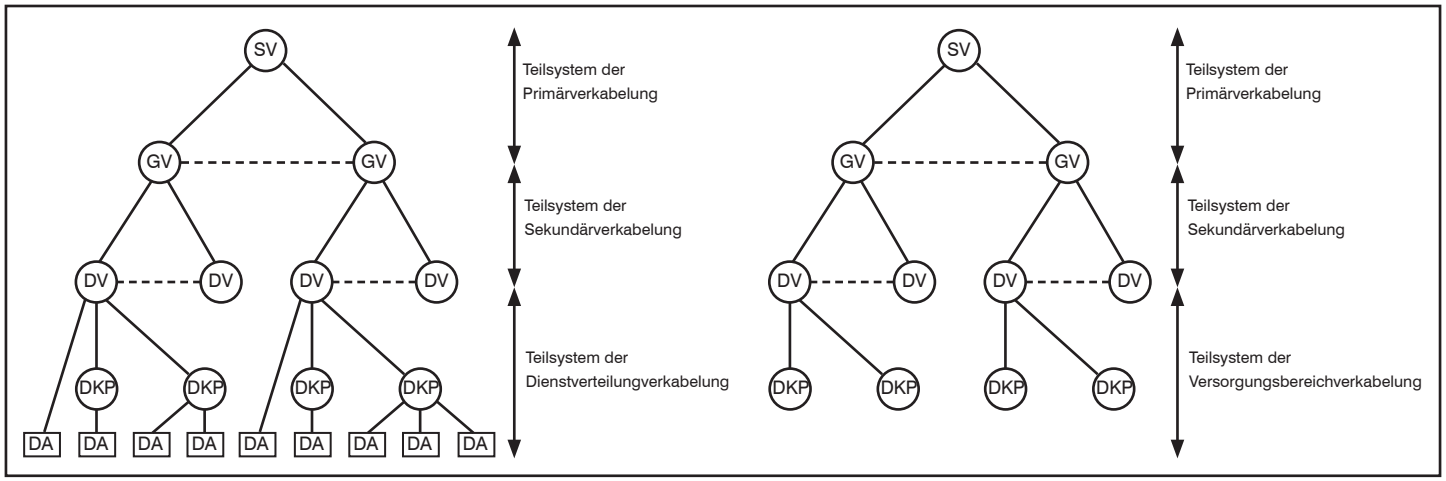

Abbildung 5: Unterschiede Typ A (links) und Typ B (rechts) nach EN 50173-6

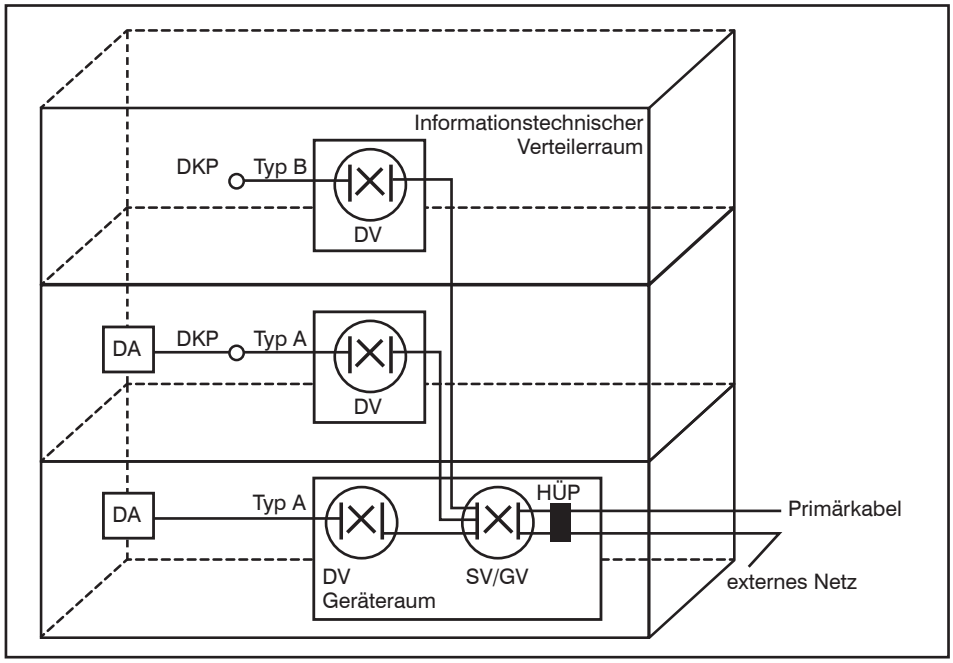

Abbildung 6: Beispielhafte räumliche Anordnung der Teilelemente nach EN 50173-6

separaten Punkt/Raum für den Diensteverteiler festzulegen? Eine Zusammenlegung hätte folgende Vor- und Nachteile:

- Die Platzierung der Verteiler richtet sich natürlich nach dem im Tertiärbereich bzw. in der Diensteverkabelung/ Versorgungsbereichverkabelung gewählten Medium mit deren Längenrestriktionen. Ist die geplante Lage und Anzahl der Etagenverteiler ausreichend, so kann davon ausgegangen werden, dass auch der Diensteverteiler optimal platziert wäre.

- Soll keine vollständige separate aktive Netzwerk-Technologie eingesetzt werden, sondern ggf. mit Hilfe von VLANs ein gemeinsames Netzwerk für die unterschiedlichen Dienste benutzt werden, so ließe sich dies mit einem gemeinsamen EV/DV besser realisieren.

- Ist dagegen eine organisatorische Trennung beim Betrieb der unterschiedlichen IT-Welten (Büronetze und Gebäudedienstnetze) gefordert, so lässt sich diese Trennung besser bei Nutzung von unterschiedlichen Räumen sicherstellen. Das ist also eher eine „politische“ als eine technische Frage.

Bemerkenswert ist es, dass die Verbindung zwischen dem DA und dem Endgerät nicht zwingend mit Hilfe von flexiblen Kabeln (also Kabel mit Aderlitzen) realisiert werden muss, sondern auch mit Kabeln mit fester Ader vorgesehen werden kann, sofern man davon ausgeht, dass der Zugang und das Biegen der Schnüre während des Betriebs nicht vorkommt. Dieser Fall wird vermutlich bei vielen Installationen vorkommen und erlaubt es größere Streckenlängen aufzubauen, da die flexiblen Kabel in der Regel eine deutlich höhere Signaldämpfung haben als Kabel mit festem Aderaufbau. Beispiel: Ein AWG22 hat bei 500 MHz eine Dämpfung von ca. 36 dB/100m und ein AWG26 z.B. 56 dB/100m. Allerdings ist dabei zu beachten, dass nicht jeder RJ45-Stecker an ein Installationskabel mit AWG22/AWG23 angeschlossen werden kann, hier ist eine geeignete Produktauswahl notwendig.

Deutlich schwieriger als die Planung des Diensteverteilers dürfte die Festlegung der im Gebäude verteilten Diensteanschlüsse sein. Wo sieht man präventiv bei einem Neubau diese vor, gerade dann, wenn es noch keine konkrete Anforderung zur Anbindung von speziellen Gebäudediensten gibt? Hier würde man sich etwas mehr Hilfe in der Richtlinie wünschen. Als Empfehlung zur Ausstattung wird mindestens 1 Anschluss pro Dienstebereich in Form eines symmetrischen 8-adrigen Kupferkabels ausgesprochen (konkret: min. Klasse D). Dieser Anschluss wird vermutlich in den seltensten Fällen in Form einer Standarddose realisiert, stattdessen sind je nach Montageort auch spezielle RJ45-Buchsen vorzusehen, die eine verbesserte Kabelzuführung oder platzsparende Montage möglich machen.

Bei allen Empfehlungen und Spezifikationen in der Norm bleibt die Glasfaserlösung als Medium mit Ausnahme des Primär- und Sekundärbereiches außen vor. Dies bedeutet aus Sicht des Autors letztendlich, dass in einem modernen, normkonformen Gebäude mindestens für die Verkabelung nach EN 51073-6 das Medium Twisted-Pair unvermeidbar ist und damit die Frage gestellt werden muss, wie sinnvoll eine zu den Büros verlegte Glasfaserverkabelung ist („Fiber to the Desk“ oder „Fiber tot he Office“).

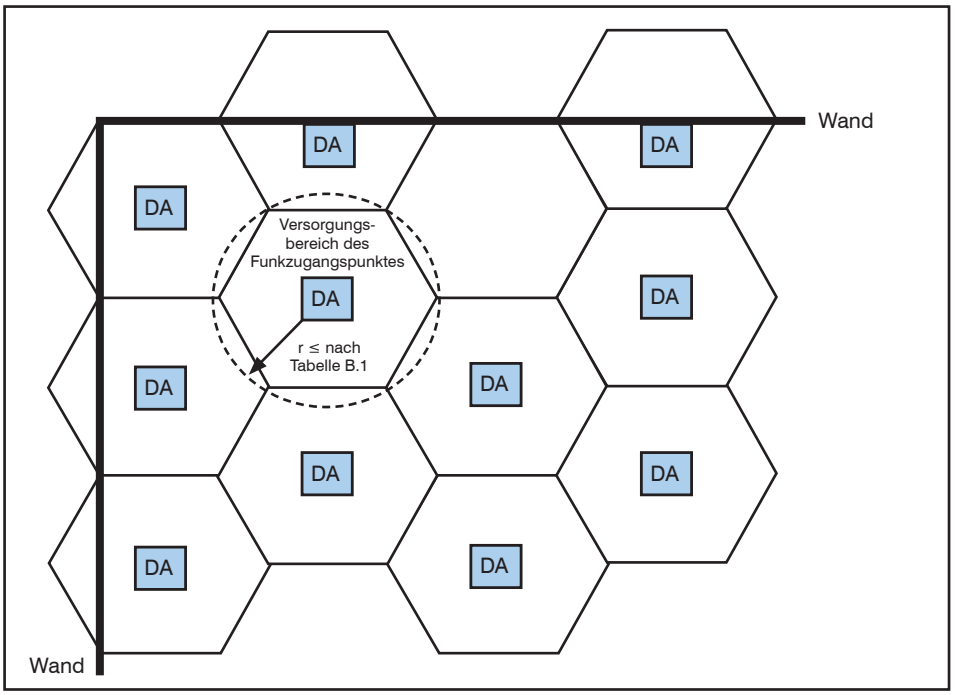

Abbildung 7: Funknetzplanung nach EN 50173-6

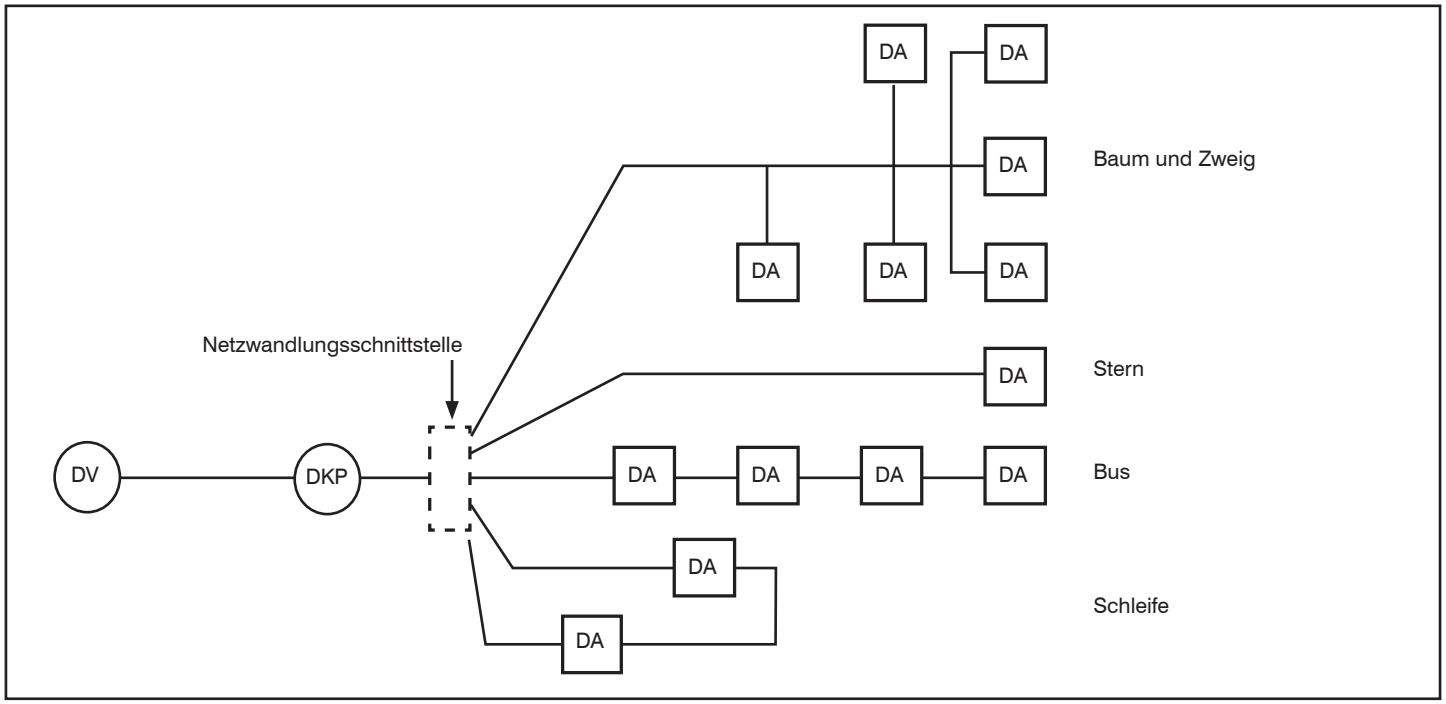

Abbildung 8: Anbindung von speziellen Kommunikationsanlagen

Fazit

Trotz der Tatsache, dass die EN 50173-6 bereits mehr als 2 Jahre alt ist, wird sie nur sehr schleppend bei den Planungen von neuen Gebäuden berücksichtigt, egal ob es Büro- oder Industriegebäude sind. Die Spezifikation einer neuen Topologie in der Norm, welche ergänzend zu bisher bekannten Topologien vorgesehen werden kann, zwingt den Planer dazu, sich mit einigen wesentlichen, durchaus neuen Aspekten bei der Planung einer Verkabelung für verteilte Gebäudedienste auseinanderzusetzen. Auch die klassische TGA-Planung wird kurzfristig damit konfrontiert, dass die raum- oder gar etagenübergreifende Kommunikation der Regelungs- und Alarmierungstechnik IP-/Ethernet-basierend erfolgt und damit auch die Nutzbarkeit einer anwendungsneutralen IT-Gebäudeverkabelung große Vorteile mit sich bringt. Trotz der Nutzbarkeit dieser europäischen Normen bleibt die Grundfrage offen, in wessen Zuständigkeitsbereich diese Verkabelung fällt, wird dies im Rahmen der klassischen IT-Planung berücksichtigt oder eher im Rahmen der TGA-Planung? Wer ist verantwortlich für die frühzeitige Berücksichtigung dieser Verkabelung, die IT-Abteilung? Der klassische IT-Verkabelungsplaner wird vermutlich eher den Grundgedanken der Norm verstehen und umsetzen können als der TGA-Planer, dessen Welt doch sehr stark von proprietären Kommunikationstechniken geprägt ist. Bisher!

Maximale Leitungslängen bei der Planung von Twisted-Pair-Anschlüssen

Insbesondere in Zusammenhang mit der Planung von passiven Anschlüssen für WLAN-Access Points gibt es eine interessante Betrachtung bezüglich der einzuplanenden maximalen Leitungslänge. Die Standard-Planung sieht in den allermeisten Fällen die Einhaltung einer Maximallänge von 90 m für die festverlegte Verbindung vor (also zwischen Rangierfeld des DV oder EV und dem Diensteanschluss bzw. dem informationstechnischen Anschluss). Immer wieder stößt man bei erforderlichen größeren Leitungslängen auf die Fragen, lässt man eine größere Länge zu, bis zu welcher Meteranzahl oder muss man einen neuen Verteiler – in der Regel nur für eine Handvoll Anschlüsse - einplanen. Normativ gibt es keine zwingende Vorschrift zur Einhaltung der 90 m, entscheidend ist die Einhaltung der elektrotechnischen Werte je nach geforderter Übertragungsqualität. Fordert man also z.B. die Einhaltung der Klasse EA zur Sicherstellung von 10GBaseT für Channel Link bzw. Permanent Link, so müssen alle diesbezüglichen Grenzwerte auch bei IPL > 90 m bzw. ICL > 100 m eingehalten werden. Durch Verwendung von besseren Materialien, insbesondere eines besseren Installationskabels, lassen sich diese Längen tatsächlich überschreiten. Doch wie viel länger darf das Installationskabel sein? Hier sind maßgeblich die Leitungsdämpfungen zu betrachten, dies ist zum einen die Ohmsche Leitungsdämpfung zur Sicherstellung einer Stromversorgung mit Hilfe von Power over Ethernet und zum anderen die frequenzabhängige Leitungsdämpfung zur Sicherstellung der Datenrate. PoE und die „nachrichtentechnischen“ Parameter haben unterschiedlichen Einfluss auf die maximale Länge. Es ist aber davon auszugehen, dass mit höchstwertigen Kabeltypen 105 Meter Installationskabel und mehr möglich sind. Hier sind unbedingt die unterschiedlichen Dämpfungsbeläge von verschiedenen Kabeln zu vergleichen, dazu folgende Beispiele eines Kabelherstellers (Werte bei 500 MHz mit dem Ziel Klasse EA sicherzustellen für 10GBaseT):

AWG22 (Leoni Kat.7A):	35,9 dB/100m
AWG23 (Leoni Kat.7A):	37,9 dB/100m
AWG23 (Leoni Kat.7):	38,2 dB/100m
AWG23 (Leoni Kat.6A):	41,2 dB/100m
AWG26 (Leoni Kat.7flex):	56,0 dB/100m

Zum Vergleich: Ein Kategorie-6A-Kabel darf nach Norm 45,3 dB/100m haben. Es lohnt sich also bei erforderlichen großen Leitungslängen statt eines AWG23 ein besseres AWG22 zu nehmen, was immerhin eine Reichweitenerhöhung von 5 Meter und mehr bringen kann.

ComConsult Veranstaltungskalender

TCP/IP-Netze erfolgreich betreiben, 24.10.-26.10.16 in Bonn

Garantietermin

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

Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 24.10.-26.10.16 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,-- netto

Interne Absicherung der IT-Infrastruktur, 24.10.-26.10.16 in Bonn

Garantietermin

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: €1.890,-- netto

IT-Verträge: verhandeln, verändern, verklagen - Überblick für Nichtjuristen, 25.10.16 in Bonn

Garantietermin

Die Veranstaltung beinhaltet einen vertiefenden Überblick über das bei der Beschaffung bzw. dem Vertrieb von IT-Produkten und Dienstleistungen anwendbare Vertragsrecht. Teilnehmern wird eine belastbare Orientierung im Dickicht der verschiedenen Vertragstypen, Vertragsklauseln, Vertragsmuster und regelungsbedürftigen Einzelheiten vermittelt.

Preis: € 1.090,-- netto

ComConsult Technologie-Tage 2016, 07.11.-08.11.16 in Köln

Garantietermin

Die ComConsult Technologie-Tage 2016 wenden sich an Führungskräfte und Entscheider und analysieren wie unsere IT in Zukunft aussehen wird. Die Kernthemen sind: Strategien für das Rechenzentrum der Zukunft, Skalierbarkeit im Technologie-Mix 2020, Kommunikations-Strategie 2020, Sicherheits-Strategie 2020.

Preis: € 1.990,-- netto

Mobile Device Management: Technik und juristische Rahmenbedingungen, 07.11.-08.11.16 in Köln

Garantietermin

Die Anforderung an IT-Abteilungen, mobile (und teilweise auch privat genutzte) Geräte wie Smartphones und Tablets in das Firmennetz einzubinden, wächst rasant. Dieses Seminar erläutert detailliert die technischen und rechtlichen Maßnahmen, um einerseits die IT-Sicherheit zu gewährleisten und auf der anderen Seite Verstöße gegen Datenschutzrecht, Persönlichkeitsrecht und Betriebsverfassungsrecht auszuschließen.

Preis: € 1.590,-- netto

IT-Projektmanagement Kompaktseminar, 07.11.-09.11.16 in Aachen

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 Termineinhaltung sicherstellen können.

Preis: € 1.890,-- netto

RZ-Kopplung: Georedundanz für Rechenzentren, 09.11.16 in Berlin

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,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 09.11.-11.11.16 in Berlin

Das Seminar liefert eine Einschätzung aktueller und neuer RZ-Technologien und bietet Ihnen auf der Basis jahrzehntelanger Erfahrung bewährte Best-Practice-Hinweise.

Preis: € 1.890,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 09.11.-11.11.16 in Berlin

Garantietermin

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

Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 09.11.-10.11.16 in Berlin

Garantietermin

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

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
24.10. - 26.10.16 in Bonn
13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen

Internetworking
14.11. - 18.11.16 in Aachen
03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
02.05. - 05.05.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
15.11. - 18.11.16 in Aachen
27.06. - 30.06.17 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
24.10. - 26.10.16 in Frankfurt
13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf

Session Initiation Protocol Basis-Technologie der IP-Telefonie
09.11. - 11.11.16 in Berlin
05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt

Umfassende Absicherung von Voice over IP und Unified Communications
28.11. - 30.11.16 in Bonn
08.05. - 10.05.17 in Frankfurt
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf
18.09. - 19.09.17 in Düsseldorf

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

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

Impressum

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

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

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

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