Januar 2026

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

RZ-Migration: Kommunikation ist der Schlüssel zum Erfolg

von Gian Luca Ehlers

Eine Rechenzentrums-Migration ist etwas Besonders. Gerade hier wird deutlich, wie eng die verschiedenen Prozesse und Systeme miteinander verzahnt sind. Eine RZ-Migration gehört zu den anspruchsvollsten IT-Aufgaben und bringt ein hohes Risiko mit sich. Sie ist weitaus mehr als das Verschieben oder Aktualisieren von Hardware wie Servern oder Switches.

Seite 9

Die neue Norm EN IEC 62676-4:2025 für Videoüberwachungsanlagen

von Leon Scheidgen

Wer Videoüberwachungsanlagen plant oder betreibt, muss sich früher oder später mit der internationalen Normenreihe IEC 62676 „*Video surveillance systems for use in security applications*“, bzw. ihrer deutschen Übersetzung, der DIN EN IEC 62676, beschäftigen.

Seite 24

Brauchen Ihre Server demnächst Wasseranschlüsse?

von Dr. Behrooz Moayeri

Bereits seit Jahren steht der ausschlaggebende, limitierende Faktor bei der Gestaltung von Rechenzentren fest: die Abwärme. Die Kühlung von RZ-Komponenten hat mit der Leistungsdichte nicht Schritt gehalten. Für die meisten heute betriebenen Rechenzentren sind schon 10 Kilowatt pro Rack zu viel. Dabei steht die leistungsintensive Künstliche Intelligenz vor der Tür. Spätestens mit dem Einzug von KI ist es Schluss mit klassischen Methoden der RZ-Kühlung.

Seite 2

ITSM leicht gemacht

Wie moderne FitSM-Trainings Komplexität reduzieren und echte Verbesserungen ermöglichen

von Dierk Söllner

Viele kleine IT-Service-Provider, IT-Abteilungen und Startups leiden unter wachsender Komplexität, fehlenden Prozessen und unpraktischer Theorie in klassischen ITSM-Frameworks. FitSM bietet einen klaren Ansatz: Mit weniger Aufwand werden spürbare Verbesserungen erzielt, die direkt im Alltag wirken. Dieser Artikel gibt konkrete Tipps für schnellen und nachhaltigen Erfolg und macht Mut zur Umsetzung.

Seite 14

Webinar der Woche

Microsoft Defender XDR Administrator

Seite 23

Neues Jahr, neue Gefahren

Was könnte im Bereich der IT-Sicherheit 2026 auf uns zukommen?

von Dr. Markus Ermes

Auch im neuen Jahr werden weder die Welt der IT-Sicherheit noch die der Angreifer und Hacker stillstehen. Auf der einen Seite können wir uns auf interessante, durch künstliche Intelligenz unterstützte Werkzeuge gefasst machen, auf der anderen werden wir sie wohl auch selbst benötigen.

Seite 30

Brauchen Ihre Server demnächst Wasseranschlüsse?

von Dr. Behrooz Moayeri

Bereits seit Jahren steht der ausschlaggebende, limitierende Faktor bei der Gestaltung von Rechenzentren fest: die Abwärme. Die Kühlung von RZ-Komponenten hat mit der Leistungsdichte nicht Schritt gehalten. Für die meisten heute betriebenen Rechenzentren sind schon 10 Kilowatt pro Rack zu viel. Dabei steht die leistungsintensive Künstliche Intelligenz vor der Tür. Spätestens mit dem Einzug von KI ist es Schluss mit klassischen Methoden der RZ-Kühlung.

Die Leistungsexplosion

Man kann es nicht mehr als Entwicklung bezeichnen: Angemessener wäre, von der Leistungsexplosion bei Prozessoren zu sprechen. Innerhalb von acht Jahren hat sich der Leistungsbedarf der jeweils neuesten Generation von Grafikprozessoren (Graphics Processing Unit, GPU) vervierfacht: von 300 Watt auf 1,2 kW. Selbst wenn wir davon ausgehen, dass ein Server mit einem 1,2-kW-Prozessor statt einer Höheneinheit (HE) drei haben wird, kommen wir auf mindestens 400 Watt pro HE. Wenn man berücksichtigt, dass die GPU nicht der einzige Verbraucher in einem solchen Server ist, ist von 500 Watt pro HE auszugehen. Bei 40 HE pro Rack ergeben sich 20 kW Leistung pro Schrank. Das Gros dieser Leistung wird in Wärme umgewandelt, denn der Anteil, der in Form von Signalenergie über Datenleitungen die Racks verlässt, ist vernachlässigbar.

Nun sind allein 20 kW pro Rack kein Grund, den Weg der klassischen Luftkühlung zu verlassen. Jedoch sind 1,2 kW pro Chip nicht das Ende der Fahnenstange. Die Chip-Hersteller arbeiten an neuen Prozessor-Generationen, bei denen man von 5 kW pro Chip ausgeht, also dem vierfachen Wert im Vergleich zu den neuesten GPUs. Multiplizieren Sie 20 kW mit vier: Bei 80 kW pro Rack reicht die reine Luftkühlung längst nicht mehr aus.

Luft- versus Flüssigkeitskühlung

Haben Sie schon mal darüber nachgedacht, warum Sie es bei 90 Grad oder gar 100 Grad in der Sauna aushalten können, während selbst eine kurze Berührung mit 90 bis 100 Grad heißem Wasser mit einer Hautverletzung einhergeht? Flüssigkeiten sind viel dichter als Gase und haben deswegen erstens eine wesentlich höhere Wärmekapazität und zweitens eine um Größenordnungen höhere Wärmeleitfähigkeit.

Dort wo Luftkühlung an Grenzen stößt, beginnt die Domäne der Flüssigkeitskühlung. Neu ist Flüssigkeitskühlung nicht. Bereits für einige Großrechner des letzten Jahrtausends wurde Flüssigkeitskühlung, in der Regel Wasserkühlung, genutzt. Die Großrechner sind mittlerweile von vielen kleineren Rechnern verdrängt, für die eine Luftkühlung bis heute ausgereicht hat. Physikalisch ist dies einfach zu erklären: Der im wahrsten Sinne des Wortes „Hot Spot“-Großrechner wich den vielen „Warm Spots“, verteilt auf eine größere RZ-Fläche.

Nun werden die „Warm Spots“ dank Nvidia & Co. zu neuen Hot Spots. Anders als im letzten Jahrtausend gibt es sie heute in einem modernen RZ gleich in großer Zahl. Es geht nicht nur darum, einen Hot Spot zu kühlen, sondern jedes Rack oder zumindest mehrere Racks als Hot Spot zu behandeln. Die Flüssigkeitskühlung kommt wieder, diesmal quasi flächendeckend.

Kühlungslösungen im Vergleich

Bei der Planung eines zukunftsorientierten RZ-Kühlungssystems kommen verschiedene Kühlungslösungen infrage:

- Raumbasierende Umluftkühlgeräte (ULKG) in Kombination mit einer Outdoor-Kältemaschine: Diese Lösung wird in vielen Re-

RZ-Migration: Kommunikation ist der Schlüssel zum Erfolg

von Gian Luca Ehlers

Eine Rechenzentrums-Migration ist etwas Besonders. Gerade hier wird deutlich, wie eng die verschiedenen Prozesse und Systeme miteinander verzahnt sind. Eine RZ-Migration gehört zu den anspruchsvollsten IT-Aufgaben und bringt ein hohes Risiko mit sich. Sie ist weitaus mehr als das Verschieben oder Aktualisieren von Hardware wie Servern oder Switches. In Wirklichkeit handelt es sich um einen komplexen Gesamtablauf, bei dem zahlreiche technische und organisatorische Abläufe ineinandergreifen müssen. Während der Planung gilt es, viele Anforderungen zu berücksichtigen, die auf den ersten Blick nicht unbedingt erkennbar sind. Dazu zählen sowohl bauliche Rahmenbedingungen, Energieversorgung und Kühlung als auch die Verkabelung der einzelnen Racks und die Verortung der Systeme. Hinzu kommen mögliche externe Faktoren, wie Anbindungen an das WAN oder der Aufbau eines zweiten Rechenzentrums.

Dieses Zusammenspiel der vielen Variablen führt dazu, dass eine RZ-Migration nicht nur eine Frage der Umsetzung, sondern vor allem der Planung ist. Änderungen an einem System können Auswirkungen auf mehrere andere Bereiche haben. Daher ist es wichtig, dass Abhängigkeiten zwischen den Aufgaben möglichst frühzeitig erkannt und sauber dokumentiert werden, um spätere Engpässe und Verzögerungen zu vermeiden. Zuständigkeiten müssen klar benannt sein, damit alle Beteiligten wissen, wer Entscheidungen trifft oder bei Problemen anzusprechen ist. Ebenso wichtig ist die Einhaltung vorher strukturierter Prozesse, sodass jede Änderung nachvollziehbar geplant, bewertet und freigegeben werden kann. Ohne diese Struktur steigt das Risiko, dass Migration unvorhersehbare Nebenwirkungen erzeugen oder im laufenden Betrieb Störungen verursachen.

Kommunikation ist entscheidend

Die beste Planung wird schnell an Wirkung verlieren, wenn sie nicht durch eine klare und abgestimmte Kommunikation begleitet wird. In einer RZ-Migration sind viele unterschiedliche Teams und Fachbereiche beteiligt – von Infrastruktur und Netzwerkspezialisten bis hin zu Experten für Datenbanken, Storage und IT-Sicherheit. Der Erfolg einer Migration hängt maßgeblich davon ab, wie gut die beteiligten Personen und Teams miteinander kommunizieren: Dabei geht es darum, Informationen zielgerichtet und transparent auszutauschen, um so Entscheidungen gemeinsam und effizient treffen zu können.

Weiterführend dazu verweise ich auf den Artikel Geordnete Kommunikation ist der Schlüssel zum guten Service meines Kollegen Dr. Moayeri. Dort beschreibt er, wie Kommunikationsmängel und fehlende Struktur im IT-Service Störungen verursachen und warum klare Prozesse oder der Einsatz eines ITSM-Tools entscheidend sein können.

All diese Aspekte zeigen, dass die Kommunikation nicht nur ein begleitender Faktor einer RZ-Migration ist, sondern auch zu ihren wesentlichen Bestandteilen gehört.

Mögliche Hindernisse

Nachteile der E-Mail-Kommunikation

Oft arbeiten die beteiligten Teams und Mitarbeiter voneinander abgegrenzt und verfolgen ihre eigenen Aufgaben. In vielen Unternehmen erfolgt die Kommunikation mit anderen Teams überwiegend über den altbekannten E-Mail-Verkehr.

Besonders in Migrationsprojekten stößt der klassische E-Mail-

ITSM leicht gemacht

Wie moderne FitSM-Trainings Komplexität reduzieren und echte Verbesserungen ermöglichen

von Dierk Söllner

Viele kleine IT-Service-Provider, IT-Abteilungen und Startups leiden unter wachsender Komplexität, fehlenden Prozessen und unpraktischer Theorie in klassischen ITSM-Frameworks. FitSM bietet einen klaren Ansatz: Mit weniger Aufwand werden spürbare Verbesserungen erzielt, die direkt im Alltag wirken. Dieser Artikel gibt konkrete Tipps für schnellen und nachhaltigen Erfolg und macht Mut zur Umsetzung.

Ziel dieses Beitrags ist es, einen praxisnahen Weg für IT Service Management aufzuzeigen, der sich speziell an kleine und mittlere IT-Service-Provider, IT-Abteilungen und Startups in der Wachstumsphase richtet. Mit einfachen Frameworks wie FitSM wird gezeigt, wie Komplexität reduziert und messbare Verbesserungen im Alltag erzielt werden können. Der Artikel macht Mut zum Umsetzen und bietet konkrete Ansätze für den schnellen Erfolg.

Warum ITSM oft scheitert und FitSM neue Wege geht

Kleine und mittlere IT-Service-Provider sowie IT-Abteilungen stehen vor typischen Hürden: Die Arbeitslast wächst, die betreute Technologie wird umfangreicher und komplexer, und die Prozesse bleiben oft unstrukturiert. Serviceanfragen werden immer noch per E-Mail oder Telefon abgewickelt, eine nachhaltige Dokumentation fehlt und das Know-how einzelner Mitarbeiter geht bei Kündigung oder Renteneintritt verloren. Zwischen technischer Komplexität und organisatorischem Anspruch geraten Teams schnell in den reaktiven Feuerwehrmodus, ohne Struktur und Raum für gezielte Verbesserung.

Viele klassische ITSM-Frameworks wie ITIL® oder ISO 20000 gelten im Mittelstand als zu komplex und bürokratisch. Umfangreiche Dokumentation, theoretische Modelle, langwierige Rollen- und Prozessmodelle sowie teure Schulungen und Tools schrecken ab. Was für Großunternehmen praktikabel und notwendig ist, bremst kleine Organisationen: Sie verlieren sich in Theorie und Wissensaufbau, statt Verbesserungen und Nutzen zu erleben. Der initiale Mehrwert bleibt auf der Strecke, und der Aufwand steht in keinem sinnvollen Verhältnis.

FitSM – Das pragmatische Framework im Überblick

FitSM steht für ein leichtgewichtiges und praxisnahes Framework im IT Service Management. Die Grundprinzipien sind Pragmatismus, Konsistenz und ausreichende Strukturen ohne Overhead. FitSM setzt konsequent auf Klarheit in Prozessen, verständliche Rollen und minimal erforderliche Dokumentation. Ziel ist: IT Service Management muss für jede Organisation unabhängig von Größe und Reifegrad sofort greifbar und umsetzbar werden. FitSM hat das Beste aus anderen Frameworks übernommen und in ein überschaubares und trotzdem vollständiges Framework überführt.

FitSM basiert auf den bekannten ITSM-Frameworks ITIL®, COBIT und ISO20000 und integriert deren zentrale Ansätze. Dennoch unterscheidet sich FitSM bewusst von ihnen: Während diese Frameworks mit umfangreichen Prozess- und Rollenmodellen sowie hunderten Seiten an Vorgaben und Zertifizierungsmöglichkeiten arbeiten, setzt FitSM konsequent auf Reduktion und Klarheit. Das Framework ist frei verfügbar, die Prozesse sind kompakt beschrieben und auf das Wesentliche fokussiert. Komplexe Rollenstrukturen, überbordende Dokumentationsanforderungen und teure Zertifizierungen sucht man hier vergeblich.

KI-Einsatz im Contact Center

Mit Nils Wantia sprach Christiane Zweipfennig

Künstliche Intelligenz (KI) gewinnt im Contact Center zunehmend an Bedeutung – ein Wandel, der die Branche nachhaltig prägt. Während früher menschliche Mitarbeiter den Kern der Kundenkommunikation bildeten, übernehmen heute fortschrittliche KI-Systeme Routinen und Analysen mit beeindruckender Geschwindigkeit. Die Zukunft der Kundenbetreuung wird daher nicht mehr ausschließlich durch menschliche Interaktion bestimmt, sondern durch ein Zusammenspiel, in dem Künstliche Intelligenz Abläufe effizienter gestaltet, Wartezeiten verkürzt und personalisierte Betreuung unterstützt.

Nils Wantia ist seit über 8 Jahren bei der ComConsult GmbH beschäftigt und leitet das Competence Center Kommunikationslösungen. Während zu Beginn seiner Tätigkeit Contact-Center-Themen meist nur innerhalb größerer Ausschreibungen zu UC-Lösungen behandelt wurden, gewannen sie in den Jahren seit der Corona-Pandemie zunehmend an Bedeutung. Heute gehören die Planung und Implementierung von Kundenservice-Lösungen zu seinen Aufgabenschwerpunkten innerhalb der Projektarbeit. In diesem Interview berichtet er von seinen Erfahrungen aus mehreren aktuellen Projekten, in denen der Einsatz von Künstlicher Intelligenz im Contact Center immer mehr im Fokus steht.

Worin bestehen aus deiner Sicht die Hauptgründe für den Anstieg von Contact-Center-Projekten in den letzten Jahren?

Oftmals ist es eine Herausforderung, Contact-Center-Systeme zu integrieren, denn sie beste-hen nicht nur aus einer einzigen Lösung, sondern immer aus einem Zusammenspiel mehrerer Komponenten: TK/UC-Systeme, Contact-Center-Lösungen, KI-Anwendungen wie Bots und Customer-Relationship-Management-Systeme (CRM) etc. Dadurch ergeben sich komplexe Schnittstellen und Abstimmungsbedarfe zwischen den einzelnen Bestandteilen. In vielen Projekten bringt das potenziell eine große Umstellung für die Kunden mit sich, besonders wenn sie ihre Contact-Center-Lösungen das letzte Mal vor fünf oder mehr Jahren erneuert haben. Hier hilft unsere gezielte Beratung, um dem Kunden diese neue Situation verständlich zu ma-chen, den Sinn der einzelnen Bausteine zu erklären und den Weg zu einer integrierten Lösung aufzuzeigen. Die spannenden Aspekte solcher Projekte liegen daher oft in den klassischen Beratungsleistungen, die Transparenz schaffen und die Implementierung begleiten.

> Komplexes Zusammenspiel von TK/UC-System, Contact-Center-Lösung, KI-Anwendungen und CRM-System

Momentan bearbeiten wir mehrere Contact-Center-Projekte unterschiedlicher Größe – angefangen von einem großen IT-Dienstleister über einen Versicherungskonzern bis hin zu einem öffentlichen Auftraggeber.

Besonders im Bereich des Kundenservices haben sich in den letzten Jahren Anwendungen aus dem Bereich der Künstlichen Intelligenz etabliert. Was ist der Grund dafür?

Die neue Norm EN IEC 62676-4:2025 für Videoüberwachungsanlagen

von Leon Scheidgen

Wer Videoüberwachungsanlagen plant oder betreibt, muss sich früher oder später mit der internationalen Normenreihe IEC 62676 „*Video surveillance systems for use in security applications*“, bzw. ihrer deutschen Übersetzung, der DIN EN IEC 62676, beschäftigen. Sie definiert Standards für Videoüberwachungsanlagen für Sicherungsanwendungen, von der Planung über die Installation bis zum Betrieb, inklusive Anforderungen an Bildqualität, Schnittstellen und Leistungsprüfungen für Komponenten wie Kameras und Videoanalyse-Server. Mit dieser Normenreihe erhalten Fachplaner, Errichter und Betreiber von Videoanlagen ein mächtiges Werkzeug, mit dem sie die fachgerechte Errichtung der Überwachungslösung sicherstellen und spätere Anpassungen vermeiden können. Der vierte Teil der Reihe, die Norm 62676-4 „Anwendungsregeln“, wurde jüngst einer wichtigen Aktualisierung unterzogen. In diesem Artikel werden die wesentlichen Neuerungen und Verbesserungen im Vergleich zur alten Norm aus dem Jahr 2015 unter die Lupe genommen.

Die Normenreihe IEC/EN 62676 ist in mehrere, voneinander unabhängige Teile gegliedert. Der vierte Teil „umfasst die Planung, Gestaltung, Installation, Prüfung, Inbetriebnahme und Wartung von Videoüberwachungssystemen (VSS) […] zur Nutzung in Sicherheitsanwendungen“ [4]. Die bisher geltende Fassung trat im Jahr 2014 in Kraft.

Seitdem haben sich die technischen Anforderungen und Sicherheitsbedürfnisse jedoch rasant weiterentwickelt. Die Festlegungen der Norm EN 62676-4:2015 gelten mittlerweile als überholt, da sie neuen Technologien wie z. B. einer Videoanalyse mit künstlicher Intelligenz (KI) oder höheren Kameraauflösungen nicht gerecht werden können. Um diesen Veränderungen Rechnung zu tragen, trat im Oktober 2025 die Norm IEC 62676-4:2025 in Kraft, die die Fähigkeiten und Einschränkungen moderner digitaler IP-Kameras berücksichtigt. Eine Übernahme bzw. Übersetzung als DIN-EN-IEC-Norm wird im Januar/Februar 2026 erwartet [4].

Hier ein Überblick über die verschiedenen Normen, die herausgebenden Organisationen und ihre Veröffentlichungsdaten:

- Auf internationaler Ebene: IEC (International Electrotechnical Commission) [2]
  - IEC 62676-4:2025
  - Veröffentlichungsdatum: 09.10.2025
  - Diese Norm ersetzt die erste Edition aus dem Jahr 2014: IEC 62676-4:2014.
- Auf europäischer Ebene: CENELEC (Europäisches Komitee für elektrotechnische Normung) [3]
  - EN IEC 62676-4:2025
  - Erscheinungsdatum: 28.11.2025
  - Die IEC-Norm wurde unverändert als europäische Norm übernommen. Sie ersetzt die erste Edition EN 62676-4:2015.
- Auf deutscher Ebene: DIN (Deutsches Institut für Normung)

Neues Jahr, neue Gefahren:
Was könnte im Bereich der IT-Sicherheit 2026 auf uns zukommen?

von Dr. Markus Ermes

Auch im neuen Jahr werden weder die Welt der IT-Sicherheit noch die der Angreifer und Hacker stillstehen. Auf der einen Seite können wir uns auf interessante, durch künstliche Intelligenz unterstützte Werkzeuge gefasst machen, auf der anderen werden wir sie wohl auch selbst benötigen. Denn auch Angreifer, insbesondere im Umfeld der zielgerichteten Angriffe (engl.: Advanced Persistent Threat – APT), können von den neuen Möglichkeiten der KI profitieren. Gleichzeitig kann die KI selbst ein Risiko darstellen. Schauen wir uns ein paar Beispiele an!

Die KI als Fehlerquelle oder Informationsabfluss

Ein Bereich, in dem das Risikobewusstsein zwischen Experten und weniger technikaffinen Nutzern kaum größer sein könnte, ist die Zuverlässigkeit und Vertrauenswürdigkeit einer KI.

Die aktuellen Large Language Models (LLMs) wie ChatGPT, Gemini und Grok erscheinen für einen unbedarften Nutzer fast schon wie Magie. Man gibt eine Anfrage ein und bekommt eine Antwort, die gut und richtig klingt. Und dabei geht es nicht nur um Recherchen, sondern auch um Bilderzeugung oder Programmierung. Leider hat die aktuell gängige Technologie der LLMs eine entscheidende Schwäche: Durch den Wahrscheinlichkeits-basierten Ansatz zur Erzeugung der Antwort wird nicht die richtige Information, sondern die wahrscheinlichste ausgegeben. In Kombination mit der Tatsache, dass die meisten LLMs „von Hause aus“ darauf ausgelegt sind, dem Nutzer zu gefallen und Konflikte zu vermeiden, entstehen so faktisch falsche Antworten. Wenn ich mir dann auch noch Quellcode für eine Software generieren lasse, können solche nicht offensichtlichen Fehler auch zum Sicherheitsrisiko werden.

Ein anderer wichtiger Aspekt: In den meisten Fällen nutzen die Hersteller aktueller Cloud-KIs die eingegebenen Anfragen für das weitere Training. Werden dabei vertrauliche Informationen in die KI eingegeben, landen diese praktisch „in der KI“. Zwar ist es nicht einfach, die ursprünglichen Trainingsdaten einer KI zu extrahieren, doch man liest regelmäßig von Beispielen, bei denen genau das passiert ist.

Diese beiden Aspekte sind aus Sicht der Informationssicherheit eine enorme Herausforderung. Die Überprüfung von Informationen und Quellcode kann zwar teilweise automatisiert werden, doch kommen die besten Ergebnisse immer noch von Menschen. Gleiches gilt für die Eingabe von Daten in eine KI: Hier muss ein Bewusstsein geschaffen werden. Ergänzend lassen sich Techniken der Data Loss Prevention (DLP) einsetzen.

KI als technisches Angriffswerkzeug

Doch nicht nur unsere Kollegen und Mitarbeiter haben Zugriff auf KIs, sondern auch Angreifer. Und gerade bei APTs, die häufig von Staaten unterstützt werden, kann dadurch eine neue Gefahr auftreten: eine auf Angriffe optimierte KI, insbesondere im Umfeld von Payloads von Angriffen oder dem Auffinden von Schwachstellen. Eine eigene KI zu entwickeln und zu trainieren ist zwar enorm aufwendig, aber mit staatlichen Mitteln durchaus machbar.