ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Februar 2020

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Gebäude der Zukunft: IT-Infrastruktur für die digitalisierte Raumdecke

von Hartmut Kell

Die zunehmende Digitalisierung moderner und vor allem neuer Gebäude geht damit einher, dass insbesondere die Verkabelungsinfrastruktur den derzeit nur schwer absehbaren Anforderungen gerecht wird und demzufolge frühzeitig geplant werden muss. Eine einfache Erweiterung der klassischen Arbeitsplatzverkabelung um eine kleine oder große Anzahl von zusätzlichen Datenanschlüssen, basierend auf denselben Planungskonzepten und denselben Technologien, greift mit Sicherheit zu kurz. Die Mehrzahl der Anbieter von Verkabelungslösungen hält sich bei einem neuen Einsatzumfeld, nämlich der Vernetzung von Raumdeckenbereichen, sehr zurück, statt offensives Marketing zu betreiben. Aber bedeutet das, dass die Raumdeckenverkabelung für IT-Anwender und Fachplaner uninteressant oder gar unbedeutend ist? Dies ist aus Sicht des Autors zu verneinen.

Der nachfolgende Artikel widmet sich diesem, vermutlich in Zukunft deutlich an Bedeutung gewinnenden Thema.

weiter auf Seite 5

Zentraler oder dezentraler Internetzugang?

von Dr. Behrooz Moayeri

Viele Organisationen betreiben einen zentralen Internetzugang für eine Mehrzahl ihrer Standorte. Das bedeutet, dass der Weg zum Internet für die nichtzentralen Standorte zunächst über ein privates Wide Area Network (WAN) zum zentralen Standort führt und es erst dort ins Internet geht. Dies ist auch als „Backhauling" bekannt. Einige Cloud-Provider wie Microsoft empfehlen, ein Backhauling bei der Kommunikation mit der Cloud zu vermeiden. Stattdessen wird zum Beispiel für den Zugriff auf Office 365 von Microsoft empfohlen, den Internetzugriff möglichst am User-Standort vorzusehen. Dies würde mehrere dezentrale Internetzugänge statt eines zentralen Internetzugangs bedeuten.

weiter auf Seite 20

Windows 7 ist tot, es lebe Windows 10. Stimmt leider nicht!

von Cornelius Höchel-Winter

Nach wie vor ist Windows 7 auf circa 25 % aller Desktops weltweit in Betrieb. Und der Großteil dieser Installationen dürfte auf den kostenpflichtigen Extended-Security-Updates-Support von Microsoft „verzichten". Die Risiken für die Unternehmen, die Windows 7 weiterhin betreiben, sind jedoch hoch, es drohen vermehrt Angriffe auf die ungeschützten Systeme und im Schadensfall sogar zusätzliche finanzielle Risiken wegen Verstoßes gegen die DSGVO, Compliance-Regeln, Versicherungsbedingungen oder Schadensersatzansprüche, wenn eigene Systeme genutzt werden, um Dritten Schaden zuzufügen. Woher kommt dieses Festhalten an veralteter, hochgradig gefährlicher Software? Wie bekommt man den „Never touch a running system"-Unsinn aus den Köpfen von Administratoren und IT-Verantwortlichen?

Microsoft geht mit Windows 10 ja mittlerweile wie Apple den Weg, regelmäßige Betriebssystem-Updates auszurollen. Wie kann dieses Konzept „Windows as a Service" in der Praxis umgesetzt werden und was bedeutet es für Unternehmen?

weiter auf Seite 22

Geleit

Distributed Cloud: Erobern Hyperscaler unsere RZs?

auf Seite 2

Standpunkt

Die Kunst des Schwachstellenmanagements

auf Seite 14

Aktueller Kongress

ComConsult Netzwerk Kongress

ab Seite 16

Neue Sonderveranstaltung

IT-Gebäudeverkabelung – Wohin geht der Weg?

ab Seite 13

Geleit

Distributed Cloud: Erobern Hyperscaler unsere RZs?

Ein Gespenst geht um: Distributed Cloud. Gemeint sind Ansätze wie AWS Outposts und Azure Stack. Wie sehen diese Ansätze aus? Was bedeutet Distributed Cloud?

Bei Distributed Cloud wird eine Public Cloud um Lokationen in den Rechenzentren (RZs) der Kunden erweitert. Die Steuerung und das Management des Gesamtkonstrukts bleiben beim Cloud-Betreiber. Der Ansatz stößt auf große Aufmerksamkeit. Gartner geht im Dokument „Top 10 Strategic Technology Trends for 2020“ so weit, Distributed Cloud zu den 10 wichtigsten technologischen Trends des Jahres zu zählen (Quelle: Gartner, Inc.: Top 10 Strategic Technology Trends for 2020, 21.10.2019).

Wenn der Ansatz auf Akzeptanz stößt, bedeutet er nicht weniger als ein Vordringen der Hyperscaler in die RZs ihrer Kunden. Das kann nur auf Kosten der traditionellen Ausrüster im RZ gehen. Es stellt sich die Frage, ob die Hyperscaler dabei sind, unsere RZs zu erobern. Wenn das so kommt, steht uns eine grundlegende Änderung des Marktes für RZ-Produkte und zugehörige Dienstleistungen bevor. Allein die Möglichkeit eines solchen Wandels ist Motivation genug, sich mit dem Ansatz zu beschäftigen.

Beispiel AWS Outposts

Um den Ansatz Distributed Cloud zu verstehen, schauen wir uns ein Beispiel an, nämlich AWS Outposts. Seit wenigen Monaten hat AWS Outposts den Status General Availability (GA) erreicht.

Laut Amazon handelt es sich bei AWS Outposts um einen „vollständig verwalteten Service“ [1]. Es gibt keine Einschränkung für Orte, in denen Outposts eingesetzt werden können. Diese Orte können Co-Locations, aber auch private RZs sein. Warum sollte ein Kunde AWS Outposts kaufen? Die Motivation kann technisch oder politisch-strategisch sein. Technisch kann mit der Ausdehnung der Cloud eine Reduzierung der Latenz zwischen dem Kunden und der Cloud-Ressourcen erreicht werden. Zum Beispiel kann damit das produzierende Gewerbe industrielle Steuerung mit hohen Anforderungen an die Echtzeitfähigkeit der Anwendungen in der Distributed Cloud betreiben. Politisch-strategische Motivation für die Nutzung der Distributed Cloud liegt zum Beispiel dann vor, wenn man aus regulatorischen

Gründen die Datenverarbeitung und -speicherung auf eigene Liegenschaften beschränken will. Man muss jedoch bedenken, dass die Gesetzgebung der USA für US-amerikanische Unternehmen weiterhin gilt. Das trifft auch auf das Gesetz namens Clarifying Lawful Overseas Use of Data Act (kurz CLOUD Act) zu. Laut diesem Gesetz müssen Unternehmen mit Sitz in den USA den Zugriff US-amerikanischer Behörden auf die von diesen Unternehmen verwalteten Systeme ermöglichen. Für die US-Gesetzgebung ist unerheblich, wo sich diese Systeme befinden.

Zurück zu AWS Outposts: Laut Amazon bietet Outposts die gleiche Hardware, Services, APIs und Tools wie unter AWS bekannt. Originalton Amazon: „Ihre Outposts-Infrastruktur und AWS-Services werden genau wie in der Cloud von AWS verwaltet, überwacht und aktualisiert.“ [2]

Outposts sind nach Amazon-Angaben mit der nächstgelegenen AWS-Region verbunden. Diese Verbindung ist Voraussetzung für die Funktionalität von Outposts. Daher empfiehlt Amazon, die Verbindung zwischen Outposts und der nächstgelegenen AWS-Region hochverfügbar auszulegen.

Bei der Outposts-Lösung, die jetzt den GA-Status erreicht hat, handelt es sich um die „native“ Variante mit demselben Stack wie unter AWS bekannt. Eine zweite Variante von Outposts soll in 2020 folgen. Diese zweite Option basiert auf dem Software-Defined Data Center (SDDC) von VMware.

Outposts ist ausschließlich auf Hardware verfügbar, die von Amazon spezifiziert ist und in Racks einschließlich Top-of-the-Rack-Switches geliefert wird.

Auf AWS Outposts verfügbare Dienste

Bereits jetzt sind einige von der AWS-Cloud bekannte Dienste wie Server (EC2), Block-Speicher (EBS), Kubernetes (EKS) und Datenbanken (Amazon RDS) auch auf AWS Outposts verfügbar. Lokale Objektspeicher (S3) werden im Laufe des Jahres 2020 folgen.

Kunden können ihre Virtual Private Clouds (VPCs) bis zu ihren eigenen Rechenzentren erweitern. In der jeweiligen AWS-Region verfügbare Dienste stehen auch den Ressourcen in der Cloud-Erweiterung zur Verfügung.

Microsoft Azure Stack

Das Microsoft-Angebot für Distributed Cloud heißt Azure Stack. Wie bei AWS Outposts ermöglich Microsoft mit Azure Stack die Nutzung von Diensten, die unter Azure verfügbar sind, in der Cloud-Erweiterung bis zum Kundenstandort.

Distributed Cloud: Erobern Hyperscaler unsere RZs?

Eine Besonderheit von Azure Stack besteht darin, dass eine Lösung auf der Basis von Azure Stack mit der Public Cloud verbunden sein kann, aber nicht muss.

Das Portfolio von Azure Stack umfasst die folgenden Lösungen [3]:

- Azure Stack Edge (früher: Azure Data Box Edge): Hierbei handelt es sich um eine Appliance, die Verarbeitung und Speicherung von Daten im Sinne von Edge Computing unterstützt. Vorgesehen für die Ausführung auf Azure Stack Edge sind die Services virtuelle Computer, Kubernetes-Cluster, NVIDIA-GPU-Unterstützung und Unterstützung von Hochverfügbarkeit. Auch eine akkubetriebene Ausführung der Appliance war zum Zeitpunkt der Verfassung dieser Zeilen angekündigt.

- Azure Stack HCI: Diese Lösung ist eine Hyper-Converged Infrastructure auf der Basis von zwei Knoten. Sie kann in verschiedenen Ausführungen zum Beispiel für virtuelle Desktops und Microsoft-SQL-Dienste eingesetzt werden. Technisch ist Azure Stack HCI ein Windows Server 2019 Cluster.

- Azure Stack Hub: Das ist die Bezeichnung für eine Rack-integrierte Lösung, die die Möglichkeit bietet, Apps in einer lokalen Umgebung auszuführen und Azure-Dienste im eigenen Rechenzentrum bereitzustellen.

Ist Distributed Cloud die Zukunft von Hybrid Cloud?

Zumindest im ComConsult-Kundenkreis ist zu beobachten, dass sich die meisten Unternehmen am Modell Hybrid Cloud orientieren. Einerseits wird Cloud-Computing von fast jedem Unternehmen genutzt. Andererseits kann kaum ein mittleres bis großes Unternehmen kurzfristig auf ein eigenes RZ verzichten. Einige Gründe hierfür sind wie folgt:

- Viele IT-Anwendungen haben einen langen Lebenszyklus. Es gibt zahlreiche Applikationen, die noch einige Jahre genutzt werden sollen. Zumindest für einen Teil dieser Applikationen ist die Verlagerung in die Cloud technisch nicht möglich, nicht sinnvoll oder nicht wirtschaftlich. Solange solche Applikationen genutzt werden, verbleiben sie im eigenen RZ.

- Die Cloud ist bisher weit entfernt von den physischen Kundenlokationen, in denen zum Beispiel Güter industriell produziert werden. Die Digitalisierung der Produktion war schon vor der Cloud Wirklichkeit. Industrielle Steuerung und Regelung ist auf kurze Latenzen angewiesen. Wenn die Ressourcen dafür in der Cloud sind, werden die Anforderungen an die Echtzeitfähigkeit der industriellen Anwendungen unter Umständen nicht erfüllt.

- Es gibt weiterhin Bedenken gegen die Public Clouds, insbesondere was Datensicherheit und Datenschutz betrifft.

Distributed Cloud ist die Reaktion der Cloud-Provider auf die oben genannten Umstände. Mit der Distributed Cloud wandern die Cloud-Ressourcen näher zu den Umgebungen und Dingen, die mit der Cloud interagieren sollen. Damit wird die Cloud echtzeitfähig bzw. die Echtzeitanwendungen Cloud-fähig.

Aber Distributed Cloud löst nicht alle Probleme, die bisher Cloud-Computing Grenzen gesetzt haben. Eine Anwendung, die aufgrund ihrer Architektur bisher nicht Cloud-fähig war, wird es auch mit der Distributed Cloud nicht werden. Die Cloud-Provider orientieren sich nun mal stark an Internetstandards. Internetstandards für Anwendungen sind vor allem das Internet Protocol (IP) und das Web Interface. Weicht eine Anwendung von diesen Standards ab, gelten für diese Anwendung viele der Vorteile der Cloud nicht.

Ein weiteres Problem ist das Betreibermodell. Regularien und Vorgaben gibt es nicht nur bezüglich des Standorts, an dem Daten verarbeitet und gespeichert werden. Selbst wenn Distributed Cloud die Verarbeitung und Speicherung von Daten von den Provider-RZs in die Kunden-RZs verlagert, stellt sich die Frage, wer die Ressourcen in der Distributed Cloud verwaltet, auf sie Zugriff hat und eventuell verpflichtet ist, Dritten (d.h. vor allem ausländischen Staaten) Zugang zu den Daten und Ressourcen in der Distributed Cloud zu gewähren.

Nun könnten die Cloud-Provider auf die Idee kommen, die Cloud-Technologie auch entkoppelt vom zentralen Betreibermodell intensiv zu vermarkten. Spätestens dann wird der Markt für Server, Speicher, Netz- und Sicherheitskomponenten, Virtualisierung und Management von Rechenzentren neu aufgemischt.

Verweise

[1] https://aws.amazon.com/de/outposts/
[2] Ebd.
[3] https://azure.microsoft.com/de-de/blog/expanding-the-azure-stack-portfolio-to-run-hybrid-applications-across-the-cloud-datacenter-and-the-edge/

LESERBRIEF

Gerne können Sie mir Ihre Meinung und Kommentare zu diesem Artikel mitteilen. Per E-Mail oder direkt online.

Sie erreichen mich unter
moayeri@comconsult.com

SEMINAR

Hybrid Cloud: RZ der neuen Generation 11.03.-13.03.20 in Bonn

Dieses Seminar befasst sich mit Hybrid Cloud als DIE Variante des IT-Betriebs für die meisten mittleren und großen Organisationen. Die Hybrid Cloud ist das RZ der neuen Generation, weil weder das eigene RZ noch externe Clouds in der absehbaren Zeit aus der IT-Umgebung der meisten Unternehmen wegzudenken sind. Das Seminar geht auf verschiedene Aspekte der Planung und des Betriebs der Hybrid-Cloud einschließlich Netz, Server, Storage, Security, Backup und Bereitstellung von Anwendungen ein.
Das Seminar richtet sich an alle Planer und Betreiber, Führungskräfte und Entscheider, die sich mit Planung und Betrieb von Rechenzentren und Cloud-Nutzung / Cloud-Anbindung befassen. Konkret richtet sich dieses Seminar auch an alle, die bewerten wollen ob es sinnvoll ist, Teile ihrer Infrastruktur in die Public Cloud zu verlagern. Außerdem werden Optimierungsmöglichkeiten für bereits bestehende Cloud-Projekte besprochen.

Referenten: Dr. Markus Ermes, Simon Oberem, Markus Schaub, Timo Schmitz
Preis: 1.890,-- € netto

Gebäude der Zukunft: IT-Infrastruktur für die digitalisierte Raumdecke

Fortsetzung von Seite 1

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

Klassische IT-Verkabelung: Historische Entwicklung und Grundanforderungen

Bevor man sich mit der Grundidee einer Kommunikationsverkabelung im Deckenbereich auseinandersetzt, ist es aus Sicht des Autors zwingend notwendig, die historische Entwicklung der bisherigen, traditionellen Verkabelungstechniken ausgehend von den sich ändernden Anforderungen an diese zu kennen.

Kommunikationsanschlüsse gibt es seit Einführung der Netzwerktechnik, diese Welt war zu Anfang (Beginn der 90er-Jahre) noch relativ klar getrennt in Anschlüsse für Sprachkommunikation (= Telefonie) und Anschlüsse für Informationstechnik. Die Trennung wurde Mitte dieses Jahrzehnts nominell mit der ersten Verabschiedung von Normen wie z.B. der ISO/IEC 11801 und der EN 50173 aufgehoben, es sollte in neuen Gebäuden nur noch eine einzige „anwendungsneutrale Kommunikationsverkabelung“ geben. Danach sollte jeder Kommunikationsanschluss unabhängig von der Nutzung gleich aussehen. Die dafür vorgesehenen Planungsregelwerke und Produkte sahen ein sehr beschränktes Einsatzumfeld vor: Kommunikationsanschlüsse für Geräte am Büroarbeitsplatz, die im Wesentlichen aus Datenein- und -ausgaberäten bestanden wie z.B. PCs, Telefone, Drucker. Zu diesem Zeitpunkt war noch keine Rede von Kommunikationsanschlüssen

- im Produktionsumfeld,
  zur Energieversorgung von elektronischen Geräten,
- zur Vernetzung von Überwachungskameras,
- für IT-Geräte der Gebäudeleittechnik.

Der Hauptanteil der passiven Kommunikationsanschlüsse wurde unmittelbar in der Nähe von (Büro-)Arbeitsplätzen platziert. Erste, wenige Anschlüsse platzierte man ab Mitte der 90er-Jahre unterhalb von Decken, um WLAN-Access-Points zu versorgen. Diese Einsatzumgebung prägte massiv die technischen Anforderungen an die Gestaltung der Anschlüsse, wichtige zu nennende Anforderungen sind:

Universalität: An jedem Kommunikationsanschluss soll jede Form von Kommunikationstechnik durch einfaches Umrangieren möglich sein. Die Art und Weise, wie verschiedene Kommunikationsanwendungen gewechselt werden, hat sich durch die massive Durchdringung von framebasierenden Kommunikationstechniken in den letzten 20 Jahren verändert. Bei leitungsgebundener Kommunikation überwiegt deutlich das Ethernet-Zugangsverfahren. Der unumschränkte Einsatz von Ethernet-Techniken bis zum Arbeitsplatz stellt derzeit „das“ Maß der Universalität dar. Es bestimmt die übertragungstechnischen Qualitäten des Kommunikationsanschlusses.

Nutzungszeitraum: Bei der Bewertung des mittel- und insbesondere langfristigen Nutzbarkeitszeitraumes einer Verkabelung ist eine spekulative Betrachtung nicht vermeidbar. Natürlich garantiert eine „universelle Verkabelung“ eine hohe Vielseitigkeit und damit einen großen Nutzbarkeitszeitraum. Die Nutzungseigenschaften und damit der Nutzungszeitraum eines Übertragungsmediums orientieren sich nicht nur an den elektrotechnischen Eigenschaften des Mediums (Datenübertragung und Stromübertragung). Vielmehr spielt – und dies wird ein wichtiger Punkt bei der Betrachtung der digitalisierten Decke werden – auch die ausreichende Anzahl an Anschlüssen bei der Nachhaltigkeitsbewertung einer Kommunikationsverkabelung eine Rolle (siehe Erläuterung dazu später).

Installationsfreundlichkeit: Die Installationsfreundlichkeit hat aus der Sichtweise des Nutzers der Verkabelung zunächst eine untergeordnete Rolle, sie ist relevant für den Planer bei der Erstinstallation, dort verursacht sie höhere Investitionskosten. Ein System darf in einem vereinfachten Ansatz als „installationsfreundlich“ bezeichnet werden, wenn es „günstig“ ist.

Betriebsfreundlichkeit: Bei der Betrachtung einer „betriebsfreundlichen“ Kommunikationsverkabelung sind Anforderungen zu nennen, die primär in Zusammenhang mit der Fehleranfälligkeit und der Fehlerbehebbarkeit sowie den Erweiterungsmöglichkeiten zu sehen sind. Beispielsweise ist eine Anschlussschnur (bestehend aus Anschlusskabel und Stecker) zwar nicht Gegenstand der festen Verkabelung, hat aber erfahrungsgemäß einen großen Einfluss auf die Übertragungsqualität der zu nutzenden Strecke. Weitere Vorteile im Betrieb entstehen durch Nutzbarkeit von elektronischen Komponenten, die eine lange Lebensdauer haben. Werden beispielsweise Switches o.ä. unter ungünstigen thermischen Rahmenbedingungen montiert, so ist mit einer höheren Ausfallrate zu rechnen; dies war viele Jahre der Nachteil von Kanaleinbau-Switches zum Aufbau einer Fiber-to-the-Office-Verkabelung.

Ausreichende Anzahl: Mit den ersten Normierungen wurde neben den technischen Spezifikationen die Idee einer „flächendeckenden, strukturierten Verkabelung“ als Planungsansatz für alle modernen (Büro-)Gebäude eingeführt. Dies bedeutet, dass bei der Planung unter Berücksichtigung der oben genannten Anforderungen eine Verkabelung in einem Gebäude vorgesehen wird, die in einem Nutzungszeitraum von mindestens 10 Jahren weder in größerem Maße verän-

dert noch erweitert werden muss. Konkret wären also alle Räume mit potenziell möglichen Office-Arbeitsplätzen oder Geräten ausreichend „vorzuverkabeln“.

Lösungen der klassischen Verkabelung im Detail

Nachdem nun die Grundanforderungen genannt sind, ist es im nächsten Schritt notwendig, anhand von Beispielen konkrete technische Lösungen für klassische Verkabelungen zu beschreiben, die aus diesen Grundanforderungen resultieren bzw. sich in den letzten Jahren so entwickelt haben.

Die Grundanforderung der „Universalität“ und „Nachhaltigkeit“ führt durch die mögliche Steigerung der Datenraten und des Bedarfs nach Stromübertragung im Office-Umfeld dazu, dass sich technische Lösungen für die Tertiärverkabelung (Verkabelung zwischen Etagenverteiler und Endgerät) mit Übertragungsqualitäten der Klasse EA etabliert haben. Ferner werden bei der Planung weitestgehend Maximallängen von 90 m bis 110 m für den Permanent-Link eingehalten. Damit bleibt aktuell die maximal mögliche Datenrate für derartige Distanzen auf 10 Gbit/s beschränkt. Da aus Sicht des Autors kein Bedarf nach einer höheren, flächendeckend benötigten Datenrate auch nur ansatzweise absehbar ist, können die Anforderungen, die sich bei einer Nutzbarkeit der normierten Datenrate von 25 oder 40 Gbit/s ergeben würden, ignoriert werden. Es wäre ohnehin kaum vorstellbar, wie mit den deutlich verkürzten Maximallängen von weniger als 50 m eine wirtschaftliche Kommunikationsverkabelung in einem Gebäude realisiert werden könnte. (siehe Tabelle 1)

Datenrate	IEEE-Standard	Jahr	Bezeichnung	EN 50173 / Strecke	IEC11801 Komponente
100 Mbit/s		1995	100BaseT	Klasse D	Kat. 5
1 Gbit/s		1999	1000BaseT		
2,5/5 Gbit/s		2016	2,5/5GBaseT		
10 Gbit/s		2006	10GBaseT	Klasse E_A	Kat. 6_a
25/40 Gbit/s		2016	25/40GBaseT	Class I + II	Kat. 8_a

Tabelle 1: Übersicht der im Tertiärbereich relevanten, kupferbasierenden Ethernet-Techniken

Eine Selbstverständlichkeit ist der Abschluss der Tertiärstrecke mit einem RJ45-Anschluss (auf Glasfaser basierende Lösungen werden in diesem Artikel nicht betrachtet), montiert in einer Datendose. Diese Selbstverständlichkeit hat folgende Gründe:

1. Es wird davon ausgegangen, dass an diesen Port Geräte angeschlossen werden, die ebenfalls einen RJ45-Port haben und damit durch Verwendung von Anschlussschnüren mit RJ45 an beiden Enden den Betrieb vereinfachen.

2. Unter der Annahme, dass dieser Anschluss mehr oder weniger häufig gewechselt wird, bedingt durch Umzüge, Austausch von IT-Geräten o.ä. wird der Betrieb einfacher, wenn die RJ45-Buchse in einem festen Gehäuse fixiert wird. Das lose Ende eines Twisted-Pair-Kabels mit angeschlossener RJ45-Buchse wäre unpraktisch; würde aber übertragungstechnisch denselben Zweck erfüllen.

Selbst bei einem Anschluss für einen Access-Point, bei dem vermutlich kaum der zweite genannte Grund von Bedeutung ist, erfolgt die technische Lösung exakt wie am Arbeitsplatz; eine Dose wird verwendet.

Grundsätzlich kann festgehalten werden, dass

- die bisherigen technischen Lösungen weitestgehend etabliert und ähnlich sind,
- die technischen Lösungen wenig innovativ sind (trotz der intensiven Diskussionen zum Thema Power over Ethernet gab es auch hier keinen nennenswerten Einfluss auf die Lösungen),
- die Anforderungen beim Neubau von Bürogebäuden berücksichtigt und ähnlich umgesetzt werden.

Deutlich komplexer sind die Lösungen, mit denen man für eine ausreichende Anzahl an Anschlüssen sorgen muss. Folgende „Probleme“ müssen gelöst werden:

- Es muss eine Prognose getroffen werden, wie viele LAN-Anschlüsse im Nutzungszeitraum leitungs-(draht-) gebunden sein werden und wie viele WLAN-basierend. Aktuell ist eine klare Tendenz zur „bequemeren“, funkbasierenden Technik zu erkennen, damit nimmt theoretisch die Anzahl der Leitungen ab. Sehr viele Planungen sehen „nur noch“ maximal 2 Anschlüsse pro Arbeitsplatz vor, erste „mutige“ Planungen gar nur einen Anschluss, um wenigstens PoE sicherstellen zu können.

- Starre Arbeitsplatzlösungen sind nicht immer der Standard, viel mehr häufen sich Konzepte, bei denen die Mitarbeiter nur temporär in einem Flächenbereich oder gar an einem Platz sitzen werden. Häufige Umzüge im Gebäude oder zumindest im Raum dürfen zu keinen aufwendigen Nachverkabelungen führen, man muss frühzeitig in der Planung voraussehen, wo welche Dichte an Leitungen benötigt wird. Das ist im Prinzip nur mit einer „Überversorgung“ von Anschlüssen sicher abzudecken.

Ein immer häufiger eingesetztes Element ist der Sammelpunkt, auch unter dem Begriff „Consolidation Point“ bekannt: Der Einsatz von Sammelpunkten (nachfolgend mit SP abgekürzt) bzw. Consolidation Points soll gemäß EN 50173-1 dem Nutzer die Möglichkeit geben, längere Anschlussschnüre vorzusehen, diese sind ohne SP auf üblicherweise maximal 5 Meter begrenzt. Der SP stellt einen Verteilerpunkt dar, der keine aktiven Komponenten beinhaltet, sondern lediglich Buchsen, welche die dauerhaft festinstallierten Tertiärkabel (nach EN „Stammkabel“ genannt) abschließen. In die Buchsen werden Stecker gesteckt, die an nicht dauerhaft verlegte Kabel angeschlossen werden (Sammelpunkt-Kabel). Diese Kabel werden zu einer Anschlussdose bzw. der darin befindlichen Anschlussbuchse (Teilnehmeranschlusseinheit TA) geführt. (siehe Abbildung 1)

Achtung, es gibt bei sehr vielen Planungen ein Missverständnis bzw. eine Fehldeutung: Das Teilelement oder der Begriff Sammelpunkt wird dort auch dann verwendet, wenn zwischen Sammelpunkt und Endgerät keine Buchse/Dose mehr geplant wird. Dies ist im Sinne der Norm falsch!

Für den Nutzer sind die SPe „unsichtbare“ Teile der IT-Verkabelung, die für den Betrieb im Regelfall nicht zugänglich sein müssen; erst bei größeren Umzügen mit Veränderungen der TA ist eine Zugänglichkeit erforderlich. (siehe Abbildung 2)

Grundidee einer digitalen Decke

Mit dem Aufbau einer „traditionellen“ Kommunikationsverkabelung wird die deutliche Mehrzahl der Dosen auf einer Höhe von 0 bis ca. 120 cm montiert werden, also im Prinzip unterhalb der Kopfhöhe. Warum benötigt man zusätzlich zu den Anschlüssen für Access Points weitere Kommunikationsanschlüsse in Deckenhöhe, warum benötigt man ein Netzwerk dort?

Zentraler oder dezentraler Internetzugang?

Fortsetzung von Seite 1

Dr. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Argumente gegen Backhauling

Es gibt vier Hauptargumente gegen Backhauling:

- Reduzierung der Latenz beim Zugriff auf das Internet und damit dem Cloud-Zugriff,
- Aushebeln von Konfigurationen, die anhand der User-IP-Adresse die Kommunikation regeln,
- Umgehung zentraler Sicherheitskomponenten wie Proxies, die bei manchen Cloud-Anwendungen wie Microsoft Teams Probleme bereiten könnten, und
- Reduzierung der WAN-Kosten durch Auslagerung der Internet- und Cloud-Kommunikation auf dezentrale Internetzugänge.

Das letztgenannte Argument wird eher von den Unternehmen selbst vorgebracht als von den Cloud-Providern.

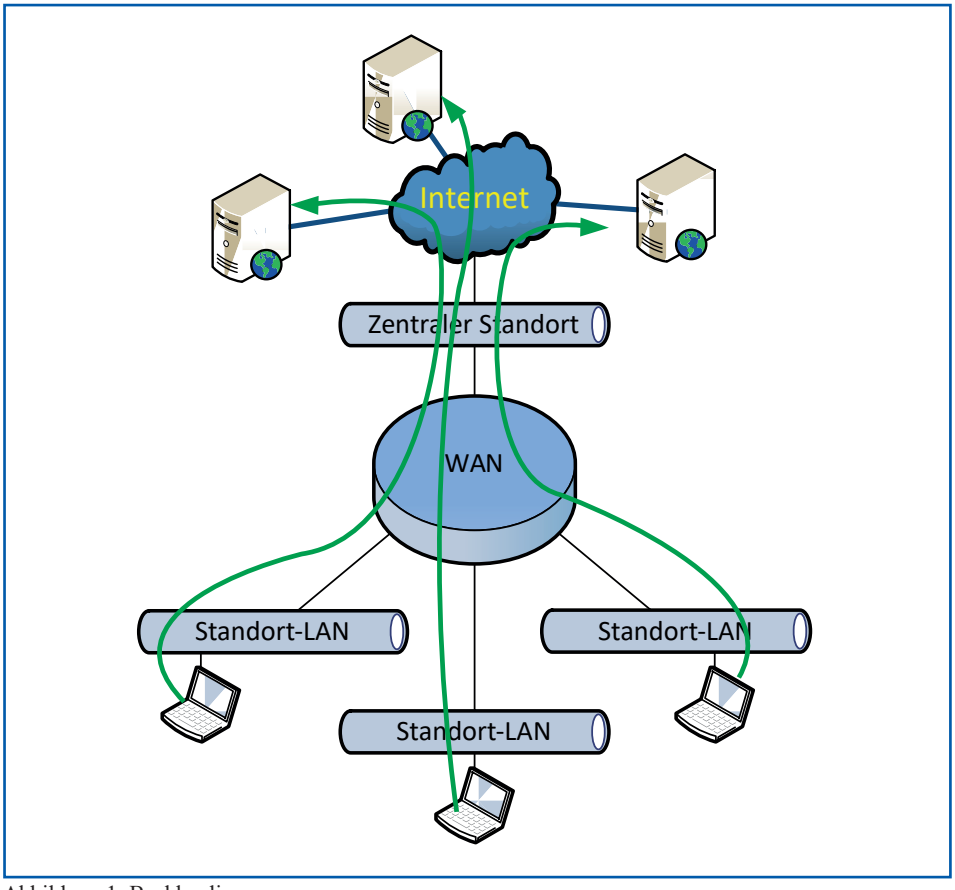

Abbildung 1: Backhauling

Den drei Argumenten wollen wir hier auf den Grund gehen.

Latenzarmes Netzdesign

In der Tat kann ein Backhauling mehr Latenz bedeuten. Wenn zum Beispiel der zentrale Standort mit dem Internetübergang in Deutschland ist und von anderen Kontinenten aus der Weg ins Internet zunächst über ein WAN nach Deutschland führt, fügt das WAN zusätzliche Millisekunden in zwei- bis dreistelliger Höhe zur Latenz hinzu. Das verlängert die Antwortzeit vieler Anwendungen, bei manchen in nicht akzeptablem Maße.

Gilt das aber für jede Art Backhauling? Die Antwort ist nein. Wenn innerhalb Deutschlands mehrere Standorte einen zentralen Internetzugang teilen, kann der direkte Weg jedes Standorts ins Internet sogar mehr Latenz als der Weg über das WAN bedeuten. Das ist zum Beispiel dann der Fall, wenn der Internetweg ungünstiger als der WAN-Weg ist (s. Abbildung 2). Ich kenne solche Fälle. An einer Betrachtung von Fall zu Fall führt kein Weg vorbei.

Eine andere Frage ist, ob sich die Antwortzeit einer Anwendung durch geringfügig mehr Latenz spürbar verändert. Im Falle von Office 365 ist zu berücksichtigen, dass Microsoft nicht in jedem Land Rechenzentren unterhält. Oft müssen User in einem Land auf Office-365-Ressourcen in einem anderen Land zugreifen. Dabei fallen Round-Trip-Zeiten bis 100 Millisekunden oder sogar mehr an. Wenn die Anwendungen dies tolerieren, dann spielen wenige Millisekunden mehr oder weniger keine entscheidende Rolle. Aber auch das ist von Fall zu Fall zu klären.

Windows 7 ist tot, es lebe Windows 10. Stimmt leider nicht!

Fortsetzung von Seite 1

Cornelius Höchel-Winter arbeitet als Senior-Consultant, Autor, Trainer und Referent auf Seminaren und Kongressen seit 2001 für die ComConsult Firmengruppe. Schwerpunkte seiner Tätigkeit sind die Bereiche Data Center, Virtualisierung, Storage, Netzwerke, Cloud Computing und Systemintegration, sowie Evaluierungen neuester Hard- und Softwareprodukte und die Beobachtung aktueller Entwicklungen im IT-Markt. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen.

Je nach Quelle ist Windows 7 auf gut 25 % aller Desktops weltweit in Betrieb. Deutschland steht mit einem Anteil von rund 16 % nur unwesentlich besser da1. Und außer für Unternehmenskunden, die einen kostenpflichtigen Supportvertrag für weitere Sicherheitsupdates (ESU – Extended Security Updates) abgeschlossen haben, gibt es für Windows 7 überhaupt keine Updates mehr! Für ein 10 Jahre altes Betriebssystem, bei dem wie bei einer alten rostigen Fregatte in letzter Zeit immer mehr Sicherheitslücken geschlossen werden mussten, allein im letzten Jahr über 250! Niemand kann behaupten, er habe das nicht gewusst. Das Presseecho der letzten Tage war groß genug.

Tickende Zeitbomben

Aber das ist ja noch nicht alles! Nach wie vor gibt es signifikante Anteile von Rechnern mit Windows XP, Windows Vista und Windows 8, alles Betriebssysteme, für die es seit Jahren keine Updates mehr gibt. Und Microsoft hat nicht nur den Support für Windows 7 eingestellt, sondern auch für alle Versionen des Windows Server 2008. Ende Januar wird auch der Internet Explorer 10 zu Grabe getragen. Das Sicherheitsunternehmen Kaspersky hatte bereits im August 2019 vor einer „tickenden Cyber-Zeitbombe“ in diesem Zusammenhang gewarnt . Das Unternehmen ESET hat diese Bezeichnung Anfang Januar wiederholt . Seitdem wird die Metapher von der Zeitbombe in allen Pressemeldungen zum Supportende von Windows 7 genutzt. Ist das übertrieben? (siehe Abbildung 1)

Nein! Die Risiken gerade für die Unternehmen, die uralte Betriebssysteme betreiben, sind hoch. Wenn Sicherheitslücken nicht mehr geschlossen werden, können Angriffe auf solche Systeme nicht mehr verhindert werden! In der Folge müssen Sie mit Daten-Leaks oder Datenverlust rechnen. Da nutzen auch Firewalls und Virenscanner nicht mehr viel. Kaspersky und Mitbewerber werben diesbezüglich tatsächlich nicht für eigene Produkte, sondern empfehlen dringend ein Upgrade auf ein aktuelles Betriebssystem.

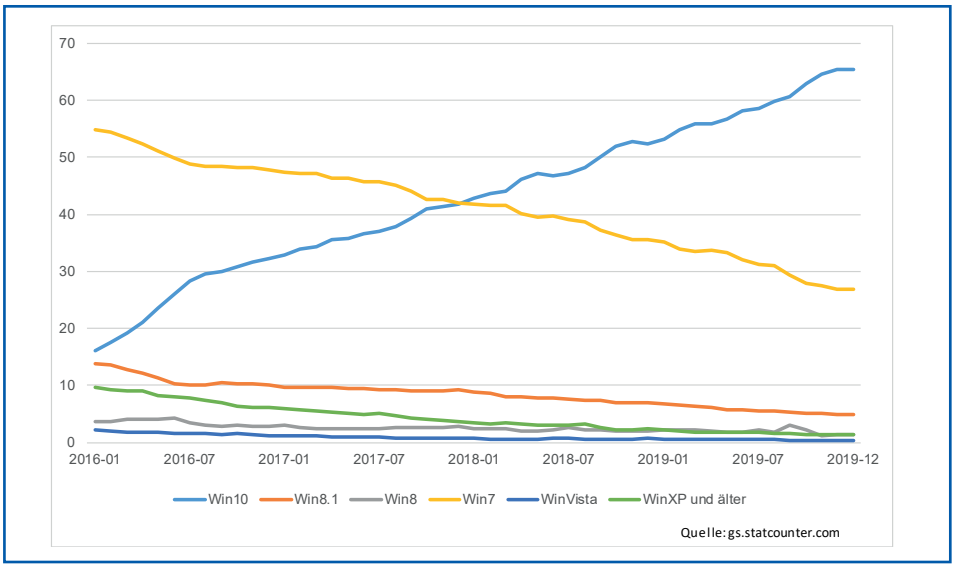

Abbildung 1: Anteile der Windows-Desktop-Betriebssysteme weltweit

Finanzielle Risiken

ESET verweist in seiner Presseerklärung außerdem auf die DSGVO und auf die gerade im privaten Umfeld beliebten Versicherungen gegen Online-Schäden und Cyberkriminalität. Die Versicherungsbedingungen wie auch die DSGVO setzen Umgebungen voraus, die dem Stand der Technik entsprechen! Wenn Sie mit Windows 7 ins Internet gehen, gefährden Sie Ihren Versicherungsschutz, und wenn Sie mit Windows 7 personenbezogene Daten verarbeiten, verstoßen Sie gegen die DSGVO.

Darüber hinaus gefährden solche Altlasten nicht nur die eigene Umgebung, sondern in hohem Maße auch andere. Gerade solche nicht mehr gepflegten Systeme werden bevorzugt von sogenannten Botnetzen übernommen und dienen als Angriffsknoten in DDoS-Attacken (Distributed Denial of Service). Und nebenbei bemerkt, auch in diesem Fall drohen unter Umständen hohe Schadenersatzforderungen.

Argumente der “Impfgegner”

Vor diesem Hintergrund ist es schwer nachzuvollziehen, dass sich Unternehmen auf das Abenteuer „Weiterbetrieb von Windows 7“ einlassen. Die finanziellen Risiken sind allemal höher als die Kosten für ein Upgrade. Nichtsdestotrotz werden als