November 2026

ComConsult
BERATUNG • PLANUNG • SCHULUNG

Der Netzwerk Insider



Post-Quanten-Kryptografie:

Bereits eine konkrete Planungsaufgabe?

von Andrés Gammersbach
Ursprünglich war ich gar nicht auf der Suche nach Quantencomputern oder Post-Quanten-Kryptografie, kurz PQC (Post Quantum Cryptography). Bei einer Recherche zum WLAN-Standard IEEE 802.11 stieß ich zufällig auf das Projekt P802.11bt. Es läuft seit dem 10. September 2025 und soll die Sicherheitsmechanismen von WLAN um PQC-Verfahren erweitern.

Seite 9

Tool-gestützter Netzbetrieb

von Stephan Bien

Seite 15

Spine-Leaf-Architektur im Rechenzentrum

Aufbau, Vorteile und Einsatzbereiche

von Ben Grünbauer

Seite 26

Schwerpunkte der absehbaren IT-Projekte

von Dr. Behrooz Moayeri
Wiederholt berichteten wir an dieser Stelle über die von ComConsult wahrgenommenen Schwerpunkte der absehbaren IT-Projekte, so zum Beispiel in der Ausgabe Januar 2025. Zwar ist unsere Wahrnehmung anhand der Aufträge, die ComConsult erhält und bearbeitet, möglicherweise nicht ganz repräsentativ, jedoch ergibt die Vielzahl von dabei berücksichtigten Projekten und verschiedenen Organisationen eine vollständigere Sicht im Vergleich zur Sicht einer einzelnen Institution.

Seite 2

Das KI-native Unternehmen: ein Praxisleitfaden für den Mittelstand

von Darav Taha
Viele Mittelständler probieren KI an einzelnen Stellen aus und bleiben im Pilotmodus stecken. Der Sprung zum KI-nativen Unternehmen gelingt, wenn KI zur Infrastruktur der Wertschöpfung wird und die IT die Daten sicher zugänglich macht.

Seite 33



Webinar der Woche

ITIL®-Einführung

vom Server-Hinsteller zum Business-Ermöglicher

Seite 25

Sicherheit von Rechenzentren in geopolitisch angespannten Zeiten – wenn die reale Welt die IT einholt

von Dr. Markus Ermes
Sichere Rechenzentren – dabei denken wohl die meisten von uns an sichere Netzwerke, Firewalls, Intrusion-Detection-Systeme und Netzwerksegmentierung.

Seite 30



Schwerpunkte der absehbaren IT-Projekte

von Dr. Behrooz Moayeri

Wiederholt berichteten wir an dieser Stelle über die von ComConsult wahrgenommenen Schwerpunkte der absehbaren IT-Projekte, so zum Beispiel in der Ausgabe Januar 2025.

Zwar ist unsere Wahrnehmung anhand der Aufträge, die ComConsult erhält und bearbeitet, möglicherweise nicht ganz repräsentativ, jedoch ergibt die Vielzahl von dabei berücksichtigten Projekten und verschiedenen Organisationen eine vollständigere Sicht im Vergleich zur Sicht einer einzelnen Institution.

Rechenzentren im Fokus

Ungefähr eineinhalb Jahrzehnte nach dem Aufkommen von Cloud Computing steht die Zukunft von Rechenzentren (RZ) weiter im Fokus vieler Firmen und Behörden. Cloud Computing selbst hat im zurückliegenden Jahrzehnt verschiedene Hype-Wellen aufgewiesen und sich damit unterschiedlich auf die RZ-Strategien von Institutionen ausgewirkt. Dabei hatte der externe Einfluss auf diese Strategien in der Regel eine größere Relevanz als eigenständige Präferenzen. Zum Beispiel hat die starke Cloud-Ausrichtung des Herstellers Microsoft die Cloud- und RZ-Konzepte von fast allen Institutionen wesentlich beeinflusst. Ein anderer Triebfaktor für Clouds waren die Pandemie Anfang des 2020er-Jahrzehnts und der damit verbundene Zwang zur Telearbeit. Nicht zu vernachlässigen sind auch regulatorische Einflüsse. Beispielsweise haben Energieeffizienzvorgaben das Ende mancher Rechenzentren besiegelt. Auch die neuen gesetzlichen Vorgaben an die Verfügbarkeit und Sicherheit von IT haben die Organisationen veranlasst, RZ-Standortredundanz zu realisieren.

Wenn ich in der Vergangenheitsform schreibe, heißt es nicht, dass die Entwicklung abgeschlossen ist. Immer mehr Organisationen werden von den oben genannten externen Einflüssen erfasst. Die Notwendigkeit der Professionalisierung des RZ-Betriebs betrifft immer mehr Branchen und Einzelinstitutionen. Das stellen wir auch in unseren Projekten fest. Der Gegenstand dieser Projekte reicht von RZ-Standortredundanz über RZ-Umzug bis hin zur verlässlicheren Dokumentation von Rechenzentren samt Verkabelung und IT-Komponenten.

Künstliche Intelligenz

Immer noch ist Künstliche Intelligenz mehr Hype als Realität. Trotzdem wirkt sie sich zunehmend auf die IT von Firmen und Behörden aus. Anfangs gingen viele IT-Verantwortliche davon aus, dass KI untrennbar mit der Nutzung von Hyperscaler-Clouds verbunden ist. Dies hat sich geändert. KI On Premises (OnPrem) ist nicht mehr bloß ein frommer Wunsch. Einerseits haben die teilweise berechtigten Vorbehalte gegen Cloud-Nutzung einen Markt für OnPrem-KI geschaffen. Andererseits hat das Downsizing der KI-Modelle den Leistungshunger etwas relativiert.

So gibt es in einer zunehmenden Anzahl von RZ-Projekten die Anforderung, die Auswirkungen von KI auf Energieversorgung und Kühlung zu berücksichtigen.

Neben der technischen Planung für OnPrem-KI geht es in vielen Organisationen um die Nutzungsszenarien von KI. Als Beispiele sind KI-gestützter Betrieb von Netz und IT-Sicherheit (NetOps und



Post-Quanten-Kryptografie: Bereits eine konkrete Planungsaufgabe?

von Andrés Gammersbach

Ursprünglich war ich gar nicht auf der Suche nach Quantencomputern oder Post-Quanten-Kryptografie, kurz PQC (Post Quantum Cryptography). Bei einer Recherche zum WLAN-Standard IEEE 802.11 stieß ich zufällig auf das Projekt P802.11bt. Es läuft seit dem 10. September 2025 und soll die Sicherheitsmechanismen von WLAN um PQC-Verfahren erweitern. Dazu zählen Verfahren für die Authentifizierung, digitale Signaturen und Schlüsselvereinbarung sowie entsprechende Anpassungen bestehender Schlüsselverwaltungs- und Handshake-Protokolle [1].

P802.11bt ist noch kein veröffentlichter Standard, sondern ein laufendes Standardisierungsprojekt. Es zeigt jedoch, dass die praktische Integration von PQC bereits vorbereitet wird. Bis dahin war mir das Thema kaum geläufig. Quantencomputer kannte ich vor allem aus den Nachrichten. Umso neugieriger machte mich, wie nah PQC der praktischen Anwendung bereits gekommen ist.

Ich begann mit der Recherche und bemerkte, dass meine Kollegen sich ebenfalls mit dem Thema beschäftigt haben. Dr. Markus Ermes hat bereits 2022 im Netzwerkinsider einen Artikel „https://www.comconsult.com/der-loechrige-weg-zur-post-quanten-kryptographie/“ zu PQC verfasst, sowie zuletzt Lea Joosten „https://www.comconsult.com/quanten-eine-gefahr-fuer-unsere-netze/“. Auch das BSI (Bundesamt für Sicherheit in der Informationstechnik) behandelt PQC nicht mehr nur als Forschungsthema. Es veröffentlicht konkrete Empfehlungen und betrachtet die Migration zu quantensicheren Verfahren als langfristig notwendige Aufgabe [2].

Zukunftsmusik?

Viele verbinden Quantencomputer mit Universitäten, Spezialhardware und wissenschaftlichen Durchbrüchen. Gelegentlich erscheinen Meldungen über neue Quantenprozessoren, steigende Qubit-Zahlen oder Fortschritte bei der Fehlerkorrektur. Das Thema ist spannend, wirkt aber zunächst wenig relevant für den eigenen Alltag.

Bei PQC ist der erste Eindruck ähnlich. Gemeint sind kryptografische Verfahren, von denen angenommen wird, dass sie auch mit Quantencomputern nicht effizient gebrochen werden können. Sie laufen auf klassischer Hardware und unterscheiden sich damit von der Quantenkryptografie, insbesondere der Quantenschlüsselverteilung (Quantum Key Distribution, QKD), die eine spezielle quantenphysikalische Infrastruktur benötigt [2], [3]. Falls Sie sich fragen, worum es sich hierbei handelt: Mein Kollege Dr. Philipp Rüßmann hat erst vor Kurzem einen Blogbeitrag „https://www.comconsult.com/quantenphysik-als-ausweg-aus-dem-quantendilemma/“ dazu geschrieben.

Je tiefer ich in das Thema einstieg, desto deutlicher wurde: Es geht nicht mehr nur um die Frage, ob PQC irgendwann relevant wird. Die Vorbereitung auf die Migration sollte bereits heute beginnen. Das BSI hat seine Empfehlungen deshalb mehrfach erweitert und nennt in der Technischen Richtlinie TR-02102 geeignete quantensichere Verfahren [4].



Tool-gestützter Netzbetrieb

von Stephan Bien

Die klassischen Aufgaben eines Netzbetriebs haben sich in den Grundzügen in den vergangenen Jahren nicht wesentlich verändert. Neben der Überwachung des einwandfreien Betriebs stehen das Konfigurations-, Fehler-, Performance/Accounting-, sowie Sicherheits-Management im Vordergrund der Betrachtung.

Das bewährte CLI-Management ist in vielen Switch- und Routing-Infrastrukturen immer noch allgegenwärtig. Allerdings stößt man in softwaredefinierten Infrastrukturen sowie komplexeren Umgebungen mit einer mehrstufigen Sicherheits-Infrastruktur schnell an seine Grenzen.

Die Netzlandschaft wird durch hybride Cloud-Strukturen, IoT- und Edge-Devices zunehmend verteilter, dynamischer und komplexer, während Personal, Budget und weitere verfügbare Betriebsressourcen weitgehend konstant bleiben oder gar gekürzt werden.

Der Netzbetrieb muss trotz steigender Komplexität skalierbar bleiben. Daraus ergibt sich der Bedarf nach Echtzeit-Telemetrie, Ende-zu-Ende-Transparenz sowie einer stärkeren Automatisierung der Ursachenanalyse und Fehlerbehebung.

Durch den Einsatz von leistungsfähigen Tools lässt sich der Netzbetrieb deutlich vereinfachen oder gar erst bewerkstelligen. Dabei können Rollout-Prozesse von neuen Infrastrukturen gleichermaßen bedient werden wie die täglichen Arbeiten eines Administrations-Teams.

Das Fundament eines Netzbetriebs

Ein solider Netzbetrieb bildet die Grundlage für eine leistungsfähige, sichere und zukunftsfähige IT-Infrastruktur. Durch die intelligente Vernetzung von Systemen, Anwendungen und Endgeräten gewährleistet er eine hohe Verfügbarkeit, stabile Performance und maximale Sicherheit im Unternehmensalltag. Moderne Netzarchitekturen setzen dabei auf zentrale Verwaltung und kontinuierliches Monitoring, um Ausfälle frühzeitig zu erkennen und zu beheben.

Dabei spielen die klassischen Netzmonitoring-Tools eine elementare Rolle, da sie Transparenz über den Zustand und die Leistung der Netzinfrastruktur schaffen. Durch die kontinuierliche Überwachung von Netzkomponenten können Störungen, Engpässe oder Sicherheitsvorfälle frühzeitig erkannt und behoben werden, bevor sie den Geschäftsbetrieb beeinträchtigen. Darüber hinaus liefert ein Monitoring wertvolle Daten für die Kapazitätsplanung.

So mögen zu Projektbeginn für eine PoE-Leistungsberechnung nur die Gerätekategorien WLAN Access Point und IP-Telefone herangezogen worden sein. Die von den Endgeräten geforderten PoE-Leistungsklassen sowie das kumulierte PoE-Budget je Access-Switch wurden inklusive einer Leistungsreserve berechnet und entsprechende Switch-Typen beschafft und ausgerollt. Der spätere Aufbau weiterer PoE-fähiger Endgeräte konnte nun ohne Zutun des Netzbetriebs erfolgen. Die Überwachung der PoE-Leistungsdaten kann hier planerische Lücken aufdecken und prädiktiv auf Probleme hinweisen, bevor sie für die Anwender relevant werden.

Auch das Gegenteil kann der Fall sein. Der gemäß Datenblatt des Herstellers geforderte PoE-Leistungsbedarf kann im realen Betrieb deutlich geringer ausfallen. So lassen sich unnötige Investitionen mit Hilfe eines Realitäts-Checks im Netzmonitoring verhindern.

Einen Schritt weiter geht ein proaktives Monitoring. Statt erst auf Störungen zu reagieren, wenn sie bereits Auswirkungen haben, werden Leistungsdaten, Ergebnisse und Trends analysiert, um potenzielle Probleme frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten.



RZ-Migration: Vorbereitung, Begleitung und Durchführung

Mit Dr. Markus Ermes und Miomir Tomovic sprach Christiane Zweipfennig

Ein Rechenzentrumsumzug ist für Unternehmen ein komplexes Vorhaben, bei dem zahlreiche Faktoren berücksichtigt werden müssen. Dazu gehören unter anderem Planung und Dokumentation, Risikoanalyse, Infrastruktur und Verkabelung, Ressourcen und Logistik, Kommunikation und Koordination sowie die schrittweise Durchführung der Migration.

Dr. Markus Ermes hat gemeinsam mit seinen Kollegen von ComConsult bereits eine Vielzahl von Kunden bei Rechenzentrumsprojekten begleitet. Das Spektrum reicht von der Standortfindung und Umfeldanalyse über die Ausschreibungen und Planung von Interconnects, Rechenzentrumsflächen und Verkabelung bis hin zur Besiedlung von Rechenzentren.

Miomir Tomovic ist seit 1997 im Projektgeschäft tätig, mit besonderem Schwerpunkt auf der Financial-Service-Industrie. In seiner langjährigen beruflichen Laufbahn hat er unterschiedliche Themenbereiche und Projekte begleitet. Ein wesentlicher Schwerpunkt seiner Tätigkeit liegt im Programm- und Projektmanagement. In dieser Funktion unterstützt er als externer Projektleiter seit Juni des vergangenen Jahres einen Rechenzentrumsumzug.

Ein Kunde aus dem Finanzsektor plante den Umzug seines Rechenzentrums. Wie war der grobe Ablauf des Projekts?

M. Tomovic: Das Projekt läuft bereits seit rund zwei Jahren. Ausgangspunkt des Kunden war, dass ein neues Rechenzentrum benötigt wurde, woraufhin zunächst die entsprechende Standortsuche sowie die Auswahl geeigneter Dienstleister erfolgten. Ich selbst bin im Juni des letzten Jahres als Projektleiter in das Projekt eingestiegen.

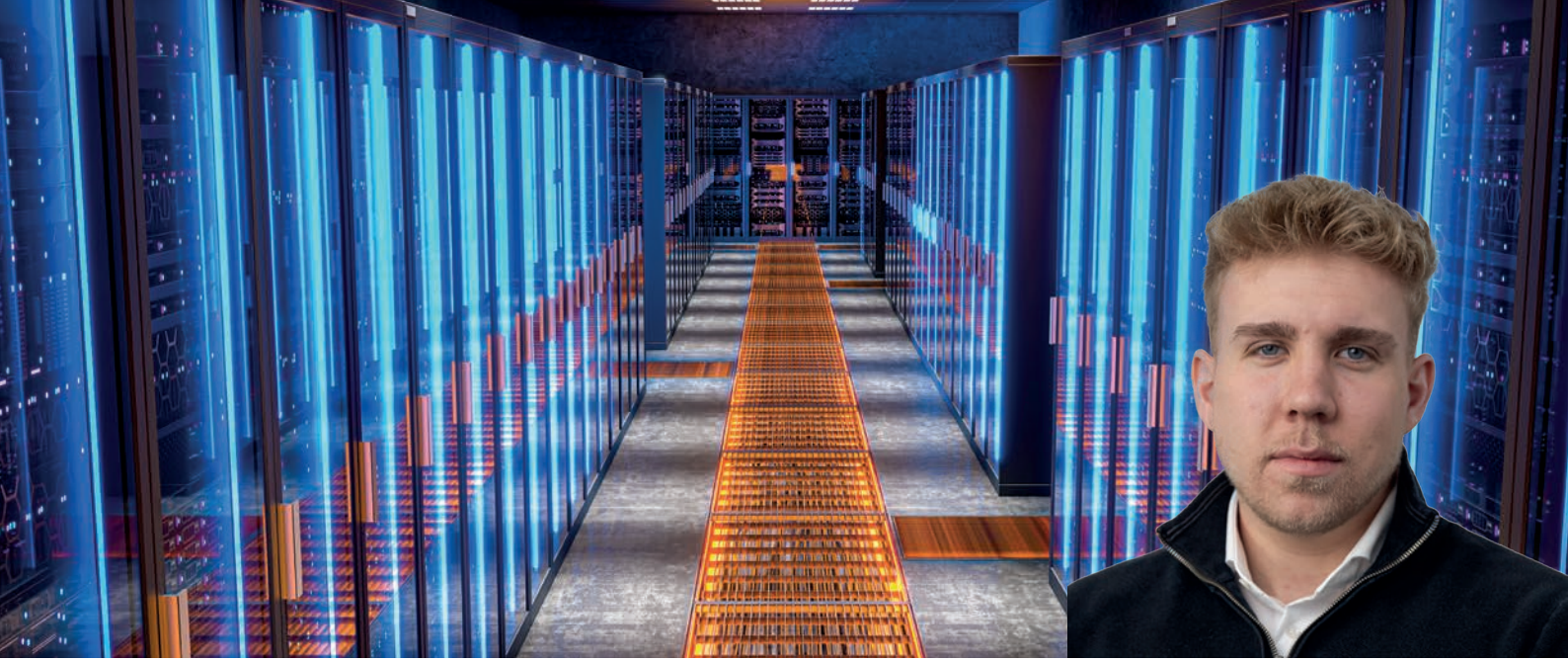
M. Ermes: Wir von ComConsult beschäftigen uns seit 2024 mit dem Projekt. Zu Beginn lag unser Fokus auf der Ist-Aufnahme. Zwar gab es bereits eine Dokumentation, diese war jedoch an einigen Stellen nicht vollständig. Daher haben wir die Gegebenheiten vor Ort mit Zettel und Stift noch einmal detailliert überprüft und dokumentiert, welche Systeme aufgenommen worden waren und welche nicht, und welche Systeme in das neue Rechenzentrum verlagert werden sollten.

> Standortsuche, Ist-Aufnahme, Planung, Vorbereitung, Umzug in mehreren Wellen

Auf Basis dieser Ist-Aufnahme haben wir anschließend den Platzbedarf für den neuen Standort ermittelt – einschließlich der Anzahl und Größe der benötigten Schränke. Dabei wurde die ursprüngliche Planung noch um zusätzliche Schränke als Reserve erweitert.

Im nächsten Schritt erfolgte die Planung der passiven Verkabelung sowie die strukturierte Zuordnung der Systeme zu den einzelnen Schränken. Auch die Anforderungen an Stromversorgung und Wärmeentwicklung mussten dabei berücksichtigt werden.

Darüber hinaus haben wir die Unterlagen für die einzelnen Um-



Spine-Leaf-Architektur im Rechenzentrum

Aufbau, Vorteile und Einsatzbereiche

von Ben Grünbauer

Aktuell beschäftigen wir uns im Rahmen eines Kundenprojekts intensiv mit der Infrastruktur eines bestehenden Rechenzentrums. Ein Teil unserer Arbeiten findet dabei direkt an der vorhandenen Netzwerkinfrastruktur statt. Unter anderem werden ältere Access-Leaf-Switches zurückgebaut. Hintergrund dafür ist, dass Teile der bestehenden Hardware mittlerweile ihr End of Life (EoL) erreicht haben und deshalb ersetzt oder außer Betrieb genommen werden müssen.

Gerade bei solchen Arbeiten bekommt man einen interessanten Einblick in den Aufbau und die Zusammenhänge innerhalb eines Rechenzentrumsnetzwerks. Während ein Switch im laufenden Betrieb häufig als selbstverständlicher Bestandteil der Infrastruktur wahrgenommen wird, wird spätestens beim Austausch deutlich, wie viele Systeme, Verbindungen und Abhängigkeiten dahinterstecken. Bei der Arbeit im Rechenzentrum bin ich unweigerlich auch mit der Spine-Leaf-Architektur in Berührung gekommen. Begriffe wie Access-Leaf, Leaf oder Spine begegnen einem dort nicht nur auf Plänen und in Dokumentationen, sondern als tatsächliche Bestandteile der vorhandenen Infrastruktur. Dadurch habe ich angefangen, mich intensiver mit der Architektur dahinter zu beschäftigen: Welche Aufgabe übernehmen die einzelnen Switches eigentlich? Wie sind sie miteinander verbunden? Und warum wird gerade in Rechenzentren häufig auf eine solche Struktur gesetzt?

Hieraus ist die Idee für diesen Blog entstanden. Denn das grundlegende Prinzip einer Spine-Leaf-Architektur ist zunächst relativ einfach, bringt aber einige Eigenschaften mit sich, die besonders für moderne Rechenzentren interessant sind. Im Folgenden geht es deshalb darum, wie eine Spine-Leaf-Architektur aufgebaut ist, welche Vorteile sie bietet und in welchen Bereichen sie eingesetzt wird.

Aufbau einer Spine-Leaf-Architektur

Das grundlegende Prinzip hinter Spine-Leaf ist zunächst relativ einfach. Die Architektur besteht aus zwei Ebenen: der Spine- sowie der Leaf-Ebene.

Die Leaf-Switches bilden dabei die Ebene, an der beispielsweise Server, Storage-Systeme und weitere Komponenten des Rechenzentrums angebunden werden. Leaf-Switches stellen damit den Zugang zur eigentlichen Netzwerkstruktur bereit. Je nach Aufbau des Rechenzentrums können sich solche Switches direkt in oder in der Nähe der Server-Racks befinden.

Oberhalb der Leaf-Ebene befindet sich die Spine-Ebene. Die dort eingesetzten Spine-Switches bilden das leistungsfähige Rückgrat der Architektur und sorgen dafür, dass die verschiedenen Leaf-Switches miteinander kommunizieren können.

Der entscheidende Punkt liegt allerdings in der Verbindung dieser beiden Ebenen: Jeder Leaf-Switch wird mit jedem Spine-Switch verbunden. Ein Leaf besitzt somit nicht einen einzelnen Weg in das Netzwerk, sondern mehrere mögliche Verbindungen über die vorhandenen Spine-Switches.

Möchte ein Server an einem Leaf mit einem Server an einem anderen Leaf kommunizieren, führt der Weg über einen der Spine-Switches. Vereinfacht sieht der Datenweg damit folgendermaßen aus:

Sicherheit von Rechenzentren in geopolitisch angespannten Zeiten – wenn die reale Welt die IT einholt

von Dr. Markus Ermes



Sichere Rechenzentren – dabei denken wohl die meisten von uns an sichere Netzwerke, Firewalls, Intrusion-Detection-Systeme und Netzwerksegmentierung. Man denkt vielleicht auch noch an Zugangskontrollen, Cages bei Colocation-Anbietern und Schlössern an den Racks.

Aber immer wieder gibt es auch Meldungen über Schäden an Rechenzentren, bis hin zur Zerstörung der Rechenzentren. Waren es bisher eher Naturkatastrophen oder Unfälle, häufen sich die Meldungen aus Russland und Westasien, dass Rechenzentren gezielt angegriffen und so stark beschädigt werden, dass der Betrieb eingestellt wird und alle dort gespeicherten Daten verloren sind.

Ich möchte diesmal die Frage stellen: Können wir aus diesen Ereignissen etwas für unsere eigenen Rechenzentren und Dienste in der Cloud lernen? Dabei werden alte Bekannte aus der Welt der Redundanz eine Rolle spielen.

Wo liegen Gemeinsamkeiten?

Groß angelegte Angriffe auf Rechenzentren in Deutschland und Europa sind glücklicherweise sehr unwahrscheinlich, aber das grundlegende Problem bleibt: Was passiert, wenn ein komplettes Rechenzentrum ausfällt? Das ist die große Gemeinsamkeit.

Und hier möchte ich zwischen einem eigenen Rechenzentrum – auch ein Colocation-Anbieter gehört in diese Kategorie – und Cloud-basierten Diensten unterscheiden.

Die Sicherheit im eigenen Rechenzentrum

Das eigene Rechenzentrum ist meistens gut beherrscht. Es gibt eine Risiko-Analyse für die verschiedenen Szenarien, die zum vollständigen Ausfall führen können. Dazu gehören zum Beispiel:

- Ein Brand im Rechenzentrum
- Ein länger anhaltender Stromausfall
- Ausfall zentraler Systeme (meistens Storage)
- Malware-Infektion, insbesondere Ransomware

Je nachdem, wie lange ein möglicher Ausfall verkraftet werden kann, gibt es unterschiedliche Maßnahmen, die die Risiken mindern können, allen voran: Backup.

Das KI-native Unternehmen:
ein Praxisleitfaden für den Mittelstand

von Darav Taha



Viele Mittelständler probieren KI an einzelnen Stellen aus und bleiben im Pilotmodus stecken. Der Sprung zum KI-nativen Unternehmen gelingt, wenn KI zur Infrastruktur der Wertschöpfung wird und die IT die Daten sicher zugänglich macht. Dieser Leitfaden übersetzt Erkenntnisse aus dem Aufbau KI-nativer Firmen in einen pragmatischen Fahrplan für den Mittelstand.

Die meisten mittelständischen Unternehmen haben KI längst ausprobiert. Ein Team testet einen Chatbot, die Marketingabteilung erzeugt Texte, jemand lässt sich lange Dokumente zusammenfassen. Trotzdem bleibt das Gefühl, dass der große Nutzen ausbleibt. Die Werkzeuge liegen verstreut herum, jeder probiert für sich, und am eigentlichen Geschäft ändert sich wenig.

Die Mitarbeiter trifft daran keine Schuld. Die Ursache liegt in der Herangehensweise: KI wird an vorhandene Abläufe angehängt. Man nimmt einen bekannten Prozess und fragt, wo sich etwas mit KI ergänzen lässt. Diese Logik führt zu netten Vorführungen und kleinen Zeitgewinnen. Das Unternehmen verändert sie kaum.

KI-native Unternehmen gehen den umgekehrten Weg. Sie fragen zuerst, welche Aufgaben ohne KI strukturell teuer und langsam sind, und bauen ihre Wertschöpfung um diese Antworten herum. Dort ist KI Teil der Infrastruktur, so selbstverständlich wie Strom oder das Netzwerk.

Dieser Leitfaden zeigt, wie der Mittelstand diesen Schritt geht. Er stützt sich auf aktuelle Erkenntnisse aus dem Aufbau KI-nativer Firmen und überträgt sie auf die Realität gewachsener Unternehmen mit bestehender IT, begrenzten Ressourcen und hohen Anforderungen an Datenschutz und Sicherheit. Eine Vorbemerkung vorweg: Der Startpunkt darf klein sein. Wer heute mit verstreuten Experimenten arbeitet, hat alles, was es für den Anfang braucht. Es geht um eine klare Reihenfolge und um wenige, gut gewählte Entscheidungen.

Was KI-nativ für den Mittelstand bedeutet

Ein KI-natives Unternehmen setzt KI als feste Schicht seiner Wertschöpfung ein. Aufgaben werden von vornherein so gestaltet, dass KI sie übernimmt oder unterstützt. Die Menschen kümmern sich um Urteil, Beziehungen und Entscheidungen. Das Ziel ist mehr Wirkung je Mitarbeiter. Ein kleines Team erbringt damit Leistungen, für die früher eine ganze Abteilung nötig war.

Drei Fähigkeiten machen KI heute im Unternehmen nutzbar. Erstens steht Wissen auf Abruf bereit: KI durchsucht in Sekunden technische Normen, alte Projektunterlagen oder einen Liefervertrag und fasst das Wesentliche zusammen. Zweitens erledigt KI Aufgaben eigenständig, etwa einen ersten Angebotsentwurf oder die Aufbereitung von Messwerten aus der Produktion. Drittens automatisiert sie wiederkehrende Abläufe, zum Beispiel die wöchentliche Auswertung der Auftragslage oder die Pflege von Artikelstammdaten. Diese drei Fähigkeiten zusammen lassen ein kleines Team arbeiten wie eine deutlich größere Mannschaft.

Für die IT und den CIO verändert das die Rolle grundlegend. Drei Aufgaben rücken in den Mittelpunkt, bewusst in dieser Reihenfolge.