

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG | Ausgabe-Nr.: 204



DER PREIS DER KI

Was Geschäftsführer jetzt über künftige Kostentreiber
der künstlichen Intelligenz wissen müssen

DIGITAL SOVEREIGNTY

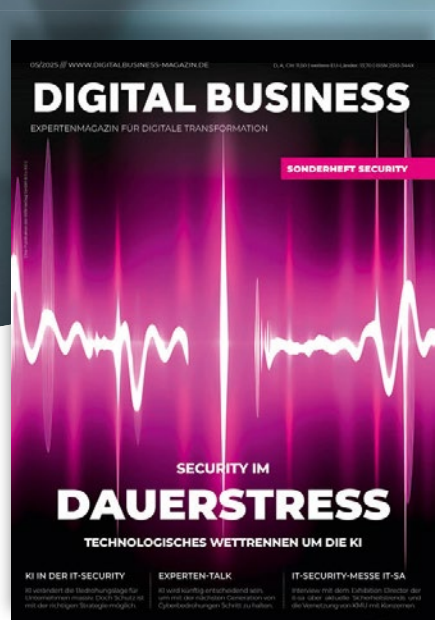
Mit klarer Architektur und Partnern gewinnen Unternehmen mehr Kontrolle über Daten und Cloud-Strukturen.

WORK & PEOPLE

Rund 6,5 Millionen Babyboomer gehen bis 2030 in Rente – und nehmen viel Wissen mit. Die Lösung heißt KI.

TECH & FUTURE SYSTEMS

Für KMU wird „Krypto-Agilität“ von der Theorie zur harten Anforderung für den Marktzugang.



Hier geht's zur aktuellen Ausgabe



Die nächste Ausgabe

Sonderheft Security

erscheint am 17. September 2026

Wer sich mit IT-Security beschäftigt – gleich ob für Produktion, Industrie oder Online-Handel – kommt an diesem Sonderheft nicht vorbei

EDITORIAL

Liebe Leserin, lieber Leser

- erinnern Sie sich an die Aufbruchstimmung vor zwei, drei Jahren? Damals schien künstliche Intelligenz wie eine unerschöpfliche Ressource aus der Steckdose: skalierbar, ubiquitär und vor allem – billig. Wir haben experimentiert, Prompts geschrieben und Copiloten implementiert. Doch im Juli 2026 ist die Schonfrist für Experimente abgelaufen. Wer heute die IT-Budgets plant, merkt: Die Rechnung für die Intelligenz wird neu geschrieben. Maschinelles Denken ist im Sommer 2026 zu einem variablen, teuren Produktionsfaktor geworden. Die Ära der „Gratis-Mentalität“ ist vorbei – willkommen in der KI-Ökonomie.

Vom Software-Hype zum harten Infrastruktur-Engpass

Unser Titelthema „Der Preis der KI“ beleuchtet eine Entwicklung, die viele Geschäftsführer kalt erwischt. Der weltweite Boom stößt an physische Grenzen: Strommangel, blockierte Rechenzentren in den USA und steigende Kosten für die neue „Frontier-Klasse“ wie Claude Fable 5 verwandeln KI in einen knallharten Engpassmarkt. Für den Mittelstand bedeutet das: KI ist kein planbarer Fixkostenblock mehr, sondern ein dynamischer Kostenfaktor, der bei falscher Steuerung direkt an der Marge frisst. Besonders die neuen, autonomen Agenten agieren nicht mehr als bloße Werkzeuge, sondern als „digitale Mitarbeiter“, deren Denkschleifen die Kosten in Echtzeit vervielfachen können.



Die neue Management-Maxime: Orchestrierung statt Gießkanne

Die Lösung liegt nicht im Verzicht, sondern in der aktiven Steuerung. Eine zentrale Erkenntnis dieser Ausgabe lautet: „Das stärkste Modell sollte am wenigsten arbeiten.“ CIOs müssen heute eine Infrastruktur schaffen, die Aufgaben intelligent verteilt. Manuel Haug von Celonis zeigt auf, dass Kontextmodelle hierbei zum entscheidenden Hebel werden: Nur wer der KI beibringt, das eigene Unternehmen zu verstehen, senkt den Token-Verbrauch und sichert den ROI.

Dass der Weg vom Labor in die Produktion dennoch steinig bleibt, bestätigt unser Experten-Talk: Während die Logistik mit Modulen wie „Batch AI“ bereits messbare Produktivitätssprünge feiert, dümpeln viele Projekte noch als riskante „Schatten-KI“ vor sich hin. Arkadiusz Krowczynski warnt eindringlich: Ohne zentrales Identitätsmanagement werden autonome Agenten zur tickenden Zeitbombe für die IT-Sicherheit. •

Ich wünsche Ihnen eine erkenntnisreiche Lektüre und den Mut zu wirtschaftlich nachhaltigen Entscheidungen!

Ihr

HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS

heiner.sieger@win-verlag.de



BUSINESS TECHNOLOGY & INNOVATION

- 20 **Unterschätzt, aber unverzichtbar**
Warum das klassische Modell der Application Management Services neu gedacht werden muss und wie das gelingt.



TECH & FUTURE SYSTEMS

- 30 **Krypto-Agilität: Pflicht für Zulieferer**
Ende der Schonfrist. Zwei Jahre nach den finalen NIST-Standards für PQC drängen BSI und Konzerne auf Umsetzung.

06

Titelstory / Der Preis der KI

Effizienz wird zur umfassenden Unternehmensaufgabe: Was Geschäftsführer jetzt über die künftigen Kostentreiber der künstlichen Intelligenz wissen müssen.

AI



DIGITAL SOVEREIGNTY

- 52 **Das passende Rechenzentrum finden**
Colocation hilft dem Mittelstand, steigende Anforderungen an die IT zu erfüllen. Eine Checkliste für Geschäftsführer.



SECURITY INSIGHT

- 34 **Handeln, bevor es brennt:**
Eine Molkerei macht sich cyberfest
- 36 **Experten-Talk:**
Security-Strategien im Zuge der EU-Regulierungswelle
- 39 **Fünf Warnzeichen, bei denen Infrastruktur zum Risiko wird**



DIGITAL HEALTH

- 48 Vom Patienten- zum Versorgungsportal
Leistungsgruppen, Fachkräftemangel,
Kostendruck: Die strategische Infrastruktur für
Krankenhäuser muss neu gedacht werden.

KI & INTELLIGENT ENTERPRISE

- 06 Warum Kontextmodelle zum
Erfolgs- und Kostenfaktor bei Unternehmens-
KI werden
08 Warnsignale aus den USA:
Ist der KI-Boom vorbei?
10 Der neue Preis der Intelligenz:
Warum Orchestrierung jetzt Chefsache ist
12 Identitätssicherheit ermöglicht den zuverlässigen
Einsatz von KI-Agenten
14 Proof of Concept, und dann?
Der Mittelstand und seine KI-Wahrheit
18 Automatisierte Systeme:
KI wird im E-Mail-Marketing zum Erfolgsfaktor

BUSINESS TECHNOLOGY & INNOVATION

- 20 Unterschätzt, aber unverzichtbar:
Application Management Services im
Cloud-Zeitalter
22 Das ERP als Prozesslandkarte
für KI und Mensch
24 Messbar höhere Prozesseffizienz
26 Vom schönen Scheitern:
KI im Enterprise-Stack
28 Strategien für intelligentes
Content Management

TECH & FUTURE SYSTEMS

- 30 Krypto-Agilität: Pflicht für Zulieferer

NEWS

- 32 Frisch ausgepackt

DIGITAL BUSINESS

04 2026

CYBER RISK & RESILIENCE

- 33 Titel
34 Handeln, bevor es brennt:
Eine Molkerei macht sich cyberfest
36 Experten-Talk:
Security-Strategien im Zuge der EU-
Regulierungswelle
39 Fünf Warnzeichen, bei denen Infrastruktur
zum Risiko wird

QUANTENCOMPUTING

- 40 Vorschau zur Quantum Effects:
Sollten KMU schon jetzt in Quantentechnologien
investieren oder erst 2030?

WORK & PEOPLE

- 42 Effiziente HR Automation für KMU
44 Unternehmensdemenz:
Wie KI das Erfahrungswissen rettet

SUSTAINABILITY & IMPACT

- 46 KI-Energieverbrauch:
Effizienz wird zur Unternehmensaufgabe

DIGITAL HEALTH

- 48 Vom Patientenportal zum Versorgungsportal
50 Mit KI-Agenten zu optimierten und
vernetzten Prozessen

DIGITAL SOVEREIGNTY

- 52 Wahl des Rechenzentrums:
Checkliste für die Geschäftsführung
54 Raus aus der Hyperscaler-Falle
56 Souveräne KI für Europa
58 Erhalt der Handlungsfähigkeit

LEGAL & COMPLIANCE

- 60 Die lange Suche nach einem
Datenschutz-Siegel

- 03 Editorial
61 Marketplace
62 Vorschau
62 Impressum

Warum Kontextmodelle zum Erfolgs- und Kostenfaktor bei Unternehmens-KI werden

Der Einsatz agentischer KI treibt die Kosten in die Höhe. Kontextmodelle helfen, KI-Systeme effizienter zu steuern, validere Ergebnisse zu erzielen, den Token-Verbrauch zu senken und Enterprise AI so wirtschaftlicher zu machen. /// von Manuel Haug



DER AUTOR
Manuel Haug Field CTO, Celonis.

„ Der reale Ressourcenverbrauch rückt in den Fokus der Kostenbetrachtung und Unternehmen stehen **plötzlich vor einer neuen Herausforderung**: Die Ausgaben für KI-Anwendungen entwickeln sich von klassischen, planbaren Fixkosten zu dynamischen Nutzungskosten. *Manuel Haug*

IN VIELEN UNTERNEHMEN IST DERZEIT EINE NEUE ART DES FEILSCHENS ZU BEOBACHTEN. Dabei geht es jedoch nicht um Panini-Bilder, sondern um Tokens: Wer hat noch Budget übrig, wer kann wie viel abgeben? Entwickler diskutieren darüber, wie sich Prompts optimieren lassen, welches Modell effizienter arbeitet oder warum bestimmte KI-Anfragen besonders ressourcenintensiv sind. Das Ziel: möglichst viel aus jedem Token herauszuholen.

Was zunächst nach technischen Spielereien klingen mag, entwickelt sich zunehmend zu einer Managementfrage von wachsender betriebswirtschaftlicher Tragweite. Tokens sind die kleinsten Texteinheiten, in die Sprachmodelle (Large Language Models, LLMs) Eingabetexte zerlegen, um Anfragen verarbeiten zu können. Dabei kann es sich je nach Modell um Wörter, Wortbestandteile, Silben oder Zeichenkombinationen handeln. Je umfangreicher eine Anfrage und je mehr Kontext berücksichtigt werden muss, desto höher der Token-Verbrauch. Dass das Thema derzeit stark an Bedeutung gewinnt, liegt an einer grundlegenden Veränderung der KI-Nutzung: Kam generative

KI bislang meist in Form von Chatbots oder Copiloten zum Einsatz, treten mittlerweile agentische KI-Systeme in den Vordergrund. KI-Agenten sind in der Lage, Aufgaben autonom auszuführen, Entscheidungen vorzubereiten und komplexe Prozesse zu koordinieren. Dabei interagieren sie untereinander und lösen eigenständig Folgeprozesse aus. Damit verändern sich auch die Anforderungen an die zugrundeliegende Infrastruktur. Denn im Vergleich zu klassischen Copiloten reagieren KI-Agenten nicht nur auf einzelne Eingaben, sondern bearbeiten Aufgaben in mehreren Schritten, greifen auf unterschiedliche Informationen zu und berücksichtigen zusätzliche Zusammenhänge. Dafür brauchen sie deutlich mehr Rechenkapazitäten, und das erhöht den Token-Verbrauch erheblich.

KI-Nutzung wächst, Kostenfrage wird lauter

Die Anbieterseite bekommt die zunehmenden Aktivitäten agentischer KI in Form eines massiv gestiegenen Anfragevolumens zu spüren. Dieses bringt die zugrundeliegende Infrastruktur an ihre Belastungsgrenzen und führte in der

Vergangenheit bereits zu Ausfällen und eingeschränkter Verfügbarkeit. In der Folge passen viele KI-Anbieter ihre Preisstrukturen an und ersetzen günstige Flatrate-Abonnements durch Abrechnungsmodelle, die die tatsächliche Belastung widerspiegeln sollen.

Diese Entwicklungen fallen in eine Phase, in der die Nutzung von Unternehmens-KI ohnehin stark wächst: Laut einer Studie des Instituts für Arbeitsmarkt- und Berufsforschung (IAB) nutzte 2025 bereits jedes vierte Unternehmen in Deutschland generative KI. Das waren fünfmal mehr als noch 2023. Bei weiteren neun Prozent ist der Einsatz schon in Planung.

Was in der Experimentierphase vieler Unternehmen oft kaum ins Gewicht fiel, kann bei breiter Nutzung daher schnell zum relevanten Kostenfaktor werden. Der reale Ressourcenverbrauch rückt in den Fokus der Kostenbetrachtung und Unternehmen stehen plötzlich vor einer neuen Herausforderung: Die Ausgaben für KI-Anwendungen entwickeln sich von klassischen, planbaren Fixkosten zu dynamischen Nutzungskosten. Ein Abrücken von den eigenen KI-Initiativen ist für die meisten keine realistische Option. Laut dem Process Optimization Report 2026 sehen 86 Prozent der Führungskräfte in der DACH-Region KI als wichtigsten Faktor, um wettbewerbsfähig zu bleiben. Gleichzeitig wollen 85 Prozent der Unternehmen innerhalb der nächsten zwei bis drei Jahre zu sogenannten „agentischen Unternehmen“ werden. Konkret bedeutet das: Sie wollen Produktivität und Innovation durch die gezielte Automatisierung mit KI-Agenten steigern. Vor diesem Hintergrund stellt sich zunehmend die Frage, wie Unternehmen den KI-Einsatz wirtschaftlich steuern und skalieren können.

Warum KI-Agenten Geschäftskontext brauchen

Der Schlüssel dazu liegt im Kontext, wie sich besonders bei agentischen Systemen zeigt. Um im Unternehmensumfeld relevante und korrekte Ergebnisse zu liefern, müssen KI-Agenten verstehen, wie ein Unternehmen tatsächlich funktioniert: welche Prozesse existieren, welche Regeln gelten und welche Entscheidungen operativ sinnvoll sind. Fehlen diese Informationen, arbeiten KI-Agenten ineffizient. Sie durchsuchen unnötig große Datenmengen, formulieren umfangreiche Anfragen und liefern häufiger Ergebnisse, die überprüft oder korrigiert werden müssen. All diese Arbeitsschritte verbrauchen zusätzliche Tokens.

Dass Unternehmen diese Problematik erkennen, lässt sich ebenfalls anhand von Zahlen aus dem Process Optimization Report belegen: Acht von zehn Befragten erwarten, dass KI ohne Verständnis des Unternehmenskontexts keinen nachhaltigen Return on Investment liefern wird. Zudem zählt die Schwierigkeit, KI ausreichenden Unternehmenskontext bereitzustellen, zu den größten Herausforderungen beim Einsatz von Enterprise AI. Genau an dieser Stelle setzen Kontextmodelle an.

Wie Kontextmodelle KI-Agenten effizienter machen

Kontextmodelle schaffen eine zusätzliche Ebene zwischen Unternehmensdaten und KI-Modellen. Sie verbinden Pro-

zessdaten, Unternehmenswissen und operative Entscheidungslogik miteinander und stellen strukturierte Informationen für KI-Systeme bereit.

So ermöglichen sie es KI-Agenten, ein besseres Verständnis dafür zu entwickeln, wie Prozesse, Daten und Entscheidungen in einem Unternehmen zusammenhängen. Gleichzeitig können Kontextmodelle dazu beitragen, den Ressourcenverbrauch von KI-Anwendungen zu reduzieren.

Als intelligente Vermittlungsschicht zwischen Unternehmensdaten und Large Language Models sorgen sie dafür, dass nur relevante Informationen verarbeitet werden. So präzisiert ein Kontextmodell beispielsweise die Datenextraktion und übermittelt nur die Informationen an das LLM, die für die konkrete Aufgabe tatsächlich benötigt werden. Dadurch kann sich die Menge der Input-Daten deutlich reduzieren. Da Kontextmodelle Prozesszusammenhänge verstehen, können sie außerdem doppelte oder unnötige Informationen herausfiltern, bevor eine Anfrage an ein Sprachmodell gesendet wird. Gleichzeitig muss die zugrundeliegende Prozesslogik nicht bei jeder Anfrage erneut ausführlich beschrieben werden, weil sie bereits strukturiert im Kontextmodell hinterlegt ist. Prompts können so verkürzt werden. Auch der Informationsabruf wird gezielter: Statt große Datenmengen oder Dokumente unspezifisch zu durchsuchen, erhält die KI genau die Informationen, die sie zur Bearbeitung einer Anfrage benötigt. Das kann nicht nur den Ressourcenverbrauch senken, sondern auch die Qualität der Ergebnisse verbessern. Wenn KI-Systeme zielgerichteter arbeiten, sinkt außerdem der Aufwand für zusätzliche Prüf- und Korrekturschleifen.

Kontext als Steuerungsebene für Enterprise AI

Kontextmodelle übernehmen damit zunehmend die Rolle einer Steuerungsebene für Enterprise AI. Sie helfen KI-Agenten, sich innerhalb komplexer Unternehmensprozesse zu orientieren und effizienter zu arbeiten.

Der Vergleich mit einem Navigationssystem liegt nahe: Ohne Orientierung müssen KI-Agenten ihren Weg selbst durch Daten, Prozesse und Entscheidungen finden. Mit zusätzlichem Geschäftskontext erhalten sie dagegen eine strukturierte Grundlage, um schneller zum gewünschten Ergebnis zu gelangen.

Die Diskussion um Enterprise AI dürfte sich deshalb in den kommenden Jahren weiter verschieben. Stand bislang vor allem die Leistungsfähigkeit der Modelle im Mittelpunkt, wird es künftig stärker um ihre effiziente Nutzung gehen.

Kontextmodelle werden dabei eine wichtige Rolle spielen. Denn je stärker Unternehmen agentische KI in ihre operativen Abläufe integrieren, desto wichtiger wird die Fähigkeit, KI-Systemen den richtigen Geschäftskontext bereitzustellen – nicht nur für bessere Ergebnisse, sondern auch für einen wirtschaftlichen KI-Einsatz. •

Warnsignale aus den USA: Ist der KI-Boom vorbei?

Der KI-Boom galt als grenzenlos. Jetzt bremsen ihn Strommangel, Bürgerproteste und Politik. Der Anfang vom Ende der billigen KI. Warum das den Mittelstand härter trifft als Big Tech. /// von Heiner Sieger

SEIT EINIGEN JAHREN KANNT DER KI-BOOM NUR EINE RICHTUNG: nach oben. Mehr Modelle, mehr Rechenzentren, mehr Kapital. Grenzen schienen ein technisches Problem, das sich mit Geld lösen lässt. Dieser Glaube wird jetzt erschüttert – ausgerechnet in den USA.

Dort hat das Forschungsunternehmen Data Center Watch berechnet, dass binnen etwas mehr als einem Jahr Rechenzentren im Wert von über 60 Milliarden Dollar verzögert oder ganz gestoppt wurden – blockiert durch Bürgerproteste, lokale Auflagen und erste politische Moratorien. Ein Bloomberg-Bericht kommt zu dem Schluss, dass rund die Hälfte der für 2026 geplanten US-Rechenzentren verspätet oder gestrichen wird.

Daleep Singh, Chefvolkswirt von PGIM, dem Vermögensverwalter des US-Finanzkonzerns Prudential Financial warnt in seiner aktuellen Analyse und nennt noch höhere Zahlen: „Wir betrachten aktuelle eine Gegenreaktion gegen KI als das vielleicht am meisten unterschätzte Risiko. Tatsächlich lehnen mehr als 70 Prozent der Amerikaner, die kürzlich im Rahmen einer Gallup-Umfrage befragt wurden, den Bau eines Rechenzentrums in ihrer Gemeinde ab. Allein im ersten Quartal 2026 wurden Rechenzentrumsprojekte im Wert von 130 Mrd. US-Dollar blockiert oder auf Eis gelegt.“

Der Boom endet damit nicht unbedingt. Aber er verliert, was ihn bislang ausmacht: sein Tempo. Genau das verändert die Rechnung für jedes Unternehmen, das gerade sein Geschäftsmodell auf KI ausrichtet.

Der Denkfehler: KI ist kein Softwaremarkt

Wer KI plant, denkt meist in Software: skalierbar, flexibel, jederzeit verfügbar. Das ist der entscheidende Irrtum. KI ist Infrastruktur. Hinter jedem Modell stehen Serverhallen, Stromleitungen, Kühlwasser. Und diese Grundlage lässt sich nicht per Update verdoppeln.

Die Zahlen zeigen die Dimension. Rechenzentren verbrauchen in Deutschland bereits rund 21 Terawattstunden Strom pro Jahr – etwa vier Prozent des gesamten Verbrauchs. In Frankfurt, dem wichtigsten Standort Europas,

stößt das Netz schon heute an Grenzen. Weltweit rechnet die Internationale Energieagentur (IEA) bis 2030 mit bis zu 900 Terawattstunden.

Fatih Birol, Direktor der IEA, fasst es nüchtern zusammen: „Der Stromverbrauch von Rechenzentren, KI und Kryptowährungen könnte sich bis 2030 mehr als verdoppeln.“ Die Konsequenz daraus ist unbequem: Der Engpass der KI liegt nicht im Code. Er liegt im Stromnetz.

USA: Der Moment, in dem der Markt dreht

Was passiert, wenn diese Grenze erreicht ist, lässt sich derzeit in den USA studieren: Der Bundesstaat Maine hat als erster ein echtes Moratorium verhängt: Neue Rechenzentren über 20 Megawatt sind bis November 2027 gestoppt, bis ein Expertenrat die Folgen für Umwelt und Versorgung geprüft hat. New York arbeitet an einem dreijährigen Bausperr. Mindestens ein Dutzend weiterer Bundesstaaten prüft ähnliche Schritte – getragen von Demokraten und Republikanern gleichermaßen. Bemerkenswert ist die Breite der Allianz. Als Senator Bernie Sanders im Dezember 2025 ein landesweites Moratorium forderte, stützte er sich auf einen Brief von rund 200 Umweltorganisationen. Seine Begründung: „Wir müssen den unkontrollierten Ausbau energieintensiver KI-Infrastruktur stoppen.“

Hinzu kommt ein zweiter, oft übersehener Engpass: Selbst genehmigte Projekte scheitern an fehlenden Transformatoren, Schaltanlagen und Netzkapazitäten. Der Widerstand von unten trifft auf Materialmangel von oben. Was hier entsteht, ist ein Muster. Nicht die Nachfrage bremst den Markt, sondern seine äußeren Grenzen. Das ist eine andere Qualität von Risiko – eine, gegen die auch viel Kapital wenig ausrichtet.

Europa: Warum es hier genauso kommt

Europa wirkt stabiler. Doch das ist eine Momentaufnahme, kein Naturgesetz. Die strukturellen Bedingungen sind dieselben – und teils schwieriger: höhere Strompreise, strengere Regulierung, langsamere Genehmigungen. Was in den USA sichtbar wird, ist für Europa kein Sonderfall, sondern ein Vorlauf. Die Wirtschaft reagiert erwartbar. Ralf Wintergerst,

„Nicht mehr Innovation steuert den Zugang, sondern der Preis. Wer zahlen kann, bekommt Kapazität. Wer nicht, wartet. Das ist die stille Verschiebung hinter den Schlagzeilen aus den USA. Nicht das Ende der KI. Sondern **das Ende der billigen KI.**“

Heiner Sieger

Präsident des Digitalverbands Bitkom, warnt: „Ohne leistungsfähige Rechenzentren wird Deutschland seine digitale Souveränität nicht sichern können.“ Der Bundesverband der Deutschen Industrie sieht KI als Schlüssel für Wettbewerbsfähigkeit. Gegen diese Wachstumslogik formiert sich bereits Widerstand. Die Organisation AlgorithmWatch hält fest: „Der Ausbau von Rechenzentren für KI steht im direkten Spannungsfeld zu Klima- und Ressourcenzielen.“

Dass daraus mehr werden kann als eine Fachdebatte, zeigt der Blick auf ein grundsätzliches Muster. Der US-Autor Nicholas Carr, früher Executive Editor der Harvard Business Review und Autor von „The Shallows“, beschreibt es so: „Technologien setzen sich nicht allein wegen ihrer Effizienz durch – sie müssen auch gesellschaftlich akzeptiert werden.“ Genau hier liegt der Punkt: In Deutschland konkurrieren Rechenzentren nicht nur mit Klimazielen, sondern mit dem Strombedarf von Industrie, Wärmepumpen und Elektromobilität. Wird Strom knapp, wird die Frage politisch. Dann folgt unausweichlich der Widerstand – so wie in den USA.

Die eigentliche Antwort: Das Ende der billigen KI

Die Entwicklung deckt auf, was sich aktuell tut: Der KI-Markt wechselt die Vorzeichen. Solange Rechenleistung im Überfluss verfügbar war, sank ihr Preis – und mit ihm die Schwelle, KI überall einzusetzen. Sobald der Ausbau langsamer wächst als die Nachfrage, dreht sich diese Logik um. Aus einem Wachstumsmarkt wird ein Engpassmarkt. Und in Engpassmärkten gelten andere Regeln: Nicht mehr Innovation steuert den Zugang, sondern der Preis. Wer zahlen kann, bekommt Kapazität. Wer nicht, wartet. Das ist die stille Verschiebung hinter den Schlagzeilen aus den USA. Nicht das Ende der KI. Sondern das Ende der billigen KI.

Warum das den Mittelstand härter trifft als Big Tech

Genau an dieser Gabelung trennen sich die Wege. Große Konzerne bauen eigene Rechenzentren, sichern sich langfristig Strom und verhandeln Kapazitäten direkt. Amazon, Microsoft und Google investieren dreistellige Milliardenbeträge – sie gestalten den Engpass mit. Für alle die von Ihnen abhängig sind. Stichwort: Digitale Souveränität. Siehe deutscher Mittelstand. Er bezieht KI als Dienstleistung über Cloud-Plattformen, meist von den genannten US-Anbietern. Das schafft zwar Flexibilität – aber eine gefährliche Abhängigkeit. Denn wenn Kapazität knapp wird, bedienen Anbieter zuerst ihre größten Kunden.

DER AUTOR

Heiner Sieger

ist Chefredakteur des Magazins Digital Business.

Die Folgen sind konkret und operativ:

- Kundenservice und Vertrieb: Chatbots, automatisierte Angebote, Lead-Generierung laufen dauerhaft über externe Modelle. Steigen deren Preise, steigen sofort die laufenden Kosten – nicht einmalig, sondern in jedem Prozessschritt.
- Marketing und Content: Personalisierung und automatisierte Kampagnen rechnen sich nur, solange Rechenleistung günstig ist. Kippt der Preis, kippt der Business Case.
- Produktion und Logistik: KI in Wartung, Planung und Qualitätskontrolle arbeitet in Echtzeit. Wird Kapazität teurer oder unzuverlässig, trifft das direkt die Marge.

Daron Acemoglu, Ökonom am Massachusetts Institute of Technology (MIT), legt den Finger in die Wunde: „Der wirtschaftliche Nutzen von KI wird oft überschätzt, während ihre sozialen Kosten unterschätzt werden.“ Für den Mittelstand heißt das übersetzt: Wer seinen Business Case allein auf günstige KI baut, kalkuliert mit einer Variable, die er nicht selber kontrolliert. Und eigene Kontrolle gehörte immer zu den Erfolgsfaktoren des Mittelstands.

Quintessenz

Nein, der KI-Boom ist nicht vorbei. Aber der Glaube an seine Grenzenlosigkeit bekommt Risse. Er wächst nicht mehr entlang dessen, was technisch möglich ist. Sondern er stößt an Grenzen entlang dessen, was Energie, Infrastruktur und Gesellschaft zulassen. Die Warnsignale aus den USA sind kein amerikanisches Phänomen – sie sind ein Blick in die europäische Zukunft. •



Der neue Preis der Intelligenz: Warum Orchestrierung jetzt Chefsache ist

Der Sommer 2026 ist eine Zäsur. Mit Frontier-Modellen wie Claude Fable 5 wird maschinelles Denken zum variablen, teuren Produktionsfaktor. Für Entscheider heißt das: Die Gefahr liegt in ungesteuerten autonomen Agenten, die Kosten und Risiken in Echtzeit vervielfachen. Aktive Steuerung wird zur Überlebensfrage für die IT.
/// von Heiner Sieger

DIE ZEIT, IN DER SICH KI-KOSTEN ÜBER EINE HANDVOLL PAUSCHALER CHATGPT-PLUS-LIZENZEN in der Schatten-IT abwickeln ließen, ist vorbei. Sie fühlt sich im Juli 2026 bereits wie eine längst vergangene Epoche an. Die Geschwindigkeit der technologischen Entwicklung hat die ökonomischen Spielregeln nicht über Jahre, sondern zuletzt in wenigen Wochen pulverisiert.

Die Integration generativer KI in die Kernprozesse – von der automatisierten Lieferkettenanalyse bis zum autonomen Kundendienst – ist Realität. Doch mit der enormen Leistungsfähigkeit der neuesten Modelle ist auch die Komplexität ihrer Steuerung explodiert.

Das Strategiepapier eines führenden KI-Anbieters brachte es diesen Monat auf den Punkt: Die Einführung der neuesten Modellgeneration ist keine reine Technologieentscheidung mehr; sie verändert das Risikoprofil und die Kostenstruktur des gesamten Unternehmens fundamental.

Vom Werkzeug zum autonomen Akteur

Um diese neue Kostendynamik zu verstehen, müssen Entscheider den Blick vom reinen „Token-Preis“ (der Abrechnungseinheit für Textbausteine) auf das „Geschäftsergebnis“ lenken. Ältere Modelle waren Werkzeuge: Man gab einen Input hinein, erhielt einen Output und zahlte dafür. Die neuen „agentischen“ Systeme, angeführt von

Spitzenmodellen wie Claude Fable 5, agieren dagegen als autonome Mitarbeiter. Sie lesen nicht nur; sie planen, nutzen externe Software-Tools, prüfen ihre eigenen Ergebnisse, korrigieren sich und starten neue Versuche.

Diese Autonomie ist der entscheidende neue Kostentreiber. Ein unkontrollierter Agent kann für eine komplexe Aufgabe Tausende von Zwischenschritten generieren. Die Kosten entstehen nicht mehr nur durch das Lesen und Schreiben, sondern durch das „Denken“ in Schleifen. Intelligenz wird zum variablen Input der Wertschöpfung – vergleichbar mit Cloud-Computing-Kapazität, aber ungleich schwerer vorherzusagen.

Die neue Vier-Klassen-Gesellschaft

Der Markt spiegelt diese neue Realität Mitte 2026 radikal wider. Die Preisspanne zwischen einem einfachen Basis-Modell und der absoluten Spitzenklasse ist gigantisch geworden (siehe Tabelle). Die neuen Flaggschiffe, sogenannte „Frontier-Modelle“, sind für Aufgaben konzipiert, die tiefe logische Schlussfolgerungen, langfristige Planung und agentisches Handeln erfordern. Sie sind die „Formel 1“ der KI – extrem leistungsfähig, aber exorbitant teuer im Betrieb und geopolitisch sensibel, wie kurzfristige staatliche Zugangsbeschränkungen in den USA jüngst zeigten. Darunter etabliert sich eine breite Schicht von effizienten Arbeitsmodellen für den Alltag.

PREIS-EXPLOSION AN DER SPITZE: DIE HIERARCHIE 2026

Die Preise für KI-APIs werden international pro 1 Million Tokens (1M) in US-Dollar abgerechnet. Die Einführung der neuen Frontier-Klasse hat die Spreizung extrem vergrößert. (Stand: Juli 2026, basierend auf aktuellen Anbieterdaten).

Modellklasse	Beispiel (Stand 07/26)	Input-Preis (pro 1M Tokens)	Output-Preis (pro 1M Tokens)	Faktor (Input Sonnet vs. Output Frontier)
Frontier / Agentic	Claude Fable 5	\$ 10,00	\$ 50,00	25 x teurer
High-End	Claude Opus 4.8, GPT-4-Turbo-Nachf.	~ \$ 5,00	~ \$ 25,00	12,5 x teurer
Mid-Range	Claude Sonnet 5	~ \$ 2,00	~ \$ 10,00	Basis-Referenz
Efficiency	Claude Haiku 3.5, Mistral NeMo	< \$ 1,00	< \$ 3,00	Sehr günstig

DER AUTOR

Heiner Sieger ist Chefredakteur des Magazins Digital Business. Der Beitrag wurde mit Unterstützung unseres KI-Assistenten erstellt.

„Die neuen Flaggschiffe, sogenannte „Frontier-Modelle“, sind für Aufgaben konzipiert, die tiefe logische Schlussfolgerungen, langfristige Planung und agentisches Handeln erfordern. Sie sind die **„Formel 1“ der KI** – extrem leistungsfähig, aber exorbitant teuer im Betrieb und geopolitisch sensibel.

Heiner Sieger

Die neue Management-Maxime: Orchestrierung

Angesichts dieser Preisstruktur (50 Dollar für eine Million Output-Tokens in der Spitze!) wird eine alte IT-Weisheit zur überlebenswichtigen Management-Regel: **Das stärkste Modell sollte am wenigsten arbeiten.**

Der betriebswirtschaftliche Imperativ lautet „Routing“ oder „Orchestrierung“. Es ist die Aufgabe des CIOs, eine technische Infrastruktur zu schaffen, die Aufgaben intelligent verteilt. Nicht jeder Mitarbeiter und nicht jeder Prozessschritt benötigt die „Formel 1“.

Ein modernes KI-System im Mittelstand gleicht 2026 eher einer professionellen Organisation als einem einzelnen Software-Tool:

- **Die „Praktikanten“ (Efficiency-Modelle):** Übernehmen schnelle Klassifikationen, Datenextraktion und Vorfilterung.
- **Die „Sachbearbeiter“ (Mid-Range/High-End):** Erledigen den Großteil der Analyse, Recherche und Entwurfserstellung.
- **Die „Chef-Strategen“ (Frontier-Modelle):** Werden nur für kritische Entscheidungspunkte, finale Qualitätskontrollen bei hohen Risiken oder komplexe Planungsaufgaben hinzugezogen – oft nur für fünf Prozent des gesamten Prozessablaufs.

Szenario 2026: Die Kosten der Autonomie

Ein konkretes Rechenbeispiel verdeutlicht die Gefahr ungesteuerter Agenten. Ein mittelständischer Maschinenbauer möchte eine automatisierte Risikoanalyse seiner 50 wichtigsten Lieferanten durchführen, basierend auf aktuellen Nachrichten und Finanzberichten.

- **Der ungesteuerte Ansatz („Viel hilft viel“):** Man setzt einen autonomen Agenten auf Basis von Claude Fable 5 darauf an, ohne Einschränkungen. Der Agent liest Unmengen an Daten, ruft Dutzende Such-Tools auf, verfängt sich in irrelevanten Details und schreibt lange Zwischenberichte.

- Die Rechnung: Aufgrund der extremen Preise und der vielen autonomen Schleifen können pro Lieferant schnell 15 bis 20 Euro an reinen API-Kosten auflaufen. Bei 50 Lieferanten sind das **1.000 Euro** für einen einzigen Report-Lauf – regulatorische Risiken der Datenerhaltung bei Frontier-Modellen noch nicht eingerechnet.
- **Der orchestrierte Ansatz („Routing“):** Ein günstiges Modell übernimmt die Recherche und Filterung der Nachrichten. Ein Mittelklasse-Modell fasst die Fakten zusammen. Nur die finale Bewertung des Gesamtrisikos wird an das Frontier-Modell übergeben, und das auch nur bei Unklarheiten.
- Die Rechnung: Die teuerste Intelligenz wird nur punktuell genutzt. Die Kosten pro Lieferant sinken auf unter zwei Euro. Gesamtkosten: **ca. 100 Euro**

FAZIT & CHECKLISTE FÜR DEN CIO (Stand Juli 2026)

KI-Governance ist keine Bremse mehr, sondern die Voraussetzung für den skalierbaren Betrieb. Ohne ein striktes „Control Layer“ sind agentische Systeme ein unkalkulierbares finanzielles und operatives Risiko.

- 1. Harte Limits sind Pflicht:** Implementieren Sie zwingend Budgetobergrenzen pro Team, Nutzer und vor allem pro autonomem Agenten-Prozess.
- 2. Routing-Strategie definieren:** Das teuerste Modell darf niemals der Standard sein. Definieren Sie Eskalationsregeln: Wann ist eine Aufgabe komplex oder riskant genug für die Frontier-Klasse?
- 3. Compliance-Check:** Achtung bei neuen Spitzenmodellen wie Fable 5. Diese unterliegen oft strengeren Datenhaltungsregeln (z. B. 30 Tage Speicherpflicht beim Anbieter) und sind für vertrauliche Daten eventuell tabu. Prüfen Sie die AGBs vor dem Einsatz.

LESEN SIE ONLINE WEITER...

ONLINE-DOSSIER: Agenten & TCO

Wie kalkuliert man die Total Cost of Ownership (TCO) für autonome KI-Agenten? Aktuelle Preisdaten und vertiefende Szenarien zur Orchestrierung finden Sie in unserem Online-Dossier. Scannen Sie den Code.



Identitätssicherheit ermöglicht den zuverlässigen Einsatz von KI-Agenten

KI-Agenten sind längst tief in den Unternehmensnetzwerken verankert – doch die IT-Sicherheit hinkt hinterher. Statische API-Schlüssel, unkontrollierte OAuth-Freigaben und eine wachsende Schatten-KI schaffen erhebliche Risiken. Die Lösung liegt nicht in isolierten KI-Richtlinien, sondern in der Rückbesinnung auf bewährtes Identitätsmanagement. /// von Arkadiusz Krowczynski

DER RASANTE EINZUG KÜNSTLICHER INTELLIGENZ IN DIE UNTERNEHMENSWELT hat eine neue Ära der Automatisierung eingeläutet. Um komplexe Arbeitsabläufe zu optimieren und die allgemeine Produktivität zu steigern, integrieren Organisationen zunehmend KI-Agenten in ihre IT-Landschaften. Diese hochgradig vernetzten Assistenten agieren längst nicht mehr in isolierten Chat-Fenstern. Sie greifen auf E-Mails zu, kommunizieren mit SaaS-Plattformen, lesen Produktionsdatenbanken aus und können eigenständig Support-Tickets erstellen.

Doch während die operativen Fähigkeiten dieser Systeme exponentiell wachsen, hinkt die IT-Sicherheit oftmals hinterher. Viele Chief Information Security Officer (CISO) verweisen bei Fragen zur KI-Strategie auf Richtlinien, die sich noch in der Ausarbeitung befinden. Dieser abwartende Ansatz erkennt jedoch die Realität: Die KI ist bereits tief in den Netzwerken verankert worden und ihre unkontrollierte Ausbreitung erfordert umgehendes Handeln statt künftiger Konzeptpapiere.

Die unsichtbare Bedrohung: Schatten-KI und das Privilegien-Problem

Ähnlich zur Schatten-IT in der Vergangenheit hat sich mittlerweile eine sogenannte Schatten-KI etabliert. Mitarbeiter verknüpfen externe KI-Werkzeuge häufig eigenmächtig über

OAuth-Berechtigungen mit ihren Unternehmenskonten, um beispielsweise smarte Meeting-Assistenten mit dem Firmenkalender interagieren zu lassen. Durch jede dieser unregulierten Freigaben entsteht aber eine neue, nicht-menschliche Identität mit weitreichenden Zugriffsrechten auf sensible Firmendaten – und diese Identität entzieht sich der Kontrolle durch die IT-Abteilung.

Ein strukturelles Sicherheitsrisiko besteht zudem in der technischen Anbindung dieser Agenten. Aktuell basieren viele KI-Automatisierungen auf statischen API-Schlüsseln, die mit dauerhaften und umfassenden Zugriffsrechten ausgestattet worden sind. Solche fest im Code verankerten Geheimnisse behandeln den KI-Agenten faktisch wie einen Supersuser. Dies widerspricht nicht nur den Prinzipien von Zero Trust und Least Privilege, sondern öffnet auch Angreifern Tür und Tor. Sollte ein KI-System durch eine Prompt Injection kompromittiert werden, könnten Cyber-Kriminelle weitreichende Administrator-Schlüssel erbeuten. Die regelmäßige Rotation dieser statischen Token stellt Entwicklungs-Teams zudem vor enorme logistische Hürden, weshalb veraltete Schlüssel häufig jahrelang unangetastet als tickende Zeitbomben in den Systemen verbleiben.

Erschwerend kommt hinzu, dass herkömmliche Abwehrmechanismen hier blind sind. Für klassische Netzwerk-Sicherheitslösungen erscheint

der Datenverkehr eines KI-Agenten als völlig legitimer API-Traffic. Endgeräte-Überwachungen registrieren lediglich einen autorisierten Prozess innerhalb einer regulären Sitzung. Im Falle eines Sicherheitsvorfalls bleibt somit oft unklar, in wessen Auftrag ein Agent gehandelt hat und, ob die ausgeführte Aktion überhaupt legitim war.

Moderne Identitätssicherheit als Fundament

Um autonome KI-Agenten robust abzusichern, bedarf es keiner isolierten KI-Policy, sondern vielmehr der Rückbesinnung auf die Kernprinzipien des Identitätsmanagements. KI-Agenten müssen als vollwertige digitale Identitäten betrachtet werden, die ebenso strengen Sicherheitsvorgaben, Compliance-Regeln und Lebenszyklus-Management-Prozessen unterliegen wie menschliche Nutzer oder Maschinen. Im Zentrum steht dabei ein modernes Identity and Access Management (IAM), das Identitäten plattformübergreifend verwaltet.

Anstatt KI-Systemen pauschale Zugänge zu gewähren, muss ein dynamischer Token-Austausch nach dem Least Privilege-Prinzip etabliert



- **Cross App Access (XAA):**

Da KI-Workflows oft mehrere Applikationen umfassen, droht der Autorisierungskontext schnell verloren zu gehen. XAA löst dieses Problem, indem der Identity Provider (IdP) zeitlich befristete, kryptografisch signierte Delegationsnachweise ausstellt. Diese übertragen die exakte Benutzeridentität und die spezifischen Berechtigungen sicher über die Grenzen verschiedener Dienste hinweg.

Evolution statt Revolution des Identity Providers

Die Einführung einer solchen KI-Governance bedeutet nicht, dass bestehende IAM-Systeme ausgetauscht werden müssen, oder ein Duplikat entsteht. Vielmehr wird der etablierte

DER AUTOR

Arkadiusz Krowczynski

ist Principal Product Acceleration Specialist bei Okta.

Bild: Octa



werden. Der Agent agiert in diesem sogenannten On-Behalf-Of-Szenario (OBO) lediglich als Stellvertreter des anfragenden Nutzers, nicht als allmächtiger Administrator.

Zwei technologische Standards treiben diesen Paradigmenwechsel maßgeblich voran:

- **Model Context Protocol (MCP):**
Dieser Standard fungiert gewissermaßen als universelle Schnittstelle (vergleichbar mit einem USB-C-Anschluss) für KI-Anwendungen. Er normiert, wie sich Sprachmodelle mit externen Datenbanken, APIs und Werkzeugen verbinden. MCP macht transparent, welche Ressourcen einem Agenten überhaupt zur Verfügung stehen und welche Aktionen er auslösen kann.

Identity Provider (IdP) erweitert. Das System kommuniziert über Standardprotokolle mit ihm und nutzt dessen Vertrauensbasis. Wenn ein Anwender künftig einen KI-Prozess anstößt, authentifiziert der MCP-Server die Anfrage und bittet den IdP um einen Token. Der IdP stellt daraufhin einen nur kurzzeitig gültigen Token aus, dessen Gültigkeitsbereich exakt auf diese spezifische Aufgabe – etwa das Zurücksetzen eines Passworts – zugeschnitten ist. Das Resultat sind lückenlos auditable Protokolle, die exakt ausweisen, welcher Agent im Auftrag welches Nutzers auf eine bestimmte Schnittstelle zugegriffen hat.

Fazit

Der unkontrollierte Einsatz von KI-Agenten mündet in einer Schatten-

KI und führt zu erheblichen Sicherheitsrisiken für Unternehmen, insbesondere durch weitreichende Zugriffsrechte und fest verankerte, statische API-Schlüssel. Um diese Gefahr zu bannen, bedarf es keiner isolierten KI-Richtlinien, sondern einer Rückbesinnung auf bewährte Sicherheitskonzepte des Identitätsmanagements. Autonome KI-Systeme müssen zwingend als vollwertige digitale Identitäten betrachtet und zentral über ein modernes Identity and Access Management (IAM) verwaltet werden. •

TO-DOS: KI-SICHERHEIT FÜR DAS INTELLIGENT ENTERPRISE

Aus den beschriebenen Prinzipien der Identitätssicherheit ergeben sich für Unternehmen konkrete Handlungsempfehlungen für den sicheren Betrieb von KI-Agenten:

- **Agenten registrieren und verwalten:**
Jede KI-Instanz muss als eigenständige Identität erfasst und in die Governance aufgenommen werden. Jeder Agent benötigt zugewiesene Eigentümer und einen verwalteten Lebenszyklus – vom Onboarding bis zur Abschaltung.
- **Statische Geheimnisse eliminieren:**
Der Code von KI-Agenten muss überprüft und dauerhafte, fest programmierte API-Schlüssel oder Passwörter entfernt werden. Dynamische Authentifizierungsmethoden sind hier die bessere Wahl.
- **Granulare Berechtigungen definieren:**
Keine pauschalen Zugriffsrechte gewähren, denn beim Least-Privilege-Prinzip werden Berechtigungen auf das absolut notwendige Minimum und bestenfalls auf einzelne Aufrufe beschränkt.
- **Integration in den bestehenden Identitätsanbieter:**
Isolierte Identitäts-Silos für KI vermeiden, denn die Steuerung der KI-Agenten sollte direkt in die bestehende Identitätsplattform eingebunden werden, um etablierte Anmeldekanäle und Multi-Faktor-Authentifizierungen zu nutzen.
- **Transparenz bezüglich Schnittstellen schaffen:**
Alle von KI-Agenten genutzten Tools und MCP-Server sollten nach ihrem individuellen Risikopotenzial registriert und klassifiziert werden. Ein System mit Schreibzugriff auf Code erfordert strengere Kontrollen als ein Werkzeug zum reinen Dokumentenabruf.
- **Notfall-Abschaltung etablieren:**
IT-Verantwortliche müssen bei Anomalien oder kompromittierten Systemen mittels eines Kill-Switch in der Lage sein, sofort sämtliche Zugriffe eines spezifischen KI-Agenten widerrufen zu können.
- **Kryptografische Signierung sicherstellen:**
Jede von einer KI initiierte Aktion sollte idealerweise kryptografisch signiert sein und sowohl die Identität des KI-Agenten als auch die des autorisierenden menschlichen Nutzers enthalten.

Proof of Concept, und dann? Der Mittelstand und seine KI-Wahrheit

Der Mittelstand ist das Rückgrat der deutschen Wirtschaft. Und genau hier entscheidet sich gerade, wer die digitale Zukunft aktiv gestaltet – und wer ihr hinterherläuft. Auch in Sachen KI. Das DIGITAL BUSINESS Magazin fragt bei Experten nach: „Ehrliche Bestandsaufnahme 2026: Wie viel Prozent der deutschen Mittelständler nutzen Ihrer Erfahrung nach künstliche Intelligenz heute wirklich produktiv – und welche der vielen Pilotprojekte sind tatsächlich in den Regelbetrieb übergegangen und nicht in der berüchtigten ‚Proof-of-Concept-Hölle‘ gelandet?“

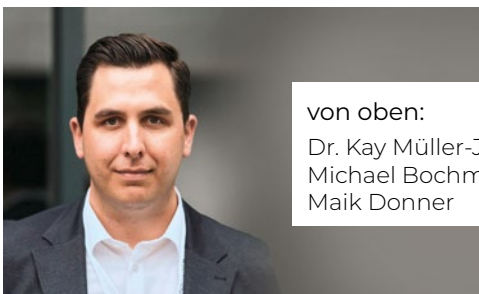
/// von Konstantin Pfliegl



DR. KAY MÜLLER-JONES

Managing Partner & Head of Consulting bei
Tata Consultancy Services Deutschland

(Bild: TCS)



von oben:

Dr. Kay Müller-Jones,
Michael Bochmann, Lukas Keller,
Maik Donner

Viele Statistiken zeigen oft nur die halbe Wahrheit, weil sie in erster Linie formelle, strategische Großprojekte erfassen. In der Praxis ist der deutsche Mittelstand in Sachen KI-Nutzung deutlich besser als sein Ruf. Längst nutzt eine große Zahl an Betrieben KI im Arbeitsalltag, etwa zur Angebotserstellung, zur Analyse von Lagerbeständen oder im Kundenservice. Nicht zu vergessen die nützliche Schatten-KI, die zwar informell, aber bereits hochproduktiv läuft.

Angebrochene Pilotprojekte: kein Scheitern

Dass viele Initiativen in der Pilotphase stecken bleiben oder nicht in den Produktivbetrieb übergehen, sehe ich pragmatisch. Ein abgebrochenes Pilotprojekt muss kein Scheitern bedeuten, sondern kann ein wertvoller Erkenntnisgewinn im agilen Prozess sein. Vorausgesetzt, Unternehmen lernen daraus schnell, was für sie funktioniert.

Die eigentliche Hürde liegt beim Übergang in den skalierbaren Regelbetrieb. Hier scheitern viele an einer falschen Herangehensweise. Sie agieren „Technology First“ statt „Purpose First“. Welche Entscheidungen beziehungsweise Prozesse soll die Technologie in welcher Weise verbessern? Die KI definiert diesen Zweck nicht selbst, sondern folgt den Prioritäten, die Führungskräfte setzen – oder eben nicht setzen. Fehlt das klare Zielbild, verstärkt sie lediglich bestehende Muster, statt strategischen Wert zu erzeugen. Die Brücke zur erfolgreichen Skalierung ruht auf drei Säulen: Ein klarer Business Case, Datenqualität als strategisches Asset und eine Governance, die als Tempomacher statt als Bremse wirkt. Erst wenn der Zweck die Technologie bestimmt, wird aus dem Proof-of-Concept echter, wertschöpfender Regelbetrieb. •

MICHAEL BOCHMANN

Chief Product & Technology Officer bei
DocuWare

(Bild: Docuware)

Nur knapp zehn Prozent der deutschen Mittelständler haben KI vollständig in ihre Prozesse integriert. Das zeigt der KI-Index des Deutschen Mittelstands-Bundes von Anfang 2025. Die KfW kommt in ihrer Erhebung vom Februar 2026 auf 20 Prozent produktive Nutzung. Selbst dieser Wert täuscht: Auf Mitarbeiterebene stellt das ifo Institut fest, dass nur jeder fünfte Beschäftigte KI regelmäßig und intensiv nutzt.

Fehlende Projekte und Datenqualität

Der Grund liegt selten in der Technologie. Er liegt in der Frage davor: Was genau soll die KI lösen? Wer mit „KI für die Buchhaltung“ startet, hat kein Projekt. Wer fragt: „Wie viele Eingangsrechnungen verarbeiten wir heute manuell, und was kostet uns das?“ hat einen Anwendungsfall. Nur

enge Problemdefinitionen mit messbarem Erfolgskriterium überleben den Schritt in den Regelbetrieb.

Dazu kommt ein grundsätzliches Problem: die Datenqualität. Viele Mittelständler setzen KI auf ein Fundament, das dafür nicht vorbereitet ist. Informationen stecken in Papierakten, in E-Mail-Anhängen, in Laufwerken, die niemand außer der jeweiligen Abteilung kennt. Wer schlechte Daten eingibt, bekommt schlechte Ergebnisse.

Unternehmen, die KI etwa für die automatische Klassifizierung und Datenextraktion aus Eingangsbelegen einsetzen, berichten von stabilen Erkennungsraten und messbaren Zeitersparnissen. Der Unterschied zu gescheiterten Projekten: Die Lösung ist in bestehende Workflows eingebettet, nicht parallel dazu aufgebaut.

Was den Mittelstand bremst, ist oft nicht fehlendes Budget, sondern fehlende Prozessklarheit. Der erste Schritt ist kein Technologieprojekt, sondern eine ehrliche Bestandsaufnahme: Welcher Prozess kostet uns heute am meisten und warum. •

LUKAS KELLER

Head of Business Development Central Europe bei
Tieto Tech Consulting

(Bild: Tieto/Thomas Unterberger)

Tieto hat kürzlich mehr als 200 KI-Verantwortliche und Führungskräfte aus deutschen Unternehmen befragt – aus Branchen wie produzierender Industrie, Finanzwirtschaft, Telekommunikation und Energie. Das Ergebnis offenbart eine bemerkenswerte Wahrnehmungslücke: 60 Prozent der Befragten stuften sich als „fortgeschritten“ ein und berichten, mehrere KI-Piloten erfolgreich in den Produktivbetrieb überführt zu haben. Weitere 17 Prozent beurteilen sich als sehr „weit fortgeschritten“ und sehen künstliche Intelligenz bereits umfassend in ihre Kernprozesse integriert.

Selbstbild – und Wirklichkeit

Die Realität sieht nüchterner aus: Tatsächlich haben erst 7 Prozent der befragten Unternehmen KI vollständig in ihre Kernprozesse integriert und zum strategischen Rückgrat ihrer Wertschöpfung gemacht. Zwischen Selbstbild und Wirklichkeit klafft also eine erhebliche Lücke – die klassische PoC-Fälle lässt grüßen. Immerhin strebt derzeit die Hälfte der Befragten aktiv an, zu echten KI-Vorreitern zu werden.

Welche Pilotprojekte schaffen den Sprung in den Regelbetrieb? Jene, bei denen Führungskräfte schnell messbare Ergebnisse und mittelfristige Wettbewerbsvorteile erkennen. Laut unserer Studie dominieren drei Anwendungsfelder: Effizienzsteigerung, IT-Sicherheit und Risikomanagement sowie datengetriebene Entscheidungsfindung wie Marktanalysen oder Predictive Analytics. •

MAIK DONNER

Industry Manager AI bei
Cosmo Consult

(Bild: Cosmo Consult)

Der deutsche Mittelstand ist 2026 zweigeteilt: Es gibt jene Unternehmen, die künstliche Intelligenz produktiv und wertschöpfend nutzen, und alle anderen. Die erstgenannten sind in der Minderheit. Die letztgenannten stecken nach wie vor in der berüchtigten „PoC-Hölle“ fest oder korrigieren gerade mühsam den Kurs.

Rolle Rückwärts

Der Grund dafür ist ein strategischer Wendepunkt. Wir beobachten ihn aktuell: Viele Mittelständler, die vor ein, zwei Jahren euphorisch mit isolierten, use-case-getriebenen Pilotprojekten gestartet sind, machen heute eine

sprichwörtliche „Rolle rückwärts“. Sie stellen fest, dass das punktuelle Lösen von Einzelproblemen mit proprietären Spezial-Tools langfristig wartungsintensiv, nicht skalierbar, und schlicht zu teuer ist. Datensicherheit, Governance und die nahtlose Einbindung in bestehende ERP- und CRM-Prozesse lassen sich mit solchen Einzellösungen nicht nachhaltig abbilden. Demgegenüber stehen die Vorreiter, die das Thema plattformbasiert gelöst haben. Wer auf eine integrierte Plattform setzt, bringt KI-Anwendungen nicht nur deutlich schneller, sondern vor allem effizient, sicher und skalierbar in den echten Regelbetrieb. Die Plattform liefert das nötige Fundament für Daten, Berechtigungen und standardisierte Prozesse.

Mein Fazit: Der Erfolg von KI entscheidet sich nicht am coolsten Use Case, sondern an der Architektur. Nur wer plattformübergreifend denkt, entkommt der PoC-Hölle dauerhaft. •

CHRISTIAN FELDMANN

Berater für digitale Transformation bei der GWS

(Bild: GWS)

Die Diskussion um den Einsatz von KI im Mittelstand ist aktuell deutlich weiter als die tatsächliche Nutzung. In vielen Unternehmen gibt es erste Initiativen oder Pilotprojekte. Von einer breiten produktiven Nutzung im Regelbetrieb kann man aber noch nicht sprechen – unserer Einschätzung nach nutzen es vielleicht 10 bis 15 Prozent produktiv.

Bestehende Prozesse

Die zentrale Herausforderung liegt dabei weniger in der Technologie selbst als in ihrer Einbettung in bestehende Prozesse. KI entfaltet ihren Nutzen nicht automatisch, sondern muss konsequent an konkrete Geschäftsprozesse, belastbare Datenstrukturen und klare wirtschaftliche Ziel-

setzungen gekoppelt werden. Das fehlt in vielen Projekten. Was wir häufig sehen: Proof-of-Concepts zeigen technisch beeindruckende Ergebnisse, bleiben aber Insellösungen. Der Übergang in den produktiven Einsatz scheitert oft daran, dass der Nutzen nicht ausreichend konkretisiert wurde oder Prozesse und Verantwortlichkeiten nicht mitgedacht wurden.

Da, wo KI wirklich produktiv eingesetzt wird, ist der Ansatz ein anderer. Unternehmen starten nicht mit der Technologie, sondern mit der Frage: Welcher Prozess soll messbar verbessert werden? Erst daraus ergeben sich sinnvolle Anwendungsfälle. KI wird dann gezielt als unterstützendes Element integriert – nicht zum Selbstzweck.

Die ehrliche Bestandsaufnahme lautet daher: KI ist im Mittelstand angekommen, aber nicht flächendeckend wirksam. Der entscheidende Schritt vom Experiment zur Wertschöpfung gelingt da, wo Methodik, Prozessverständnis und klare Zielbilder zusammenkommen. •

PHILLIP KORZINETZKI

Director Marketing & Communications bei der PSI Software BU Logistics

(Bild: PSI)

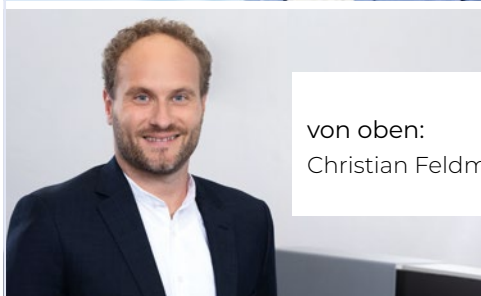
In einer Umfrage von PSI und Civey gab etwa ein Drittel der deutschen Mittelständler an, künstliche Intelligenz bis Jahresende in der Intralogistik einsetzen zu wollen. Das größte Potenzial sehen die Unternehmen in den Bereichen Lageroptimierung und Bestandsverwaltung.

Diese Einschätzung erscheint optimistisch, denn noch immer wird KI auch in der Industrie vor allem für administrative Zwecke genutzt, beispielsweise um Informationen auszuwerten oder Dokumente zu analysieren. Die Steuerung geschäftskritischer Logistikprozesse wird hingegen nur in eingeschränktem Maße durch KI unterstützt.

KI-Skepsis

Viele Unternehmen stehen künstlicher Intelligenz noch immer skeptisch gegenüber. Letztlich scheitern viele Ansätze, ohne jemals produktiv im Einsatz gewesen zu sein. Denn gerade im Mittelstand gilt: So innovativ eine Idee auch sein mag – am Ende zählen nur greifbare Vorteile für klar definierte Einsatzzwecke und eine reibungslose Integration. Um künstliche Intelligenz als wirklichen Helfer im operativen Alltag zu verankern, hat PSI seine KI-Lösungen jahrelang bei Kunden in anspruchsvollen Lagerumgebungen getestet und optimiert. Daraus ist mit Batch AI ein erstes KI-Modul im WMS-Standard hervorgegangen. Batch AI ermöglicht es, Kommissionierprozesse um bis zu 20 Prozent effizienter zu gestalten.

Nach diesem Muster werden PSIWms in den kommenden Monaten weitere KI-Bausteine hinzugefügt, die Anwendern operative Mehrwerte für spezifische Anwendungsbereiche bieten und damit dazu beitragen, den KI-Einsatz in der Logistik voranzutreiben. •



von oben:
Christian Feldmann, Phillip Korzinetzki



KI KANN VIEL.

Aber kennt sie auch Ihr Unternehmen?

Viele mittelständische Unternehmen testen KI – doch der große Durchbruch bleibt häufig aus. Der Grund: Standard-Tools kennen weder interne Prozesse noch gewachsenes Erfahrungswissen. Erst wenn KI auf das eigene Unternehmenswissen zugreifen kann, wird aus Technologie ein echter Produktivitäts-Turbo.

DIE ENTWICKLUNG VON KI IST IN EINEM RASANTEN TEMPO VONSTATTEN GEGANGEN. Laut einer aktuellen Studie von „bitkom e.V.“ hatten 2025 erst 17 % der deutschen Unternehmen ab 20 Beschäftigten eine KI im Einsatz. 2026 sind es bereits 41 %. Von den 604 befragten Unternehmen gaben 48 % an, den Einsatz von KI-Tools zu planen oder zumindest zu diskutieren. Diese Entwicklung macht deutlich, dass die Akzeptanz deutscher Unternehmen gegenüber dieser noch neuartigen Technologie rasant zunimmt. Hat sich KI also bewährt?

Nicht das „ob“, sondern das „wie“

So einfach ist es nicht: In der gleichen Studie gaben 52 % jener Unternehmen an, die KI nutzen, dass sie durch die genutzten Tools ihre Wettbewerbssituation verbessert habe. Da ist also – um eine bewährte, saloppe Formulierung zu nutzen – noch Luft nach oben. Woran hakt es im deutschen Mittelstand? Entscheidend für den Erfolg ist weniger, ob eine KI genutzt wird, sondern wie eine KI genutzt wird. Ein Tool allein macht noch keinen Sommer. Traditionelle LLMs wie ChatGPT, Claude, Gemini und weitere generieren aus vorhandenen Informationen einen Sinn. Ergo liefern sie das, was für sie am wahrscheinlichsten ist, was sie für richtig erachten. Manchmal funktioniert das gut. Manchmal kommt es zu Halluzinationen.

Wenn der Standard nicht reicht

Die zentrale Frage für den deutschen Mittelstand ist daher zweifaltig: Was will ich mit einer KI erreichen, und wie komme ich dahin? Für einen effizienten Nutzen eines Tools braucht es Vorarbeit. Wer ein Tool für spezielle Zwecke benötigt, muss dieses herstellen oder ein existierendes nach den eigenen Wünschen modifizieren. Standard-Programme werden das gewünschte Ziel, wenn überhaupt, nur nach langer Zeit und über steinige Umwege erreichen können. Nur wenige Produkte auf dem Markt erlauben eine solche Personalisierung. COSMA ist eines davon.

Das Beste beider Welten

COSMA ist eine Enterprise-KI-Plattform, die speziell für den deutschen Mittelstand und Großunternehmen entwickelt wurde. Sie kombiniert modernste KI-Technologie mit hohen Datenschutzstandards, ermöglicht so das barrierefreie Arbeiten mit Unternehmensdaten, sichert Firmenwissen, und ist auf diese Weise personalisierbar. Damit bildet es eine



Ausnahme auf dem KI-Markt. Unternehmen erhalten hier die Antworten, die für sie wirklich zählen und auf deren Informationen sie sich verlassen können. Denn während herkömmliche LLMs mit Weltwissen trainiert sind, greift COSMA zusätzlich auf die individuellen, einzigartigen Datenquellen des Unternehmens zu, das Expert*innen eingeben und sichern können. Nutzer*innen profitieren vom Besten beider Welten. Sie sind dabei nicht auf Großkonzernen und deren Angebote angewiesen, können das KI-Tool jedoch nahtlos an alle Microsoft-Lösungen anschließen. Mitarbeitende haben Zugang zu allen LLM-Modellen, ohne Datenschutzbedenken haben oder Compliance-Risiken fürchten zu müssen.

Ihre ersten KI-Use Cases mit COSMA

Probieren Sie COSMA selbst aus. Besuchen Sie unsere Website und fragen Sie Ihre Demo-Umgebung von COSMA an.

Jetzt testen



Kontakt

COSMO CONSULT Gruppe
Schöneberger Str. 15 • 10963 Berlin
Tel: +49 30 343815-0
info@cosmoconsult.com
www.cosmoconsult.com



COSMO CONSULT digitale Lösungen für das Business von morgen

COSMO CONSULT zählt zu den international führenden Microsoft-Partnern für Unternehmenssoftware und Digitalisierungsberatung. Dank tiefgreifender Branchenexpertise, KI und Automatisierung entstehen durchgängige, maßgeschneiderte Lösungen – mit Fokus auf strategischen Wandel und die Menschen, die ihn vorantreiben.

Automatisierte Systeme: KI wird im E-Mail-Marketing zum Erfolgsfaktor

KI eröffnet Unternehmen neue Möglichkeiten, die Qualität ihrer Kundenkommunikation gezielt zu verbessern. Während oft noch über neue Tools diskutiert wird, entstehen die größten Effekte dort, wo Daten und Systeme intelligent zusammenspielen. Wer die richtigen Voraussetzungen schafft, sichert sich wichtige Wettbewerbsvorteile. /// von André Görmer

ES GIBT DREI BEREICHE, IN DENEN KI IM E-MAIL-MARKETING HEUTE ECHTEN MEHRWERT SCHAFFT: Im E-Mail-Marketing unterstützt Künstliche Intelligenz nicht nur dabei, Prozesse zu automatisieren. Sie hilft, Inhalte präziser auszusteuern, Nachrichten sichtbarer zu machen und Kampagnendaten schneller auszulesen. So lassen sich Entscheidungen datenbasiert verbessern. Die folgenden drei Anwendungsbereiche zeigen deutlich, welche Voraussetzungen Unternehmen schaffen sollten, um dieses Potenzial zu nutzen.

- **Smarte Inboxes:**

Postfächer werden zunehmend durch intelligente Filter und Relevanzsignale strukturiert. Erfolgreiches E-Mail-Marketing beginnt nicht erst beim Versand, sondern bei der Frage, ob eine Nachricht überhaupt als relevant erkannt wird. KI hilft dabei, Versandzeitpunkte, Betreffzeilen und Frequenzen besser an Nutzungsmuster anzupassen. Voraussetzung ist jedoch eine disziplinierte Versandpraxis, die aus Empfängerreaktio-

nen lernt, statt Verteilergröße mit Relevanz zu verwechseln.

- **Personalisierte Inhalte:**

KI kann Verhaltensdaten, Interessen und Transaktionen auswerten, um Inhalte und Empfehlungen passgenauer auszusteuern. Der Fortschritt liegt dabei weniger in automatisch erzeugten Texten als in einer besseren Fit zwischen Inhalt und Bedarf. Personalisierung wird erst dann wertvoll, wenn sie mehr Relevanz statt mehr Komplexität schafft.

- **Testing und Segmentierung:**

Klassische A/B-Tests bleiben relevant, stoßen bei dynamischen Kampagnen jedoch an Grenzen. KI erkennt Muster schneller, optimiert laufend und ermöglicht vor allem schnelleres Lernen statt nur schnellerer Tests. Dafür braucht es verknüpfte Datenquellen, klare KPI-Logiken und integrierte Systeme. Wo diese Grundlagen vorhanden sind, verbessert KI nicht nur die operative Aussteuerung, sondern auch die Qualität von Entscheidungen sowie Ergebnissen.

Barrierefreiheit wird entscheidend

Damit KI in allen drei Bereichen wirkt, braucht es eine Grundlage, die oft unterschätzt wird: Barrierefreiheit. Barrierefreie E-Mails sind klar strukturiert, verständlich formuliert und technisch sauber aufgebaut. Das verbessert nicht nur das Leseerlebnis für den Menschen, sondern auch die Auswertbarkeit für Systeme. Strukturierte Inhalte, Alt-Texte, ausreichende Kontraste, verständliche Sprache und Screenreader-Kompatibilität sind deshalb kein Zusatz, sondern ein Qualitätsstandard digitaler Kommunikation. Was barrierefrei gestaltet ist, ist meist auch robuster und lesbarer.

Mit den regulatorischen Anforderungen ist das Thema zudem verbindlicher geworden. Das Barrierefreiheitsstärkungsgesetz und der European Accessibility Act schaffen verbindliche Anforderungen an die Barrierefreiheit digitaler Produkte und Dienstleistungen. Diese müssen so gestaltet sein, dass sie für Menschen mit Behinderungen leicht zugänglich und nutzbar sind.

Technologie allein reicht nicht

Die nächste Entwicklungsstufe von KI im E-Mail-Marketing liegt in Systemen, die Inhalte und Varianten vor dem Versand intelligenter bewerten und personalisierte Kommunikation vorausschauend optimieren. Entscheidend sind die Grundlagen: saubere Daten, integrierte Systeme und Kommunikation, die für Menschen wie Systeme gleichermaßen verständlich ist. •



DER AUTOR

André Görmer

(Mapp) ist Vorsitzender der Working Group E-Mail im BVDW.

Tata Communications: Das Netzwerk hinter KI

KI ist derzeit der wichtigste Innovationstreiber, ist das Netzwerk aber nicht darauf ausgelegt, leidet die Leistung. Mit dem Intelligent Unified Network Fabric von Tata Communications können Unternehmen KI-Workloads sicher und in Echtzeit ausführen.

WÄHREND INVESTITIONEN IN KI RASANT STEIGEN, verlassen sich viele Unternehmen auf eine veraltete Infrastruktur, die nicht dafür ausgelegt ist. Das führt zu einer versteckten „Netzwerk-Steuer“, die die Leistung einschränkt, die Kosten für Datenbewegungen erhöht und die Bereitstellung verlangsamt. Mit der Verbreitung von KI werden veraltete Netzwerke zum Hindernis bei der Übersetzung von KI-Investitionen in geschäftlichen Nutzen.

Warum KI nicht skaliert

Unternehmen investieren in GPUs und Cloud-Plattformen, vernachlässigen jedoch das entscheidende Bindeglied: das Netzwerk. KI ist auf kontinuierliche Hochgeschwindigkeits-Datenbewegungen über Clouds, Rechenzentren und Edge-Umgebungen hinweg angewiesen.

Das Problem liegt im veralteten Design traditioneller Architekturen, die für vorhersehbaren Datenverkehr wie E-Mail, SaaS und Surfen im Internet entwickelt wurden. KI-Workloads sind jedoch anders: Sie erzeugen kontinuierliche Datenströme mit hohem Volumen und erfordern niedrige Latenzzeiten. Selbst minimale Störungen beeinträchtigen die Modellgenauigkeit und verzögern Ergebnisse.

Das hat erhebliche geschäftliche Auswirkungen: Langsame Datenbewegungen behindern das Modelltraining. Dies verzögert die Markteinführung und führt zu verpassten Marktchancen. Datensouveränität bringt weitere Komplexität mit sich, da traditionellen Netzwerken die Transparenz fehlt, wohin sensible Daten übertragen werden dürfen.

Das macht ein Netzwerk KI-fähig:

- **Intelligent & dynamisch:** Ein selbstoptimierendes System, das den Datenverkehr live an die Anforderungen der Anwendungen anpasst.
- **Skalierbar & nahtlos:** Elastische Skalierung über das Multi-Cloud- und Edge-Ökosystem hinweg, für eine konsistente Leistung verteilter KI-Workloads.
- **Secure by Design:** Integration von Governance und Datensouveränität in die Netzwerkstruktur zur Überwachung sensibler Datenbewegungen.

Netzwerke für KI ausbauen

Das Intelligent Unified Network Fabric von Tata Communications vereint Konnektivität, Sicherheit und Transparenz in einer Plattform. Es ermöglicht anwendungsspezifische Netzwerkarchitekturen, die Leistung, Latenz und Sicher-

Amit Kapoor

Vice President und
Head of Continental Europe bei
Tata Communications

heit auf KI-Workloads abstimmen. Mit dem einheitlichen Konnektivitäts-Framework bewegen sich Daten, Anwendungen und Modelle nahtlos über Clouds, Rechenzentren und Edge-Umgebungen hinweg. Die End-to-End-Transparenz hilft, Governance-, Souveränitäts- und Sicherheitsanforderungen durchzusetzen.

Die „ThreadSpan™“-Plattform ermöglicht Unternehmen Kontrolle in Echtzeit, sowie Automatisierung und Optimierung. So wird die Netzwerkinfrastruktur eine strategische Basis für KI-Skalierung.

Der Erfolg von KI definiert sich nicht mehr nur durch die Modellkomplexität, sondern die Effektivität der Datenbewegungen. Erfolgreiche Unternehmen behandeln das Netzwerk als strategisches Gut statt als nachträglichen Gedanken.



TATA COMMUNICATIONS

Unterschätzt, aber unverzichtbar: Application Management Services im Cloud-Zeitalter

Nur acht Prozent der IT-Entscheider wollen künftig auf Application Management Services im SAP-Betrieb (SAP AMS) verzichten. Warum das klassische Modell trotzdem neu gedacht werden muss und wie das gelingen kann. /// von Ulrich Kreitz

IT-ABTEILUNGEN BALANCIEREN AUF EINEM SCHMALEN

GRAT: S/4HANA-Migrationen laufen, Cloud-Rollouts kommen hinzu, KI-Use Cases stehen in der Planung und gleichzeitig muss der laufende SAP-Betrieb stabil bleiben. In dieser Gleichzeitigkeit entscheidet sich, welche Aufgaben intern zu lösen sind und welche besser ein externer Partner übernimmt.

Entweder alles im Rahmen von Application Management Services auszulagern oder alles intern zu behalten war lange die Antwort, die viele für eindeutig hielten. Diese greift heute zu kurz. Die SAP-Trendumfrage 2026, bei der mehr als 200 Unternehmen aller Größen zu ihren aktuellen und künftigen SAP-Betriebsmodellen befragt wurden, liefert dafür eine klare Datengrundlage. Sie zeigt: AMS bleiben gesetzt. Mehr als 80 Prozent der Unternehmen planen sie fest in ihre SAP-Strategie ein – aber mit grundlegend veränderten Erwartungen.

Warum SAP AMS auch im Cloud-Zeitalter relevant bleiben

Lediglich acht Prozent der Befragten geben an, künftig auf SAP AMS verzichten zu wollen. Das ist ein deutliches Signal, aber kein Freifahrtschein für das klassische Betriebsmodell. Denn parallel dazu verschieben sich die Anforderungen massiv.

Hybride SAP-Architekturen sind der Normalfall, nicht die Ausnahme. Laut Trendumfrage fürchten 43 Prozent der Befragten Kontrollverluste durch die Cloud, 35 Prozent nennen Datenschutz- und Compliance-Bedenken als Grund, On-Premise-Systeme zu behalten, und 33 Prozent schreckt der technische und organisatorische Aufwand einer vollständigen Migration ab. Solange diese hybride Realität anhält, bleibt der Bedarf an AMS, die genau diese Spannungsfelder professionell managen, hoch.

Was CIOs heute von einem AMS-Partner erwarten

Die Erwartungen haben sich verschoben: weg vom reaktiven Ticket-Abarbeiten, hin zu echter Mitverantwortung. Rund die Hälfte der Befragten haben folgende Erwartungen:

- Nachhaltige Absicherung von SAP-Security und Compliance
- Transparente Service-Level-Agreements und planbare Kosten
- Wunsch nach spürbarer Entlastung ihrer internen IT-Ressourcen
- Kontinuierliche Betreuung und Optimierung als Standard moderner AMS
- Unterstützung beim Management hybrider Landschaften

„AMS sind die Co-Piloten für eine sichere und erfolgreiche Reise in die Zukunft. Sie entlasten interne Ressourcen und sichern Stabilität, sodass die Systeme trotz Turbulenzen ruhig und sicher laufen“, erklärt Yvonne Kern, Teamleitung Vertrieb Managed Services bei NTT Data Business Solutions. Auf dieser Grundlage verändert sich auch die Auswahl der Anbieter: Branchenexpertise und Prozess-Know-how nennen 64 Prozent als wichtigstes Kriterium. Persönliche Ansprechpartner und lokale Präsenz folgen mit 51 Prozent: Ein klares Signal, dass Unternehmen bei der AMS-Wahl auf Nähe und inhaltliche Tiefe setzen, nicht auf globale Skalierung um jeden Preis.

Welches AMS-Liefermodell zu welchem Unternehmen passt

Hier zeigt die Studie ein differenziertes Bild, was die Botschaft für IT ist. Es gibt kein universell richtiges Modell, sondern ein Spektrum:

Liefermodell	Zustimmung	Wann sinnvoll?
Shared-Service-Teams (standardisiert)	34 Prozent	Cloud-Strategien mit vorgegebenen Update-Zyklen, Skalierungsbedarf
24x7-Support	33 Prozent	SAP als geschäftskritische Always-on-Plattform, internationale Rollouts
Dedizierte Serviceteams (kundenspezifisch)	27 Prozent	Regulierte Branchen, spezialisierte Geschäftsmodelle
Rein lokale Leistungserbringung	15 Prozent	Datensouveränität oder kurze Entscheidungswege als Priorität
Shoring-Modell	12 Prozent	Kostenoptimierung bei standardisierbaren Prozessen



WAS SIND SAP APPLICATION MANAGEMENT SERVICES?

SAP Application Management Services (AMS) umfassen Dienstleistungen für Betrieb, Wartung und Weiterentwicklung von SAP-Anwendungen. Sie entlasten interne IT-Ressourcen und sichern Stabilität, Sicherheit und Verfügbarkeit der Systeme. Der Leistungsumfang reicht von Applikationssupport und Change-Management bis zur Betreuung hybrider und cloudbasierter SAP-Landschaften.

„Gefragt sind Dienstleister, die Kunden über den Betrieb hinaus bei der Weiterentwicklung ihrer Systemlandschaft **proaktiv beraten** – mit Fokus auf Zukunftsfähigkeit, Innovation und strategischen Roadmaps.“ *Ulrich Kreitz*

Ulrich Kreitz verantwortet seit April 2022 als Teil der Geschäftsleitung den Bereich Managed Services der Business Unit Deutschland bei NTT Data Business Solutions. Bei der Weiterentwicklung des Bereichs legt er den Schwerpunkt auf Themen wie KI, Liefermodelle und Cloud-Technologien.

Bild: NTT Data Business Solutions

DER AUTOR



SAP AMS als strategischer Baustein – nicht als Standardlösung für alle

So entsteht das entscheidende Prinzip für moderne IT-Betriebsmodelle: AMS übernehmen die Aufgaben, für die sie am stärksten sind: 24/7-Verfügbarkeit, hybride Landschaftssteuerung, kontinuierliche Optimierung, Security-Governance. Sie fügen sich dabei in ein Gesamtmodell ein, das interne Teams, DevOps-Ansätze und spezialisierte Services einschließt.

Typische Vorbehalte gegenüber AMS bleiben real und sollten beim Setup mitgedacht werden: Abhängigkeit vom Anbieter, möglicher Kontrollverlust, der Aufwand der Umstellung und die Frage, welches Wissen intern bleiben muss, um strategisch steuerungsfähig zu bleiben. Moderne AMS-Modelle adressieren genau diese Punkte durch klare SLAs, definierte Governance-Strukturen und transparentes Reporting, wobei Ansatz und Tiefe je nach Anbieter deutlich variieren.

IT-Dienstleister im SAP-Umfeld verfolgen dafür unterschiedliche Konzepte: Manche setzen auf globale Skalierung mit standardisierten Prozessen, andere auf lokale Nähe mit dedizierten Teams, wieder andere auf modulare Pakete, die sich eng am SAP-Produktstandard orientieren. NTT Data Business Solutions beispielsweise kombiniert proaktiven Applikationssupport, SAP Release Management und einen dedizierten Service Delivery Mana-

ger in einem End-to-end-Paket zu einem festen monatlichen Preis. Dass dieses Modell in der Praxis trägt, zeigt Mann+Hummel: Das Unternehmen rollte SAP S/4HANA Cloud in 24 Ländern innerhalb von sechs Monaten mit Hilfe von NTT Data Business Solutions aus.

Drei Fragen, die CIOs jetzt stellen sollten

Kein IT-Setup ist dauerhaft optimal. Die Umfrage liefert den Rahmen, um das eigene Modell kritisch zu überprüfen.

Folgende drei Leitfragen helfen dabei:

1. Stabilität:

Welche Teile der SAP-Landschaft erfordern 24/7-Verfügbarkeit und wer gewährleistet diese heute zuverlässig?

2. Governance:

Wie genau sind SLAs, Verantwortlichkeiten und Reporting gegenüber einem AMS-Partner definiert und reichen sie für hybride Architekturen aus?

3. Weiterentwicklung:

Liefert der aktuelle Betriebspartner proaktive Impulse für neue Releases, KI-Use Cases und Innovationen oder beschränkt er sich auf Ticketbearbeitung?

Gefragt sind Verlässlichkeit, Governance-Kompetenz und partnerschaftliche Verantwortung – über den gesamten Lebenszyklus hinweg. •

Das ERP als Prozesslandkarte für KI und Mensch

Effizienz entscheidet heute über den Markterfolg – und KI gilt als zentrale Stellschraube. Doch klassische ERP-Systeme sind rein datenfokussiert: Das entscheidende Prozesswissen steckt nur in den Köpfen der Anwender. Damit KI wirklich entlastet, muss sich das ERP zur digitalen Prozesslandkarte wandeln, die Mensch und Maschine gleichermaßen führt. /// von Ralf Bachthaler

DARUM GEHT ´S

ERP als Prozesslandkarte: Klassische ERP-Systeme sind rein datenfokussiert – das eigentliche Prozesswissen steckt nur in den Köpfen der Anwender. Um KI sinnvoll zu nutzen, muss sich das ERP vom Datenzentrum zur digitalen Prozesslandkarte weiterentwickeln, die Abläufe formal abbildet.

KI braucht Prozesswissen: Eine KI kann übertragene Aufgaben nur korrekt bearbeiten, wenn sie weiß, welche Schritte in welcher Reihenfolge und mit welchen Daten auszuführen sind.

BPMN und schrittweises Vorgehen: Zur digitalen Abbildung der Abläufe empfiehlt sich die Prozesssprache BPMN, die von KI unmittelbar verstanden wird. Statt die gesamte Prozesslandschaft zu kartographieren, genügt es zunächst, die zentralen Kernprozesse mit dem größten Automatisierungspotenzial zu dokumentieren – für schnelle erste Effizienzgewinne.

DAS KLASSISCHE ERP IST DATENFOKUSSIERT: Anwender finden darin die Informationen, die sie für ihre täglichen Aufgaben benötigen, und verarbeiten diese in verschiedensten Masken und Ansichten. Wie genau diese Arbeits-

schritte aussehen, ist in der Regel nicht im System, sondern in den Köpfen der User hinterlegt. In Zeiten zunehmender KI-Unterstützung ergibt sich daraus eine zentrale Herausforderung: Solange die KI keine Gedanken lesen kann, bleibt ihr das Prozesswissen verschlossen. Ein Status quo, der sich ändern muss: Als IT-Kern der Geschäftsabläufe darf das ERP nicht länger nur als Datenzentrale fungieren. Das ERP muss sich parallel weiterentwickeln zur digitalen Prozesslandkarte der Unternehmen.

Die Effizienz der täglichen Abläufe ist zum entscheidenden Erfolgsfaktor der heutigen Zeit geworden. In dem Maße, in dem die steigende internationale Konkurrenz nationale Preisniveaus unterbietet und die anhaltend volatile Wirtschaftslage Lieferketten und Absatzmärkte beeinträchtigt, gilt es für Unternehmen, flexibler, produktiver und wirtschaftlicher zu werden, um weiterhin erfolgreich am Markt zu bestehen. Die eigenen Kapazitäten zu erhöhen, indem Belegschaften aufgestockt und Teams erwei-

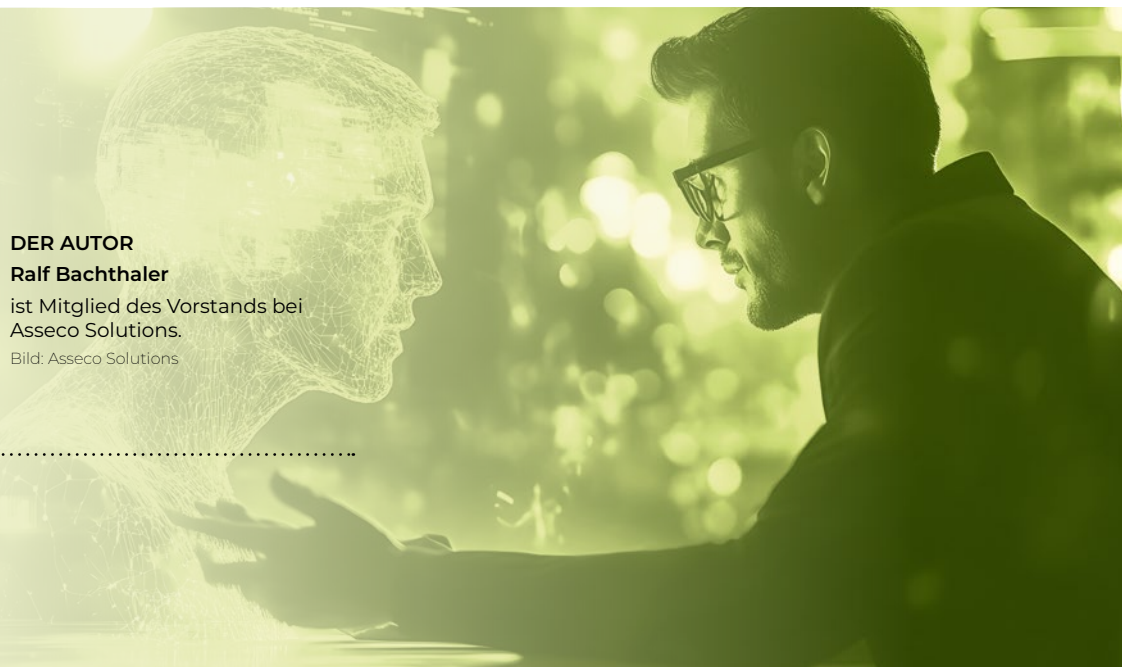


DER AUTOR

Ralf Bachthaler

ist Mitglied des Vorstands bei Asseco Solutions.

Bild: Asseco Solutions



tert werden, stellt dabei in der Praxis oft keine Option dar. Der Fachkräftemangel hält den Arbeitsmarkt weiterhin fest im Griff. Als einzige Stellschraube für mehr Effizienz bleibt dann nur die Technologie; in der heutigen Zeit konkret: künstliche Intelligenz.

Das Potenzial der intelligenten Technologie entwickelt sich in rasantem Tempo weiter. So ist sie bereits heute in der Lage, verschiedenste Aufgaben hochgradig automatisiert zu bearbeiten und damit im Idealfall ganze Prozessketten selbstständig zu übernehmen, etwa die vor- und nachgelagerten Prozessstufen eines Fertigungsablaufs. In einem solchen Szenario kümmert sich die KI um die Auftragsanlage im ERP-System, die Verfügbarkeitsprüfung des benötigten Materials, bei Bedarf die Bestellung von Nachschub sowie die Bestätigung von Auftrag und Liefertermin an den Kunden. Standardabläufe, durch die Mitarbeiter im Normalfall wertvolle Zeit durch monotone Klickarbeit verlieren. Übernimmt die KI den manuellen Aufwand, wird der Mensch zum Supervisor: Er überwacht und prüft die Arbeit der KI, gibt KI-Vorschläge frei und fällt Entscheidungen, die über das Kompetenzspektrum der KI hinausgehen.

Orientierungslose KI

Ein solches KI-Szenario wird jedoch auf klassischem Weg nicht ohne weiteres Realität. Denn damit eine KI die ihr übertragenen Aufgaben tatsächlich in korrekter Weise bearbeiten kann, benötigt sie Prozesswissen: Welche Schritte sind in welcher Reihenfolge auszuführen, um die Aufgabe zu bearbeiten? Welche Daten müssen an welchem Prozessschritt zwingend vorliegen, damit der Ablauf weiter vorangehen kann? In der traditionell datengetriebenen ERP-Welt ist dieses Wissen nur in den Köpfen der Anwender

zuvor aufwendige Individualprojekte zur Implementierung zu starten.

Schrittweise vorgehen

Auch wenn das Ziel in einer vollständigen digitalen Abbildung der Unternehmensprozesse besteht, um den KI-Einsatz optimal skalieren zu können, ist es nicht erforderlich, die gesamte Prozesslandschaft zu kartographieren, bevor mit einer KI-Unterstützung begonnen werden kann. Eine praxistaugliche Alternative besteht beispielsweise darin, zunächst die zentralen Kernprozesse zu dokumentieren, die das größte Automatisierungspotenzial aufweisen. So können Unternehmen bereits zeitnah von ersten Effizienzgewinnen profitieren, während im Anschluss Schritt für Schritt weitere Prozesse für eine KI-Unterstützung dokumentiert werden. Konkret empfiehlt sich die Prozesssprache Business Process Model and Notation (BPMN) zur digitalen Abbildung der Unternehmensabläufe. Entsprechend dokumentierte Prozesse können unmittelbar von der KI verstanden werden. Die Übertragung der realen Abläufe in die BPMN-Sprache ist dabei zu gewissen Teilen auch systemgestützt möglich, etwa mithilfe eines Regelwerks. Das ERP-System kann als wertvolle Quelle fungieren, da digitale Spuren wie Zeitstempel konkrete Hinweise darauf geben, wie Aufgaben im System tatsächlich bearbeitet werden.

Generell liefert eine digitale Prozesslandkarte im ERP-System nicht nur eine zentrale Grundlage für Effizienzgewinne durch künstliche Intelligenz. Auch im Arbeitsalltag der menschlichen User ergeben sich daraus Vorteile. Wenn etwa die ERP-Lösung Anwender Schritt für Schritt durch ihre aktuelle Aufgabe leitet, müssen diese nicht länger selbst ihren Weg durch komplexe Masken und Ansichten bah-

„ Als IT-Kern der Geschäftsabläufe darf das ERP nicht länger nur als Datenzentrale fungieren. Das ERP muss sich parallel weiterentwickeln zur digitalen Prozesslandkarte der Unternehmen.

Ralf Bachthaler

vorhanden. Dieses informelle Know-how zu formalisieren und der KI zu vermitteln, macht die Implementierung von KI-Automatisierungen bislang oft zu zeitaufwendigen Individualprojekten. Und der Aufwand wiederholt sich, sobald das nächste KI-Szenario realisiert werden soll.

In Zeiten, in denen der Bedarf an Effizienzsteigerungen durch KI-Automatisierungen kontinuierlich steigt, ist ein Umdenken erforderlich. Es gilt, die Unternehmensprozesse generell in den Fokus zu rücken und bereits vorausschauend mit ihrer Dokumentation zu beginnen. Wer auf diese Weise eine digitale Landkarte seiner individuellen Abläufe entwickelt, schafft nicht nur die zentrale Grundlage dafür, dass beispielsweise KI-Agenten auf korrekte Art und Weise an Aufgaben mitarbeiten und damit für echte Entlastung sorgen. Eine digitale Prozesslandkarte ermöglicht es auch, KI bei Bedarf flexibel an beliebigen Stellen des Gesamtprozesses einzusetzen, ohne

nen. Eine prozessorientierte Arbeitsweise kann die tägliche Arbeit deutlich beschleunigen und Fehlerquoten senken.

Vom Daten- zum Prozessfokus

In Zeiten, in denen die Effizienz in signifikanter Weise über den Markterfolg eines Unternehmens entscheidet, ist die Unterstützung durch KI unerlässlich geworden. Einen wirklichen Nutzen können entsprechende Initiativen jedoch nur entfalten, wenn die KI zum einen das tut, was sie tun soll, und gleichzeitig Implementierungsaufwände überschaubar bleiben.

Moderne ERP-Systeme können und müssen ein Fenster in die Prozesswelt öffnen: Wenn die individuellen Prozesse eines Unternehmens im System dokumentiert werden, ergibt sich eine verlässliche Landkarte der täglichen Arbeit, die beide – Mensch und KI – auf dem korrekten und effizientesten Weg durch ihre Aufgaben führt. •

Messbar höhere Prozesseffizienz

Die Philipp Hafner GmbH ist ein führender Anbieter für kundenindividuelle Lösungen im Bereich Fertigungsmesstechnik. Um bei der Projektabwicklung eine ähnliche Präzision wie auf Produktseite zu erzielen, fiel bei dem Mittelständler 2022 die Entscheidung für die Implementierung eines durchgängigen ERP-Systems mit Zuschnitt auf den Sondermaschinenbau. /// von Axel Schmidhäuser

DIE KERNKOMPETENZ DES FAMILIENBETRIEBS PHILIPP HAFNER MIT SEINEN 120 BESCHÄFTIGTEN liegt in der dimensionellen Messung eng tolerierter Werkstücke. Die hochpräzisen Messmaschinen kommen primär in der Automobilindustrie zum Einsatz. Gemessen werden Achs-, Lenkungs-, Getriebe- und Motorenteile sowie Felgen, Bremsscheiben und Teile für die E-Mobilität. Den grundsätzlichen Ansatz des schwäbischen Unternehmens beschreibt der kaufmännische Leiter Eckhard Rau als klassisch für den Maschinenbau: Während viele Hochpräzisionsteile selbst gefertigt werden, stammen diverse Komponenten wie Motoren und Steuerungstechnik von renommierten Industrieausrüstern und einige Fertigungsteile von Spezialbetrieben. Die Kunst bestehe darin, alle Bauteile optimal miteinander zu kombinieren und die eigene Expertise hinsichtlich des mechanischen Aufbaus, der Werkstoffauswahl sowie der softwareseitigen Verarbeitung der Messdaten einzubringen.

Im Gegensatz zu dem hohen Produktniveau bestand hinsichtlich der Orchestrierung der eigenen Geschäftsprozesse sehr lange Nachholbedarf. Bereits 2008 gab es deshalb erste Überlegungen in Richtung der Implementierung eines durchgängigen ERP-Systems, allerdings hatte der Bau eines neuen Firmengebäudes zunächst Vorrang. 2015 erfolgte dann der Umzug an den neuen Standort. Mit Blick auf das daran anschließende ERP-Vorhaben kam dem zum Projektleiter ernannten Eckhard Rau zugute, dass im Zuge der Gebäudeplanung der gesamte Fertigungsdurchlauf strategisch komplett neu aufgesetzt worden war. Optimale Platzausnutzung, kurze Wege und sauber aufeinander abgestimmte Abläufe boten beste Vor-

aussetzungen, um die äußerst heterogene Software-Landschaft nun ebenfalls auf ein solides Fundament setzen zu können.

Ablösung der isolierten Systeminseln

Dass viele Abläufe zuvor extrem papierlastig und manuell geprägt waren, lag in erster Linie an der Vielzahl dezentraler Einzelsysteme. „Der Plan war folglich, alle vorherigen Software-Inseln, bestehend aus verschiedensten Word-, Excel- und Access-Anwendungen, isolierten Systemen für die Buchhaltung, die Zeiterfassung, die Personalabrechnung und CRM sowie dem herstellerseitig nicht mehr gepflegten PPS-System, abzulösen. Sie sollten in einer Software zusammengeführt werden, um eine größtmögliche Digitalisierung der Prozesse zu erzielen“, bekräftigt der ERP-Verantwortliche. Als essenziell für die angestrebten integrierten Abläufe nennt er zudem die Automatisierung der CAD-Schnittstelle.

Die mit den Key Users definierten prozessualen Kernanforderungen wurden an ca. zehn ERP-Anbieter versendet, die sich laut eigenen Aussagen im Umfeld der Unikatfertigung bewegen. Die Zahl potenzieller Kandidaten reduzierte sich jedoch schnell auf nur noch drei, weil bei den meisten weitreichende Anpassungen notwendig gewesen wären, um ihre jeweiligen Systemstandards für die Losgröße 1+ tauglich zu machen.

Diesen Ansatz bewertet Eckhard Rau als äußerst kritisch: „Wer den Bau von Bohrmaschinen in Kleinserien abbilden kann, weiß noch lange nicht, was den Bau hochindividueller Messmaschinen ausmacht.“ Dabei gehe es eben nicht darum, die Stücklisten vorangegangener Aufträge zu duplizieren und darin einige Variationen vorzunehmen. Denn dass eine Anlage zweimal verkauft werde, geschehe bei Hafner nur in Ausnahmefällen. Die Regel sei vielmehr, dass jede Maschine mechanisch und elektrisch neu konstruiert werde, wobei viele Konstruktionsinhalte erst im fortlaufenden Fertigungsprozess entstehen und nach und nach unkompliziert ins ERP-System gebracht werden müssen. Da die letztlichen Ausprägungen der Maschinen meist erst weit nach Konstruktionsbeginn feststehen, war der Umgang mit dynamischen Produktstrukturen, die sich analog



DER AUTOR

Axel Schmidhäuser,
Leading Expert bei ams.Solution



Im Juni 2015 bezog die Philipp Hafner GmbH ein hochmodernes neues Firmengebäude. Im Zuge der Gebäudeplanung wurde der gesamte Fertigungsdurchlauf grundlegend analysiert und strategisch komplett neu aufgesetzt.

„allein um den Gesamteindruck und das Look & Feel“, sagt der ERP-Verantwortliche. Er verweist darauf, dass die meisten Key User nur die Arbeit mit einem weitgehend starren System gewohnt waren, weswegen sie viele der Features einer modernen ERP-Lösung gar nicht kannten. Mit Blick auf die zu erwartenden Arbeitserleichterungen seien sie von Beginn an hochmotiviert gewesen.

Dass ams.erp sogar die komplette Individualisierung der persönlichen Arbeitsbereiche erlaubt, sei dabei erst in den Schulungen klar geworden. „Bis dahin hatten wir gar nicht realisiert, wie flexibel die Anwender in der Bearbeitung ihrer täglichen Aufgaben sein werden.“

Viele Informationen lassen sich miteinander verketten und schnell auffinden. Das ist ziemlich einzigartig“, stellt Eckhard Rau fest. Der Projektleiter betont, dass diese Flexibilität nicht über aufwendige Programmieranpassungen erkaufte werden musste. Das auch von den ams-Consultants ausgegebene Ziel, selbst speziellere Prozesse komplett im Software-Standard abzubilden, wurde erreicht.

Als einen der größten Nutzen von ams.erp nennt Eckhard Rau den Effizienzgewinn, der sich aus der durchgängigen Digitalisierung der geschäftlichen Kernabläufe und den dahinterstehenden Mengengerüsten ergibt. Sämtliche Informationen rund um Bedarfsanforderungen, Mate-

„Sämtliche Informationen rund um Bedarfsanforderungen, Materialwirtschaft und Bestellungen werden **direkt im System verarbeitet** und müssen nicht mehr ausgedruckt und eingescannt werden. Ebenso werden eingehende Aufträge nicht mehr in Papierform mit handschriftlichen Vermerken weitergegeben.“

Axel Schmidhäuser

zum Projektfortschritt mitentwickeln, eines der zentralen Kriterien.

Flexible Informationsbereitstellung

Das Rennen machte ams.erp von ams.Solution. Über die Stücklistenstrukturen und die Artikelverwaltung hinaus überzeugte das System die Key User vor allem mit seiner anpassungsfähigen Bedienbarkeit. „Neben den Funktionalitäten für eine bessere Projektabwicklung ging es vor-

rialwirtschaft und Bestellungen werden direkt im System verarbeitet und müssen nicht mehr ausgedruckt und eingescannt werden. Ebenso werden eingehende Aufträge nicht mehr in Papierform mit handschriftlichen Vermerken weitergegeben. Vielmehr werden die empfangenen Mails samt den PDF-Dokumenten der Angebote automatisch im System hinterlegt und dokumentiert.

Somit stehen allen Projektbeteiligten jederzeit sämtliche relevanten Informationen digital zur Verfügung. •



noris network

SOUVERÄNITÄT FÜR KI – MADE IN GERMANY Von High-Density Housing bis zum souveränen LLMAaaS

- **Flexible Abrechnungsmodelle:** tokenbasierte Nutzung bis zum dedizierten KI-Cluster
- **Vertrauenswürdig:** Datenverarbeitung in Deutschland ohne Speicherung von Tokens
- **Performant & verfügbar:** Neuste GPU-Generationen mit redundantem Design
- **Full Managed Service:** Betrieb des gesamten Software-Stacks bis zum API-Endpunkt
- **High-Performance Housing:** Wassergekühlte GPU-Cluster im Referenzdesign bis 200 kVA
- **High-Density-Kühlung:** Luftgekühlte Racks bis 50 kVA für High-End-GPUs

Vom schönen Scheitern: KI im Enterprise-Stack

KI ist überall angekommen, doch oft nur als Spielwiese.

Damit Large Language Models (LLMs) echten Mehrwert liefern, brauchen sie mehr als gute Formulierungen: Sie brauchen Kontext. Nur tief verknüpft mit Firmendaten und Prozessen wird aus dem Hype ein verlässliches Enterprise-Werkzeug. /// von Ron Boes

KI IST IN DEN UNTERNEHMEN ANGEKOMMEN – ZUMINDEST AUF DEN ERSTEN BLICK. Texte werden automatisiert erstellt, Produktbeschreibungen übersetzt, E-Mails zusammengefasst, Chatbots getestet. Kaum eine Digitalstrategie kommt noch ohne KI-Bezug aus.

Und doch bleibt der Schritt vom Experiment in den produktiven Betrieb schwierig. Auch Studien zeigen das. Eine aktuelle Omdia-Befragung unter 1.130 Endanwendern und Entscheidern zeigt beispielsweise: Rund 89 Prozent der Unternehmen optimieren ihre Geschäftsprozesse noch nicht gezielt mit KI. Nur 18 Prozent haben umfassende Kennzahlen für alle KI-Anwendungen definiert. Vielen fehlt damit die Grundlage, um zu bewerten, ob KI-Projekte tatsächlich Zeit sparen, Kosten senken oder zusätzlichen Umsatz bringen. KI wird also vielerorts ausprobiert. Genau hier beginnt aber die eigentliche Herausforderung: Ein Large Language Model, das überzeugend formuliert, ist noch lange kein verlässlicher Bestandteil eines Unternehmensprozesses. Aber warum?

Ein LLM kennt keine Kundenhistorie, keine Vertragsdetails, keine offenen Tickets, keine Preislogiken und keine internen Freigaberegeln. Es kann Sprache erzeugen, versteht aber nicht automatisch, welche Antwort in einem konkreten Geschäftskontext richtig, zulässig und hilfreich ist.

Gerade in komplexen Enterprise-Landschaften mit CRM, Commerce, Service, Marketing Automation, ERP und Datenplattformen entsteht der Mehrwert nicht durch das Modell allein. Er entsteht dadurch, dass ein LLM mit dem richtigen Kontext verbunden wird.

Ein Service-Chatbot muss wissen, wer der Kunde ist, welche Produkte im Einsatz sind, welche Service-Level gelten und welche Fälle offen sind. Ein Sales Assistant wird erst dann nützlich, wenn er Aktivitäten, Angebote, Bestellungen, Gesprächsnotizen und aktuelle Kundensignale zusammenführen kann. Erst dann wird aus einer generischen KI-Antwort eine belastbare Empfehlung.

Der Use Case entscheidet

Viele KI-Initiativen starten mit der Technologie. Neue Tools sind schnell verfügbar, Demos beeindrucken und die Einstiegshürde ist niedrig. Aus Business-Sicht ist das aber selten der richtige Ausgangspunkt.

Die entscheidenden Fragen lauten: Wo entsteht Reibung im Prozess? Wo verlieren Kunden Orientierung oder

Vertrauen? Wo verbringen Mitarbeitende zu viel Zeit mit manuellen Aufgaben? Und wo kann KI einen messbaren Unterschied machen?

Hier sind einige erfolgreiche Beispiele: Im Commerce kann ein KI-gestützter Verkaufsberater Kunden durch komplexe Entscheidungen führen. Im Service kann ein virtueller Agent Anfragen analysieren, klassifizieren, übersetzen und Lösungsvorschläge machen. Im Vertrieb kann KI relevante Informationen bündeln und Besuchsvorbereitung oder Nachbereitung vereinfachen.

KI ist in diesen Szenarien wertvoll, weil sie einen konkreten Prozess verbessert: durch schnellere Reaktionen im Service, bessere Conversion im Commerce, eine vollständigere Datenbasis im Vertrieb oder spürbare Entlastung der Mitarbeitenden.

Transparenz schafft Vertrauen

Aber wie gelingt das? Sobald LLMs produktiv eingebunden werden, reicht es nicht, wenn eine Antwort plausibel klingt. Unternehmen müssen genau nachvollziehen können, warum eine Antwort entstanden ist, welche Daten genutzt wurden und welche Aktion ein System ausführt oder vorschlägt.

Diese Transparenz bedeutet: Kontrolle über Datenquellen, Berechtigungen, Prozesslogik, Systemzugriffe, Aktionen und Übergaben an Menschen. Dafür braucht es klare Leitplanken: Welche Daten darf ein LLM verwenden? Welche Systeme darf es abfragen? Welche Aktionen darf es ausführen? Wann braucht es eine menschliche Freigabe? Und wie lässt sich später prüfen, warum ein bestimmter Vorschlag gemacht wurde? Erst wenn diese Fragen beantwortet sind, entsteht Vertrauen – bei Kunden, Mitarbeitenden und im Management.

Vom Pilotprojekt zur Enterprise-Fähigkeit

In vielen Unternehmen entstehen KI-Initiativen zunächst in einzelnen Fachbereichen. Das ist nicht falsch. Problematisch wird es, wenn daraus eine unverbundene Landschaft aus Pilotprojekten entsteht: viele einzelne Tools, viele Datensilos, aber keine gemeinsame Grundlage für Skalierung, Sicherheit und Kontrolle. Das Grundproblem dieser Situation: auf diese Weise wird es niemals gelingen, zu einer Skalierung von KI auf die gesamten Unternehmensprozesse zu gelangen.

DER AUTOR

Ron Boes ist Director Portfolio & Innovation bei SYBIT.



„Sobald LLMs produktiv eingebunden werden, reicht es nicht, wenn eine Antwort plausibel klingt. Unternehmen müssen **genau nachvollziehen** können, warum eine Antwort entstanden ist, welche Daten genutzt wurden und welche Aktion ein System ausführt oder vorschlägt.“

Ron Boes

KI braucht im Enterprise-Kontext deshalb eine Architektur, die wiederverwendbar ist. Sie muss grundlegende Funktionen bereitstellen: Datenanbindung, Integration, Sicherheitskonzepte, Rollenmodelle, Monitoring, Orchestrierung und Schnittstellen zu bestehenden Systemen.

Auf dieser Basis lassen sich dann nachhaltig unterschiedliche KI-Anwendungen entwickeln: ein Service Agent, ein Sales Assistant, ein digitaler Verkaufsberater oder eine interne Wissenssuche. Unternehmen müssen dann nicht bei jedem Use Case von vorne beginnen. Sie schaffen eine Grundlage, auf der neue Anwendungen schneller, sicherer und kontrollierter entstehen können.

KI wird zur Fähigkeit der Organisation

Konzepte wie Retrieval Augmented Generation, Tool Calling, Agenten oder standardisierte Schnittstellen wie das Model Context Protocol prägen derzeit ebenfalls die Diskussion. Entscheidend ist aus Business-Sicht aber auch hier die Steuerung: Ein Agent beispielsweise braucht ebenfalls eindeutige Ziele, definierte Datenzugriffe, Berechtigungen, Eskalationsregeln und Protokollierung. Die gute Nachricht: Unternehmen müssen dafür nicht erst ein perfektes Datenprojekt abschließen. Aber sie müssen verstehen, welche Daten für welchen Use Case relevant sind, in welcher Qualität sie vorliegen und wie sie kontrolliert genutzt werden können. Ebenso wichtig ist die Einbindung der Fachbereiche.

Gute KI-Use-Cases entstehen dort, wo Mitarbeitende täglich mit Kunden, Prozessen und Systembrüchen arbeiten.

Hier kann auch oft klein gestartet werden, wenn der richtige Ansatz gewählt wird. Am Ende geht es darum:

1. Relevante Use Cases finden
2. Business Impact & Machbarkeit priorisieren
3. Daten & Architektur vorbereiten
4. Menschen befähigen

LLMs werden Customer Experience nicht allein verändern. Verändern werden sie Unternehmen, die KI ganzheitlich mit ihren Prozessen, Daten und Systemen verbinden. KI im Enterprise-Stack ist dann nichts weniger als eine grundlegende neue Fähigkeit der Organisation.

Die zentrale Frage lautet: Wie schaffen Unternehmen die Grundlage, damit diese Integration transparent, kontrollierbar und skalierbar wird?

Die Antwort lautet: Durch die passende Enterprise Architektur. Wer diese Grundlage schon jetzt bei „kleineren“ Use Cases legt, kann KI nicht nur ausprobieren. Er kann sie nach und nach produktiv über alle Geschäftsprozesse hinweg nutzen – und zwar dort, wo sie Kundenbeziehungen, Mitarbeitende und Geschäftsprozesse wirklich besser macht. •

Strategien für intelligentes Content Management

Unternehmen sind heute gefordert, aus unstrukturierten Daten in Verträgen oder Berichten einen Mehrwert zu holen. Box hat kürzlich mit KI Agent eine Lösung präsentiert, mit der sich datenschutzkonform Inhalte analysieren und Prozesse automatisieren lassen. Michael Pietsch von Box erklärt im Gespräch, warum eine zentrale Content-Verwaltung und genau definierte Governance heute so wichtig sind. /// von Stefan Girschner

Herr Pietsch, Box hat sein KI-gestütztes Lösungsportfolio Box AI kürzlich um den KI Agent erweitert. Welche Funktionen bietet der KI Agent Anwendern und wie lässt sich dieser in vorhandene Anwendungen integrieren?

Michael Pietsch | Der Box Agent geht über klassische KI-Assistenten hinaus: Er versteht Anfragen in natürlicher Sprache, analysiert Unternehmensinhalte und verarbeitet auch große Mengen unstrukturierter Daten wie Verträge, Berichte oder Präsentationen. Für Anwender bedeutet das vor allem eine deutliche Zeitersparnis, da der Box Agent Dokumente zusammenfassen, Inhalte vergleichen, Handlungsempfehlungen ableiten und auch neue Dokumente erstellen kann. Zudem ist er in der Lage, mehrstufige Aufgaben eigenständig auszuführen. Ein besonderer Vorteil ist die direkte Integration in die Box-Plattform, wodurch der Agent unmittelbar auf vorhandene Unternehmensinhalte zugreift. Über Box AI Studio können Unternehmen darüber hinaus eigene Agenten entwickeln und individuell

an ihre Anforderungen anpassen. In Verbindung mit Box Automate lassen sich diese Agenten nahtlos in bestehende Workflows und Geschäftsprozesse einbinden.

Wie verändert die Integration von KI-Agenten die Arbeitsweise und Prozesse in Unternehmen?

MP | Wir beobachten derzeit einen grundlegenden Wandel. KI wird nicht mehr nur zur Informationssuche oder Inhaltserstellung eingesetzt, sondern übernimmt zunehmend eigenständig Aufgaben. Mitarbeitende erhalten direkt Ergebnisse, Analysen und Handlungsempfehlungen, statt Informationen aus verschiedenen Quellen manuell zusammenzutragen. Besonders bei wiederkehrenden Prozessen wie Vertragsprüfung, Rechnungsverarbeitung oder Onboarding können KI-Agenten viele Schritte automatisieren und auf Unternehmenswissen zugreifen. Das ermöglicht schnellere Entscheidungen, höhere Produktivität und besser skalierbare Prozesse.

„ KI wird nicht mehr nur zur Informationssuche oder Inhaltserstellung eingesetzt, sondern übernimmt zunehmend eigenständig Aufgaben.

Michael Pietsch



DER GESPRÄCHSPARTNER

Michael Pietsch

ist Vice President DACH & Eastern Europe bei Box. Er verfügt über mehr als 20 Jahre Erfahrung in der IT-Branche und hatte Führungspositionen bei Oracle, Rubrik, Boomi, EMC und Palo Alto Networks inne. Pietsch beschäftigt sich unter anderem mit der digitalen Transformation, der Zukunft der Arbeit und den Auswirkungen von KI auf Unternehmen.

Bild: Box

Der Mensch bleibt zentraler Bestandteil der Wertschöpfung: Kritische Entscheidungen werden weiterhin von Mitarbeitenden getroffen, während Routineaufgaben zunehmend durch KI automatisiert werden. Gleichzeitig entstehen durch den Einsatz von KI neue Berufsbilder entlang der Wertschöpfungskette, insbesondere an der Schnittstelle zwischen Technologie, Daten und Geschäftsprozessen. Die Kombination aus menschlicher Expertise und KI verändert damit nicht nur die Arbeitsweise von Unternehmen, sondern auch die Rollen und Anforderungen im Arbeitsmarkt nachhaltig.

Welcher Maßnahmen sind erforderlich, um KI sicher und datenschutzkonform nutzen zu können? Ist hierfür die Implementierung einer Sicherheitsarchitektur von Drittanbietern erforderlich?

MP | Der sichere Einsatz von KI beginnt nicht bei der Technologie, sondern bei klaren Governance-Regeln. Unternehmen benötigen Transparenz über Datenzugriffe, Berechtigungen und die Nutzung von KI-Systemen. Deshalb wurde der Box Agent von Anfang an auf Basis unserer bestehenden Sicherheits-, Governance- und Compliance-Architektur entwickelt. Er greift ausschließlich auf Inhalte zu, für die Nutzer bereits berechtigt sind, und Kundendaten werden nicht zum Training externer Sprachmodelle verwendet.

Mit Lösungen wie Box Zones und Box Shield oder Box Governance unterstützen wir Unternehmen zudem bei Datenschutz, Datenresidenz und Compliance-Anforderungen. Zusätzliche Sicherheitssysteme von Drittanbietern sind grundsätzlich nicht erforderlich, da wir Governance, Sicherheit und KI in einer integrierten Plattform zusammenführen.

In einer neuen Studie hat Box den Einsatz von KI-Agenten in Unternehmen untersucht: Demnach erzielen bereits 80 Prozent der Unternehmen einen ROI von mindestens zehn Prozent. Welche Maßnahmen empfehlen Sie, um das Potenzial von KI-Systemen optimal zu nutzen und diese verantwortungsvoll steuern zu können?

MP | Die Ergebnisse des „State of AI in the Enterprise Report 2026“ zeigen, dass erfolgreicher KI-Einsatz heute vor allem eine Organisationsfrage ist. Die Unternehmen mit den höchsten Erträgen setzen KI nicht isoliert ein, sondern integrieren sie systematisch in ihre Geschäftsprozesse.

Drei Faktoren sind dabei entscheidend: Erstens benötigen KI-Agenten Zugang zu vertrauenswürdigen Unternehmenswissen. Das bedeutet vor allem, dass unstrukturierte Daten aus Dokumenten, Verträgen oder Präsentationen erschlossen, normalisiert und in strukturierte, semantisch nutzbare Daten überführt werden müssen. Nur so entsteht eine belastbare Grundlage für hochwertige KI-Ergebnisse. Zweitens müssen Governance-, Sicherheits- und Compliance-Strukturen von Anfang an mitgedacht werden. Und drittens sollten Unternehmen auf offene Plattformen setzen, um nicht von einzelnen Technologien oder Anbietern abhängig zu werden. Unsere Empfehlung lautet daher, mit konkreten Anwendungsfällen zu starten, den Geschäftsnutzen messbar zu machen und KI-Agen-

ten als Bestandteil durchgängiger Workflows zu etablieren. Dort entstehen die größten Produktivitäts- und Effizienzgewinne.

Box verspricht Unternehmen, mit einer intelligenter Content Management-Plattform mehr aus den vorhandenen unstrukturierten Daten herausholen zu können. Welche Strategie empfehlen Sie auf dem Weg zu einem intelligenten Content Management? Und wie kann Box seine Kunden dabei unterstützen?

MP | Der wichtigste Schritt ist, Inhalte nicht nur als Dokumente, sondern als strategischen Unternehmenswert zu verstehen. Zwar verfügen Unternehmen über einen großen Wissensschatz in Verträgen, Berichten oder Präsentationen, dieser bleibt jedoch häufig unstrukturiert und verteilt über verschiedene Bereiche im Unternehmen, wodurch er nur eingeschränkt nutzbar ist.

Für intelligentes Content Management müssen Inhalte zentral verfügbar sein, über ihren gesamten Lebenszyklus hinweg strukturiert verwaltet werden und durch klare Governance sowie Metadaten unterstützt werden. Box unterstützt genau diesen Ansatz durch zentrale Content-Verwaltung, automatische Strukturierung und die Nutzung von Wissen aus unstrukturierten Daten. Mit Box AI, Box Agent, Box Automate und Box AI Studio lassen sich Inhalte analysieren, in Prozesse überführen und individuell anpassen. Der Mehrwert entsteht vor allem durch die intelligente Nutzung bereits vorhandener Informationen, die bessere Entscheidungen, effizientere Prozesse und mehr Innovation ermöglicht.

Natürlich möchten wir auch die digitale Souveränität ansprechen: Welche Vorgehensweise empfehlen Sie Unternehmen aus dem DACH-Raum, unabhängiger von den großen US-Hyperscalern zu werden?

MP | Das Ziel ist nicht die vollständige Entkopplung von internationalen Technologieanbietern, sondern digitale Souveränität. Unternehmen müssen jederzeit die Kontrolle darüber behalten, wo Daten gespeichert und verarbeitet werden, wer Zugriff hat und welche Technologien eingesetzt werden.

Im DACH-Raum bedeutet das den Einsatz offener, flexibler Plattformen, die Datenresidenz, transparente Zugriffsrechte und eine Vermeidung von Abhängigkeiten von einzelnen KI- oder Cloud-Anbietern ermöglichen. Dazu gehören die gezielte Steuerung von Datenstandorten, regionale Speicheroptionen, die Kontrolle von Verschlüsselungsschlüsseln sowie ein zentrales Governance- und Compliance-Modell.

Mit Box wird dieser Ansatz umgesetzt: Über Box Zones können Inhalte in Regionen wie der EU und künftig der Schweiz gespeichert und verarbeitet werden. Gleichzeitig bleibt die Nutzung unterschiedlicher KI-Anbieter möglich, ohne eine exklusive Bindung einzugehen. Digitale Souveränität bedeutet damit nicht weniger Innovation, sondern den kontrollierten Einsatz moderner KI-Technologien im Rahmen von Compliance- und Geschäftsanforderungen. •

Krypto-Agilität: Pflicht für Zulieferer

Juli 2026: Die Schonfrist ist vorbei. Zwei Jahre nach den finalen NIST-Standards für Post-Quanten-Kryptografie (PQC) drängen BSI und Konzerne auf Umsetzung. Für den Mittelstand wird „Krypto-Agilität“ von der abstrakten Theorie zur harten architektonischen Anforderung für den Marktzugang – besonders in der vernetzten Lieferkette.

/// von Heiner Sieger

Der große Umbau: Warum Krypto-Agilität jetzt über den Marktzugang entscheidet

Wer im Sommer 2026 noch glaubt, das Thema Quantencomputer-resistente Verschlüsselung sei reine Zukunftsmusik für Forschungslabore, der hat den entscheidenden Taktwechsel in der Industrie verpasst. Die Zeit der akademischen Diskussionen ist vorbei. Seit die US-Behörde NIST (National Institute of Standards and Technology) die ersten Standards für Post-Quanten-Kryptografie (PQC) finalisiert hat – namentlich Algorithmen für den Schlüsselaustausch und digitale Signaturen –, läuft der Countdown für die Wirtschaft.

Doch die eigentliche Herausforderung, vor der IT-Architekten und CTOs im Mittelstand heute stehen, ist nicht mathematischer, sondern struktureller Natur. Es geht nicht nur darum, einen alten Algorithmus wie RSA durch einen neuen zu ersetzen. Es geht um eine fundamentale Än-

derung der Systemarchitektur hin zur „Krypto-Agilität“.

Die tickende Zeitbombe

Jahrzehntlang wurde Kryptografie in Software und Firmware oft stiefmütterlich behandelt. Verschlüsselungsbibliotheken wurden tief in den Applikationscode eingebacken, Zertifikate fest verdrahtet. „Never touch a running system“ galt insbesondere für die Sicherheitsschicht.

Diese monolithische Architektur ist im Jahr 2026 eine tickende Zeitbombe. Krypto-Agilität bedeutet die Fähigkeit eines Systems, kryptografische Mechanismen – Algorithmen, Schlüssellängen, Protokolle – mit minimalem Aufwand und idealerweise ohne Unterbrechung des laufenden Betriebs auszutauschen. Dustin Moody, Mathematiker beim NIST und Leiter des PQC-Standardisierungsprojekts, warnte bereits früh vor der Komplexität dieser Aufgabe: „Der Übergang zur Post-Quanten-Kryptografie wird

ein langer, komplizierter Prozess sein. Er wird nicht über Nacht geschehen.“

Heute zeigt sich: Wer diese Warnung ignoriert hat und seine Systeme nicht architektonisch entkoppelt hat, steht vor einem massiven Problem. Anstatt dass eine Maschinensteue-

„ Krypto-Agilität bedeutet die Fähigkeit eines Systems, kryptografische Mechanismen – Algorithmen, Schlüssellängen, Protokolle – mit **minimalem Aufwand** und idealerweise ohne Unterbrechung des laufenden Betriebs **auszutauschen**.

Heiner Sieger

DER AUTOR

Heiner Sieger

ist Chefredakteur des Magazins Digital Business. Für die Recherchen setzte er einen Verlagsinternen KI-Assistenten ein.

rung direkt eine spezifische Bibliothek aufruft, muss sie über eine abstrakte Schnittstelle, einen „Crypto-Wrapper“, kommunizieren, der im Hintergrund die aktuell sicherste Methode bereitstellt.

BSI und Verbände erhöhen den Druck

Diese architektonische Flexibilität ist keine Kür mehr, sondern Pflicht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland hat seine Tonlage über die Jahre deutlich verschärft und drängt nun, Mitte 2026, massiv auf die technische Umsetzung in der Breite. Die Haltung der Behörde ist seit langem klar und heute aktueller denn je: „Das BSI empfiehlt, bereits jetzt Maßnahmen für die Migration zu quantencomputer-resistenter Kryptografie zu ergreifen“, heißt es in den grundlegenden Positionspapieren. Und weiter: „Ein Abwarten, bis leistungsfähige Quantencomputer verfügbar sind, ist keine Option, da die Migration komplexer Systeme viel Zeit in Anspruch nehmen wird.“

Dieser regulatorische Druck trifft auf eine nervöse Lieferkette. Besonders im Maschinen- und Anlagenbau sowie der Automobilindustrie, den Herzstücken der DACH-Wirtschaft, wächst die Unruhe. Das Problem sind die Produktlebenszyklen. Eine Produktionsmaschine oder ein Steuergerät in einem Fahrzeug, das 2026 ausgeliefert wird, ist oft noch weit bis in die 2030er Jahre im Einsatz.

Branchenverbände warnen ihre Mitglieder: Große OEMs passen ihre Einkaufsbedingungen an. Wer als Tier-N-Zulieferer keine Roadmap für Krypto-Agilität in seinen Komponenten vorweisen kann, wird bei Neuprojekten zunehmend aussortiert. Die Konzerne wollen das Risiko „veraltete Kryptografie“ nicht importieren. Krypto-Agilität wird damit vom IT-Security-Thema zum harten Kriterium für den Marktzugang.

Handungsleitfaden:

Vom Inventar zur Migration

Für mittelständische Unternehmen bedeutet dies, dass sie jetzt handeln müssen. Aber wie? Der Umbau der Architektur geschieht nicht über Nacht.

Experten raten zu einem pragmatischen Drei-Stufen-Plan.

- **Schritt eins** ist die schonungslose Inventur. Die wenigsten Unternehmen wissen genau, wo in ihrer heterogenen IT- und OT-Landschaft welche Verschlüsselung eingesetzt wird. Wo verstecken sich alte RSA-Schlüssel in der Firmware von Sensoren? Ohne automatisierte Tools zur „Crypto Discovery“ ist dieser Wildwuchs kaum zu bändigen. Man muss wissen, was man hat, bevor man es agil machen kann.
- **Schritt zwei** ist die Risikoanalyse und Priorisierung. Nicht jedes System muss sofort umgebaut werden. Entscheidend ist die Lebensdauer der Daten und der Systeme. Daten, die auch in zehn Jahren noch vertraulich sein müssen, haben höchste Priorität. Hier greift das Bedrohungsszenario „Harvest Now, Decrypt Later“ (siehe Kasten). Jen Easterly, Direktorin der US-Cybersicherheitsbehörde CISA, brachte die globale Dringlichkeit auf den Punkt: „Quantencomputing stellt eine neue Grenze technologischer Möglichkeiten dar, aber es stellt auch eine einzigartige und existenzielle Bedrohung für unsere Datensicherheit dar. Wir müssen jetzt handeln, um uns auf eine Post-Quanten-Zukunft vorzubereiten.“
- **Schritt drei** ist die architektonische Umsetzung. Hier gilt die Faustregel: „Build new agile, wrap old secure.“ Neue Softwareprojekte sollten von Tag eins an krypto-agil konzipiert werden, unter Nutzung moderner Abstraktionsschichten. Bei Legacy-Systemen helfen oft vorgelagerte Sicherheits-Gateways, die die moderne Kommunikation nach außen übernehmen.

Quintessenz: Agilität als Versicherung

Die Umstellung auf krypto-agile Architekturen ist ein Kraftakt. Doch die Investition ist alternativlos. Im Juli 2026 ist klar: Krypto-Agilität ist die notwendige Versicherung für die digitale Souveränität in der kommenden Ära. Wer jetzt die Architektur öffnet, bleibt im Geschäft. •

DIE BEDROHUNG: HARVEST NOW, DECRYPT LATER (HNDL)

Warum die Eile, wenn leistungsfähige Quantencomputer vielleicht erst in einigen Jahren verfügbar sind? Der Grund ist die Angriffsstrategie „Harvest Now, Decrypt Later“.

Staatliche Akteure und hochspezialisierte kriminelle Gruppen saugen bereits heute massenhaft verschlüsselten Datenverkehr ab (Harvest Now). Sie können ihn zwar aktuell mit herkömmlichen Methoden nicht entschlüsseln, speichern ihn aber kostengünstig in riesigen Data Lakes. Sobald ein ausreichend starker Quantencomputer verfügbar ist – der sogenannte „Q-Day“ – können diese alten Datenbestände nachträglich entschlüsselt werden (Decrypt Later). Für Unternehmen bedeutet das: Jedes heute verschlüsselte Datum, das auch im Jahr 2030 oder 2035 noch geheim sein muss (z.B. langfristige Geschäftsstrategien, Forschungsergebnisse, biometrische Daten), ist bereits jetzt gefährdet, wenn es nicht mit post-quanten-sicheren Verfahren geschützt wird.



NEWS

CYBER RESILIENZ: DREI VIERTEL DER UNTERNEHMEN BERICHTEN VON SICHERHEITSVORFÄLLEN

In den vergangenen zwölf Monaten waren 75 Prozent der Unternehmen in Deutschland von einem Cybersicherheitsvorfall betroffen. Das zeigt eine Studie von ManageEngine. Unternehmen müssen mit einer zunehmend komplexen Bedrohungslage umgehen, zugleich aber ihre Cyberresilienz und Vorbereitungen auf mögliche Sicherheitsvorfälle kontinuierlich verbessern.

Phishing und Social Engineering prägen die Bedrohungslage weiterhin und machen mehr als die Hälfte (56 Prozent) aller erfassten Vorfälle aus. Gleichzeitig richten deutsche Unternehmen den Blick zunehmend über die aktuellen Gefahren hinaus: 45 Prozent der Befragten sehen KI-gestützte Angriffe als größtes Cyberrisiko für ihr Unternehmen in den nächsten zwölf Monaten. Das zeigt die wachsende Sorge, dass künstliche Intelligenz Cyberangriffe komplexer, leichter skalierbar und schwerer erkennbar machen könnte. •

MAINFRAME: 70 PROZENT DER AUSSTIEGSPROJEKTE WERDEN SCHEITERN

Mehr als 70 Prozent der Mainframe-Ausstiegspunkte, die 2026 angestoßen werden, erzielen nicht den erwarteten Nutzen, prognostizieren die Analysten von Gartner. Der Grund: Die Fähigkeiten von Tools auf Basis generativer KI werden überschätzt. Bis zum Jahr 2030 werden 75 Prozent der Anbieter von Mainframe-Ausstiegslösungen ihre Ausrichtung ändern oder den Betrieb einstellen, sobald die veränderten Marktbedingungen greifen.

„Zwischen den Marketingversprechen rund um GenAI und der tatsächlichen Fähigkeit dieser Technologien, komplexen Legacy-Code zu transformieren und zu migrieren, klafft eine wachsende Lücke“, so Alessandro Galimberti,

VOM PILOTPROJEKT ZUR BREITEN UMSETZUNG: WIE DER MITTELSTAND MIT KI UMGEHT

Drei von vier mittelständischen Unternehmen in Deutschland nutzen künstliche Intelligenz bereits produktiv. Doch nur jedes Vierte hat sie vollständig in ihre Kernprozesse integriert. Das geht aus der Studie „AI zwischen Vision und Umsetzung – Wie der Mittelstand den Schritt von Pilotprojekten zur breiten Umsetzung schafft“ von Cancom und ServiceNow hervor. Besonders deutlich wird laut Studie der Zusammenhang zwischen strategischer Verankerung und tatsächlichem Reifegrad: Unternehmen mit einem klaren „AI-First“-Ansatz haben KI deutlich häufiger vollständig operationalisiert als Unternehmen, die KI nur auf Bereichsebene umsetzen. •

CLOUD-DIENSTE: AUSFALL HAT MASSIVE AUSWIRKUNGEN AUF GESCHÄFTSBETRIEB

Eine Umfrage des Digitalverbands Bitkom hat ergeben, dass neun Prozent der Unternehmen in Deutschland im Moment des Ausfalls der Cloud-Dienste nicht mehr weiterarbeiten könnten. Zwei Prozent erwarten, dass sie sechs bis elf Stunden durchhalten würden. Und 24 Prozent der Unternehmen würde ein Cloud-Ausfall nicht so hart treffen, dass sie ihren Geschäftsbetrieb irgendwann einstellen müssten. •

VP Analyst bei Gartner. Gleichzeitig übe der hohe Druck von Investoren auf Anbieter starken Einfluss darauf aus, KI in ihre Angebote zu integrieren, unabhängig davon, ob dies die Ergebnisse tatsächlich spürbar verbessert.

„In Kombination mit der geschäftskritischen Bedeutung vieler Mainframe-Anwendungen, die sie faktisch too big to fail macht, sowie dem zunehmenden Verlust erfahrener Fachkräfte entsteht für Führungskräfte im Bereich Infrastruktur und Betrieb (I&O) eine gefährliche Risikolage. Schlecht geplante Ausstiegsstrategien werden dadurch zunehmend untragbar.“ •

**SECURITY INSIGHT**

Cyber Risk & Resilience

© AI Studio - R/stockadobe.com, © iamguru/stockadobe.com

Handeln, bevor es brennt

Wie sich eine mittelständische Molkerei cyberfest macht.

S. 34

Geschäftskritische Kommunikation

S. 39

Fünf Warnzeichen, bei denen Infrastruktur zum Risiko wird.

Experten-Talk

S. 36

Die richtigen Security-Strategien im Zuge der EU-Regulierungswelle.

Handeln, bevor es brennt: Eine Molkerei macht sich cyberfest

Cyberangriffe treffen die Lebensmittelindustrie längst real – mit Produktionsstillständen und Millionenschäden. Die Hohenloher Molkerei handelte, bevor der Gesetzgeber zwang: Wie der Mittelständler frühzeitig auf Cyberresilienz setzte und damit ein Signal an die ganze Branche sendet. /// von Axel Amelung

DARUM GEHT ´S

NIS-2-Richtlinie: Die europäische Vorgabe stellt deutlich strengere Anforderungen an das Cyberrisikomanagement vieler Unternehmen. Sie war ein wesentlicher Auslöser dafür, dass die Hohenloher Molkerei frühzeitig organisatorische und technische Grundlagen schuf.

ISMS & BCM: Im Mittelpunkt des Sicherheitskonzepts stand der Aufbau eines strukturierten Informationssicherheits-Management-Systems (ISMS) sowie eines Business Continuity Managements (BCM).

Proaktive Cyberresilienz: Statt erst auf regulatorischen Druck oder Sicherheitsvorfälle zu reagieren, identifizierte die Molkerei frühzeitig kritische Prozesse, legt Verantwortlichkeiten fest und baut Sicherheitsstrukturen systematisch auf. So wird die eigene Widerstandsfähigkeit gezielt gestärkt, statt sich von äußeren Anforderungen treiben zu lassen.

Gemeinsame Verantwortung: Cyberresilienz ist keine Aufgabe der IT-Abteilung allein. Nachhaltige Sicherheitsstrukturen entstehen nur, wenn Management, Fachbereiche und externe Spezialisten an einem Strang ziehen – getragen von der klaren Unterstützung aus der Unternehmensführung.

DIE DIGITALISIERUNG DER LEBENSMITTELINDUSTRIE SCHREITET MIT HOHER GESCHWINDIGKEIT VORAN.

Produktionsanlagen werden vernetzt, Lieferketten digital gesteuert und betriebliche Prozesse zunehmend automatisiert. Was Effizienz und Transparenz erhöht, vergrößert zugleich die Angriffsfläche für Cyberkriminelle. Gerade die Milchwirtschaft hat in den vergangenen Jahren erfahren, welche Auswirkungen erfolgreiche Cyberangriffe haben können: Produktionsstillstände, Lieferprobleme und erhebliche wirtschaftliche Schäden sind längst keine abstrakten Risiken mehr, sondern reale Bedrohungen für die operative Stabilität von Unternehmen.

Vor diesem Hintergrund hat die Hohenloher Molkerei eG entschieden, Informationssicherheit nicht als reine IT-Aufgabe zu betrachten, sondern als strategisches Zukunftsthema.

Rechtzeitig handeln statt zu spät reagieren

Ein wesentlicher Auslöser für diese Entscheidung war die europäische NIS-2-Richtlinie, die deutlich strengere



DER AUTOR

Axel Amelung

ist Leiter Vertrieb und Regulierungsexperte
bei TÜV Trust IT.
Bild: TÜV Trust IT





Anforderungen an das Cyberrisikomanagement vieler Unternehmen stellt. Obwohl sich die Molkerei zu Projektbeginn noch knapp unterhalb der KRITIS-Schwelle bewegte, entschied sich das Unternehmen bewusst dafür, frühzeitig die notwendigen organisatorischen und technischen Grundlagen zu schaffen.

Das Ziel war klar definiert: nicht erst auf regulatorischen Druck zu reagieren, sondern die eigene Resilienz proaktiv zu stärken und die Entwicklung bewusst selbst zu gestalten – statt sich von äußeren Anforderungen treiben zu lassen.

Genau darin liegt eine wichtige Erkenntnis für die gesamte Branche. Cyberresilienz entsteht nicht erst dann, wenn gesetzliche Vorgaben greifen oder Sicherheitsvorfälle eintreten. Erfolgreiche Unternehmen beginnen frühzeitig damit, kritische Prozesse zu identifizieren, Verantwortlichkeiten festzulegen und Sicherheitsstrukturen systematisch aufzubauen.

Maßgeschneiderte Sicherheitsstrukturen für den Mittelstand

Gemeinsam mit dem Team der TÜV Trust IT entwickelte die Hohenloher Molkerei ein Sicherheitskonzept, das gezielt auf die Unternehmensgröße und die spezifischen Anforderungen der Branche zugeschnitten ist.

Im Mittelpunkt stand der Aufbau eines strukturierten Informationssicherheits-Management-Systems (ISMS) sowie eines Business Continuity Managements (BCM). Der Ansatz war dabei bewusst pragmatisch: keine überdimensionierten Compliance-Strukturen, sondern eine wirtschaftlich angemessene Lösung, die den tatsächlichen Risiken und Anforderungen der Organisation entspricht.

In mehreren Projektphasen wurden der bestehende Sicherheitsstatus analysiert, kritische Geschäftsprozesse identifiziert und klare Verantwortlichkeiten für die Informationssicherheit definiert. So entstand Schritt für Schritt eine belastbare Sicherheitsstruktur, die sowohl zukünftigen regulatorischen Anforderungen gerecht wird als auch die operative Stabilität der Molkerei nachhaltig stärkt.

Der Ansatz zeigt exemplarisch, worauf es im Mittelstand ankommt: Informationssicherheit muss zur Organisation passen. Entscheidend ist nicht die größtmögliche Anzahl an Maßnahmen, sondern ein ausgewogenes Verhältnis zwischen Risiko, Aufwand und betrieblichem Nutzen.

Klare Unterstützung aus der Unternehmensführung

Der Erfolg des Projekts basiert maßgeblich auf der klaren Unterstützung durch die Geschäftsführung.

Für Martin Boschet, geschäftsführender Vorstand der Hohenloher Molkerei eG, ist Informationssicherheit eine strategische Entscheidung: „Informationssicherheit ist für uns ein zentrales Zukunftsthema. Deshalb haben wir uns bewusst dafür entschieden, rechtzeitig die richtigen Strukturen aufzubauen. Mit diesem Projekt haben wir den richtigen Weg eingeschlagen und mit unserem Partner genau die Unterstützung gefunden, die wir dafür brauchen.“ Die Zusammenarbeit sei geprägt von Vertrauen, Pragmatismus und einem klaren Verständnis für die Anforderungen des Unternehmens. Auch Arnd Wollinger, Prokurist und kaufmännischer Leiter der Hohenloher Molkerei, treibt das gemeinsame Projekt operativ voran.

Für andere Unternehmen der Lebensmittelindustrie liefert das Projekt eine wichtige Erkenntnis: Cyberresilienz ist keine Aufgabe der IT-Abteilung allein. Nachhaltige Sicherheitsstrukturen entstehen nur dann, wenn Management, Fachbereiche und externe Spezialisten gemeinsam an einem Strang ziehen.

Die Zusammenarbeit mit der Hohenloher Molkerei zeigt, wie erfolgreich Informationssicherheit umgesetzt werden kann, wenn Management, Fachbereiche und Partner an einem Strang ziehen. Der pragmatische Ansatz des Unternehmens und die klare strategische Entscheidung für mehr Cyberresilienz sind entscheidende Erfolgsfaktoren. Die Hohenloher Molkerei setzt damit bereits heute ein wichtiges Zeichen für die gesamte Milchwirtschaft. Während viele Unternehmen noch am Anfang der Auseinandersetzung mit Themen wie Cyberresilienz und Business Continuity stehen, wurden hier frühzeitig die notwendigen Grundlagen geschaffen.

Die Erfahrung aus diesem Projekt zeigt deutlich: Auch mittelständische Unternehmen können sich strukturiert und wirtschaftlich angemessen auf steigende Cyberrisiken vorbereiten. Entscheidend ist ein Ansatz, der regulatorische Anforderungen berücksichtigt und gleichzeitig zur Größe, Organisation und Realität des Unternehmens passt.

Die Hohenloher Molkerei hat diesen Weg rechtzeitig eingeschlagen und sendet damit ein starkes Signal an die gesamte Branche. Denn Cyberresilienz beginnt nicht mit einer gesetzlichen Verpflichtung, sondern mit der strategischen Entscheidung, Verantwortung für die eigene Zukunftsfähigkeit zu übernehmen. •

Security-Strategien im Zuge der EU-Regulierungswelle

In diesem Jahr sind von der EU verabschiedete Cybersicherheitsgesetze wie NIS2, Digital Operational Resilience Act (DORA) und Cyber Resilience Act (CRA) von der Bundesregierung in deutsches Recht umgesetzt worden. Welche Maßnahmen und Strategien empfehlen Sie Unternehmen, um die Vorgaben zu erfüllen und die aktuell gültigen Standards bei Governance, Compliance und Cyberresilienz zu erfüllen? /// von Stefan Girschner

DR. STEPHAN KILLICH

Mitglied der Geschäftsführung bei der ConSense GmbH

(Bild: Consense)

Unternehmen sollten die aktuellen regulatorischen Anforderungen nicht als einzelne Compliance-Projekte betrachten, sondern als Chance, ihre Governance-, Risk- und Compliance-Strukturen nachhaltig weiterzuentwickeln. Entscheidend ist dabei ein integrierter Ansatz, der Informationssicherheit, Risiko- und Qualitätsmanagement miteinander verbindet.

Ein erster Schritt ist eine strukturierte Bestandsaufnahme: Wo steht das Unternehmen heute im Vergleich zu den Anforderungen von NIS2, DORA oder CRA? Auf dieser Grundlage lassen sich Handlungsfelder identifizieren,

Verantwortlichkeiten festlegen und wirksame Maßnahmen ableiten. Wichtig ist, dass Risiken nicht nur punktuell betrachtet, sondern kontinuierlich bewertet und gesteuert werden. Ebenso entscheidend sind transparente Prozesse und ei-

ne nachvollziehbare Dokumentation. Nur wenn Zuständigkeiten, Maßnahmen und Nachweise klar geregelt sind, lässt sich Compliance dauerhaft sicherstellen. Regelmäßige Audits und ein konsequentes Maßnahmenmanagement helfen dabei, Schwachstellen frühzeitig zu erkennen und gezielt zu adressieren. Gleichzeitig entsteht Cyberresilienz nicht allein durch Technik. Gut geschulte Mitarbeitende, ein hohes Sicherheitsbewusstsein und klare Kommunikationswege im Ernstfall sind wesentliche Erfolgsfaktoren. Auch Notfall- und Wiederanlaufpläne sollten regelmäßig überprüft werden.

Die größte Herausforderung besteht heute oft nicht darin, einzelne Anforderungen umzusetzen, sondern diese dauerhaft und effizient im Unternehmensalltag zu verankern. Eine zentrale Plattform für Prozesse, Risiken, Maßnahmen und Nachweise kann Unternehmen dabei unterstützen, regulatorische Vorgaben nachhaltig zu erfüllen und ihre Organisation kontinuierlich weiterzuentwickeln. •



RALF SIEFEN,

CEO und Vorsitzender der Geschäftsführung der Data Center Group

(Bild: DC-Datacenter-Group GmbH)

Die neuen regulatorischen Anforderungen verdeutlichen: Cyberresilienz endet nicht an der Firewall. Wer digitale Prozesse, kritische Anwendungen und sensible Daten schützen will, muss auch die physische Infrastruktur konsequent in die Sicherheitsstrategie einbeziehen. Dazu gehört zunächst eine fundierte Analyse der bestehenden IT- und Rechenzentrumsumgebung: Wo liegen geschäftskritische Systeme? Wie ausfallsicher sind Energieversorgung, Kühlung, Brandschutz, Zutrittskontrolle und Monitoring? Welche Abhängigkeiten bestehen zu Dienstleistern, Standorten und Lieferketten?

Auf dieser Basis braucht es eine klare Strategie, die technische, organisatorische und bauliche Maßnahmen verbindet. Aus unserer Sicht sind drei Aspekte zentral: Erstens müssen Governance, Verantwortlichkeiten,

Dokumentation, Risikoanalysen und Notfallprozesse geregelt und regelmäßig überprüft werden. Zweitens sollten Unternehmen auf Standards bei Verfügbarkeit, physischer Sicherheit, Betriebskonzepten, Wartung und Lifecycle-Management setzen. Drittens ist Resilienz als Prozess zu verstehen: Redundanzen, regelmäßige Tests, Notfallübungen, Monitoring sowie Schulungen helfen, Risiken frühzeitig zu erkennen und im Ernstfall handlungsfähig zu bleiben. NIS2, DORA und CRA erhöhen den Druck, schaffen aber auch Klarheit: Die Rechenzentrums-Infrastruktur ist ein zentraler Bestandteil der Resilienz von Unternehmen. •

**TIM BERGHOF**

Security Evangelist bei der G Data CyberDefense AG

(Bild: G Data CyberDefense AG)

Es ist eine positive Entwicklung, dass IT-Sicherheit Eingang in immer mehr neue Gesetze findet. Geschäftsführungen sind nun in letzter Konsequenz für die Sicherheit und Resilienz des Unternehmens verantwortlich. Die Verabschiedung eines Gesetzes oder das Datum des Inkrafttretens macht aber noch kein Unternehmen sicher. Jetzt ist Tempo bei der Umsetzung gefragt. Und hier besteht noch an zahlreichen Stellen erheblicher Nachholbedarf. Wir erleben im direkten Austausch mit Kunden eine Rückfrage immer wieder: Es herrscht noch große Unsicherheit bei der Frage, ob das eigene Unternehmen nun von einer Regelung wie NIS-2 betroffen ist oder nicht. Was jedoch feststeht: Gerade mittelständische Unternehmen müssen sich dringend von der Vorstellung verabschieden, dass sie alle Vorgaben „in-house“ und mit eigenen finanziellen und

personellen Mitteln bestreiten können. Die Suche nach geeigneten Dienstleistern hat also besondere Dringlichkeit. Hier schlummert eine Menge ungenutztes Potenzial.

Es ist nachvollziehbar, dass Unternehmen vermeidbare Kosten einsparen wollen. Das erklärt auch teilweise die Zurückhaltung bei der Umsetzung, gerade in der letzten Phase der Gesetzgebung. Kosten sind jedoch kein gesetzlich argumentierbares Umsetzungskriterium. Bei aller Diskussion um Ausgaben und strategisch kluge Investitionen wird eine weitere Sache allzu gern vergessen: Standards beschreiben die Mindestanforderungen – nicht das maximal Erlaubte. •

**THORSTEN JÜNGLING**

Director of Practice Group Security & Network bei Kyndryl Germany

(Bild: Kyndryl)

In Sachen Regulierung wächst der Handlungsdruck. Das zeigt auch der „Readiness Report“ von Kyndryl, demnach 82 Prozent der Unternehmen geopolitische Entwicklungen und Regularien inzwischen als stärkeren Einflussfaktor für IT-Entscheidungen sehen als noch vor einem Jahr. Entsprechend investieren viele Unternehmen, um sich im Hinblick auf NIS2, DORA und den CRA abzusichern.

Doch in dieser Geschäftigkeit lauert auch eine Gefahr: Wer alle regulatorischen Anforderungen erfüllt, wiegt sich schnell in falscher Sicherheit. Die Urheber KI-gestützter Angriffe suchen längst nach Schwachstellen, die aktuelle Regularien noch gar nicht adressieren. Compliance allein schützt daher nicht vor Bedrohungen. Vorausschauende Unternehmen verstehen Compliance daher nur als Ausgangspunkt einer Cyberresilienz-Strategie. Sie machen Cyberrisiken zur Aufgabe der Geschäftsleitung und verankern diese in Governance, Risikomanagement und Business Continuity. Zudem setzen sie auf Monitoring, standardisierte Incident-Response-Prozesse, ein wirksames Management von Lieferkettenrisiken und Security-by-Design.

Wettbewerbsvorteile entstehen nicht durch Compliance allein, sondern dort, wo Unternehmen ihre Sicherheitsmaßnahmen kontinuierlich anpassen. Kurzum: Compliance erfüllt die Vorgaben. Den Unterschied macht adaptive Resilienz. •

Wettbewerbsvorteile entstehen nicht durch Compliance allein, sondern dort, wo Unternehmen ihre Sicherheitsmaßnahmen kontinuierlich anpassen. Kurzum: Compliance erfüllt die Vorgaben. Den Unterschied macht adaptive Resilienz. •



HENNING DITTMER

RVP DACH bei Ping Identity

(Bild: Ping Identity)

NIS2, DORA und der Cyber Resilience Act verfolgen im Kern dasselbe Ziel: Unternehmen sollen nachweisbar widerstandsfähiger werden, nicht nur besser dokumentieren. Wer diese Vorgaben als reine Compliance-Übung versteht, verfehlt ihren eigentlichen Zweck. Resilienz entsteht nicht in Richtlinien oder Ordnern, sondern in der Sicherheitsarchitektur. Der gemeinsame Nenner aller drei Regelwerke

ist die Identität. Die meisten Angreifer brechen heute nicht mehr ein – sie loggen sich ein. Kompromittierte Zugangsdaten, schwache Authentifizierung und über Jahre gewachsene Berechtigungen gehören nach wie vor zu den häufigsten



Einstiegspunkten von Angriffen. Genau deshalb rücken Zugriffskontrolle, Nachvollziehbarkeit und kontinuierliches Risikomanagement in den Mittelpunkt der Regulierung.

Unternehmen sollten drei Prioritäten setzen. Erstens: Phishing-resistente Authentifizierung muss zum Standard werden. Zweitens: Identity- und Access-Management muss zentral gesteuert werden, damit Berechtigungen über alle Systeme hinweg transparent und kontrollierbar sind. Drittens: Vertrauen darf nicht nur beim Login entstehen. Jeder Zugriff sollte anhand von Kontext, Gerätezustand und Session-Risiko bewertet werden. Wer Identität zum Fundament seiner Sicherheitsarchitektur macht, erfüllt regulatorische Anforderungen nicht nur auf dem Papier. Er schafft genau das, was NIS2, DORA und der CRA erreichen sollen: operative Resilienz anstatt Compliance. •

ALEXANDER OPEL

Experte für IT-Sicherheit bei der Eset Deutschland GmbH

(Bild: Eset)

Neue gesetzliche Vorgaben verbessern die Cybersicherheit nicht von selbst. Sie zwingen Unternehmen aber dazu, sich ehrlich mit der eigenen Angriffsfläche auseinanderzusetzen. Genau hier sehen wir in der Praxis häufig die größten Defizite. Vielen fehlt ein vollständiger Überblick über ihre Systeme und Endpunkte. Wer seine Angriffsfläche nicht kennt, übersieht Schwachstellen. Deshalb setzen Sicherheitsmaßnahmen häufig an

der falschen Stelle an. Ein Zero-Trust-Ansatz bleibt deshalb eine wichtige Grundlage. Heute muss dieser Ansatz jedoch über klassische Zugriffskontrollen hinausgehen. Wir nennen das „Zero Trust Plus“. Unternehmen



müssen Angriffe erkennen, richtig einordnen und schnell darauf reagieren können. Dafür braucht es kontinuierliche Telemetrie, aktuelle Threat Intelligence sowie XDR oder MDR, um sicherheitsrelevante Informationen zusammenzuführen und zu bewerten. Erst dieses Zusammenspiel ermöglicht es, Sicherheitsvorfälle früh zu erkennen.

Cybersecurity ist damit keine reine Aufgabe der IT. Prioritäten werden im Management gesetzt. Die IT setzt diese Prioritäten technisch um und entwickelt Schutzmaßnahmen weiter. Wer Sicherheit als fortlaufende Aufgabe versteht, erfüllt regulatorische Anforderungen fast automatisch. Vor allem aber verkürzt sich das Zeitfenster zwischen Angriff und Reaktion. Genau das entscheidet darüber, ob aus einem Sicherheitsvorfall eine beherrschbare Störung oder eine echte Krise wird. •

THOMAS MIERSCHKE

Area Vice President DACH bei Proofpoint

(Bild: Proofpoint)

Die Umsetzung wichtiger Cybersicherheitsvorschriften in Deutschland sollten Unternehmen als Ausgangspunkt für den Aufbau von Cyberresilienz betrachten. Die heutige Bedrohungslandschaft entwickelt sich weitaus schneller als die regulatorischen Vorgaben. Das ist zum großen Teil auf KI zurückzuführen, die Phishing, Social Engineering und andere Angriffe überzeugender

und leichter skalierbar macht.

Weil Angreifer schneller agieren als herkömmliche Reaktionszyklen, müssen Unternehmen die Risiken für und durch Mitarbeiter, Daten und KI minimieren. Es besteht jedoch



die Gefahr, dass sich Unternehmen vom KI-Hype ablenken lassen und die Grundlagen aus den Augen verlieren. KI ersetzt bestehende Cyberrisiken nicht, sondern beschleunigt sie. Um den regulatorischen Anforderungen und Bedrohungen gerecht zu werden, sollten Unternehmen einen risikobasierten Ansatz verfolgen, der ihre größten Risiken priorisiert, die Governance stärkt und regelmäßig die mit neuen Technologien und Dritten verbundenen Risiken bewertet. Zwar können KI-gestützte Sicherheitsfunktionen eine wichtige Rolle spielen, doch Unternehmen können die Risiken am stärksten minimieren, indem sie die Grundlagen richtig gestalten. Cyberhygiene, Daten-Governance und Risikomanagement für Lieferanten und Partner sind ebenso wichtig wie Schulungen der Mitarbeiter. •

Fünf Warnzeichen, bei denen Infrastruktur zum Risiko wird

In Krankenhäusern, Banken, Versicherungen und Behörden läuft ein erheblicher Teil der geschäftskritischen Kommunikation per Fax – nicht aus Gewohnheit, sondern aus regulatorischer Notwendigkeit. Weil dieser Kanal jedoch als selbstverständlich gilt, wird die dahinterliegende Infrastruktur kaum hinterfragt. /// von Uwe Geuss

WENN DIE GESCHÄFTSKRITISCHE KOMMUNIKATION PER FAX AUSFÄLLT, kann es im Ernstfall teuer werden. Bei der Anschaffung von ERP-Systemen oder Cloud-Plattformen, die zur IT-Infrastruktur gehören, ist eine sorgfältige Prüfung vor Vertragsabschluss längst Standard. Bei Fax-Diensten hingegen vergessen Organisationen die entscheidende Frage: Was passiert, wenn der Dienst ausfällt? Diese Frage ist heute drängender als je zuvor. Die Anforderungen an die IT-Infrastruktur sind zuletzt erheblich gestiegen. Bedrohungslagen sind komplexer geworden, Abhängigkeiten zwischen Systemen haben zugenommen und gesetzliche Rahmenbedingungen sind deutlich strenger. Diese fünf Warnzeichen sollten IT-Verantwortliche bei der Anbieterwahl und -bewertung auf dem Schirm haben:

1. Fehlende Verfügbarkeitswerte für die Infrastruktur

Eine „hohe Verfügbarkeit“ ist häufig keine verbindliche Zusage, sondern ein Werbeversprechen. Was zählt, sind vertraglich fixierte Prozentwerte für Verfügbarkeit und Wiederherstellungszeiten. Anbieter, die hier ausweichen oder nur allgemein antworten, signalisieren damit, dass sie im Ernstfall nicht in der Pflicht stehen wollen.

2. Nur ein Standort und ein Netzwerkbetreiber

Ein einzelnes Rechenzentrum, ein einzelner Netzwerkpfad oder eine einzelne Stromquelle – jeder dieser Punkte ist ein potenzieller Totalausfall. Zuverlässige Anbieter betreiben ihre Infrastruktur geografisch verteilt und mehrfach abgesichert, sodass der Ausfall einer Komponente den Gesamtbetrieb nicht gefährdet.

3. Failover-Tests der IT-Infrastruktur nur auf dem Papier

Ein nicht erprobtes Notfallkonzept ist im Ernstfall kaum mehr als eine Absichtserklärung. Entscheidend ist, ob ein Anbieter regelmäßige Failover- und Recovery-Tests durchführt und das auch dokumentiert nachweisen kann. An der Frage „Wann haben Sie zuletzt einen Failover getestet?“ lassen sich seriöse Anbieter erkennen.

4. Reaktive statt proaktive Störungskommunikation

Störungen lassen sich nie vollständig ausschließen. Der entscheidende Unterschied liegt darin, wie ein Anbieter

damit umgeht. Proaktive Erstinformation, laufende Status-Updates, klar definierte Verantwortlichkeiten, eine schnelle Störungsbehebung und am Ende ein transparenter Bericht über Ursache und Maßnahmen sind die Merkmale, an denen Unternehmen einen verantwortungsvollen Dienstleister erkennen. Wer erst durch Beobachtung oder Rückfrage von einem Ausfall erfährt, sollte die Zusammenarbeit hinterfragen.

5. IT-Infrastruktur: Keine externen Audits

Kein seriöser Anbieter sollte erwarten, dass seine Kunden sich nur auf sein Wort verlassen. Unabhängige Prüfungen – ob ISO-Zertifizierungen, SOC-Berichte oder branchenspezifische Compliance-Nachweise – sind der belastbare Beleg dafür, dass die Anforderungen an Sicherheit und Resilienz nicht nur intern behauptet, sondern extern verifiziert wurden. Fehlen diese Nachweise, fehlt auch die Grundlage für eine fundierte Entscheidung.

Wer die richtigen Fragen stellt, entscheidet besser

Die Anforderungen an die IT-Infrastruktur sind in den vergangenen Jahren erheblich gestiegen – komplexere Bedrohungslagen, strengere Vorgaben an die IT-Sicherheit, mehr Systemabhängigkeiten. Wer geschäftskritische Kommunikation auf einen Fax-Dienst aufbaut, sollte dessen Resilienz genauso ernst nehmen wie jeden anderen Teil seiner IT-Infrastruktur. Die gute Nachricht: Zuverlässigkeit lässt sich prüfen. Wer die Red Flags kennt und die richtigen Fragen stellt, bekommt die Antworten, die er benötigt. •

DER AUTOR

Uwe Geuss

ist Chief Technology Officer
bei Retarus.

Bild: Retarus



„ Wer geschäftskritische Kommunikation auf einem Fax-Dienst aufbaut, sollte dessen Resilienz genauso ernst nehmen wie jeden anderen Teil seiner IT-Infrastruktur.“

Uwe Geuss

Quanten-Einstieg: Jetzt oder 2030?

Lohnt sich das Investment in eine Technologie, deren Hardware-Zyklen extrem kurz sind? Dr. Christian Tobeck* gibt eine ehrliche Einschätzung für den Mittelstand: Während der breite Markt noch warten kann, müssen angehende Marktführer 2026 bereits Teams formen. Ein Blick auf Risiken, fehlendes privates Kapital und den Standort Deutschland. /// von Heiner Sieger

Herr Dr. Tobeck, wir stehen kurz vor der Quantum Effects 2026. In den vergangenen zwei Jahren hat sich die Debatte massiv von theoretischen Qubits hin zu ‚Logical Qubits‘ und Fehlertoleranz verschoben. Welchen Reifegrad werden wir in Stuttgart sehen: Erleben wir dieses Jahr den endgültigen Durchbruch der Quantentechnologie in die industrielle Serienanwendung?

Dr. Christian Tobeck | Ich würde Ihnen gerne mitteilen, dass wir dieses Jahr schon Serienanwendungen haben werden. Es hat sich 2025 sehr viel getan, aber leider ist man immer noch recht weit von einer „universellen“ Lösung entfernt und bewegt sich weiterhin in speziellen Nischen. Die Quantencomputer sind noch verhältnismäßig klein, und man ist immer noch dabei zu verstehen, für welche Probleme ein Quantencomputer am besten eingesetzt werden kann.

Der Quantum Effects Award gilt mittlerweile als Gradmesser für Marktreife. Nach welchen Kriterien bewerten Sie 2026 die Einreichungen?

CT | Zunächst muss gesagt werden, dass sich der Award nicht nur an Quantencomputing-Technologien (Hardware und Software), sondern auch an die Quantensensorik sowie Quantenkommunikation und -netzwerke richtet, die ebenfalls eine sehr große Rolle innerhalb der Quantentechnologien spielen und leider häufig vernachlässigt werden.

Bei der Bewertung legen wir großen Wert auf einen möglichen Impact auf dem Markt und darauf, wie die Produkte eine bessere oder effizientere Lösung gegenüber herkömmlichen Ansätzen bieten können. Nichtsdestotrotz werden natürlich auch Lösungen mit einer gewissen Eleganz nicht vernachlässigt.

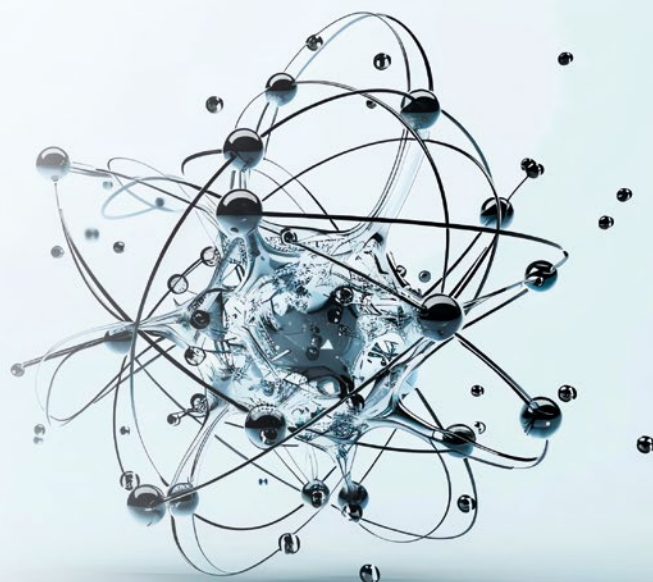
„ Deutschland ist in Ausbildung und Forschung im Bereich der Quantentechnologien **absolute Spitzenklasse**. Leider hapert es an vielen Stellen. Es fehlen große private Investoren, die bereit sind, mehrere hundert Millionen Euro zu investieren. Und viele der vom Staat getätigten Investitionen sind im weltweiten Vergleich **noch zu gering**.

Dr. Christian Tobeck



DER GESPRÄCHSPARTNER

Dr. Christian Tobeck,
Interim Geschäftsführer,
Fokusbereich Wissenschaft bei
EIN Quantum NRW



2026 ist die Migrationsfrist für Post-Quanten-Kryptographie (PQC) in vielen Sektoren ein brennendes Thema. Wird die Messe in Stuttgart – und speziell das NRW-Ökosystem – konkrete ‚Out-of-the-box‘-Lösungen bieten, mit denen IT-Leiter ihre Infrastruktur jetzt gegen künftige Quantenangriffe absichern können?

CT | Ja, die Fristen und Empfehlungen, auf quantensichere Kommunikation bis 2029 und 2030 umzustellen, rücken immer näher. Generell gibt es zwei Wege, den Datentransfer zu schützen. Betroffen ist vor allem der asymmetrische Schlüsselaustausch beim Aufbau einer Kommunikation, insbesondere die RSA- und ECC-Algorithmen. In Kombination mit KI werden zunehmend effizientere Methoden gefunden, diese – insbesondere mit Quantencomputern – zu brechen. Symmetrische Verschlüsselungsverfahren sind weniger betroffen.

Nun gibt es zwei Wege, sich zu schützen: Zum einen PQC, also neue mathematische Methoden, die gegen Quantenangriffe sicher sein sollen. Hier ist insbesondere die Kryptoagilität ein wichtiger Faktor. Einige Dienste großer Technologieanbieter nutzen bereits hybride Verfahren (klassisch und PQC). Der andere Weg ist die Schlüsselübertragung auf physikalischem Weg – die Quantum Key Distribution (QKD). Von einigen Anbietern gibt es bereits Lösungen, beispielsweise für Rechenzentren in Rackgröße, um Daten sicher verschlüsselt zu übertragen. Bei QKD wird allerdings meist noch eine direkte Glasfaserverbindung benötigt, und die Entfernungen sind auf etwa 100 km begrenzt.

Für ein mittelständisches Unternehmen ist ein eigener Quantencomputer utopisch. Die Zukunft ist hybrid. Welche Fortschritte erwarten Sie bei den Software-Stacks, die Quantenbeschleuniger nahtlos in bestehende Cloud- und ERP-Umgebungen (wie SAP S/4HANA oder Microsoft Azure) integrieren

CT | Nicht nur für KMU sind Quantencomputer utopisch. Auch auf längere Sicht werden die meisten Unternehmen über die Cloud auf Quantencomputer zugreifen. Das liegt vor allem daran, dass viele QC-Technologien noch sehr wartungsintensiv sind und Spezialisten benötigen, um sinnvoll betrieben zu werden. Wie erwähnt, befinden wir uns noch in einer Findungsphase, und bis Quantencomputer nativ in Cloud- oder ERP-Umgebungen integriert werden, werden noch einige Jahre vergehen. An dieser Stelle möchte ich auch betonen, dass Quantencomputer – obwohl der Name es suggeriert – keine eigenständigen Computer sind. Sie werden eher wie eine GPU für spezielle Problemstellungen genutzt. Daher werden sie zumindest in absehbarer Zeit nicht als Standalone-Lösungen betrieben werden.

Wir beobachten in der IT einen massiven Mangel an Experten, die ‚Quantum‘ sprechen. Welche Initiativen bringt EIN-Quantum.NRW mit nach Stuttgart, um die Brücke zwischen akademischer Exzellenz und der betrieblichen Ausbildung in den Unternehmen zu schlagen? Brauchen wir den ‚Quanten-Techniker‘ als neues Berufsbild?

CT | Ja, auf der einen Seite benötigen wir Ingenieure, Physiker und Techniker, die die Geräte bauen, und auf der anderen Seite Quantenalgorithmiker, die die QC bedienen können. Bei EIN Quantum NRW haben wir ein spezielles Education-Projekt, in dem wir die Aktivitäten der einzelnen Universitäten koordinieren und abstimmen. Zudem binden wir zunehmend Fachhochschulen ein, die wir als Brückenbauer zu den Unternehmen sehen. Ich glaube, dass die Quantentechnologien so breit und interdisziplinär aufgestellt sind, dass es sinnvoller ist, in den jeweiligen Fachrichtungen Schwerpunkte zu setzen und sich aus einem „Grundstudium“ heraus zu spezialisieren. Zudem gibt es einige Projekte, um bereits ausgebildete Fachkräfte weiterzubilden.

Wir sehen viele proprietäre Plattformen der großen Hyperscaler. Besteht nicht die Gefahr, dass sich der Mittelstand in die nächste technologische Abhängigkeit begibt? Wie stark fördern der Award und Ihr Netzwerk offene Standards und Souveränität?

CT | Souveränität ist ein sehr großes Thema bei einer so vielversprechenden Technologie. Um nicht ins Hintertreffen zu geraten, wie wir es bei vielen aktuellen Hightech-Themen sehen, müssen noch einige Schritte unternommen werden. Deutschland ist in Ausbildung und Forschung im Bereich der Quantentechnologien absolute Spitzenklasse. Leider hapert es an vielen Stellen. Zum einen fehlen große private Investoren, die bereit sind, mehrere hundert Millionen Euro zu investieren. Andererseits sind viele der vom Staat getätigten Investitionen im weltweiten Vergleich noch zu gering. Hinzu kommt, dass es zu viele Regularien gibt, die verhindern, dass Unternehmen beispielsweise auf staatlich oder öffentlich finanzierter QC ihre Software einfach erproben können.

Hand aufs Herz: Viele Unternehmen zögern noch, weil die Hardware-Zyklen extrem kurz sind. Ist 2026 der richtige Zeitpunkt für den Einstieg, oder ist das Risiko, heute in eine Technologie zu investieren, die 2027 veraltet ist, für ein KMU noch zu hoch?

CT | Wie Sie bereits treffend beschrieben haben, wird ein QC in absehbarer Zeit vor allem in Rechenzentren stehen und über die Cloud verfügbar sein. Somit ist ein Einstieg grundsätzlich relativ einfach und das Risiko vergleichsweise gering. Das Problem ist jedoch, dass es noch viele offene Fragen gibt, die geklärt werden müssen. Lange Zeit wurde vor allem die Hardwareentwicklung gefördert. Um jedoch wirtschaftlichen Mehrwert zu generieren, sind die Anwendungen entscheidend – und an diesen wird noch intensiv geforscht. Aktuelle Roadmaps gehen davon aus, dass es ab etwa 2029/2030 Quantencomputer geben wird, die einen echten Mehrwert bieten können. Möchte man ein Vorreiter in dieser Technologie sein und mitbestimmen, wer am Markt die Entscheidungen trifft, sollte man bereits heute entsprechende Teams aufgebaut haben und sich mit den Systemen vertraut machen. Für den breiten Mittelstand ist es derzeit jedoch noch zu früh. •

Effiziente HR-Automation für KMU

47 Prozent der HR-Verantwortlichen priorisieren Investitionen in KI- und Automatisierungstools. Die Verbindung von Low-Code-Technologie und KI-Agenten schafft neue Spielräume für Personaler im Mittelstand. Sie erhalten standardisierte, automatisierte Lösungen, die sie individualisieren können – schneller und günstiger als mit spezialisierten HR-Tools. /// von Axel Ensinger

URLAUBSANTRÄGE, VERTRAGSDOKUMENTE UND ONBOARDINGS STAPELN SICH, da vieles davon heute noch über Papier oder Excel-Listen läuft. Diese manuellen Prozesse kosten Zeit, sind fehleranfällig und binden Ressourcen, die für strategische Themen wie Mitarbeiterbindung oder Talententwicklung fehlen. Unternehmen haben dieses Problem zwar erkannt und arbeiten daran, administrative HR-Prozesse zu digitalisieren. Dabei entscheidet vor allem die Wahl der richtigen Lösung über den Erfolg: Häufig greifen Unternehmen zunächst zu standardisierten HR-Lösungen, die aber weniger Raum für Individualisierung lassen. Um ihre Anforderungen dennoch zu erfüllen, passen Unternehmen ihre Prozesse an die Software an oder lassen die Standardsoftware kostenintensiv erweitern. Oftmals nutzen Organisationen sogar nur einen Bruchteil

der Funktionen – eine unwirtschaftliche Investition. Dabei geht es auch anders: Eine Kombination aus Low-Code-Prozessautomatisierung und KI-Agenten ermöglicht es, individuelle Workflows eigenständig und kosteneffizient aufzusetzen – und das nicht nur im HR-Bereich, sondern auch in anderen Abteilungen. Mitarbeiter können mit dieser „Agentic Process Automation“ ihre Prozesse nach ihren eigenen Bedürfnissen gestalten und mit agentischen Schritten anreichern.

Was Low-Code-Technologie leistet und wo bisher die Grenze lag

Bei Low-Code-Plattformen bauen Anwender über visuelle Prozessdesigner per Drag-and-Drop Workflows, legen dafür Berechtigungen fest und definieren individuelle Abweichungen vom Standardablauf. Da kaum Programmierkenntnisse nötig sind, lassen sich Digitalisierungsprojekte

innerhalb weniger Wochen bis Monate umsetzen – die IT-Abteilung wird entlastet, die Kosten bleiben überschaubar. Doch wie jede Technologie hat auch Low-Code-Prozessautomatisierung eine Grenze. Diese verlief bisher dort, wo regelbasierte Logik nicht mehr ausreicht: bei komplexen, kontextabhängigen Entscheidungen. Diese mussten Personaler weiterhin selbst treffen. Genau hier setzen KI-Agenten an.

Die Grenzen von Low-Code mit KI überwinden

Im Prozessdesigner lassen sich die Agenten an beliebiger Stelle zwischen Arbeitsschritten schalten. User geben ihnen eine klar definierte Aufgabe, die sie eigenständig ausführen.

Ein Agent liest und klassifiziert, ein zweiter trifft regelbasierte Vorentscheidungen, ein dritter erzeugt Dokumente, ein vierter überwacht Fristen – und an den richtigen Stellen



DER AUTOR
Axel Ensinger

ist Geschäftsführer der JobRouter GmbH.

„ Da für Low Code kaum Programmierkenntnisse nötig sind, lassen sich Digitalisierungsprojekte innerhalb weniger Wochen bis Monate umsetzen – die IT-Abteilung wird entlastet, die **Kosten bleiben überschaubar**.

Axel Ensinger

LESEN SIE ONLINE WEITER...

- Weitere Einsatzbereiche für KI-Agenten im HR-Bereich
- Höheres Level bei Automatisierung erreichen
- Datenschutz im Blick behalten
- Wie sieht die Zukunft von Low-Code-Plattformen aus?



dos, erinnert sie bei nahender Deadline erneut und stellt für den Workflow relevante Dokumente bereit.

KI-Agent für Entscheidungshilfen

Innerhalb dieses Prozesses lassen sich gezielt KI-Agenten einsetzen, die einzelne Aufgaben automatisiert übernehmen, beispielsweise die Entscheidung darüber, welche Arbeitsmaterialien der neue Mitarbeiter benötigt. In einem rein Low-Code-basierten Ablauf muss der Personaler selbst entscheiden, was benötigt wird und den entsprechenden Workflow starten. Dieser Schritt lässt sich mit KI-Agenten automatisieren, indem sie Informationen aus den Stellenbeschreibungen und früheren Onboardings – also den notwendigen Kontext – erhalten. Der KI-Agent erkennt Position, Abteilung, Standort und Hierarchieebene und schlägt auf Basis dieser Informationen die passende Ausstattung vor. Der Personaler kann entscheiden, ob er den Vorschlag übernimmt und den Prozess weiterführt oder ihn zuerst anpasst. Somit behält der Mensch die Kontrolle, spart sich aber Zeit und manuelle Recherchearbeit.

Ein weiterer Teil des Onboardings ist es unter anderem, Mitarbeiter mit bestimmten Regeln, Sicherheitsvorkehrungen oder unternehmensspezifischen Abläufen vertraut zu machen. Dazu entscheiden Personaler und andere Fachabteilungen über passende Schulungen, planen und dokumentieren sie. Die Vielzahl rechtlicher Vorgaben, Normen aus dem Arbeits- und Datenschutz sowie branchenspezifischer Regelungen erhöht den Koordinationsaufwand. Für einen schnelleren Ablauf können sie einen KI-Agenten damit beauftragen, Schulungen vorzuschlagen. Sie prüfen, welche Qualifikationen der Mitarbeiter schon hat, welche ihm für die neue Stelle fehlen und leitet daraus verpflichtende Unterweisungen ab. •

behält ein Mensch die Entscheidung. Um ihre Aufgaben zu erfüllen, greifen Agenten in der Regel kontextabhängig auf verfügbare Daten (Stammdaten, aber auch historische Daten) und Dokumente innerhalb der Low-Code-Plattform zu. Dabei ist es notwendig, bei der Datenauswahl sehr sauber zu arbeiten und die Auswahl auf „für die Erledigung der Aufgabe zwingend notwendig“ zu beschränken, um Halluzinationen vorbeugen und die Qualität zu steigern. Denn je mehr Daten zur Verfügung stehen, desto schwieriger ist es für den Agenten zu entscheiden, welche für seine Aufgabe relevant sind. Das Ergebnis spielen die Agenten an den Anwender (mit Begründung für die Entscheidung/Auswahl) zurück. Dieser entscheidet dann, ob er den weiteren Prozess auf dieser Basis fortsetzen will. Da der User jederzeit vollumfänglich Einblick in den Auswahlprozess und die Arbeitsweise der KI-Agenten hat, kann er transparent nachvollziehen und noch Anpassungen vornehmen wie zum Beispiel den zugrundeliegenden Prompt optimieren oder die Datenauswahl anpassen. Bei der Orchestrierung mehrerer spezialisierter

KI-Agenten entlang eines Prozesses spielen Low-Code-Plattformen als Prozess-Backbones ihre Stärke aus: Status, Fristen, Eskalationen, Rollen- und Rechtekonzept sowie ein lückenloser Audit-Trail sind bereits Teil der Plattform. Reine Chat-Assistenten leisten das nicht; ihnen fehlt die verbindliche Prozess- und Nachweisebene.

Beispiele Onboarding: Wie unterstützen KI-Agenten Personaler?

Die Kombination aus Low-Code- und KI-basierter Automatisierung kann Personaler entlasten und neuen Mitarbeiter eine positive Employee Experience bieten. Wie das funktioniert, zeigt ein Beispiel für den Onboarding-Prozess: Ein gelungenes Onboarding zielt darauf ab, den neuen Mitarbeiter am ersten Tag oder möglichst früh arbeitsfähig zu machen. Mit einer Low-Code-Plattform können Unternehmen den gesamten Onboarding-Workflow abbilden: von der Erfassung der Mitarbeiterdaten über die Verteilung von Aufgaben zur Einarbeitung bis hin zur Organisation von Arbeitsmitteln. Das System benachrichtigt Nutzer automatisch bei To-

Unternehmensdemenz: Wie KI das Erfahrungswissen rettet

Bis 2030 gehen mehr als 6,5 Millionen Babyboomer in Rente – und nehmen kritisches Wissen mit. Oliver Diekmann, CEO von Wingmaite, erklärt, wie KI-gestützte Sprachdokumentation den Wissensverlust im Mittelstand stoppt und die Einarbeitung neuer Mitarbeiter beschleunigt. /// von Heiner Sieger

Oliver, wie bist du auf das Thema Wissensverlust in Unternehmen gekommen?

Oliver Diekmann | Wissensmanagement betrifft jedes Unternehmen, und der Begriff ist nicht erst durch KI entstanden. Er existiert seit Jahrzehnten. Allerdings war es immer mit enormem Aufwand verbunden, Wissen systematisch zu dokumentieren und aktuell zu halten. Neue Technologien ermöglichen es jetzt erst, damit wirklich anders umzugehen. Ich selbst habe das in meiner Berufslaufbahn mehrfach leidvoll erlebt. In einer meiner früheren Unternehmungen ist von einem Tag auf den anderen ein sehr wichtiger Mitarbeiter durch Krankheit ausgefallen. Plötzlich musste ich mich selbst in seine Themen einarbeiten. Es war dokumentiert, dass wir uns für Option A und nicht für Option B entschieden hatten – aber das gesamte Warum fehlte: Welche Alternativen wurden geprüft? Was war der Kontext? Mit wem wurde gesprochen? All die Aspekte, die letztlich zu einer Entscheidung führen, musste ich mir mühsam zusammensuchen.

Das klingt nach einem grundsätzlichen Problem. Geht es also nicht nur um explizites Wissen, sondern vor allem um implizites Erfahrungswissen?

OD | Genau. Es geht nicht nur darum, das explizite Wissen zu dokumentieren, sondern auch den gesamten Weg dorthin – die Fachexpertise, das dreimalige „Warum“. Das hat mich auch bei Firmenverkäufen und Übergängen immer wieder beschäftigt. Es ist enorm schwierig, gesammeltes Wissen komplett zu übergeben. Ehrlich gesagt: Es ist schier unmöglich. Das hat jedes Mal zu großen Reibungsverlusten geführt.

Woran erkennen Entscheider, dass in ihrem Betrieb Wissensabfluss droht? Und warum ist Starten und iterativ Lernen besser, als drei Jahre an einem perfekten Plan zu arbeiten?

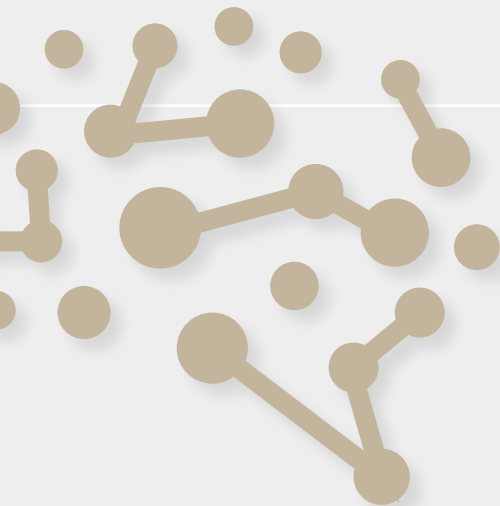
OD | Bis 2030 werden mehr als 6,5 Millionen Babyboomer in Rente gehen. Das sind in vielen Betrieben bis zu 30 Prozent der Belegschaft. Das ist ein alarmierendes Zeichen, zu-

mal wir durch den Fachkräftemangel diesen Verlust nicht annähernd ausgleichen können. Wenn ein Unternehmen ein hohes Durchschnittsalter hat, ist das bereits das Signal, sich mit dem Thema zu befassen. Im Idealfall bekommt die Person, die geht, drei bis sechs Monate eine Nachfolgerin oder einen Nachfolger an die Seite gestellt, um Wissen aufzusaugen und Verständnis aufzubauen. Dann gibt es eine Staffelstabübergabe. Aber in den meisten Fällen wird es so sein, dass keine Hand nach dem Staffelstab greift. Er fällt zu Boden und das Wissen ist verloren. Deshalb ist es so wichtig, jetzt anzufangen. Denn das zweite Problem ist: Wenn man sich erst in den letzten Wochen hinsetzt und strukturiert Wissen erfassen will, denkt man gar nicht an alles, was operativ an Fragen auftaucht.

Die Leute sind im Unternehmensalltag voll ausgelastet. Wie gewinnt ihr die erfahrenen Kolleginnen und Kollegen trotzdem für das Thema?

OD | Wir nutzen mehrere Wege, um Wissen zu aggregieren. Man kann gezielt Fragen an die Mitarbeitenden stellen, die das Unternehmen verlassen – zu ihrer Rolle, ihrem Fachbereich, aber auch zu alltäglichen Arbeitsabläufen. Unser Tool erkennt dabei Wissenslücken. Wenn eine identifiziert wird, können wir sie einer Person zuweisen. So entsteht Wissen teilweise schon on the fly während der Arbeitszeit. Gleichzeitig zeigen wir Mehrwerte auf: Das abgespeicherte Wissen hilft mir und der Firma, Zeit zu sparen – das spüre ich direkt und indirekt, und das motiviert.

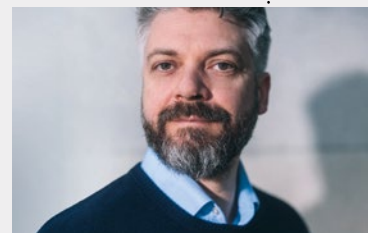
Was man außerdem nicht unterschätzen darf: Die Mitarbeitenden, die ausscheiden, haben eine sehr hohe Motivation, ihr Wissen festzuhalten. Viele sind über 40 Jahre im Betrieb, hängen an ihren Kolleginnen und Kollegen und wollen das Umfeld so hinterlassen, dass niemand Probleme bekommt. Da steckt echte emotionale Verbundenheit dahinter. Und durch die Niedrigschwelligkeit unseres Tools – man spricht per Voice-to-Voice ein – hat man innerhalb von 50 Minuten ein Arbeitsergebnis, für das man sonst mehrere Stunden gebraucht hätte. Das motiviert zusätzlich.



DER GESPRÄCHSPARTNER

Oliver Diekmann ist CEO von Wingmaite.

Bild: viktor_strasse



„ Die spürbarsten Effekte sind: Mitarbeitende befähigen sich schneller für Entscheidungen, neue Kolleginnen und Kollegen werden schneller eingearbeitet, und Informationen müssen nicht mehr in verschiedenen Tools und über verschiedene Abteilungen hinweg gesucht werden.

Oliver Diekmann

Wie lange vor dem Austritt sollte man mit der Wissenssicherung beginnen?

OD | Das hängt davon ab, wie wissensintensiv das Arbeitsumfeld ist. Aber drei Monate sind das Mindestmaß, bis zu sechs Monate wären besser. Grundsätzlich gilt: je früher, desto besser. Es ist ein typisches 80/20-Prinzip. Die ersten 80 Prozent hat man schnell erfasst. Die letzten 20 Prozent dauern länger, weil sie im Arbeitsalltag seltener vorkommen. Unser Tool lässt sich sehr niedrigschwellig integrieren. Man muss sich kein großes IT-Projekt vorstellen, sondern wir fügen uns schnell in die bestehende Landschaft ein.

Wer sollte im Unternehmen die Verantwortung für das Thema tragen?

OD | Idealerweise ist Wissen Chefsache, weil es so kritisch ist. Wir sehen aber auch, dass das Thema häufig bei HR aufgehängt wird, weil sich die Personalabteilung damit beschäftigt, neue Mitarbeitende schnell wirksam zu machen. Von Jahr zu Jahr wird das schwerer, wenn die Älteren gehen und das Wissen nicht dokumentiert ist. In manchen Unternehmen liegt es auch im Bereich Digitalisierung oder IT, weil dieses Kontextwissen grundsätzlich wichtig ist, um KI-Projekte aufzusetzen. Es kann aber ebenso ein Fachbereich sein: Wenn etwa im Vertrieb niemand die Frage beantworten kann, wie es um Kunde B steht, weil die Dokumentation fehlt – dann sollte genau dort der Startpunkt sein.

Stellt die KI den Mitarbeitenden also aktiv Fragen und bezieht bei Bedarf weitere Personen ein?

OD | Genau. Wir haben auch im Blick, wer welche Expertenrolle oder welchen Jobtitel im Unternehmen hat und wofür jemand befähigt ist. So kann es sein, dass bestimmte Inhalte von einer zweiten Person validiert werden. Mensch-zu-Mensch-Austausch bleibt ein ganz wichtiger Faktor.

Wie wird das gewonnene Wissen im Unternehmensalltag verfügbar und nutzbar gemacht?

OD | Man kann es sich ähnlich vorstellen wie bei bestehenden LMS-Systemen. Es gibt eine Chatleiste, über die

man per Voice oder Text mit dem Wissen kommuniziert. Die Frage könnte zum Beispiel lauten: „Wie ist unsere Marketingstrategie?“ Dann werden aus unterschiedlichen Dokumenten die relevanten Informationen zusammengetragen. Die spürbarsten Effekte sind: Mitarbeitende befähigen sich schneller für Entscheidungen, neue Kolleginnen und Kollegen werden schneller eingearbeitet, und Informationen müssen nicht mehr in verschiedenen Tools und über verschiedene Abteilungen hinweg gesucht werden. Man kann auch typische GenAI-Anwendungsfälle wie Recherche, Zusammenfassungen oder E-Mail-Übersetzungen direkt über unser Tool abwickeln. Mittelfristig kann man mit dem kontextualisierten Wissen auch strategisch arbeiten.

Gibt es eine Roadmap, wie Unternehmen starten sollten?

OD | Der erste Schritt ist die Frage: Wo in der Wertschöpfung sehen wir Risiken, wenn morgen wichtige Leute nicht mehr da sind? Das ergibt bereits eine Wissenslandkarte, die zeigt, wo man ansetzen muss. Governance ist in unserem Produkt integriert und muss natürlich mit dem Betriebsrat abgestimmt werden. Wir empfehlen sehr häufig einen Piloten, weil es auch darum geht, den Change-Management-Prozess zu begleiten. Jede KI-Einführung bedeutet ein Umdenken, eine Transformation. Mitarbeitende müssen sich zurechtfinden, Sorgen abbauen. In einer Pilotphase definieren wir gemeinsam ein Zielbild und eine Erwartungshaltung für drei oder sechs Monate. Wir tauschen uns regelmäßig aus und hören auf Feedback. Unsere KI entdeckt dabei auch systematisch Knowledge Gaps. So kommen wir gemeinsam schnell zu einer Basis, auf der wirklich Mehrwert gehoben wird. •

LESEN SIE ONLINE WEITER...

Lesen sie hier das ausführliche Interview oder hören Sie den Podcast mit Oliver Diekmann: [KI Wissensmanagement gegen Unternehmensdemenz](#).



KI-Energieverbrauch: Effizienz wird zur Unternehmensaufgabe

Der KI-Boom treibt die Effizienz – und den Energieverbrauch. Für Unternehmen entsteht damit ein Konflikt, der plötzlich strategisch wird: Innovationen skalieren, ohne Nachhaltigkeit und Kosten aus dem Ruder laufen zu lassen. /// von Konstantin Pfliegl

DARUM GEHT ´S

Energieintensive KI: Anwendungen, besonders große Sprachmodelle, benötigen mit jeder Nutzung erheblich mehr Rechenleistung und Strom, im Gegensatz zu klassischer Software, die oft effizienter wird.

Versteckte Energiekosten der Cloud: Auch wenn Unternehmen Cloud-Dienste nutzen, zahlen sie den Energieverbrauch indirekt über die Cloud-Kosten mit.

Zielkonflikt zwischen KI und Nachhaltigkeit: Unternehmen stehen vor dem Spannungsfeld, KI zur Wettbewerbsfähigkeit auszubauen und gleichzeitig Energieverbrauch sowie CO2-Emissionen zu reduzieren.

Fehlende Transparenz und Steuerung: Es mangelt an klaren Daten zum Energieverbrauch einzelner KI-Anwendungen, wodurch Effizienzbewertung, Steuerung und Verknüpfung mit Geschäftswert erschwert werden.

LANGE WAR DER ENERGIEVERBRAUCH VON IT EIN RANDTHEMA. Rechenzentren liefen, Cloud wurde eingekauft, Effizienz war ein Nice-to-have. Mit dem breiten Einsatz von künstlicher Intelligenz hat sich das grundlegend verändert.

Der Grund ist simpel. KI-Anwendungen, insbesondere große Sprachmodelle, sind rechenintensiv. Jede Anfrage, jede Generierung, jede automatisierte Entscheidung braucht Rechenleistung. Und die skaliert mit der Nutzung. Während klassische Software oft effizienter wird, je länger sie läuft, steigt der Ressourcenbedarf bei KI mit jeder zusätzlichen Interaktion.

Und künstliche Intelligenz steckt heute in zahlreichen Prozessen: im Kundenservice, in der Software-Entwicklung oder in der Sachbearbeitung. Während eine Google-Suche rund 0,3 Wattstunden Strom verbraucht, soll ein Prompt bei ChatGPT im Schnitt rund 18,9 Wh verbrauchen. Und plötzlich stellt sich in Unternehmen die Frage: Wie passt das zu unseren Nachhaltigkeitszielen?

Die Zahlen sind eindeutig. Laut der Internationalen Energieagentur (IEA) verbrauchten Rechenzentren 2024 weltweit rund 415 Terawattstunden Strom. Das entsprach etwa 1,5 Prozent des globalen Verbrauchs. Bis 2030 soll sich dieser Wert auf 945 TWh mehr als verdoppeln, getrieben vor allem durch KI. Zum Vergleich: Das entspricht ungefähr dem heutigen Jahresverbrauch von ganz Japan.

Nun kann man natürlich argumentieren, dass KI-Dienste in der Regel in der Cloud laufen. Und die Hyperscaler zahlen die Stromrechnung, nicht der Kunde. Das ist richtig. Doch Stromkosten werden freilich in die Cloud-Kosten eingepreist. Über die Cloud-Rechnung zahlen Unternehmen den Energieverbrauch also indirekt mit.

KI-Energieverbrauch: Regulatorischer Druck

Dazu kommt regulatorischer Druck. Mit der Corporate Sustainability Reporting Directive (CSRD) müssen Unter-



DER AUTOR

Konstantin Pfliegl

ist leitender Redakteur beim
DIGITAL BUSINESS Magazin.



nehmen ihre Nachhaltigkeitskennzahlen deutlich präziser offenlegen – inklusive der Emissionen aus der IT. Diese fallen typischerweise in die schwer fassbaren Scope-3-Kategorien: Hardware-Einkauf, Cloud-Verträge, SaaS-Nutzung. Für größere berichtspflichtige Unternehmen ist Scope 3 verpflichtend, sofern wesentlich. Was früher als technisches Detail galt, wird damit prüfungsrelevant. Und die IT muss liefern.

Genau hier entsteht ein Konflikt, der sich nicht wegdiskutieren lässt. Auf der einen Seite der strategische Zwang, künstliche Intelligenz breit einzusetzen, um wettbewerbsfähig zu bleiben. Auf der anderen Seite steigende Anforderungen an Energieeffizienz und CO₂-Reduktion. Beides gleichzeitig zu steuern, daran scheitern viele Unternehmen aktuell noch.

KI-ENERGIEVERBRAUCH: TO-DOS FÜR UNTERNEHMEN

Transparenz schaffen: Energieverbrauch und Kosten der KI-Anwendungen systematisch erfassen – nicht schätzen.

KI-Portfolio prüfen: Use Cases nicht nur nach Nutzen, sondern auch nach Effizienz und Ressourcenbedarf bewerten.

Governance etablieren: Klare Regeln für den KI-Einsatz definieren, inklusive Nachhaltigkeitskriterien.

Silos aufbrechen: IT, Finance und Nachhaltigkeit eng verzahnen statt nebeneinander steuern.

Technologie gezielt wählen: Kleinere Modelle und effiziente Architekturen als Alternative prüfen.

Reporting vorbereiten: Sicherstellen, dass IT-Daten CSRD-tauglich und audit-fähig in Scope-3-Berichte einfließen.

Langfristig denken: Nachhaltigkeit fest in der IT-Strategie verankern, nicht als nachträgliches Add-on.

„Auf der einen Seite ist der strategische Zwang, künstliche Intelligenz breit einzusetzen, um wettbewerbsfähig zu bleiben. Auf der anderen Seite steigende Anforderungen an Energieeffizienz und CO₂-Reduktion. **Beides gleichzeitig zu steuern, daran scheitern viele Unternehmen aktuell noch.**

Konstantin Pfliegl

Transparenz als Hebel

Das Problem: Nachhaltigkeitsstrategie und IT-Realität sind oft entkoppelt. ESG-Ziele stehen im Geschäftsbericht, doch die Verbindung zur IT-Infrastruktur ist dünn. Gleichzeitig treiben Fachbereiche KI-Anwendungen voran, ohne deren Verbrauch zu erfassen. Es entsteht eine neue Spielart von „Shadow AI“. Diesmal nicht als Compliance-, sondern als Effizienzproblem.

Der erste echte Hebel heißt Transparenz. Unternehmen müssen wissen, welche KI-Anwendung welche Kosten und welchen Energieverbrauch verursacht. Klingt banal, ist aber anspruchsvoll. Cloud-Anbieter liefern zunehmend Daten, doch die sind oft weder vergleichbar noch granular genug. Und vor allem fehlt die Verknüpfung zum Geschäftswert: Welche Anwendung bringt welchen Nutzen – und rechtfertigt damit ihren Ressourcen-Hunger?

Daraus folgt eine neue Steuerungslogik: KI-Projekte gehören nicht mehr nur nach Innovations-Potenzial bewertet, sondern auch nach Effizienz. In vielen Fällen tut es ein kleineres, spezialisiertes Modell genauso gut wie ein großes KI-Modell, bei einem Bruchteil des Verbrauchs. Auch die Architektur zählt: Muss wirklich jede Anfrage in die Cloud, oder läuft manches lokal besser? Auch organi-

satorisch muss sich etwas bewegen. Die Verantwortung für nachhaltige IT lässt sich nicht mehr sauber einem Bereich zuordnen. CIO, CFO und Sustainability-Verantwortliche müssen enger zusammenrücken. Entscheidungen über KI-Einsatz, Infrastruktur und Budgets werden zur Gemeinschaftsaufgabe, was neue Abstimmungsprozesse und oft auch neue Zielsysteme erfordert.

Fazit

Bei aller Dringlichkeit lohnt der nüchterne Blick: Nicht jede grüne Lösung rechnet sich und nicht jede KI-Anwendung rechtfertigt ihren Verbrauch. Unternehmen müssen lernen, diese Abwägungen bewusst zu treffen. Genau darin liegt die Chance. Wer künstliche Intelligenz effizient und zielgerichtet einsetzt, sichert sich gleich doppelt einen Vorteil – bei den Kosten und im Wettbewerb.

Die kommenden Monate werden zeigen, wie schnell Unternehmen diese Kurve kriegen. Eines steht jetzt schon fest: Nachhaltigkeit ist in der IT kein Randthema mehr. Dafür ist der Einfluss von KI auf Energie und Kosten schlicht zu groß geworden. Was lange als technisches Detail durchging, ist zur strategischen Frage geworden. Und die landet jetzt auf dem Tisch der Geschäftsführung. •

Vom Patientenportal zum Versorgungsportal

Leistungsgruppen, Fachkräftemangel, Kostendruck:

Wie digitale Versorgungsportale zur strategischen Infrastruktur für Krankenhäuser im Rahmen der neuen KHVVG/KHAG-Logik werden.

/// von Prof. Dr. Alexander Alscher



DER AUTOR

Prof. Dr. Alexander Alscher

ist Gründer und Geschäftsführer der samedi GmbH, einem führenden Software-Unternehmen für Patientenportale und digitales Patientenmanagement, deren Lösungen von 50.000 Healthcare Professionals für mehr als 40 Mio. Patientinnen und Patienten genutzt werden. Seit 2015 lehrt und forscht er als Professor an der BSP Business & Law School Berlin zu Themen der digitalen Vernetzung und Versorgungssteuerung im Gesundheitswesen.

74 PROZENT DER KRANKENHÄUSER IN DEUTSCHLAND BEWERTEN IHRE AKTUELLE WIRTSCHAFTLICHE SITUATION ALS UNBEFRIEDIGEND – das zeigt das Krankenhaus-Konjunkturbarometer des Deutschen Krankenhausinstituts (DKI) im Juni 2026. Noch bevor die Anpassung der Vergütungsstrukturen im Rahmen der Krankenhausreform wirksam werden, stehen drei von vier Krankenhäusern unter erheblichem wirtschaftlichem Druck. Mit der Umstellung von Fallpauschalen auf die neuen 61 definierten Leistungsgruppen, Vorhaltepauschalen und dem Krankenhaustransformationsfonds steuert die deutsche Krankenhauslandschaft auf einen tiefgreifenden Strukturwandel zu. Die reine Digitalisierung des KHZG reicht dabei nicht aus, sondern es braucht eine organisatorische Anpassung und Transformation der Wertschöpfungsprozesse im Krankenhaus.

Mitten in dieser Reformdynamik liegt eine Ressource, die derzeit noch zu wenig als strategisches Instrument begriffen wird: das Patientenportal. Mit fortschreitendem Rollout und Integration in die Klinik-IT lässt sich das Patientenportal vom reinen Aufnahme-, Behandlungs- und Entlassmanagement zu einer Versorgungsplattform weiterentwickeln, mit der Krankenhäuser Patientenströme proaktiv steuern. Hierbei geht es nicht nur um eine Reaktion auf den Fachkräftemangel und den Inflations-getriebenen Kostendruck, sondern im Kern um die Wettbewerbsfähigkeit und den Existenzdruck in der politisch forcierten Konsolidierung im Krankenhausmarkt.

Was Leistungsgruppen mit digitaler Steuerung zu tun haben

Die Krankenhausreform verändert die Erlöslogik fundamental. Wer künftig eine Leistungsgruppe – etwa Kardiologie, Geburten oder Endoprothetik – anbieten will, muss

definierte Mindestvoraussetzungen erfüllen: Qualifikation und Mindestanzahl des ärztlichen Personals, Geräteausstattung, strukturelle Voraussetzungen, nachgewiesene Kooperationen. Leistungen außerhalb des zugewiesenen Portfolios verlieren ihre Finanzierungsgrundlage.

Das bedeutet: Das Versorgungsportfolio eines Krankenhauses wird genehmigungsbasiert. Und genau hier beginnt die strategische Bedeutung des Patientenportals. Denn ein Portal, das Terminbuchungen und Einweisungen steuert, steuert faktisch auch den Patientenstrom in die jeweilige Leistungsgruppe. Ein Haus, das seine genehmigten Leistungsgruppen nicht aktiv befüllt, verliert auf beiden Seiten: wirtschaftlich und regulatorisch. Ein digitales Patientenportal kann genau das verhindern. Es kann Anfragen in Echtzeit mit dem eigenen Leistungsportfolio abgleichen, Patienten bei Bedarf an geeignete Einrichtungen weiterleiten und auch entgegennehmen sowie Einweisende auf Basis der genehmigten Leistungsgruppen direkt mit den richtigen Abteilungen verbinden.

Sechs Stufen: Wie aus dem Patientenportal ein Versorgungsportal wird

Das Patientenportal, wie es im Krankenhauszukunftsgesetz (KHZG) definiert wurde, ist ein erster und erfolgreicher Schritt zur digitalen Transformation im Krankenhaus. Das zeigt sich auch im Digitalradar Krankenhaus: Der Digitalisierungsgrad deutscher Krankenhäuser ist in den letzten 5 Jahren um 65 Prozent gestiegen - von durchschnittlich 33,3 Punkten in 2021 auf 55 Punkte in der aktuellen Erhebung 2026. Dabei handelt es sich um einen iterativen Prozess: Wer heute mit digitalen Terminen, Formularen und Dokumenten startet, legt die Datenbasis für morgen. Wer morgen Behandlungspfade integriert, schafft die Grund-

lage für sektorenübergreifende Koordination. Die digitale Transformation lässt sich in sechs Stufen erreichen:

- 1. Terminfindung & digitale Patientenansprache:**
Online-Buchung, automatisierte Erinnerungen, Leistungsgruppen-gesteuertes Routing von Anfragen.
- 2. KI-gestützte Patientenführung & Pfade:**
Automatisierte Triage, prädiktives Kapazitätsmanagement, individualisierte Versorgungspfade auf Basis strukturierter Daten.
- 3. Aufnahmemanagement & digitaler Empfang:**
Digitale Voranmeldung, strukturierte Anamnese, Entlastung des Empfangspersonals vor dem ersten Patientenkontakt.
- 4. Telemedizin & KI-gestütztes Behandlungsmanagement:**
Digitale Konsultationen, automatisierte Dokumentation, KI-Unterstützung und Validierung.
- 5. Nachsorge & Hospital-at-Home:**
Fernmonitoring, automatisierte Follow-up-Kommunikation, digitale Versorgungsassistenzen – das Portal endet nicht mit der Entlassung, sondern automatisiert die Patientenbetreuung zu Hause.
- 6. Sektorenübergreifende Versorgung:**
Schnittstellen zu Niedergelassenen, MVZ, KVen, Reha-Einrichtungen und Pflegediensten – das Versorgungsportal als gemeinsame Infrastruktur.

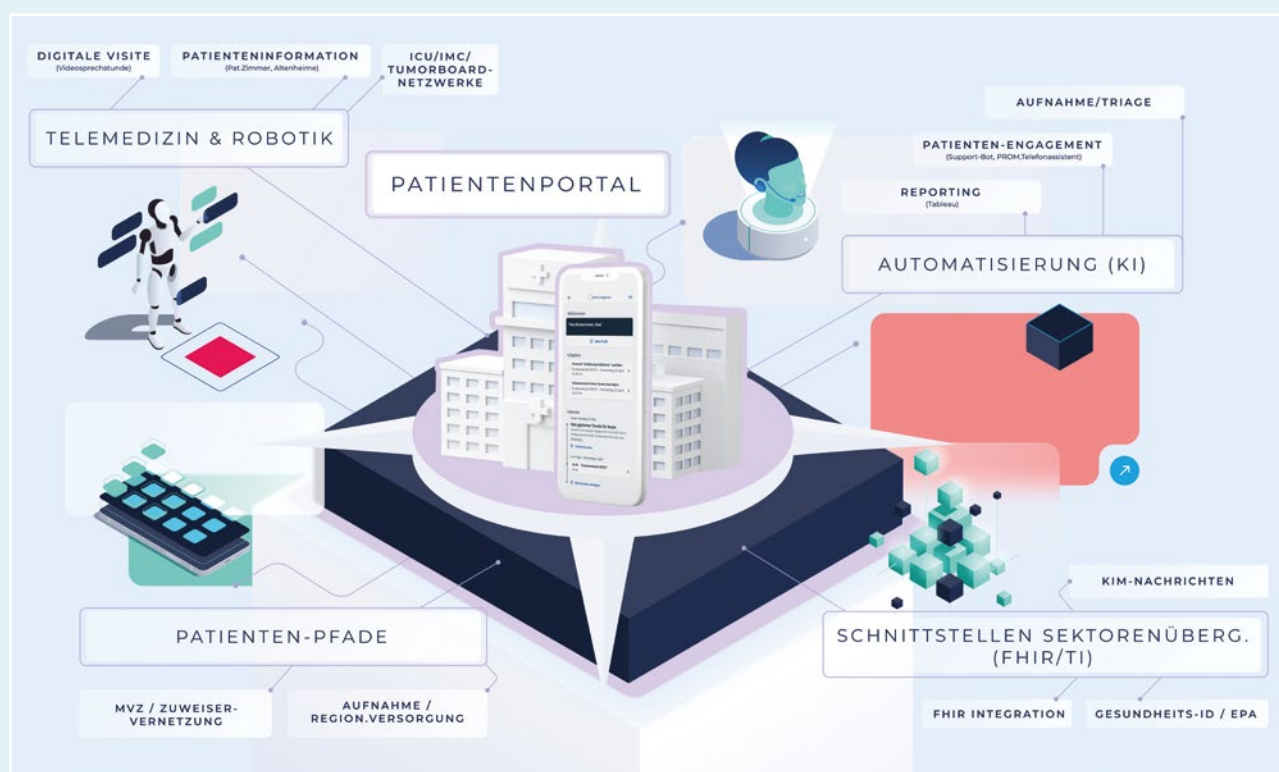
Um diese Schritte zu ermöglichen, entwickelt sich das Patientenportal in vier strategische Richtungen: (siehe Grafik unten)

Ambulantisierung:

Das Patientenportal als Versorgungsbrücke

Die Ambulantisierung stationärer Leistungen ist Teil der Reformrealität. Immer mehr Eingriffe, die bisher stationär erbracht wurden, werden künftig ambulant oder tagesstationär durchgeführt. Das entlastet Bettenkapazitäten, senkt Kosten und entspricht dem medizinischen Fortschritt. Doch die Ambulantisierung stellt neue Anforderungen an die Koordination: Wer übernimmt die Nachsorge? Wie wird der Übergang in die Häuslichkeit organisiert? Wann und wo stellen Patienten sich wieder vor? Diese Fragen sind ohne die Verzahnung von organisatorischen Verantwortlichkeiten, digitalen Prozesse und KI-Unterstützung kaum effizient abbildbar.

Das Portal wird zur Brücke zwischen stationärer Behandlung, ambulanter Nachsorge und kontinuierlichem Monitoring zu Hause. In den letzten 20 Jahren wurde viel über Case und Care Management gesprochen, nun bestehen die Möglichkeiten mittels eines konsequent weiterentwickelten Patientenportals, mit denen Krankenhäuser erstens die Sektoren-induzierte Versorgungslücke schließen können und zweitens deutlich effizienter und wirtschaftlicher werden. •



Copyright by samed

Mit KI-Agenten zu vernetzten Prozessen

Auf dem Veeva R&D and Quality Summit Europe in Kopenhagen vom 28. bis 29. Mai 2026 gab Veeva Systems einen Ausblick auf die KI-agentenbasierte Plattform Falcon und neue Features von Vault AI. Auf der Konferenz zeigten Unternehmen der Biopharma-Branche, wie sie damit Prozesse vereinfachen und standardisieren können und damit die Grundlage für den Einsatz von künstlicher Intelligenz schaffen. Mit Werner Engelbrecht von Veeva Systems sprachen wir über die Strategie des Anbieters und aktuelle Trends. /// von Stefan Girschner

Herr Engelbrecht, könnten Sie zunächst Ihre Tätigkeit bei Veeva Systems beschreiben?

Werner Engelbrecht | In meiner Funktion als Senior Director für Clinical Strategy bei Veeva Systems berate ich Kunden aus der Biopharma- und Biotech-Branche. Diese suchen vor allem Technologielösungen, um aktuellen Herausforderungen wie Effizienzsteigerung und Kostenreduktion im Vertrieb als auch die Gewährleistung der Patientensicherheit zu begegnen. Entscheidend ist, dass unsere Kunden zufrieden sind mit der Qualität unserer Lösungen.

Veeva Systems besitzt die Zertifizierung als „Public Benefit Corporation“. Was bedeutet diese Zertifizierung?

WE | Die Zertifizierung als Public Benefit Corporation schafft eine Balance zwischen Wachstum, Einkünften und Investitionen in Bereiche, wo wir keine Gewinne generieren. So unterstützen wir beispielsweise Prüfarztzentren in Österreich und weltweit, indem wir Ihnen unsere Softwarelösungen kostenfrei bereitstellen.

Worin liegt das Alleinstellungsmerkmal von Veeva Systems?

WE | Das Alleinstellungsmerkmal von Veeva Systems liegt in der Entwicklung einer Plattform, die Prozesse verarbeiten sowie Dokumente und Daten verwalten kann und nun auch im klinischen Bereich eingesetzt werden kann. Die Herausforderung für Unternehmen in der Pharma- und Biotech-Branche ist es, dass es immer mehr Prozesse gibt, die abteilungsübergreifend eine wichtige Rolle spielen. Und auch der Bereich Patientensicherheit nimmt an Bedeutung zu. Mit unserer Plattform wollen wir Unternehmen dabei unterstützen, die verschiedenen Prozesse miteinander zu verbinden und die Informationen übergreifend bereitzustellen. Wir gewährleisten auch, dass die

Daten der europäischen Kunden auch in Europa bleiben. In den USA nutzen wir die Cloud-Umgebung von Amazon Web Services, für Kunden in Europa haben wir ein eigenes Rechenzentrum in Frankfurt am Main. Unser Backup-Rechenzentrum befindet sich in Dublin in Irland.

Was halten Sie von der stark ausgeprägten Regulierung in den Bereichen Datenschutz und KI in Europa? Und wie passt dazu der Wunsch nach digitaler Souveränität?

WE | Ich bin der Auffassung, dass man bei den Regulierungen hier eine andere Perspektive einnehmen sollte. Denn Regeln wie der AI Act gewährleisten auch eine hohe Patientensicherheit. Zugleich können wir uns unseren Kunden garantieren, dass alle Prozesse kontrolliert ablaufen. Die Ansätze zu digitaler Souveränität versprechen gerade im Gesundheitswesen große Vorteile. Ein Kunde von uns, ein Krankenhaus in den Niederlanden, profitiert davon, dass der Datenaustausch von Gesundheitsdaten wie auch in der Forschung und Entwicklung auf einer sicheren Plattform abläuft. Außerdem startet die Europäische Kommission ein Projekt für den länderübergreifenden, anonymisierten Gesundheitsdaten-Austausch, um neue Medikamentenentwicklungen zu beschleunigen.

Welche Entwicklungen sehen Sie in Bereichen wie der Medikamentenzulassung?

WE | In der Medikamentenzulassung geht es heute vor allem darum, Medikamente schneller zulassen zu können. Dabei geht die Patientensicherheit immer vor. Ein großer Trend ist Real World Evidence (RWE), der sich fortsetzen wird, wodurch große Datenmengen generiert werden. Um eine schnellere Zulassung zu erreichen, werden heute oft verschiedene Studienphasen in einer Studie zusammengefasst und oft mit der Auflage, weitere Studien gemäß RWE nach der Zulassung durchzuführen.

„ Sogenannte Super Agenten koordinieren die anderen Agenten und weisen ihnen Arbeitsschritte zu. Dadurch lassen sich **Arbeitsabläufe effizient gestalten und der Mensch fungiert als Kontrollorgan. *Werner Engelbrecht***

Auf welchem Stand der Digitalisierung befindet sich derzeit die Biopharma- und Life-Sciences-Branche?

WE | Die Digitalisierung ist durch die Corona-Pandemie stark forciert worden, also kaum vergleichbar mit dem Stand vor sechs bis acht Jahren. Die betrifft insbesondere den Datenaustausch zwischen Pharmaunternehmen, medizinischen Forschungszentren und den Krankenhäusern. Früher lag die Herausforderung in der Kontrolle der Datenerhebung. Diese erfolgt heute elektronisch und automatisiert. Daher sind jetzt auch die Verordnungen der Europäischen Arzneimittel-Agentur (EMA) für die Zulassung neuer Medikamente angepasst worden.

Welche Neuerungen plant Veeva Systems in Bereich KI und Automatisierung?

WE | Zur Nutzung von KI werden absolut saubere Daten benötigt, ansonsten bringt der Output von KI keine guten Ergebnisse. Genau das haben wir mit unserer Plattform versucht, die als Basis nur saubere Daten verwendet. Und auch die Governance muss gewährleistet werden, insbesondere bei der Datenhaltung. Und hier kommt der AI Act wieder ins Spiel. Gerade bei zeitaufwendigen Prozessen im Dokumentmanagement gibt es viel Potenzial zur Automatisierung. Hierfür wird ein ganzes Netzwerk von KI-Agenten benötigt, um die einzelnen Arbeitsschritte zu automatisieren. Sogenannte Super Agenten koordinieren die anderen Agenten und weisen ihnen Arbeitsschritte zu. Dadurch lassen sich Arbeitsabläufe effizient gestalten und der Mensch

DER GESPRÄCHSPARTNER

Werner Engelbrecht

ist Senior Director, Clinical Strategy bei Veeva Systems.

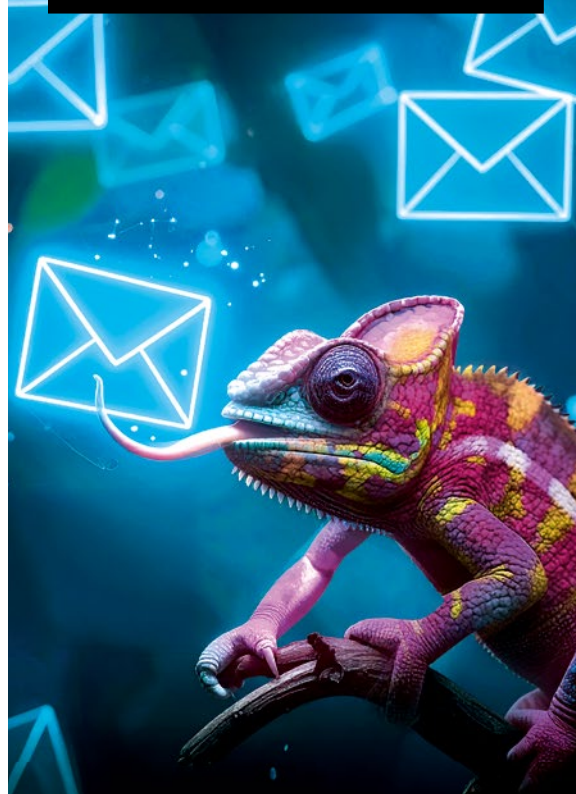


fungiert als abschließendes Kontrollorgan. Entscheidend ist es, für all diese Aktivitäten eine Abteilungs- und prozessübergreifende KI-Governance-Struktur aufzubauen.

Unter anderem geht es darum, Verbindungen vom kommerziellen CRM zur klinischen Forschung herzustellen. Daher verfolgen wir auch einen klar strukturierten Ansatz zur Integration von anderen Anwendungen. Unser Partnernetzwerk unterstützt unsere Kunden aus der Pharma- und Biotech-Branche sowie der Medizintechnikbranche dabei, die Lösungen von Veeva Systems in die vorhandene IT-Umgebung zu integrieren, um ein hohes Qualitätsmanagement zu erreichen. Übrigens gibt es heute nicht mehr die scharfe Trennung zwischen Business- und IT-Verantwortlichen. IT wird vielmehr als eine unterstützende Rolle der Business-Seite betrachtet. Der Business-Bereich definiert die Prozesse, operativen Strukturen und Technologien, während die IT-Abteilung mit ihrer Expertise beratend zur Seite steht. •

**AUS DEM
BRANCHENDICKICHT
GESCHNAPPT!**

**DER
NEWSLETTER,
DER ZU
IHNEN PASST.**



**Wissen, das kleben bleibt – jetzt den
NEWSLETTER kostenfrei sichern.**



**[www.digitalbusiness-
cloud.de/newsletter](http://www.digitalbusiness-cloud.de/newsletter)**

DIGITAL BUSINESS

eine Marke vom

**WIN
VERLAG**

Wahl des Rechenzentrums: Checkliste für die Geschäftsführung

Colocation hilft dem Mittelstand, steigende Anforderungen an die IT zu erfüllen. Bei der Anbieterwahl fällt zunehmend auch digitale Souveränität ins Gewicht. /// von Thomas Firatan

MIT EIGENEN SERVERRÄUMEN STOSSEN MITTELSTÄNDISCHE UNTERNEHMEN SCHNELL AN STRUKTURELLE GRENZEN. Das liegt nicht zuletzt an den seit Jahren steigenden regulatorischen Anforderungen. IT-Sicherheitsrichtlinien wie NIS2 fordern eine redundante Strom- und Kühlungsversorgung, physische Zutrittskontrollen und eine hohe Verfügbarkeit von IT-Systemen. Gleichzeitig verpflichtet das Energieeffizienzge-

le Rechenzentrum eines Dienstleisters verlegen. Dort finden sie eine Betriebsumgebung vor, die sie in Eigenregie nicht auf wirtschaftliche Art und Weise erreichen können.

Worauf kommt es bei der Auswahl an?

Die Auswahl des Colocation-Dienstleisters wird dabei meist vor allem anhand technischer und wirtschaftlicher Kriterien getroffen.

Solche Kriterien sind natürlich relevant und bilden eine wichtige Grundlage für die Anbieter-Auswahl.

Mittelständische Unternehmen sollten sich aber nicht darauf beschränken. Mit der Auslagerung der IT-Infrastruktur verändert sich nicht nur die technische Betriebsumgebung. Unternehmen gehen gleichzeitig eine langfristige Beziehung zu einem externen Dienstleister ein, der zentrale Teile ihrer digitalen Wert-



DER AUTOR
Thomas Firatan

ist Chief Sales Officer beim Rechenzentrenbetreiber nexspace data centers. Er verfügt über 20 Jahre Vertriebserfahrung in der Rechenzentrums- und IT-Branche und bekleidete Führungspositionen bei zahlreichen internationalen Unternehmen.
(Quelle: nexspace)

„ Bei der Auswahl eines **Colocation Partners** sollten mittelständische Unternehmen, neben technischer Leistungsfähigkeit darauf achten, dass sie die Kontrolle über ihre Daten behalten.

Thomas Firatan

setz Unternehmen zur Nachhaltigkeitsberichterstattung und hält sie dazu an, ihre IT-Infrastruktur energieeffizient zu betreiben.

Die dafür notwendigen Maßnahmen überfordern viele mittelständische Unternehmen, weil sie sich nur mit großem organisatorischem und finanziellem Aufwand umsetzen lassen. Colocation bietet einen praktikablen Ausweg: Unternehmen jeder Größe können ihre Server in das professionel-

Im Mittelpunkt stehen Fragen wie:

- Welche Verfügbarkeit wird garantiert?
- Wie leistungsfähig ist die Netzwerkanbindung?
- Welche PUE (Power Usage Effectiveness) weist das Rechenzentrum auf?
- Welche Zertifizierungen hat das Rechenzentrum?
- Wie flexibel lassen sich zusätzliche Kapazitäten bereitstellen?
- Welche Kosten entstehen?

schöpfung beherbergt. Dadurch stellt sich auch die Frage der digitalen Souveränität.

Digitale Souveränität wird zum strategischen Ziel

Dieses Thema gewinnt wegen der anhaltenden politischen Spannungen immer mehr an Bedeutung. Auf europäischer Ebene wird digitale Souveränität zunehmend als strategisches Ziel formuliert. Staaten, Unternehmen und Institutionen sollen

ihre digitalen Abhängigkeiten selbst steuern und kritische Infrastrukturen unter eigener rechtlicher und organisatorischer Kontrolle betreiben.

Für Unternehmen stellt sich damit zunehmend die Frage, wer im Ernstfall Zugriff auf geschäftskritische Daten erhalten könnte und welchen rechtlichen Rahmenbedingungen dieser Zugriff unterliegt. Besonders kritisch ist vor diesem Hintergrund der US Cloud Act. Er ermöglicht es US-Behörden unter bestimmten Voraussetzungen, von US-Unternehmen die Herausgabe von Daten zu verlangen. Das gilt auch dann, wenn die Daten an Standorten außerhalb der Vereinigten Staaten gespeichert werden.

Colocation-Auswahl ist Chefsache

Bei der Auswahl eines Colocation-Partners sollten mittelständische Unternehmen nicht nur auf technische Leistungsfähigkeit und wirtschaftliche Attraktivität achten, sondern auch darauf, dass sie die Kontrolle über ihre Daten behalten. Das erreichen sie am besten, wenn sie nicht auf einen globalen Dienstleister setzen, sondern einen lokalen Anbieter wählen, der seinen Sitz in der Europäischen Union hat und dadurch auch selbst dem Rechtsraum der DSGVO angehört. Dann haben sie bei der Speicherung und Verarbeitung ihrer Daten im Rechenzentrum des Colocation-Dienstleisters Rechtssicherheit. Die Berücksichtigung von digitaler Souveränität verändert den Charakter der Colocation-Entscheidung spürbar. Es geht nicht nur um technische Anforderun-

gen und Kosten, sondern auch um eine strategische Entscheidung. Diese lässt sich nicht allein auf IT-Ebene treffen. Sie betreffen die übergreifende Risikosteuerung und liegen damit in der Verantwortung der Geschäftsführung.

Fazit

Colocation ist für viele mittelständische Unternehmen heute die Antwort auf steigende Anforderungen an Sicherheit, Verfügbarkeit und regulatorische Konformität. Sie ermöglicht den Betrieb moderner IT-Infrastrukturen unter Bedingungen, die im eigenen Serverraum nur schwer wirtschaftlich darstellbar sind.

Die Anbietersuche sollte aber nicht nur von technischen und wirtschaftlichen Kriterien geleitet werden. Wer heute einen Colocation-Partner auswählt, entscheidet nicht nur über Rack-Fläche und Verfügbarkeit, sondern auch über die digitale Souveränität seines Unternehmens. •

Q&A:

COLOCATION IM MITTELSTAND

- **Warum entscheiden sich mittelständische Unternehmen für Colocation?**
Weil professionelle Rechenzentren Anforderungen an Verfügbarkeit, Sicherheit und Compliance häufig wirtschaftlicher erfüllen können als eigene Serverräume.
- **Welche Rolle spielt digitale Souveränität bei Colocation?**
Auch bei der Auslagerung ihrer IT-Infrastruktur an einen externen Dienstleister sollten Unternehmen die Kontrolle über ihre Daten behalten.
- **Welche Vorteile bieten europäische Colocation-Anbieter?**
Sie unterliegen dem europäischen Datenschutz- und Rechtsrahmen. Dadurch haben Unternehmen Rechtssicherheit bei der Speicherung und Verarbeitung ihrer Daten.

Colocation-Rechenzentren bieten eine professionelle Betriebsumgebung, die sich in Eigenregie nicht wirtschaftlich erreichen lässt.

© Martin Joppen / Martin Joppen GmbH



ÜBER DEINE WOLKE HINAUS

ERFAHRE DAS NEUESTE AUS DER BRANCHE

Jetzt Magazin **abonnieren**
und nichts verpassen.



www.digitalbusiness-magazin.de/abonnement

DIGITAL BUSINESS

eine Marke vom



Raus aus der Hyperscaler-Falle

Stefan Schäfer von OVHcloud erklärt, wie Unternehmen mit klarer Architektur und Partnern mehr Kontrolle über Daten und Cloud-Strukturen gewinnen. /// von Heiner Sieger

Wie hat sich das Thema digitale Souveränität in den vergangenen 12 bis 18 Monaten verändert – auch vor dem Hintergrund geopolitischer Entwicklungen?

Stefan Schäfer | Ich nehme im Markt eine deutliche Verschiebung wahr. Digitale Souveränität ist kein Randthema mehr, sondern hat sich zu einer zentralen Fragestellung für viele Unternehmen entwickelt. Auslöser sind vor allem geopolitische Spannungen, Diskussionen rund um den US CLOUD Act und nicht zuletzt die zunehmende Sensibilität gegenüber Abhängigkeiten von einzelnen Anbietern.

Was sich besonders verändert hat: Das Interesse kommt inzwischen aus der Breite des Marktes. Es sind nicht mehr nur stark regulierte Branchen oder der öffentliche Sektor, sondern auch klassische mittelständische Unternehmen, die sich intensiv mit Alternativen beschäftigen. Viele Organisationen, die zuvor klar auf US-Hyperscaler gesetzt haben, hinterfragen diese Strategie zunehmend. Themen wie mögliche Zugriffsszenarien auf Daten, politische Einflussfaktoren oder auch sogenannte „Kill-Switch“-Diskussionen tragen dazu bei, dass das Risikobewusstsein deutlich gestiegen ist.

OVHcloud beschreibt digitale Souveränität über drei Säulen: rechtlich, technologisch und operativ. Welche Dimension ist für Ihre Kunden besonders relevant – und wo sehen Sie noch Defizite?

S. Schäfer | In vielen Gesprächen erleben wir, dass Souveränität zunächst auf regulatorische Aspekte reduziert wird. Unternehmen stellen sich vor allem die Frage, ob sie vollständig der DSGVO unterliegen oder ob potenzielle Zugriffe durch den CLOUD Act ausgeschlossen sind. Diese Perspektive ist verständlich, greift aber zu kurz.

Technologische Souveränität bedeutet beispielsweise, dass Unternehmen ihre Systeme ohne große Hürden migrieren oder wechseln können. Wenn ein Anbieterwechsel mit erheblichen technischen oder finanziellen Barrieren verbunden ist, entsteht eine neue Abhängig-

keit. Genau hier kommen Themen wie Lock-in oder proprietäre Architekturen ins Spiel. Die operative Dimension wird ebenfalls häufig unterschätzt. Sie umfasst Fragen wie: Wo werden Daten tatsächlich verarbeitet? Wer betreibt die Systeme? Wer hat Zugriff im laufenden Betrieb? Diese Aspekte sind essenziell für echte Kontrolle. Wir beobachten jedoch, dass sich das Verständnis erweitert. Kunden erkennen zunehmend, dass Souveränität ein Zusammenspiel aller drei Dimensionen ist – und nicht allein durch regulatorische Compliance erreicht wird.

Sie positionieren Open Source als Schlüssel für digitale Souveränität. Wie realistisch ist eine Open-Source-First-Strategie, insbesondere im öffentlichen Sektor?

S. Schäfer | Die Dynamik in diesem Bereich ist deutlich spürbar. Gerade im öffentlichen Sektor sehen wir konkrete Initiativen, die bewusst auf Open Source setzen. Frankreich ist hier ein gutes Beispiel, aber auch in Deutschland – etwa in Schleswig-Holstein – gibt es entsprechende Entwicklungen. Gleichzeitig darf man die Herausforderungen nicht unterschätzen. Viele Organisationen stehen vor der Aufgabe, bestehende Systeme zu migrieren. Das bedeutet Aufwand, sowohl technisch als auch organisatorisch. Der Wechsel hin zu Open Source ist kein kurzfristiges Projekt, sondern ein Transformationsprozess.

Dennoch wächst die Bereitschaft, diesen Weg zu gehen. Open Source wird zunehmend als strategischer Hebel verstanden, um Abhängigkeiten zu reduzieren und langfristig mehr Kontrolle zu gewinnen. Unsere Rolle besteht darin, diese Entwicklung aktiv zu unterstützen. Wir bauen unsere Plattformen und Ökosysteme konsequent auf offenen Technologien auf und arbeiten mit Partnern zusammen, die diesen Ansatz teilen. Das gilt auch für neue Themenfelder wie Künstliche Intelligenz, bei denen offene Standards eine immer größere Rolle spielen.

Die EU treibt mit Regulierungen wie dem Data Act den Wettbewerb im Cloud-Markt voran. Welche Auswirkungen sehen Sie konkret?

„ Open Source wird zunehmend als **strategischer Hebel** verstanden, um Abhängigkeiten zu reduzieren und langfristig mehr Kontrolle zu gewinnen. Unsere Rolle besteht darin, diese Entwicklung aktiv zu unterstützen.

Stefan Schäfer

S. Schäfer | Der EU Data Act ist aus meiner Sicht ein entscheidender Schritt, weil er strukturelle Hürden abbaut. Insbesondere die Abschaffung von Egress Fees und die Verpflichtung zu standardisierten Wechselprozessen adressieren zentrale Probleme des Marktes. Für uns ist das keine grundlegende Veränderung, da wir solche Gebühren nie erhoben haben. Für viele andere Anbieter hingegen bedeutet das eine deutliche Anpassung ihrer Geschäftsmodelle. Das wird den Wettbewerb intensiver machen und vor allem die Wechselbereitschaft der Kunden erhöhen.

Allerdings reicht Regulierung allein nicht aus. Unternehmen müssen auch verstehen, welche Optionen sie haben und wie sie diese nutzen können. Hier sehen wir weiterhin Aufklärungsbedarf. Digitale Souveränität ist nicht nur eine Frage der Rahmenbedingungen, sondern auch der konkreten Umsetzung.

Viele Unternehmen wollen ihre Abhängigkeit reduzieren, haben aber keinen klaren Fahrplan. Wie sieht eine realistische Strategie aus?

S. Schäfer | Der wichtigste Punkt ist, dass der Weg zur Souveränität kein „Big Bang“ ist. Ein vollständiger, sofortiger Wechsel ist in den meisten Fällen weder realistisch noch sinnvoll. Stattdessen empfehlen wir ein schrittweises Vorgehen. Am Anfang steht immer eine fundierte Analyse der bestehenden Architektur. Darauf aufbauend lassen sich Szenarien entwickeln, wie einzelne Komponenten migriert werden können.

Ein typischer Einstiegspunkt ist beispielsweise Disaster Recovery. Unternehmen schaffen zunächst eine Ausweichumgebung bei einem alternativen Anbieter. Danach können weitere Schritte folgen, etwa die Verlagerung von Storage oder einzelnen Workloads. Entscheidend ist, dass die Geschäftsfähigkeit jederzeit erhalten bleibt. Genau hier liegt auch die größte Herausforderung – und gleichzeitig der größte Mehrwert einer strukturierten Vorgehensweise. Partner spielen dabei eine zentrale Rolle, weil sie sowohl technologisches Know-how als auch praktische Erfahrung einbringen.

Ein häufiges Argument gegen europäische Anbieter ist die vermeintliche Leistungslücke. Wie gehen Sie damit um?

S. Schäfer | Diese Diskussion führen wir regelmäßig. Fakt ist: Hyperscaler bieten eine enorme Bandbreite an Funktionen. Gleichzeitig zeigen Analysen, dass Unternehmen in der Praxis nur einen kleinen Teil dieser Features tatsächlich nutzen. Das führt zu einer wichtigen Frage: Was wird wirklich benötigt? Viele Unternehmen orientieren sich an theoretischen Möglichkeiten, nicht an ihrem tatsächlichen Bedarf.

Unsere Antwort besteht darin, genau hier anzusetzen. Wir analysieren gemeinsam mit den Kunden ihre Anforderungen und konzentrieren uns auf die Funktionen, die tatsächlich relevant sind. Parallel dazu bauen wir unser Portfolio gezielt aus, um bestehende Lücken dort zu schließen, wo sie für die Praxis entscheidend sind. Es geht also nicht darum, jedes Feature nachzubilden, sondern

darum, die richtigen Funktionen in der richtigen Qualität bereitzustellen.

Welche Rolle spielt Ihr Partner-Ökosystem bei der Umsetzung dieser Strategien?

S. Schäfer | Unsere Partner sind ein zentraler Bestandteil unseres Ansatzes. Sie sind nicht nur Vertriebskanal, sondern echte Umsetzungspartner. Interessanterweise müssen wir sie vom Thema digitale Souveränität nicht überzeugen. Viele Partner kommen gezielt zu uns, weil sie genau diese Lösungen anbieten möchten. Sie sehen darin eine klare Nachfrage im Markt.

Gleichzeitig bringen sie wertvolle Kompetenzen ein – insbesondere bei Architekturberatung, Migration und Betrieb. Diese Nähe zum Kunden hilft uns auch, unsere eigenen Angebote weiterzuentwickeln. Der Erfolg entsteht letztlich im Zusammenspiel: Technologie von uns, Umsetzungskompetenz der Partner und eine klare strategische Ausrichtung beim Kunden. •

DER GESPRÄCHSPARTNER

Stefan Schäfer

ist Marketing Director Central & Eastern Europe bei OVHcloud. Er verantwortet die Marktstrategie in der Region und beschäftigt sich intensiv mit Cloud-Souveränität, Open Source und digitalen Transformationsstrategien im europäischen Kontext.



Souveräne KI für Europa

Die EU will unabhängiger von Big-Tech-Konzernen werden. Gleichzeitig verspricht agentische KI große Effizienzgewinne. Wie lassen sich beide Ziele vereinen? /// von Nico Bäumer

DARUM GEHT ´S

Die breitere Debatte: Versäumt Europa KI-Innovationen, wenn es sich zu sehr von der restlichen Tech-Welt abkoppelt?

Agent ≠ Model: Es muss nicht Open AI oder Google sein, Agenten können auch mit lokalen Modellen betrieben werden – Human-In-The-Loop sollte Pflicht sein.

Kein Schwarz-Weiß-Denken: Absolute Souveränität wird es nie geben, es bleibt je nach Use Case abzuwägen.

DASS FEHLENDE DIGITALE SOUVERÄNITÄT REALE PROBLEME VERURSACHEN KANN, hat ein Vorfall am Internationalen Strafgerichtshof im letzten Herbst eindrucksvoll gezeigt. Nachdem der Chefankläger zeitweise keinen Zugriff mehr auf seine E-Mails hatte, entschied sich die Behörde für einen Wechsel von Microsoft zum deutschen openDesk. Auch andere Institutionen und Unternehmen stoßen ähnliche Projekte an und versuchen den Souveränitätsgedanken praktisch umzusetzen. Gleichzeitig stellt sich die Frage, wie sich der Wunsch nach mehr Unabhängigkeit mit den Effizienz- und Innovationspotenzialen agentischer KI in Einklang bringen lässt.

Schnell kommt dann auch die Frage auf, ob Europa durch das Beharren auf dem Souveränitätsprinzip Innovationen versäumt. Oder droht andererseits die Dystopie einer außer Kontrolle geratenen, unkontrollierbaren KI? Aus einer technologischen Frage wird dann nicht selten auch noch eine kulturelle Dimension abgeleitet,

die asiatische Innovationskraft und amerikanischen Unternehmergeist europäischer Zurückhaltung oder gar Rückständigkeit gegenüberstellt. Akademisierende Diskussionen auf diesem Niveau können wir uns in der Praxis allerdings nicht mehr leisten. Schließlich ist beides Realität: Geopolitische Spannungen, die Abhängigkeiten hinterfragen lassen, und KI-Agenten, die immer leistungsfähiger und zum festen Bestandteil von Unternehmensstrategien werden. Für uns als IT-Dienstleister geht es darum, wie wir einen Mittelweg finden können, der die kontrollierte und Compliance-konforme Nutzung von KI-Agenten für europäische Unternehmen ermöglicht.

Wie lassen sich Agenten und Modelle entkoppeln?

Aus der privaten und teilweise auch beruflichen Nutzung generativer KI sind es viele Menschen gewohnt, „künstliche Intelligenz“ mehr oder weniger synonym mit einem bestimmten Anbieter oder Modell zu verwenden – man nutzt ChatGPT, Claude,

Copilot, Gemini etc. Viele Anwender bleiben ihrem präferierten Chatbot treu. Um Unternehmens-KI und vor allem Agenten für Unternehmen besser zu verstehen, müssen wir uns von diesen Vorstellungen lösen. Dies beginnt damit, dass es sich bei Agenten in Unternehmen in den meisten Fällen nicht um eine monolithische All-in-one-Lösung handelt.

Das wird der Realität von gewachsenen und regulierten Geschäftsprozessen nicht gerecht. Stattdessen geht es darum, KI so in diese Prozesse zu integrieren, dass sie dort im Rahmen konkreter Anforderungen direkt Mehrwert liefert. Agenten, die darauf ausgelegt sind, können hochspezialisiert sein. Somit muss gar nicht immer ein Large Language Model (LLM) im Hintergrund laufen, auch Zugriff auf das Internet ist nicht zwingend notwendig. Ein KI-Agent kann auch auf einem lokalen Small Language Model (SLM) basieren und nur mit unternehmenseigenen Daten arbeiten. Dies wäre das höchste Level an Souveränität – für viele Anwendungsfälle aber weder wirtschaftlich sinnvoll noch notwendig.

Wichtig ist deshalb, dass Unternehmen die Flexibilität und Wahlfreiheit haben, wie sie die in ihre Software integrierten Agenten betreiben wollen. APIs und offene Interoperabilitätsstandards sorgen dafür, dass verschiedene Modelle angebunden werden können – von lokal gehostet, über europäische Anbieter in heimischen Clouds bis hin zu den großen LLMs.

Die Wahlfreiheit und Austauschbarkeit machen einen großen Teil von Souveränität aus. Außerdem trägt dieser Aspekt zur Resilienz von Infrastrukturen bei, wie sie beispielsweise durch Regularien wie DORA gefordert wird. Souveränität umfasst dabei



DER AUTOR
Nico Bäumer

ist Vorstand und CTO der dvelop AG und treibt mit seiner langjährigen Erfahrung im Produktmanagement und in der Produktentwicklung die Innovations- und Digitalisierungsstrategie des Unternehmens voran.

mehr als die Wahl des Modells. Sie betrifft den gesamten Agenten-Stack: die Kontrolle über Unternehmensdaten, die Orchestrierungsebene, die definierten Aktionen und Werkzeuge eines Agenten sowie die Nachvollziehbarkeit seiner Entscheidungen. Eine belastbare Souveränitätsstrategie berücksichtigt all diese Aspekte – und nicht nur die Frage, welches LLM im Hintergrund läuft.

Human-in-the-Loop und Agenten im Prozess

Ganz oben bei den Befürchtungen bezüglich KI-Agenten rangiert die Angst, dass sie eigenständig Entscheidungen treffen, die dem Unternehmen oder sogar Menschen schaden. Für dieses Szenario müsste allerdings zuvor ein menschlicher Nutzer die relevanten Zugänge zu sensiblen Daten an den Agenten übergeben und anschließend komplett auf den letzten menschlichen Freigabeschritt verzichten. Um das zu verhindern, werden die Mitarbeitenden einiger Branchen nicht nur entsprechend geschult, sondern auch regulatorisch ist der Human-in-the-Loop-Ansatz vorgeschrieben. Beispielsweise kann KI zwar die Vorarbeit für Kreditformalitäten im Finanzwesen erledigen, die endgültige Entscheidung, ob der Kredit gewährt wird, muss aber immer bei einem Menschen liegen.

Entscheidend ist, dass Human-in-the-Loop kein binäres Prinzip darstellt, sondern ein abgestuftes Modell entlang des jeweiligen Risikos. Je nach Prozess und Risikoklasse reicht das Spektrum von reinen Vorschlägen mit menschlicher Prüfung über freigabepflichtige Aktionen bis hin zu definierten Routineaufgaben, die ein Agent eigenständig innerhalb klarer Grenzen ausführt – stets mit vollstän-

digem Audit-Trail. Genau diese Abstufung bildet die zentrale Designfrage beim Einsatz von KI-Agenten im Unternehmen.

Wie können zukünftige souveräne Agenten aussehen?

Hinzu kommt die Integration in Geschäftsprozesse. Viele spezialisierte Agenten, die klar definierte Aufgaben in bestehenden Strukturen übernehmen, wirken deutlich weniger dystopisch als eine „autonome Super-KI“, die nach dem Black-Box-Prinzip intransparent entscheidet und unmittelbar handelt. Es ist daher zu erwarten, dass es zukünftig sehr viel mehr Agenten geben wird, die sich durch hohe Spezialisierung, tiefe Integration und menschliche Aufsicht auszeichnen. In Kombination mit Wahlfreiheit und Austauschbarkeit von Modellen, lässt sich digitale Transformation mit der Forderung nach Souveränität vereinen. Souveränität ist dabei kein Zustand, sondern eine Architekturentscheidung – und sie hat einen Preis, etwa in zusätzlicher Komplexität oder Qualitätsunterschieden zwischen Modellen. Für europäische Unternehmen ist diese Investition in vielen Fällen nicht nur strategisch sinnvoll, sondern regulatorisch geboten. Die zentrale Frage für Entscheider lautet deshalb nicht mehr „Souveränität oder Innovation?“, sondern: Welche Agenten-Architektur sichert beides – heute und bei wechselnden Rahmenbedingungen? •

STUFEN DER KI-SOUVERÄNITÄT

Level 1: Anbindung der großen LLMs: höchste Performanz und Verfügbarkeit, aber nur für unkritische Workloads geeignet.

Level 2: Nutzung europäischer LLMs gehostet in lokalen Clouds: Mehr Sicherheit durch geregelte EU-Datenresidenz – guter Kompromiss.

Level 3: Selbst gehostete LLMs: Hohe Kontrolle, aber auch Infrastruktur und Kostenfaktor. Skalierbarkeit eingeschränkt.

Level 4: Lokale (offline) SLMs: Eingeschränkte Anwendungsbereiche, aber überschaubare Ressourcen und durch Abschottung maximale Kontrolle möglich. Prinzipiell auch für kritische Daten geeignet.

Q&A:

• Heißt Souveränität im KI-Kontext, dass alles on-premise laufen muss?

Nein. Absolute Souveränität ist selten realistisch oder wirtschaftlich sinnvoll. Häufig ist ein abgestufter Ansatz optimal: sensible Daten und kritische Schritte stärker abschotten, weniger kritische Funktionen flexibel (z. B. in europäischen Clouds oder mit großen Modellen) betreiben.

• Warum ist die Trennung von Agent und Sprachmodell wichtig?

Ein Agent ist die in Prozesse integrierte „Handlungsebene“ (Ziele, Tools, Aktionen, Regeln). Das Sprachmodell ist nur eine austauschbare Komponente. Diese Entkopplung ermöglicht es, je nach Risiko, Kosten und Datenlage unterschiedliche Modelle zu nutzen – bis hin zu lokalen SLMs.

• Wann reichen lokale Modelle aus und wann braucht es große LLMs?

Für klar umrissene, wiederkehrende Aufgaben mit reinen Unternehmensdaten können SLMs ausreichend sein. Große LLMs spielen ihre Stärke aus, wenn Aufgaben breiter, sprachlich komplexer oder stärker auf Allgemeinwissen angewiesen sind. Entscheidend ist, den Modellmix an Anforderungen, Qualität und Compliance auszurichten.

• Wie verhindert man, dass Agenten außer Kontrolle geraten?

Durch abgestuftes Human-in-the-Loop-Design: von reinen Vorschlägen über freigabepflichtige Aktionen bis zu klar begrenzten Routinen. Zusätzlich braucht es Rollen- und Rechtekonzepte, sichere Tool-Anbindungen sowie vollständige Protokollierung der Agentenentscheidungen.

• Welche Rolle spielen offene Standards und APIs?

Sie sind der Schlüssel zur Wahlfreiheit: Modelle lassen sich austauschen, Komponenten lassen sich modular betreiben, und Abhängigkeiten werden reduziert. Gleichzeitig unterstützt das die Resilienz-Anforderungen, wie sie z. B. im Kontext von DORA adressiert werden.

Erhalt der Handlungsfähigkeit

Europäische Unternehmen stehen zunehmend unter Druck, ihre technologische Abhängigkeit von den USA und China zu reduzieren. Offene Standards, quelloffene Software und kontrollierbare Infrastrukturen werden zunehmend zum Schlüssel für digitale Resilienz. /// von Frank Schnicke



DER AUTOR

Frank Schnicke

ist Leiter der Abteilung „Digital Twin Engineering“ am Fraunhofer-Institut für Experimentelles Software Engineering IESE in Kaiserslautern. In seiner Abteilung werden Open-Source-Technologien wie Eclipse BaSyx erstellt, um die Digitale Souveränität von Europa durch die interoperable Bereitstellung von digitalen Zwillingen und Datenräumen zu stärken.

ALLES BEGANN MIT DER CORONA-PANDEMIE, dann folgte der Krieg in der Ukraine, schließlich kam noch der Konflikt im Nahen Osten hinzu. Die Weltwirtschaft hat sich in den vergangenen sechs Jahren rasant verändert – und die politische Landschaft mit ihr. Machtwechsel, Handelskriege und geopolitische Spannungen, insbesondere zwischen den USA und China, führten zu einem wachsenden Bedürfnis nach wirtschaftlicher Unabhängigkeit und Resilienz in Europa.

Stille Abhängigkeit im Arbeitsalltag

Gerade im Technologiesektor ist Europa stark von den USA abhängig. Ob im Finanzwesen, in der Automobilbranche, im Marketing – fast alle Unternehmen setzen Softwarelösungen für Kommunikationszwecke, Präsentationen oder Designarbeiten ein, die von US-amerikanischen Anbietern bereitgestellt werden. Dadurch entsteht eine direkte Abhängigkeit: Ausfälle, Preissteigerungen oder politisch angestoßene Änderungen – etwa beim Datenschutz – wirken sich unmittelbar auf Arbeitsprozesse aus.

In einer aktuellen Bitkom-Umfrage gaben 93 Prozent der Befragten an, dass Deutschland bei digitalen Lösungen von anderen Ländern abhängig sei. 79 Prozent forderten zudem, Deutschland solle stärker in digitale Schlüs-

seltechnologien investieren. Um die Abhängigkeit von wirtschaftlichen Großmächten wie den USA und China zu reduzieren, braucht es vor allem drei Voraussetzungen: offene Standards, quelloffene Software und eine kontrollierbare Infrastruktur.

Offene Standards für Interoperabilität

Offene Standards ermöglichen die Interoperabilität zwischen verschiedenen Systemen – zum Beispiel über standardisierte Dateiformate, Schnittstellen oder Kommunikationsprotokolle. So können Unternehmen Vendor Lock-ins vermeiden, also die starke Abhängigkeit von einem einzelnen Anbieter. Beruht eine Cloud, ein ERP-System oder eine Kollaborationsplattform auf offenen Standards, lässt sich die Infrastruktur später deutlich einfacher wechseln oder erweitern.

Ein Vendor Lock-in entsteht dagegen genau dann, wenn diese Offenheit fehlt oder durch eine starke Produktintegration überlagert wird. Ein Beispiel: Die Systeme bei Microsoft 365 wie Teams, Word, PowerPoint und Outlook sind so eng miteinander verzahnt, dass sie einen geschlossenen Arbeitsraum bilden. Ein Anbieter-Wechsel ist in der Regel teuer, komplex und technisch kaum ohne Brüche möglich. Offene Standards wie etwa im Bereich der Industrie 4.0 mit der Verwaltungsschale (AAS) wirken

„ Unternehmen sollten wichtige Systeme selbst betreiben oder **zumindest technisch die Kontrolle darüber behalten**. Gemeint ist etwa die Möglichkeit, Software auf eigenen Servern, in europäischen Rechenzentren oder in einer kontrollierten privaten Cloud laufen zu lassen.

Frank Schnicke

dem entgegen, da sie Interoperabilität herstellen und damit die Wechsel- und Kombinationsmöglichkeiten erhöhen. Sie geben jedem physischen oder digitalen Objekt – etwa Maschinen, Sensoren, Bauteilen – eine standardisierte digitale Beschreibung. Diese „digitale Hülle“ bündelt technische Daten, Zustände und Dokumentationen. Dadurch können unterschiedliche Systeme und Hersteller die Informationen direkt austauschen und weiterverarbeiten, ohne individuelle Schnittstellen entwickeln zu müssen.

Quelloffene Software für die Implementierung

Quelloffene Programme (also Open-Source) sorgen dafür, dass die Nutzungshürde für offene Standards wie die AAS weiter gesenkt werden. Wichtig ist dabei die Wahl einer passenden Open-Source-Lizenz, wie etwa der MIT-Lizenz. Im Open-Source-Bereich spricht man dabei oft von starken bzw. schwachen Copyleft-Lizenzen. Starke Copyleft-Lizenzen wie die GPL-Lizenz erfordern die komplette Veröffentlichung des Quellcodes des restlichen Programms, während schwache Copyleft-Lizenzen dies typischerweise nicht erfordern und sich dadurch auch für den kommerziellen Einsatz gut eignen.

Als Beispiel stellt Eclipse BaSyx die komplette Infrastruktur der Verwaltungsschale als Open-Source-Software unter der MIT-Lizenz bereit. So sinkt der Entwicklungsaufwand für Unternehmen, während die Einführung interoperabler Architekturen beschleunigt wird.

Den Betrieb unter eigener Kontrolle halten

Der dritte Punkt ist strategisch: Unternehmen sollten wichtige Systeme selbst betreiben oder zumindest technisch die Kontrolle darüber behalten. Gemeint ist etwa die Möglichkeit, Software auf eigenen Servern, in europäischen Rechenzentren oder in einer kontrollierten privaten Cloud laufen zu lassen. Wer ausschließlich auf externe Plattformen angewiesen ist, macht sich anfällig für politische Konflikte, Sanktionen, Preisänderungen oder Ausfälle.

Kontrollierbare Infrastruktur bedeutet nicht zwangsläufig, dass jedes Unternehmen eigene Rechenzentren betreiben muss. Entscheidend ist vielmehr, dass zentra-

le Systeme transparent, nachvollziehbar und unabhängig administrierbar bleiben. Unternehmen sollten jederzeit wissen, wo ihre Daten liegen, wer Zugriff darauf hat und unter welchen rechtlichen Bedingungen die Infrastruktur betrieben wird. Interoperable und quelloffene Systeme ermöglichen jederzeit die Migration, sollten sich die Rahmenbedingungen auf einer genutzten Hosting-Plattform verschlechtern.

Besonders relevant wird das bei sensiblen Daten, zum Beispiel in der Industrie. Wenn Produktionsdaten, Entwicklungsinformationen oder Kundendaten ausschließlich über außereuropäische Plattformen verarbeitet werden, entstehen wirtschaftliche und strategische Risiken. Europäische Cloud- und Open-Source-Lösungen können helfen, Kontrolle zurückzugewinnen und die digitale Wertschöpfung langfristig in Europa zu halten.

CHECK DIGITALE SOUVERÄNITÄT

Ziel: Strategische Resilienz

Setzen Sie konsequent auf offene Standards wie die Verwaltungsschale (AAS). Diese sichert die Interoperabilität Ihrer Systeme und verhindert den Vendor Lock-in. Nutzen Sie quelloffene Software wie Eclipse BaSyx, um Entwicklungskosten zu senken und technologisch unabhängig zu bleiben

Digitale Souveränität als Transformationsprozess

Digitale Souveränität entsteht nicht von heute auf morgen, sondern durch einen langfristigen Umbau der digitalen Infrastruktur. Offene Standards und quelloffene Software schaffen die technische Grundlage, kontrollierbare Infrastrukturen sichern die operative Unabhängigkeit von Unternehmen.

In der Praxis bedeutet das für Firmen, bestehende Abhängigkeiten realistisch zu analysieren und dort Alternativen aufzubauen, wo das Risiko besonders hoch ist. Nicht jede Abhängigkeit ist unmittelbar problematisch. Entscheidend ist die Fähigkeit, im Ernstfall handlungsfähig zu bleiben. Wie sich zeigt, ist digitale Souveränität kein Zustand, sondern vielmehr ein kontinuierlicher Prozess zwischen Effizienz, Abhängigkeit und strategischer Kontrolle. •

Die lange Suche nach einem Datenschutz-Siegel

Viele Unternehmen suchen erfolglos nach einem Datenschutz-Siegel, das bei Dienstleistern schnelle Sicherheit bietet. Doch Logos ersetzen keine Prozesse. Wer wirklich bewerten will, muss Organisation, Nachweise und Zuständigkeiten prüfen. /// von Melanie Ludolph

IN DER BERATUNGSPRAXIS TAUCHT IMMER WIEDER DIE FRAGE AUF, WORAN MAN EIGENTLICH ERKENNT, OB EIN UNTERNEHMEN DATENSCHUTZ „KANN“. Die Frage ist nachvollziehbar. Wer mit Dienstleistern zusammenarbeitet, möchte Risiken einschätzen können. Schließlich gibt es für viele Bereiche etablierte Nachweise: ISO 27001 für Informationssicherheit, TISAX in der Automobilbranche oder Wirtschaftsprüfertestate für Finanzinformationen. Beim Datenschutz fällt die Antwort dagegen überraschend schwer aus.

Der Wunsch nach einem Nachweis

Wer personenbezogene Daten an einen Dienstleister übermittelt, muss sich zwangsläufig mit dessen Datenschutzorganisation beschäftigen. Die Folge sind häufig umfangreiche Fragebögen, Dokumentenanforderungen und Prüfungen. Dahinter steckt ein nachvollziehbares Interesse auf beiden Seiten. Auftraggeber suchen nach einem objektiven Maßstab, um Risiken bewerten zu können. Dienstleister wiederum möchten ihren Datenschutzstandard möglichst einfach und nachvollziehbar belegen. Ein Zertifikat wäre dafür die ideale Lösung. Ein Blick auf ein Siegel und viele Fragen scheinen beantwortet. Genau dieses Siegel sucht die Praxis jedoch bis heute.

Eigentlich war die Idee schon da

Dabei ist der Gedanke keineswegs neu. Bereits unter dem alten Bundesdatenschutzgesetz gab es Datenschutz-Gütesiegel und Zertifizierungsmodelle. Auch die DSGVO hat Zertifizierungen ausdrücklich aufgegriffen. Die Verordnung sieht sogar eigene Datenschutz-Zertifizierungen vor. Wer damals auf eine Art „ISO für Datenschutz“ gehofft hat, konnte durchaus davon ausgehen, dass sich ein solcher Standard entwickeln würde. Passiert ist etwas anderes.

Der Markt der Fragebögen

Zwar gibt es einzelne Zertifizierungsansätze und branchenspezifische Modelle. Ein allgemein anerkannter Standard hat sich bislang jedoch nicht entwickelt. Das ist bemerkenswert. Denn der Bedarf ist offensichtlich vorhanden. Kaum ein Unternehmen prüft einen Dienstleister ausschließlich auf Basis von Werbeaussagen oder Datenschutzhinweisen. Stattdessen dominieren individuelle Prüfungen.

Wer regelmäßig Auftragsverarbeitungsverträge begleitet, kennt das Phänomen: Unternehmen verschicken umfangreiche Datenschutzfragebögen, fordern technische und organisatorische Maßnahmen an oder lassen ganze Prüfkataloge ausfüllen. Auf der anderen Seite beantworten Dienstleister dieselben Fragen immer wieder neu. Was eigentlich durch einen standardisierten Nachweis vereinfacht werden könnte, wird individuell geprüft.

Mehr als ein Zertifikat

Vielleicht liegt darin auch eine Chance. Denn die Frage, ob ein Unternehmen Datenschutz „kann“, lässt sich möglicherweise ohnehin nicht durch ein einzelnes Siegel beantworten. Datenschutz zeigt sich oft dort, wo niemand hinschaut: in klaren Zuständigkeiten, dokumentierten Prozessen, einem strukturierten Umgang mit Dienstleistern oder der Fähigkeit, neue Themen wie KI kontrolliert einzuführen. Häufig verrät bereits der Umgang mit Rückfragen viel über den Reifegrad eines Unternehmens. Werden Datenschutzfragen transparent beantwortet? Liegen Unterlagen vor? Gibt es feste Ansprechpartner und nachvollziehbare Prozesse?

Wer nach einem Siegel sucht, wird deshalb möglicherweise enttäuscht. Wer auf die Organisation dahinter schaut, erhält häufig die aussagekräftigere Antwort. •



DIE AUTORIN
Melanie Ludolph

ist Rechtsanwältin bei der europäischen Wirtschaftskanzlei Fieldfisher. Seit fast zehn Jahren berät sie Unternehmen und internationale Konzerne aus verschiedenen Branchen zu allen Aspekten des Datenschutzrechts sowie angrenzenden Rechtsgebieten.

Bild: Fieldfisher

**Dell GmbH**

Unterschweinstiege 10
60549 Frankfurt am Main

www.delltechnologies.com

Dell Technologies unterstützt Organisationen und Personen dabei, ihre Zukunft digital zu gestalten und Arbeitsplätze sowie private Lebensbereiche zu transformieren. Das Unternehmen bietet Kunden das branchenweit umfangreichste und innovativste Technologie- und Services-Portfolio für das Datenzeitalter mit dem Ziel, den menschlichen Fortschritt voranzutreiben – darunter Laptops, Desktops, Server, Netzwerke, Speichersysteme, Hybrid-Cloud-Lösungen und vieles mehr.

**Esker Software Entwicklungs- und Vertriebs-GmbH**

Dornacher Straße 3a
85622 Feldkirchen

info@esker.de

www.esker.de

Esker bietet eine globale Cloud-Plattform zur Automatisierung von Dokumentenprozessen und unterstützt Finanz-, Einkaufs- und Kundendienstabteilungen bei der digitalen Transformation in den Bereichen Order-to-Cash (O2C) und Source-to-Pay (S2P). Die Lösungen von Esker werden weltweit eingesetzt und beinhalten Technologien wie künstliche Intelligenz (KI), um die Produktivität und die Transparenz im Unternehmen zu erhöhen. Zugleich wird damit die Zusammenarbeit von Kunden, Lieferanten und Mitarbeitenden gestärkt.

**easy software**

Jakob-Funke-Platz 1

45127 Essen

+49 201 650 69-166

info@easy-software.com

www.easy-software.com

Digitalisierungsexperte und führender ECM Software-Hersteller, easy, steht seit 1990 für rechtssichere, digitale Archivierung & effiziente, automatisierte Prozesse - auch im SAP-Umfeld. Über 5.400 Kunden in über 60 Ländern und allen Branchen vertrauen auf das Unternehmen und sein starkes Partnernetzwerk. Die erstklassigen Archivierungs-, ECM-, DMS-, P2P- und HCM-Softwarelösungen & Services sind das digitale Zentrum für datenbasierte Intelligenz und machen Menschen und Organisationen erfolgreich.

**d.velop AG**

Schildarpstraße 6-8

48712 Gescher

+49 2542 9307-0

info@d-velop.de

www.d-velop.de

Die d.velop-Gruppe entwickelt und vermarktet Standard-Software zur durchgängigen Digitalisierung von dokumentenbezogenen Geschäftsprozessen On-Premises, in der Cloud und im hybriden Betrieb. Das Produktportfolio reicht vom Compliance-fähigen Dokumenten-Repository bzw. Archiv und digitalen Akten über die interne Kollaboration bis zur externen Zusammenarbeit über Organisationsgrenzen hinaus. Produkte von d.velop sind aktuell bei mehr als 15.000 Geschäftskunden und bei über 4,5 Millionen Menschen weltweit im Einsatz.

MARKETPLACE

04

DIGITAL BUSINESS

05 2026

/// Digital Sovereignty

Gewusst wer

Vermeintlich souveräne Lösungen gibt es inzwischen viele am Markt. Doch die Auswahl des passenden Anbieters fällt KMU noch schwer.

/// Supply Chain & Logistics

Sustainable Automation

Künstliche Intelligenz ist nicht nur ein Kostentreiber. Richtig eingesetzt, kann sie auch wesentlich zum Energiesparen beitragen.

/// Experten-Talk

KI vs KI

Mithalten im Hase- und Igel-Rennen:
Durch KI werden Systeme zum einen anfälliger.
Kann KI mit dem richtigen Einsatz KI besser schützen?

/// Agentic AI

Vom Agenten zur Autonomous Workforce

Bei der der Leistungsfähigkeit der Bürosoftware stellt sich Rentabilität erst durch ein Team spezialisierter Agenten ein.

Die nächste Ausgabe erscheint am 20.10.2026

Redaktionell erwähnte Firmen dieser Ausgabe

ams-solution, Asseco Solutions, Bitkom, Box, BVDW, Cancom, Celonis, ConSense, Cosmo Consult, DC-Datacenter-Group, d.velop, Docuware, Eset Deutschland, Fieldfisher, Fraunhofer IESE, Gartner, GData Cyber Defense, GWS, Inform, Kyndryl, ManageEngine, NTT Data Business Solutions, Okta, Ping Identity, Proofpoint, PSI Software, Retarus, samedi, nexspace data centers, OVHCloud, ServiceNow, Sybit, Tata Consultancy Services Deutschland, Tieto Tech Consulting, TÜV Trust IT, Veeva Systems, Wingmaite

IMPRESSUM

DIGITAL BUSINESS Magazin
www.digitalbusiness-magazin.de

HERAUSGEBER UND GESCHÄFTSFÜHRER
Matthias Bauer, Dennis Hirthammer

So erreichen Sie die Redaktion

Chefredaktion:

Heiner Sieger (v. i. S. d. P.), heiner.sieger@win-verlag.de

Tel.: +49 (89) 3866617-14

Redaktion:

Konstantin Pfliegl, konstantin.pfliegl@win-verlag.de

Tel.: +49 (89) 3866617-18

Stefan Girschner, stefan.girschner@win-verlag.de

Tel.: +49 (89) 3866617-16

Mitarbeiter dieser Ausgabe:

Axel Amelung, Prof. Dr. Alexander Alscher, Ralf Bachthaler, Nico Bäumer, Tim Berghof, Michael Bochmann, Ron Boes, Oliver Diekmann, Henning Dittmer, Maik Donner, Werner Engelbrecht, Christian Feldmann, Thomas Firatan, Uwe Geuss, André Görmer, Manuel Haug, Dr. Bernd Heinrichs, Thorsten Jüngling, Lukas Keller, Dr. Stephan Killich, Phillip Korzinetzki, Ulrich Kreitz, Arkadiusz Krowczynski, Melanie Ludolph, Thomas Mierschke, Dr. Kay Müller-Jones, Alexander Opel, Michael Pietsch, Stefan Schäfer, Axel Schmidhäuser, Frank Schnicke, Ralf Siefen, Dr. Christian Tobeck

Stellvertretende Gesamtanzeigenleitung

Bettina Prim, bettina.prim@win-verlag.de, Tel.: +49 (89) 3866617-23

Anzeigendisposition

Auftragsmanagement@win-verlag.de

Chris Kerler (089/3866617-32, Chris.Kerler@win-verlag.de)

Abonentenservice und Vertrieb

Tel.: +49 89 3866617 46

www.digitalbusiness-magazin.de/hilfe

oder eMail an

abovertrieb@win-verlag.de mit Betreff „www.digitalbusiness“

Gerne mit Angabe Ihrer Kundennummer vom Adressetikett

Artdirection/Titelgestaltung: DesignConcept Dagmar Friedrich-Heidbrink

Bildnachweis/Fotos: stock.adobe.com, Werkfotos

Druck:

Vogel Druck und Medienservice GmbH

Leibnizstraße 5

97204 Höchberg

Produktion und Herstellung

Jens Einloft, jens.einloft@vogel.de, Tel.: +49 (89) 3866617-36

Anschrift Anzeigen, Vertrieb und alle Verantwortlichen

WIN-Verlag GmbH & Co. KG

Chiemgaustr. 148, 81549 München

Telefon +49 (89) 3866617-0

Verlags- und Objektleitung

Martina Summer, martina.summer@win-verlag.de,

Tel.: +49 (89) 3866617-31, (anzeigenverantwortlich)

Zentrale Anlaufstelle für Fragen zur Produktsicherheit

Martina Summer (martina.summer@win-verlag.de, Tel.: 089/3866617-31)

Bezugspreise

Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement (6 Ausgaben):

69,00 Euro in D, A, CH und 82,20 Euro in den weiteren EU-Ländern

inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler, Auszubildende

und Wehrdienstleistende gegen Vorlage eines Nachweises auf Anfrage.

Bezugspreise außerhalb der EU auf Anfrage.

30. Jahrgang; Erscheinungsweise: 6-mal jährlich

Einsendungen: Redaktionelle Beiträge werden gerne von der Redaktion entgegen genommen. Die Zustimmung zum Abdruck und zur Vervielfältigung wird vorausgesetzt. Gleichzeitig versichert der Verfasser, dass die Einsendungen frei von Rechten Dritter sind und nicht bereits an anderer Stelle zur Veröffentlichung oder gewerblicher Nutzung angeboten wurden.

Honorare nach Vereinbarung. Mit der Erfüllung der Honorarvereinbarung ist die gesamte, technisch mögliche Verwertung der umfassenden Nutzungsrechte durch den Verlag – auch wiederholt und in Zusammenfassungen – abgegolten. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden.

Copyright © 2026 für alle Beiträge bei der WIN-Verlag GmbH & Co. KG

Kein Teil dieser Zeitschrift darf ohne schriftliche Genehmigung des Verlages vervielfältigt oder verbreitet werden. Unter dieses Verbot fällt insbesondere der Nachdruck, die gewerbliche Vervielfältigung per Kopie, die Aufnahme in elektronische Datenbanken und die Vervielfältigung auf CD-ROM und allen anderen elektronischen Datenträgern.

Ausgabe: 04/2026

ISSN 2510-344X

Unsere Papiere sind PEFC zertifiziert

Wir drucken mit mineralölfreien Druckfarben

Außerdem erscheinen beim Verlag:

AUTOCAD Magazin, BAUEN AKTUELL, r.energy,

DIGITAL ENGINEERING Magazin, DIGITAL MANUFACTURING,

e-commerce Magazin, KGK Rubberpoint, PLASTVERARBEITER, PlastKnow





Hier geht's zur aktuellen Ausgabe



Die nächste Ausgabe **Sonderheft Logistik** erscheint am 16. September 2026

Logistik ist heute das zentrale Thema der Weltwirtschaft. Wir informieren über die neuesten Entwicklungen in der Logistik und bei den Logistik-Immobilien, fragen bei Experten nach und zeigen aktuelle Lösungen anhand von Best Practice Beispielen.



WIN

VERLAG

MEDIEN.

MÄRKTE.

MENSCHEN.

EIN PARTNER.
VIELE KANÄLE.
SICHTBARKEIT
AUF ALLEN EBENEN.

AUTOCAD
MAGAZIN

BAUEN
AKTUELL

DIGITAL BUSINESS

DIGITAL ENGINEERING
MAGAZIN

DIGITAL MANUFACTURING

e-commerce magazin
DER DIGITALE WEG ZUM KUNDEN

KGK RUBBERPOINT
Kautschuk | Gummi | Kunststoffe

r.energy
ERNEUERBARE ENERGIEN UND DIGITALISIERUNG

PLAST VERARBEITER

PLAST
NOW



win-verlag.de