Oktober 2026

ComConsult
BERATUNG • PLANUNG • SCHULUNG

Der Netzwerk Insider



Netzwerk-Migration im laufenden Betrieb

von Oliver Kloß

Veraltete Netzwerk-Hardware ist für viele Unternehmen ein schleichendes Risiko. Solange sie läuft, fällt sie kaum auf. Bis plötzlich ein zentraler Switch ausfällt und ganze Serverreihen offline gehen. Genau in dieser Situation befand sich der IT-Betrieb eines Großunternehmens im KRITIS-Umfeld mit zwei georedundanten Rechenzentren, dessen bisherige Infrastruktur sich in einem zentralen Bereich dem End-of-Life näherte.

Seite 10

Welcher RZ-Auslagerungstyp bin ich?

von Dr. Behrooz Moayeri

IT-Fachkräfte werden unaufhaltsam älter. In der Anzahl der in den Ruhestand wechselnden Experten können die meisten Institutionen im Moment keinen Nachwuchs organisieren. Gleichzeitig nimmt der Umfang der IT-bezogenen Aufgaben in den meisten Organisationen zu. Vielen Unternehmen und Behörden bleibt nur die Auslagerung von Aufgaben.

Seite 2

Ganzheitliche Energieeffizienz im Rechenzentrum – Aussagekraft und Grenzen der Kennzahl PUE

von Stefan Kuitunen, Daniel Scholz, Anne Weisemann

Die Power Usage Effectiveness (PUE) ist eine wichtige Kennzahl zur Bewertung der Energieeffizienz von Rechenzentrumsinfrastruktur. Der Beitrag diskutiert die Kennzahl im Hinblick auf ihre Anwendungsmöglichkeiten und deren Grenzen im Rahmen der Effizienzbewertung sowie wichtige Einflussfaktoren.

Seite 20



Webinar der Woche

Notfallvorbereitung im Klartext

Seite 19

WLAN oder Mobilfunk: Wer kriegt das 6-GHz-Band?

von Dr. Joachim Wetzlar

Manche von Ihnen erinnern sich an meine Beispiele für praktische Anwendungen von 5G-Mobilfunk in privaten Netzen. Erste Anwendungen fand ich bereits 2018 in den Stellungnahmen [1] zum Entwurf des Antragsverfahrens für private 5G-Mobilfunketze der BNetzA.

Seite 28



Welcher RZ-Auslagerungstyp bin ich?

von Dr. Behrooz Moayeri

IT-Fachkräfte werden unaufhaltsam älter. In der Anzahl der in den Ruhestand wechselnden Experten können die meisten Institutionen im Moment keinen Nachwuchs organisieren. Gleichzeitig nimmt der Umfang der IT-bezogenen Aufgaben in den meisten Organisationen zu. Vielen Unternehmen und Behörden bleibt nur die Auslagerung von Aufgaben. Stichwort: „Reduzierung der Fertigungstiefe“. Im Bereich Rechenzentren gibt es dazu verschiedene Varianten.

Hier möchte ich darauf eingehen, welche Art RZ-Auslagerung für eine bestimmte Organisation die passende ist. Oder um etwa Modeberater-Gazetten nachzusprechen: Welcher RZ-Auslagerungstyp bin ich?

Gesamtumfang von RZ-Leistungen

Der Gesamtumfang von RZ-Leistungen lässt sich zusammengefasst in folgende Kategorien einteilen:

- Infrastruktur („grobe Technik“): RZ-Fläche, Energieversorgung, Kühlung, physikalische Sicherheit
- Physikalische IT-Komponenten: Server, Storage, Switches, Firewalls, Load Balancer, Datennetzzugänge
- Virtuelle IT-Komponenten: Server, Storage, Switches, Firewalls, Load Balancer, virtuelle Netzzugänge
- Applikationssoftware: Images und Updates für Front End, Applikation, Datenbank
- Applikationsmandant: Benutzer- und Gruppenverwaltung, Identitätsmanagement, Zugriffsregeln

Die oben genannten Kategorien bauen aufeinander auf: Ein Applikationsmandant ist auf die Bereitstellung der Software angewiesen; für die Software-Bereitstellung braucht man virtuelle IT-Komponenten wie Server und Storage; diese werden auf Basis physischer Geräte realisiert; die physischen IT-Komponenten („feine Technik“) brauchen eine Infrastruktur („grobe Technik“).

Je mehr man von den fünf genannten Leistungsgruppen auslagert, desto weniger Aufgaben verbleiben für den Auftraggeber.

Housing oder Hosting?

Die Begriffe Housing und Hosting werden immer wieder für RZ-Auslagerung verwendet, zum Beispiel in einem Beitrag meines Kollegen Oliver Flüs. In der Regel versteht man unter Housing Leistungen im Bereich der groben Technik, während Hosting zusätzlich zur groben Technik auch die physischen IT-Komponenten umfasst.

Hosting könnte man auch als Synonym für Infrastructure as a Service (IaaS) verwenden. Deshalb beginnt spätestens mit Hosting auch die Domäne der Cloud-Leistungen, für die bekanntlich drei Hauptkategorien genannt werden:

- Infrastructure as a Service (IaaS): Dabei stellt der Provider die grobe und feine Technik, d.h. die Gebäudeinfrastruktur und die physischen IT-Komponenten. Alles, was die physischen IT-Komponenten nutzt, beginnend mit virtuellen Servern bis zum Software-Betrieb, obliegt dem Auftraggeber.



Netzwerk-Migration im laufenden Betrieb

von Oliver Kloß

Veraltete Netzwerk-Hardware ist für viele Unternehmen ein schleichendes Risiko. Solange sie läuft, fällt sie kaum auf. Bis plötzlich ein zentraler Switch ausfällt und ganze Serverreihen offline gehen. Genau in dieser Situation befand sich der IT-Betrieb eines Großunternehmens im KRITIS-Umfeld mit zwei georedundanten Rechenzentren, dessen bisherige Infrastruktur sich in einem zentralen Bereich dem End-of-Life näherte. Ersatzteile wurden knapper, der Hersteller-Support lief aus, und es kam bereits regelmäßig zu Ausfällen einzelner Geräte, mit allen damit verbundenen Risiken für den laufenden Geschäftsbetrieb.

Die ComConsult wurde beauftragt, diesen Teil des Rechenzentrums zu erneuern. Die Verkabelungsplanung und -umsetzung der neuen Switches war dabei bereits in einem vorangegangenen Projekt der ComConsult erfolgt. Das hier beschriebene Projekt knüpft daran an und gliederte sich grob in zwei große Phasen: zunächst in die Auswahl und Beschaffung einer neuen Netzwerk-Infrastruktur, anschließend in die physische und logische Migration sämtlicher angeschlossener Server vom alten auf das neue Netzwerk. Und zwar im laufenden Betrieb, ohne den Geschäftsbetrieb zu gefährden. Dieser Artikel beschreibt den gesamten Weg: von der strukturierten Anbieterauswahl über die Architekturentscheidung bis hin zur kleinteiligen, oft mühsamen Praxis der eigentlichen Migration, bei der ich als mitverantwortlicher Berater die Planung und Steuerung übernommen habe.

Das Projekt eignet sich gut als Fallbeispiel, weil es zwei Dinge zeigt, die selten zusammen betrachtet werden: die strategische Entscheidungsebene, also welche Technologie und welcher Anbieter zum Einsatz kommen, und die operative Realität danach. Wie bekommt man hunderte Server ohne nennenswerten Ausfall auf eine neue Plattform? Gerade Letzteres wird in Projektplänen oft unterschätzt. Dabei steckt genau dort der größte Teil des tatsächlichen Aufwands.

Ausgangslage und Zielsetzung

Die bestehende Cisco-Infrastruktur war über Jahre gewachsen und entsprechend heterogen. Mit dem nahenden Lebensende der Hardware stand der Kunde vor der Entscheidung, entweder erneut auf bekannte Technologie zu setzen oder den Wechsel zu einem moderneren Architekturansatz zu wagen. Schnell war klar, dass eine reine Eins-zu-eins-Erneuerung der alten Struktur die eigentlichen Probleme nicht lösen würde: mangelnde Skalierbarkeit, komplexe Fehlersuche, unklare Redundanzpfade. Stattdessen wurde der Anspruch formuliert, eine moderne, hochverfügbare Spine-Leaf-Architektur aufzubauen, die beide Rechenzentren des Kunden möglichst gleichwertig bedient und im Falle eines kompletten Ausfalls eines Standorts den Betrieb über das jeweils andere Rechenzentrum aufrechterhalten kann.

Damit war der Rahmen für das Projekt gesteckt. Es ging nicht um einen reinen Hardwaretausch, sondern um eine grundlegende Neuordnung der Netzwerk- und Serverlandschaft, inklusive eines zusätzlichen Wunsches des Kunden: Im Zuge der Migration sollte gleich ein sogenanntes POD-Design eingeführt werden, bei dem Server gleichen Typs künftig physisch zusammenstehen, statt wie bisher über viele Schränke verteilt zu sein. Wenn gleichartige Server in denselben oder benachbarten Schränken stehen, lassen sich Verkabelung, Netzwerkkonfiguration und Wartung deutlich strukturierter und effizienter gestalten. Fehler sind schneller zu lokalisieren, Erweiterungen einfacher zu planen, und die Übersichtlichkeit im Rechenzentrum steigt spürbar.



ISO/IEC-27001-Audit vorbereiten und umsetzen

Mit Maren Meisterburg und Felix Horn sprach Christiane Zweipfennig

Der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) und die Vorbereitung auf ein ISO/IEC-27001-Audit sind auch für kleinere Unternehmen mit einem nicht unerheblichen Aufwand verbunden. Gerade begrenzte Ressourcen und zusätzliche Anforderungen neben dem Tagesgeschäft stellen dabei besondere Herausforderungen dar.

Maren Meisterburg ist seit über fünf Jahren im IT-Sicherheitsteam von ComConsult tätig und arbeitet dort als Senior-IT-Sicherheitsberaterin. Ihr Schwerpunkt liegt auf dem Aufbau von Informationssicherheitssystemen – von der Dokumentation bis zur Umsetzung technischer Maßnahmen. In den letzten vier Jahren war sie zusätzlich als Informationssicherheitsbeauftragte (ISB) für ComConsult aktiv und hat dort das eigene ISMS nach TISAX weitergeführt sowie zertifizieren lassen.

Felix Horn hat Informatik studiert und arbeitete drei Jahre in der Softwareentwicklung, bevor er im Oktober 2025 zu ComConsult kam. Dort verantwortet er im Team IT-Sicherheit neben allgemeinen IT-Sicherheitsaufgaben auch Bereiche der KI-Sicherheit und arbeitet in Projekten eng mit Maren Meisterburg beim Aufbau von Informationssicherheitsmanagementsystemen zusammen. Zusätzlich bringt er seine Informationssicherheitsexpertise in der ComConsult-Arbeitsgruppe „Post-Quanten-Kryptographie“ ein.

Warum kann der Aufbau eines ISMS nach ISO 27001 für ein kleineres Unternehmen eine Herausforderung sein und wo können Vorteile liegen?

Maren M.: Eine zentrale Herausforderung beim Aufbau von Managementsystemen und im Speziellen eines ISMS nach ISO 27001 liegt für kleine Unternehmen in dem damit verbundenen Verwaltungs- und Dokumentationsaufwand. Wegen begrenzter personeller und zeitlicher Ressourcen kann es schwierig sein, alle Anforderungen der Norm angemessen umzusetzen. Dabei muss insbesondere darauf geachtet werden, ein ausgewogenes Verhältnis zwischen Aufwand und Nutzen der Maßnahmen zu schaffen.

> Begrenzte Ressourcen: kurze Entscheidungswege, aber gegebenenfalls langsamere Umsetzung

Gleichzeitig ist es ein Vorteil, dass in kleinen Unternehmen gerade durch flache Hierarchien und kurze Entscheidungswege Maßnahmen häufig schneller abgestimmt und umgesetzt werden können, während in größeren Unternehmen oft langwierige Freigabeprozesse durch verschiedene Gremien erforderlich sind.

Die Maßnahmen können bei kleinen Unternehmen zwar aufgrund reduzierter Entscheidungsprozesse schnell beschlossen, wegen begrenzter Ressourcen aber gegebenenfalls nur langsam und nacheinander umgesetzt werden.



Ganzheitliche Energieeffizienz im Rechenzentrum – Aussagekraft und Grenzen der Kennzahl PUE

von Stefan Kuitunen, Daniel Scholz und Anne Weisemann

Die Digitalisierung schreitet rasant voran, getrieben durch den Einsatz immer leistungsfähigerer und häufiger genutzter IT Anwendungen, zu denen u. a. auch die Künstliche Intelligenz (KI) zählt. Mit dieser Entwicklung steigt der Energiebedarf der gesamten Informations- und Kommunikationstechnik Branche (IKT) deutlich an. Das größte Wachstum verzeichnen dabei Rechenzentren [1], welche in den letzten 15 Jahren fast eine Verdopplung ihres Energiebedarfs von 10,3 auf 21,3 TWh [2] aufweisen. Damit rückt die Branche immer stärker in den öffentlichen Fokus: Hoher Energiebedarf führt zu Forderungen der verbesserten Energieeffizienz, und die Gesetzgebung stellt strengere regulatorische Anforderungen an Betreiber.

Als etablierter Industriestandard für Energieeffizienzbewertung der Rechenzentrumsinfrastruktur hat sich die Power Usage Effectiveness (PUE) durchgesetzt. Doch wo und wie wende ich die PUE an? Wo liegen ihre Grenzen? Worauf kommt es bei einer ganzheitlichen Betrachtung der Energieeffizienz an? Antworten auf diese Fragen soll der vorliegende Artikel liefern.

Was bedeutet Power Usage Effectiveness (PUE)?

Die PUE ist eine von mehreren Kennzahlen der DIN EN 50600-4. Wie alle Kennzahlen dient sie dazu, Sachverhalte und Zusammenhänge anhand von Messdaten zu quantifizieren, um somit Bewertungen, Vergleiche und Optimierungen zu ermöglichen. Berechnet wird die PUE aus den Jahresmesswerten des Energiebedarfs eines Rechenzentrums $\mathbf{E}_{RZ}$ bezogen auf den Energiebedarf der darin betriebenen IT, bezeichnet mit $\mathbf{E}_{IT}$. Die Kennzahl PUE bewertet die Energieeffizienz der Infrastruktur eines Rechenzentrums.

$$PUE = \frac{E_{RZ}}{E_{IT}}$$

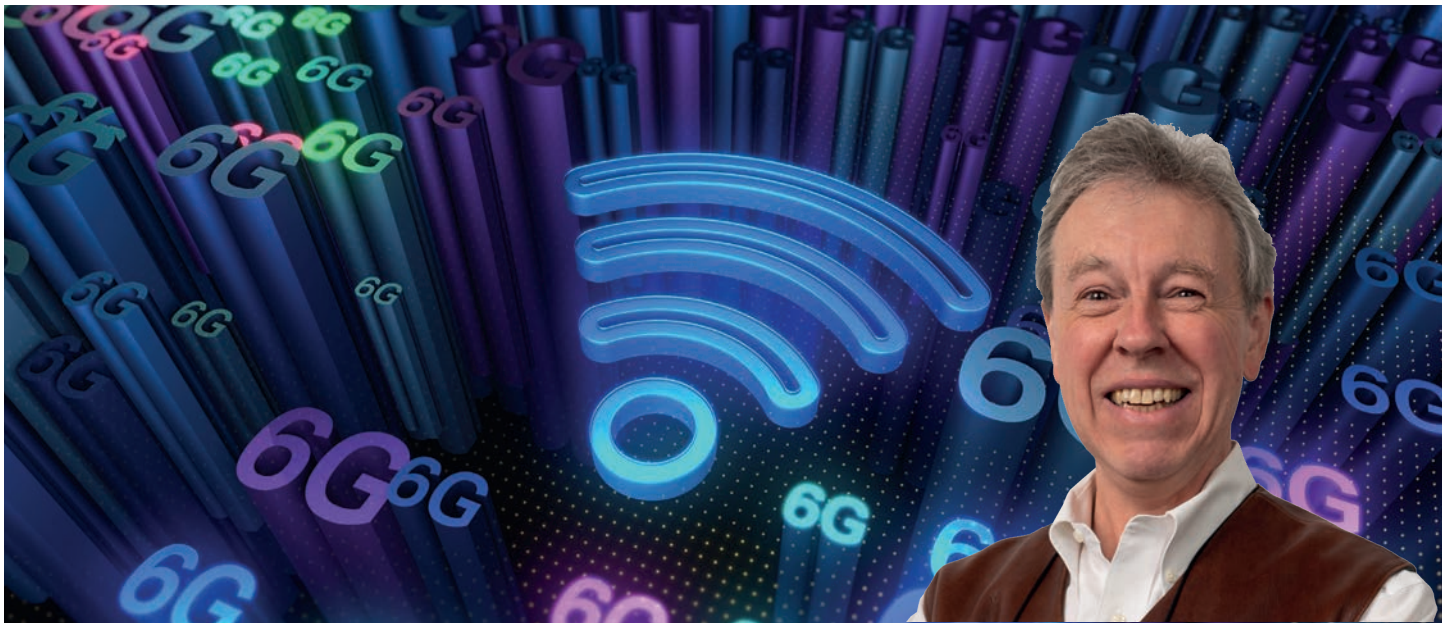
Der Energiebedarf IT E_{IT} setzt sich aus der Summe des Energiebezugs aller Server, Datenspeicher- und Datenverteilsysteme vom Rechenzentrum zusammen. Mit zunehmendem Workload der Server steigt der Energiebedarf IT des Rechenzentrums an, dabei wandeln die entsprechenden Server nahezu 100 % ihres elektrischen Energiebedarfs in Wärme um. Für den Betrieb der Server benötigt ein Rechenzentrum technische Infrastruktur, dazu zählt:

- elektrisches Verteilsystem inkl. unterbrechungsfreie Stromversorgung (USV) und Netzersatzanlagen (NEA)
- Kühlung u. a. der Serverräume, auch externe Kältebereitstellung
- sonstige Nebenverbraucher (Wärmeversorgung, Sicherheitssysteme, Leitwarte, Licht, usw.)

Zusammen ergeben der Energiebedarf der Infrastruktur $\mathbf{E}_{IN}$ und der Energiebedarf IT $\mathbf{E}_{IT}$ den Energiebedarf eines Rechenzentrums $\mathbf{E}_{RZ}$. Damit werden alle Energieflüsse in das Rechenzentrum umfasst (Abbildung 1). Aus dieser zunächst einfach klingenden Definition ergeben sich in der Praxis häufig folgende Fragen:

WLAN oder Mobilfunk: Wer kriegt das 6-GHz-Band?

von Dr. Joachim Wetzlar



Manche von Ihnen erinnern sich an meine Beispiele für praktische Anwendungen von 5G-Mobilfunk in privaten Netzen. Erste Anwendungen fand ich bereits 2018 in den Stellungnahmen [1] zum Entwurf des Antragsverfahrens für private 5G-Mobilfunketze der Bundesnetzagentur (BNetzA). Automobilhersteller wollten die in Neufahrzeuge einzubauenden Mobilfunk-Modems dazu nutzen, Software bereits auf die Fahrzeuge zu laden, solange sich diese in der Produktion befanden.

Zugegeben, das Beispiel hat mich damals überzeugt. Als es später um ein konkretes Projekt in diesem Umfeld ging, musste ich nachrechnen. Heraus kam, dass ein 5G-Netz in einer PKW-Montagehalle nicht annähernd die Kapazität bereitzustellen vermag, die man für diese Anwendung benötigt. Die zu bewegenden Datenmengen sind schier zu groß. Die Kapazität privater 5G-Mobilfunknetze ist hierzulande für diesen Zweck dank der Beschränkung auf gerade einmal 100 MHz Bandbreite (3,7 bis 3,8 GHz) nicht ausreichend.

Die Übertragungskapazität eines Funknetzes ist proportional zur nutzbaren Bandbreite. Sicher, Mobilfunk wie auch WLAN nutzen jegliche Bandbreite bestmöglich aus. Dank orthogonaler Frequenzmodulation (OFDM), vielwertiger Quadratur-Amplitudenmodulation (QAM) und Multiple Input Multiple Output (MIMO) lassen sich große Datenmengen auch durch schmale Funkkanäle quetschen. Der genannte Zusammenhang gilt dennoch: Mehr Bandbreite ergibt eine größere Kapazität.

Das ist der Grund, warum die Automobilhersteller in ihren Montagehallen nach wie vor auf WLAN setzen. In Europa kann ich in den „traditionellen“ Bändern 2,4 GHz und 5 GHz insgesamt 19 Kanäle zu je 20 MHz nutzen. Das ergibt gegenüber dem privaten 5G-Mobilfunk eine fast 4fache Kapazität. Dazu kommen seit 2021 die WLAN-Frequenzen im 6-GHz-Band, insgesamt 480 MHz.

Es wird Ihnen nicht entgangen sein, dass man in den USA bereits ein Jahr zuvor das 6-GHz-Band für WLAN freigegeben hatte. Dort stehen seither knapp 1.200 MHz zur Verfügung. Wieso sind es in Europa nur 480 MHz, d.h. die untere Hälfte des Frequenzbereichs? Zur Beantwortung dieser Frage kann man den Frequenzplan der BNetzA [2] zu Rate ziehen. Dort finde ich nach etwas Suchen den Eintrag „6525 – 7075 MHz MOBILFUNKDIENST“.

So ähnlich ist es auch in anderen Teilen der Welt. Die Wi-Fi Alliance veröffentlicht eine entsprechende Weltkarte [3]. Nur wenigen Ländern neben den USA steht das gesamte Band für WLAN zur Verfügung. In vielen Ländern sind es wie in Europa nur die unteren 480 MHz. Bemerkenswert finde ich jedoch, dass es in China gar keine Freigabe für WLAN im 6-GHz-Band gibt.

Offensichtlich sollen die genannten Frequenzen nicht für WLAN, sondern für Mobilfunk genutzt werden. Soweit ich die Mobilfunkstandards bislang kannte, war davon nicht die Rede. Jedoch tauchten bereits 2022 in der Technischen Spezifikation [4] die Netze n96 (5925 – 7125 MHz), n102 (5925 – 6425 MHz) und n104 (6425 – 7125 MHz) auf.

Als Besonderheit wird für die untere Hälfte des 6-GHz-Bandes (n102) bzw. für die Nutzung des gesamten Bandes (n96) vorgegeben, dass „shared spectrum access“ zu unterstützen ist und