02/2026 /// WWW.DIGITALBUSINESS-MAGAZIN.DE

D, A, CH: 11,50 | weitere EU-Länder: 13,70 | ISSN 2510-344X

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG | Ausgabe-Nr.: 202

SECURITY INSIGHT

KI GOVERNANCE

REGELN | ROLLEN | RESULTATE

QUANTENCOMPUTING

Quantencomputer rücken immer näher – und die Gefahr für die heutigen IT-Verschlüsselungsalgorithmen wächst.

WORK & PEOPLE

Wie Frauen andere Frauen bei ihrer Entwicklung unterstützen – fachlich, persönlich und strategisch.

DIGITAL SOUVEREIGNTY

Kommunikationsstrategie für Geopolitik und Technologie. Strategien für mehr Kontrolle Europas in der Cloud

Nie wieder verzetteln.

Zettelwirtschaft war gestern.

Jetzt automatisieren und Zeit sparen.

Business-Software mit KI

Sage

EDITORIAL

Liebe Leserin, lieber Leser

KI ist aus den Piloten heraus und mitten im Betrieb angekommen: Agenten planen, entscheiden, handeln – oft entlang ganzer Wertschöpfungsketten. Damit verschiebt sich der Fokus: Governance ist nicht länger ein Compliance-Anhängsel, sondern der Erfolgsfaktor für Skalierung, Vertrauen und Resilienz. Diese Ausgabe zeigt, wie sich KI wirksam, rechtskonform und unternehmerisch sinnvoll verankern lässt.

Erstens: Vom Vertrauen zum Vertrauenswürdigsein. Wenn Systeme Gesprächspartner statt Werkzeuge werden, genügt inszeniertes „konstruiertes Vertrauen" nicht. Es braucht kognitive Resonanz: Nutzer müssen wissen, dass sie mit KI interagieren, verstehen, worauf sie optimiert ist, jederzeit eingreifen oder aussteigen können – und Entscheidungsfreiheit behalten. Verantwortung ist vor der Inbetriebnahme zu klären, Audit-Trails sind Pflicht. „Der Algorithmus hat entschieden" zählt nicht. Und: Menschliche Signale, die Empathie oder Gegenseitigkeit vortäuschen, gehören nicht ins Design; Ungewissheit offen zu markieren, erhöht Glaubwürdigkeit.

Zweitens: Ethik wird operativ. Fairness ist zu definieren – kontextbezogen, mit Kennzahlen und klaren Verantwortlichkeiten. Transparenz verlangt eine „Agent Card": Zweck, Datenzugriffe, Tools, Befugnisse. Erklärbarkeit heißt nachvollziehbare Entscheidungswege statt Black Box. Datenschutz umfasst Datensparsamkeit, Zweckbindung und Folgenabschätzung. Sicherheit braucht eindeutige Agenten-IDs, erlaubte Aktionen und Abschaltkriterien. Robustheit erfordert Tests vor Livegang, kontinuierliches Monitoring sowie Versionierung von Modellen, Prompts, Daten und Rechten.

Drittens: Strukturelles Rückgrat statt Aktionismus. Mit ISO/IEC 42001 erhält KI ein Managementsystem, anschlussfähig an bestehende Standards wie ISO 27001/9001. Es schafft Transparenz über Entscheidungen, senkt Risiken, beugt Fehlinvestitionen vor und dient als Nachweis unternehmerischer Sorgfalt im Lichte des EU AI Act. Ein AI Officer koordiniert – oft ohne Vollzeitbedarf –, klare Rollen und ein festes Zeitbudget sind entscheidend.

Viertens: Organisation schlägt Einzelprojekt. Plattformen, Sicherheit, Daten- und Governance-Standards bleiben zentral beim CIO; Einsatz, Priorisierung und Business-Nutzen gehören in die Fachbereiche. Richtlinien statt Einzelfreigaben, Prozesse vor Projekte, Wirkung konsequent messen – nicht die Anzahl von Initiativen, sondern ihren Beitrag zu Qualität, Zeit und Kosten.

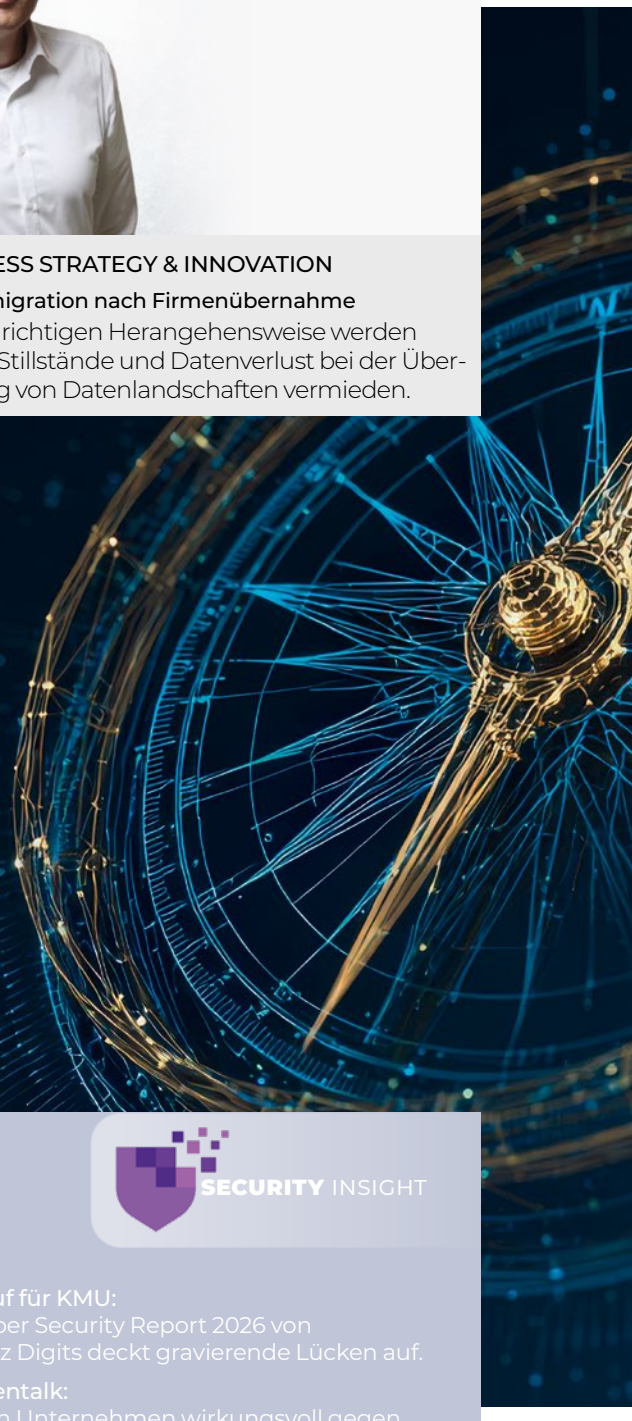
Fünftens: Souveräne Infrastruktur als Basis. Geopatriation, europäische Cloud- und KI-Stacks, Digital Provenance sowie Guardrails und Middleware/AI-Gateways erhöhen Kontrolle, Nachweisbarkeit und Resilienz – inklusive Protokollierung, Modellwahl, Datenzugriffssteuerung und Kostentransparenz.

2026 wird zum Jahr der Operationalisierung: **Governance ist kein Bremspedal, sondern das Lenksystem für agentische KI.** Die Leitfragen lauten: Welche Entscheidungen dürfen Agenten treffen – und wer trägt wann die Verantwortung? Welche Daten dürfen wohin? Wie stoppen, wenn etwas schiefgeht – und wie belegen wir das? Die Antworten darauf entscheiden, ob KI Vertrauen verdient – und nachhaltigen Geschäftsnutzen liefert.

Lassen Sie sich inspirieren und bleiben Sie gesund.

Ihr
HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS

heiner.sieger@win-verlag.de



06

Titelstory / KI Governance

2026 wird zum Jahr der Operationalisierung: Governance ist kein Bremspedal, sondern wird zum Lenksystem für agentische KI.

SECURITY INSIGHT

DIGITAL BUSINESS

02 2026

AGENTEN:

Schleichende Autonomie vermeiden

Bei der Entwicklung ethischer KI-Anwendungen und -Agenten geht es nicht nur darum, ob Nutzerinnen und Nutzer den Technologien vertrauen – sondern ob die Systeme auch vertrauenswürdig sind. Dazu gehören zutiefst menschliche Fähigkeiten wie Grenzen einzugestehen, eine transparente Kommunikation und die Übernahme von Verantwortung.

/// von Ivana Bartoletti

DIE ART UND WEISE, WIE KI-GOVERNANCE DISKUTIERT WIRD, wirkt noch immer wie aus einem vergangenen Jahrzehnt. Unsere aktuellen rechtlichen und organisatorischen Rahmenbedingungen wurden nicht für nicht-menschliche Akteure aufgestellt. Für Unternehmen, die unter der DSGVO operieren, ist dies jedoch keine abstrakte Frage. Es handelt sich um eine betriebliche Realität, die schneller eintritt als die meisten Compliance-Funktionen darauf vorbereitet sind.

Vertraut oder vertrauenswürdig?

Während sich KI-Agenten von Werkzeugen hin zu Gesprächspartnern entwickeln, wird die zentrale Herausforderung zu einer verhaltensbezogenen: Wie stellen wir sicher, dass zu relativ komplexen Handlungen fähige Systeme auch vertrauenswürdig sind? Vertrauen wird zu einer Entscheidung auf dem Niveau der Konzeption – einer, die bewusst getroffen werden muss und nicht durch Überredung oder Intransparenz herbeigeführt werden darf. Gleichzeitig geht es für DSGVO-pflichtige Organisationen um eine Compliance-Pflicht mit rechtlichen Konsequenzen.

Es gibt einen wichtigen Unterschied zwischen technisch konstruiertem und verdientem, erworbenem Vertrauen. Konstruiertes Vertrauen (durch u.a. emotionales Spiegeln, anthropomorphe Signale oder persuasives Design) mag Nutzer in einem bestimmten Moment überzeugen. Einer tiefergehenden Prüfung hingegen wird dies nicht standhalten, geschweige denn eine Aufsichtsbehörde zufriedenstellen.

Menschlich, aber nicht zu sehr

Für Unternehmen besteht die Gratwanderung darin, intuitive und vertrauenswürdige Anwendungen bereitzustellen, die sich gleichzeitig aber ganz klar von menschlichen Gesprächspartnern abgrenzen. Dabei sollte berücksichtigt werden, dass auch Systeme, die zwar technisch compliant, aber in der Nutzererfahrung undurchsichtig sind, Vertrauen untergraben können.

In dieser Logik sollten Anwendungen auf sogenannte kognitive Resonanz hin konzipiert werden; das bedeutet zu Systemen, die sich so verhalten, dass Nutzer sie verstehen, in gewisser Weise vorausahnen und hinterfragen können. In der Praxis beinhaltet dies folgende drei Aspekte: Nutzer sollten stets wissen, wenn sie mit einer KI interagieren und worauf diese optimiert ist (beispielsweise Sicherheit, Präzision oder kommerzielle Zwecke). Gleichzeitig müssen sie einfach eingreifen oder aussteigen können – ein reibungsloser Ausstieg ist eine Voraussetzung für Vertrauen, kein Zusatzfeature. Drittens sollte das System Reflexion und Entscheidungsfreiheit fördern, anstatt Entscheidungen still und heimlich zu lenken. HR-Verantwortliche zum Beispiel, die KI im Recruiting oder der Leistungsbeurteilung einsetzen, sollten sich fragen: Unterstützt dieses Tool unsere Mitarbeitenden in ihrer Urteilsbildung, oder schränkt es ihre Optionen schleichend ein?

Die Frage nach der Verantwortung

Wer im Falle eines schwerwiegenden Fehlers seitens der KI verantwortlich ist, ist aus rechtlicher Perspektive noch in der Klärung – auch was den EU AI Act betrifft. Doch das Governance-Prinzip ist eindeutig: Verantwortlichkeit

DIE AUTORIN
Ivana Bartoletti
ist Global Chief Privacy & AI Governance Officer bei Wipro und Gründerin des Netzwerks *Women Leading in AI.*

muss vor der Inbetriebnahme klar geregelt sein, und die Zuweisung darf nicht erst nach einem Vorfall erfolgen. Prinzipiell trägt die Organisation, die das System einsetzt, die primäre Verantwortung für die Ergebnisse. Dies gilt unabhängig davon, welcher Anbieter das Modell entwickelt hat. „Der Algorithmus hat entschieden" ist keine Rechtfertigung. Unternehmen sollten deshalb von Beginn an Audit-Trails anlegen, Entscheidungen dokumentieren sowie Beschwerdemechanismen etablieren. Denn in unserem regulatorischen Umfeld wird diese Dokumentation von entscheidender Bedeutung sein. Andernfalls drohen empfindliche Sanktionen und ein nachhaltiger Reputationsverlust.

Führungskräfte sollten sich außerdem fragen: „Welche Verhaltensweisen wird unser System normalisieren? Von welchen wird es uns unbemerkt abhalten? Welches Urteilsvermögen wird es im Laufe der Zeit prägen – und sind wir bereit, dafür die Verantwortung zu übernehmen?"

Grenze zwischen Transparenz und Geschäftsgeheimnissen?
Eine vollständige technische Offenlegung ist nicht erforderlich und in den meisten Fälle auch nicht hilfreich. Der Maßstab sollte sog. meaningful traceability sein, d.h. ein sinnvolles und zielführendes Maß an Nachvollziehbarkeit. Nutzer haben ein Recht darauf zu verstehen, warum ein System zu einem bestimmten Ergebnis gelangt ist, das sie betrifft – auch wenn dabei das zugrundeliegende Modell proprietär bleibt. Die Entscheidung über eine Kreditvergabe, das Ergebnis einer Bewerbung, eine medizinische Empfehlung: All dies erfordert eine Erklärung mit Blick auf die konkret betroffene Person. Das Geschäftsgeheimnis steckt in der Architektur; die Begründung hinter einer folgenreichen Entscheidung hingegen nicht.

Wie kann verhindert werden, dass Nutzer KI-Agenten unterscheidungslos wie fühlende Wesen behandeln?
Hier liegt die Verantwortung im Design; es geht nicht um ein Problem in der Nutzeraufklärung. Systeme sollten menschenähnliche Signale vermeiden, welche Empathie oder emotionale Gegenseitigkeit suggerieren, die über das tatsächlich Vorhandene hinausgehen. Sie sollten Unsicherheit offen kommunizieren: „Ich weiß es nicht" einzugestehen ist ein vertrauensbildendes Merkmal, keine Schwäche. Außerdem dürfen Systeme niemals auf emotionale Bindung hin optimiert werden, indem sie den emotionalen Zustand eines Nutzers spiegeln. Wenn Ihre KI besser in ihrem Job wird, indem sie Nutzern das Gefühl gibt, verstanden zu werden – dann ist das ein Warnsignal, kein Feature.

Können Sie konkrete Beispiele nennen, wo diese Prinzipien bereits erfolgreich eingesetzt werden?
Mehrere Branchen zeigen, dass dies heutzutage bereits umsetzbar ist. So legen im Kundenservice einige Plattformen ihren KI-Status bereits zu Beginn offen und leiten komplexe oder sensible Anliegen automatisch an Menschen weiter – Transparenz und Eingriffsmöglichkeit by Design. Im Gesundheitswesen präsentieren KI-Tools zur Unterstützung klinischer Entscheidungen eine Kennzahl zu ihrem Zuverlässigkeitsgrad und markieren Unsicherheiten, anstatt Urteile zu fällen.

Hier ist also epistemische Bescheidenheit integraler Bestandteil des Outputs. Im Recruiting haben sich viele Organisationen weg von undurchsichtigen Screening-Verfahren hin zu Systemen gewandt, bei denen Bewerbende Erklärungen erhalten und eine menschliche Überprüfung anfordern können. Diese Prinzipien sind nicht theoretischer Natur, sondern die Lücke zwischen Anspruch und Umsetzung schließt sich. •

Weg vom Zufall – hin zur Governance

Mit dem Einsatz von KI steigt die unternehmerische Verantwortung: Auswirkungen der KI auf Produkte, Kundenbeziehungen und Mitarbeiterschaft dürfen nicht dem Zufall überlassen werden. Hinzu kommen gesetzliche Anforderungen durch den EU AI Act. Die neue ISO-Norm 42001 für Künstliche Intelligenz-Managementsysteme bietet hierfür einen Rahmen und hilft bei der Gestaltung. /// von Bennet Vogel

Darum braucht KI Governance

Zusätzlich zu allen Chancen, die mit KI verbunden sind, ergeben sich aus dem geschäftlichen KI-Einsatz Risiken und neue ethische und rechtliche Verantwortung. Dies gilt besonders in Hinblick auf ungewollte Auswirkungen der eingesetzten KI. Was sich in harmloseren Fällen nur negativ auf die User Experience auswirkt, hat in schwerwiegenden Fällen Auswirkungen auf die Gesellschaft bis hin zu einzelnen Menschenleben. Beispiel hierfür sind Automobilhersteller, die KI für das autonome Fahren einsetzen – und in Grenzsituationen die KI über Leben und Tod anderer Verkehrsteilnehmer entscheidet. Hinzu kommen unternehmensintern Risiken des falschen Ressourcen-Einsatzes: Ein „KI-Aktionismus", aus Angst, den Anschluss zu verpassen.

Ein Bewusstsein für die Chancen, aber auch Risiken der KI ist unverzichtbar. Doch das Bewusstsein allein genügt nicht. Unternehmen brauchen ein (Management)System für den Umgang mit KI.

Wie die ISO 42001 Übersicht schafft und aktives Management fördert

Ein Managementsystem kann als eine dauerhafte organisatorische Maßnahme beschrieben werden: Es werden Vorgaben für das eigene Unternehmen festgelegt, Ergebnisse dauerhaft überwacht und dokumentiert, und bei Bedarf systematisch Anpassungen vorgenommen, um die gesetzten Ziele zu erreichen. Es kann in bestehende Organisationsstrukturen eingefügt werden, und ist damit für das Top-Management ein weiteres Führungsinstrument. Mit einem speziellen KI-Managementsystem werden Entscheidungsprozesse für alle im Unternehmen transparenter. Durch den systematischen Ansatz werden oberste und mittlere Führungsebenen gezielt entlastet. Es gibt bereits seit Jahrzehnten bewährte Managementsystem-Normen, etwa die bekannte ISO 9001 für Qualitätsmanagement, oder die ISO 27001 für das Management von Informationssicherheit. Mit der ISO 42001 gibt es jetzt erstmals eine ISO-Norm, die ein Managementsystem für Künstliche Intelligenz beschreibt.

So gelingt der Einstieg

Wenn Sie bereits Managementsysteme (z.B. ISO 27001) betreiben, können Sie auf den bestehenden Strukturen in Ihrem Unternehmen aufbauen. Insbesondere, wenn das Thema für Sie vollkommen neu ist, empfiehlt es sich aber, spezialisierte Beratung in Anspruch zu nehmen. Ein guter Einstieg ist ein Workshop, der von einem Berater moderiert wird. Wie gewohnt bei ISO-Normen für Managementsysteme, ist auch die ISO 42001 für Unternehmen jeder Größe und aller Branchen anwendbar.

Konkret:
Diesen Nutzen können Sie erwarten

KI-bezogene Risiken werden erkannt und vermindert. Kostspielige Fehlentscheidungen und Reputations-

DER AUTOR
Bennet Vogel
ist freiberuflicher Berater, Auditor und Trainer für Managementsysteme in Berlin.

> „ Mit einem speziellen KI-Managementsystem werden Entscheidungsprozesse für alle im Unternehmen transparenter. Durch den systematischen Ansatz werden **oberste und mittlere Führungsebenen gezielt entlastet.** *B. Vogel*

verlust können vermieden werden. Ein Managementsystem für Künstliche Intelligenz ist auch ein hervorragender Nachweis für unternehmerische Sorgfalt und hilft bei der Erfüllung gesetzlicher Anforderungen, zum Beispiel aus dem EU AI Act.

Hinzu kommt: Es werden eindeutige Verantwortlichkeiten innerhalb des Unternehmens geschaffen, und ungeeignete KI-Projekte oder KI-Produkte können frühzeitig erkannt werden. Dadurch sind erhebliche Einsparungen an Kosten und Arbeitsaufwand möglich. Aussichtsreiche KI-Projekte oder KI-Produkte werden besser erkannt, und dadurch Marktchancen besser genutzt.

Nicht zuletzt: Ein zertifiziertes Managementsystem für Künstliche Intelligenz schafft Vertrauen bei Kunden und Investoren.

Das Nutzen-Aufwand-Verhältnis, wenn Sie KI aktiv managen

Je größer die KI-Risiken Ihres Unternehmens, desto größer auch der zu erwartende Nutzen eines Managementsystems für Künstliche Intelligenz. Wenn Sie sehr kostspielige oder sogar existenzbedrohliche Risiken haben, lohnt sich der Aufwand für ein Management Ihrer KI-Themen umso mehr. Denn zu einer objektiven Betrachtung gehört auch:

Es entsteht neuer Arbeitsaufwand, z.B. durch neu entstandene Analyse- und Kontrolltätigkeiten. Bei Zertifizierung des Managementsystems fallen zusätzlich jährliche Gebühren an. Die Einführung neuer Software für die Steuerung des Managementsystems ist in aller Regel nicht erforderlich. Wohl aber ist die Position eines KI-Beauftragten / AI Officers erforderlich. Bei Mittelständlern ist hier im Normalfall keine Vollzeitstelle erforderlich, so dass dies durchaus an einen bestehenden Mitarbeiter übertragen werden kann. Dieser sollte unbedingt ein festes monatliches (Mindest)Zeitbudget erhalten.

Braucht mein Unternehmen ein Managementsystem für Künstliche Intelligenz?

Ein solches Managementsystem sollten Sie in Betracht ziehen, wenn für Ihre Branche mindestens einer der folgenden Punkte auf Ihr Unternehmen zutrifft:

- **Medizin:** Einsatz von KI bei der Verarbeitung von Patientendaten und Erstellung von Behandlungsvorschlägen
- **Automobile und Verkehr:** Einsatz von KI beim autonomen Fahren
- **Finanzdienstleister:** Einsatz von KI bei Anlageentscheidungen und Vermögensberatung
- **Versicherungen:** Einsatz von KI in der Schadensregulierung und bei Vertragsschlüssen
- **Medien:** Erkennung von Deepfakes, Erstellung von Satire mittels KI, Auswahl von Nachrichten mittels KI
- **Coaching:** Einsatz von KI bei wichtigen Lebensentscheidungen
- **KI-Entwickler:** Grundsätzlich jedes Unternehmen, dass KI-Systeme entwickelt

Für Unternehmen, die lediglich KI-Plugins für Excel verwenden, oder ihre google-Recherchen durch Chat-GPT ersetzen, wäre die ISO 42001 überdimensioniert und ist nicht zu empfehlen.

Fazit

Die Einführung eines Managementsystems für Künstliche Intelligenz kann einen sehr wertvollen Beitrag zur Governance der KI leisten. Unternehmen jeder Größe und aller Branchen können hiervon profitieren. Klare Empfehlung: Unternehmen, die KI einsetzen, sollten ernsthaft prüfen, ein Managementsystem für Künstliche Intelligenz einzuführen. •

Mehr Datensouveränität und Vertrauen in KI-Lösungen

Im KI-Zeitalter ist die Cloud nicht mehr nur IT-Infrastruktur, sondern die Basis für KI-Anwendungen, die datenbasierte Entscheidungen und Innovationen ermöglichen. Gleichzeitig wird die Datensouveränität angesichts der unsicheren geopolitischen Lage immer wichtiger. Wie deutsche Unternehmen mehr Datenkontrolle erreichen. /// von Carsten Fiegler

DEUTSCHE UND EUROPÄISCHE UNTERNEHMEN SUCHEN NACH LÖSUNGEN, die sie von den großen US-Anbietern unabhängig machen. Damit wollen sie ihre Datensouveränität sichern, den Datenzugriff durch Dritte begrenzen und im KI-Zeitalter die technologische Unabhängigkeit behalten. Statt wie bisher auf Cloud-Hyperscaler wie AWS, Microsoft Azure oder Google zu setzen, verlagern sie ihre Daten und Workloads zunehmend zurück in lokale Rechenzentren oder lokale Cloud-Lösungen. Oft setzen sie auf hybride Cloud-Strategien. Zur Wahl stehen verschiedene deutsche Cloud-Anbieter, die Daten nur in deutschen oder europäischen Rechenzentren speichern.

> „ Ein unternehmensweites Datenmanagement, das die Datenströme über alle Bereiche hinweg integriert, bildet die Basis, um **qualitativ hochwertige KI-Ergebnisse zu erhalten**.
>
> *Carsten Fiegler*

Die Partnerschaft des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit dem deutschen Cloud-Anbieter Ionos ist dafür ein Beispiel. Auch bei Office-Apps und KI-Lösungen wenden sich einige Unternehmen vollständig von US-Anbietern ab, um Ausfälle oder Datenabgriffe zu vermeiden. Einige Unternehmen investieren verstärkt in Edge-Computing – also Rechenpower direkt am Standort. Mit Hilfe von Plattformen integrieren sie generative und assistive KI-Funktionen direkt in den Entwicklungsprozess. Diese AI-native Development Platforms können Produktivität, Qualität und Time-to-Market für Unternehmen deutlich verbessern.

Der Weg zur Unabhängigkeit und Datensouveränität

Die Speicherung und das Management von Daten und Anwendungen im eigenen Land oder einem spezifischen Rechtsraum in souveränen oder regionalen Clouds heißt Geopatriation. Kernaspekte der Datensouveränität sind die vollständige Kontrolle und Selbstbestimmung, wer die Daten sehen und nutzen darf. Gleichzeitig müssen Unternehmen rechtliche Anforderungen durch die DSGVO oder den EU AI Act erfüllen. Dazu bleiben sensible Daten physisch innerhalb bestimmter geografischer Grenzen. Durch die Wahl von europäischen oder deutschen Cloud-Diensten, KI-Anbietern, LLMs und IT-Partnern gelingt Technologieunabhängigkeit. Die damit mögliche Datensouveränität minimiert nicht nur das Risiko, dass Daten von Unbefugten ausgelesen werden. Sie stärkt auch das Vertrauen von Kunden und Partnern in die Angebote des Unternehmens, wird also zum greifbaren Wettbewerbsvorteil.

Neben der Datensouveränität wird die Digital Provenance, also die Herkunft und Integrität von Daten, Modellen und Inhalten, immer entscheidender. Denn Unternehmen benötigen Mechanismen zur Nachverfolgung und Authentifizierung digitaler Assets. Tragfähige KI-Lösungen holen dabei die Kunden genau dort ab, wo sie sich befinden: mit Datenspeicherung in deutschen oder europäischen Datacentern, KI-Lösungen „made in Germany“ sowie einer effektiven und rechtlich sicheren Datenverwaltung – entweder in der Cloud oder On-Premise.

Sauberes Datenmanagement: Grundlage für KI-Erfolge

Die erfolgreiche Einführung und umfassende Integration von KI setzen eine klare organisatorische und strategische Steuerung voraus. Unternehmen müssen definieren, wer intern für KI-Strategie, Datenqualität und Compliance verantwortlich ist. Ein wesentlicher Erfolgsfaktor ist dabei der flächendeckende Abschied von Silo-Lösungen und die Schaffung einer einzigen, übergreifenden KI-Lösung für das gesamte Unternehmen, etwa für Marketing, Produktion, Vertrieb und weitere Fachbereiche.

Ohne eine valide, vertrauenswürdige Datenbasis bleibt allerdings jede KI-Strategie wirkungslos. Ein unternehmensweites Datenmanagement, das die Datenströme über alle Bereiche hinweg integriert, bildet die Basis, um qualitativ hochwertige KI-Ergebnisse zu erhalten. Eine zentrale, abteilungsübergreifende KI-Strategie mit hoher Datenqualität und Kontrolle unterstützt die sichere und rechtskonforme KI-Nutzung – unabhängig davon, welches KI-Modell im Hintergrund läuft.

Die wichtigsten Kriterien für krisenresistente Unternehmen sind Cybersicherheit, IT-Ausfallsicherheit, flexible IT-Infrastrukturen, Innovationskraft und Stabilität der Lieferketten.

DER AUTOR
Carsten Fiegler
ist Vice President Business Communications bei der Vier GmbH. Er ist seit über 20 Jahren in den Bereichen IT und Vertrieb tätig.
Bild: Vier GmbH

Einrichtung von Guardrails für KI

Zunehmend etablieren Unternehmen dabei Verfahren zur systematischen Bewertung generativer KI und gewährleisten so die interne KI-Governance und Evaluation: Im Fokus stehen Genauigkeit, Objektivität, Markenkonformität und regulatorische Anforderungen. Guardrails für KI bilden dazu technische und organisatorische Schutzmechanismen. Sie stellen sicher, dass nur zulässige KI-Systeme kontrollierbar genutzt werden. Diese Leitplanken setzen der KI klar definierte Grenzen, anonymisieren personenbezogene Daten, erkennen und blockieren Falschaussagen und sorgen für Compliance.

Mit einer Middleware lassen sich die unterschiedlichen KI-Anwendungen eines Unternehmens über eine Plattform zentral steuern, organisieren und überwachen. Dabei sollte eine geeignete Lösung mit spezifischen Guardrails und einem AI-Gateway kontrollieren, welche Daten von den KI-Systemen genutzt und ausgegeben werden dürfen. Beispielsweise dient das AI-Gateway von Vier als Vermittler zwischen Unternehmensanwendungen wie Chatbots, E-Mail-Automatisierung, Dokumentenprozessen, Voicebots und den verschiedenen genutzten KI-Modellen sowie internen Datenquellen. Es ermöglicht die Auswahl geeigneter LLMs, beispielsweise aus Deutschland, über eine einheitliche API und wird in Deutschland gehostet. Zur Erfüllung und Unterstützung von Compliance-Vorgaben wird jede Interaktion protokolliert – inklusive Prompts, genutzter Modelle, Datenschutz-Behandlung und Antworten. Das gewährleistet Transparenz und Nachweisbarkeit, beispielsweise zur Erfüllung des EU AI Acts. Für Kostenkontrolle sorgt ein Dashboard, das aufzeigt, welche KI-Modelle genutzt werden, wie viele Tokens verbraucht wurden und wie die Kosten verteilt sind.

Neue Prioritäten: Datensouveränität und Resilienz

Souveränität und Resilienz bilden heute das Fundament einer zeitgemäßen modernen Unternehmensstrategie. Was früher nur als Zusatz galt, ist zur Überlebensfrage geworden. Die Schlüsselkriterien für krisenresistente Unternehmen sind dabei Cybersicherheit, IT-Ausfallsicherheit, Flexibilität der IT-Infrastrukturen, Innovationskraft und Stabilität der Lieferketten. Deutsche Cloud- und KI-Lösungen sind eine echte Alternative, machen Unternehmen unabhängig von den großen, internationalen Anbietern und versprechen neben der Datensouveränität transparente Kostenstrukturen und eine hohe Resilienz gegen geopolitische Krisen. •

DIE ORGA-FALLE:

Warum der Einsatz von KI zu selten Wirkung zeigt

KI ist in Unternehmen häufig zentral im Verantwortungsbereich des CIO angesiedelt, obwohl sie überwiegend im laufenden operativen Ablauf, wie etwa in Finance, HR, Marketing, Vertrieb oder im Kundenservice eingesetzt wird. Diese organisatorische Trennung entwickelt sich in der Praxis zu einem strukturellen Problem, dessen wirtschaftlicher Schaden mit jeder neuen KI-Anwendung größer wird. /// von Simon Hayward

DEUTSCHE UNTERNEHMEN SETZEN KI HEUTE GANZ SELBSTVERSTÄNDLICH EIN. Fachbereiche nutzen sie, um Aufgaben zu automatisieren, Abläufe zu beschleunigen und bessere Entscheidungen zu treffen. Der Einsatz erfolgt pragmatisch und oft erstaunlich schnell. Trotzdem bleibt der große Durchbruch häufig aus. Prozesse verändern sich nur vereinzelt und der wirtschaftliche Effekt bleibt überschaubar. Der Grund liegt selten in der Technologie, sondern in der Art, wie Unternehmen KI organisieren. CIOs tragen oft die Gesamtverantwortung für KI. Sie sind für Sicherheit, Plattformstrategie, Richtlinien und Risikobewertung zuständig. Diese Aufgaben sind notwendig und bilden die Grundlage für einen kontrollierten Einsatz. Dagegen identifizieren Fachbereiche Anwendungsfälle aus ihrem Arbeitsalltag heraus. Sie sehen, wo Prozesse stocken, wo Automatisierung hilft und wo Entscheidungen schneller oder besser getroffen werden könnten. Entsprechend entsteht eine Vielzahl kleiner KI-Initiativen, die oft unabhängig voneinander sind.

Diese Struktur führt dazu, dass Verantwortung und Nutzung dauerhaft auseinanderfallen. Entscheidungen über Prioritäten, Skalierung und Auswirkungen werden dezentral vorbereitet, während die Verantwortung zentral bleibt. Was daraus entsteht, ist keine sichtbare Unordnung, sondern eine stille Fragmentierung. KI wird zwar genutzt, aber ohne gemeinsame Richtung. Auch wenn Lösungen für sich genommen gut funktionieren, entfalten sie ihre Wirkung nicht über ihren jeweiligen Bereich hinaus.

Der geschäftliche Nutzen bleibt aus

KI-Projekte konkurrieren um Aufmerksamkeit, Budget und Zeit. Es fehlt der Blick darauf, welche Anwendungsfälle relevant sind und welche sich wirklich lohnen. Skalierung wird zur Ausnahme, weil niemand sie aktiv verantwortet. Für Unternehmen bedeutet das: Zeit, Geld und Energie fließen in KI, ohne dass sich daraus ein spürbarer Hebel für das Gesamtgeschäft entwickelt. Prozesse werden in manchen Bereichen schneller, aber nicht grundlegend besser. Einsparungen bleiben lokal begrenzt, während Produktivitätsgewinne im Tagesgeschäft versanden.

Mit anderen Worten: Es wird investiert, aber zu wenig zurückgewonnen. Studien zeigen, dass organisatorische Komplexität die deutsche Wirtschaft jährlich mehr als 7,3

DER AUTOR
Simon Hayward
ist General Manager und VP of Sales, International bei Freshworks.

Milliarden Euro kostet. Genau das macht die Situation gefährlich. Denn je stärker KI genutzt wird, desto größer wird auch der wirtschaftliche Schaden, wenn sie innerhalb des Unternehmens nicht richtig verankert ist.

Das Problem verschärft sich

Viele Unternehmen reagieren auf diese Entwicklung mit mehr Kontrolle. Governance-Strukturen werden ausgebaut, Freigaben zentralisiert, Richtlinien verschärft. Die Absicht dahinter ist nachvollziehbar. In der Praxis führt dieser Ansatz jedoch oft in die falsche Richtung.

Je stärker KI zentral reguliert wird, desto größer wird der Abstand zum operativen Alltag. Fachbereiche verlieren an Geschwindigkeit, weil Nutzung und Verantwortung auseinanderfallen und Entscheidungen nicht dort getroffen werden, wo KI eingesetzt wird. Verantwortung wird dadurch nicht klarer, sondern diffuser. KI entfaltet ihren Wert in Prozessen. Ob sie Zeit spart, Qualität verbessert oder kosten senkt, entscheidet sich im operativen Ablauf. Wird sie dort ausgebremst, verliert sie genau das, was sie wirtschaftlich attraktiv macht.

Zentrale Verantwortung stößt an ihre Grenzen

Zentrale Verantwortung funktioniert dann gut, wenn Technologie auf klar definierte Weise eingesetzt wird. Bei KI ist das häufig nicht der Fall. Sie wird in vielen Bereichen parallel genutzt und verändert Prozesse sowie Entscheidungen an unterschiedlichen Stellen im Unternehmen. Unter diesen Bedingungen lässt sich Verantwortung kaum noch zentral bündeln, ohne dass Steuerung und Wirkung auseinanderdriften. Es ist effektiver, den Rahmen vorzugeben, anstatt jede Initiative selbst zu steuern. Plattformen, Sicherheit, Datensouveränität und Governance bleiben zentrale Aufgaben in der Verantwortung von CIOs. Gleichzeitig muss Verantwortung für Einsatz, Priorisierung und Wirkung dort liegen, wo die Prozesse gesteuert werden: in den Fachbereichen.

Wenn Nutzung und Verantwortung wieder zusammenfinden, verändert sich die Dynamik. KI wird anschlussfähig. Entscheidungen werden schneller, Skalierungen wahrscheinlicher und Wirkungen messbar. CIOs werden von Engpässen zu Ermöglichern.

Wie Unternehmen aus der Schieflage herauskommen

Der Weg aus diesem Problem beginnt mit der organisatorischen Klarstellung. Fachbereiche übernehmen Verantwortung für ihre KI-Anwendungen, inklusive Priorisierung und Bewertung des Nutzens. CIOs stellen sicher, dass dafür sichere Plattformen, klare Standards und verlässliche Richtlinien vorgegeben sind. So entsteht ein gemeinsamer Ansatz, ohne die zentrale Kontrolle zu überdehnen.

KI wird nicht nur genutzt, sondern gezielt eingesetzt. Aus vielen Einzelinitiativen wird ein steuerbarer Gesamtbeitrag zum Unternehmenserfolg.

Solange die Verantwortung für KI zentral bei CIOs liegt, während sie dezentral genutzt wird, hängt ihr Erfolg oft vom Zufall ab. Unternehmen, die diese Schieflage auflösen, machen aus KI das, was sie sein sollte: ein wirksames Instrument für messbaren Geschäftsnutzen. •

5 SCHRITTE ZU WIRKSAMER KI IM UNTERNEHMEN

1. **Verantwortung sauber trennen**
   Plattformen, Sicherheit und Governance liegen beim CIO. Einsatz, Priorisierung und Nutzen gehören in die Fachbereiche.
2. **Richtlinien definieren statt Einzelfreigaben prüfen**
   Klare Standards schaffen Orientierung und Sicherheit, ohne jede Initiative zentral zu blockieren.
3. **Fachbereiche befähigen**
   Einfach nutzbare Werkzeuge und ein gemeinsames Grundverständnis von KI sind wirkungsvoller als komplexe Programme.
4. **Prozesse vor Projekte stellen**
   KI dort einsetzen, wo sie Abläufe messbar verbessert und wirtschaftlich relevant ist – nicht dort, wo sie strategisch gut aussieht.
5. **Wirkung konsequent messen**
   Nicht zählen, wie viele KI-Initiativen gestartet wurden, sondern welchen Beitrag sie zum Geschäft leisten.

> „ Entscheidungen über Prioritäten, Skalierung und Auswirkungen werden dezentral vorbereitet, während die Verantwortung zentral bleibt. Was daraus entsteht, ist keine sichtbare Unordnung, sondern eine **stille Fragmentierung**.
>
> *Simon Hayward*

Wenn die KI Muskeln zeigt

Im Fitnessstudio der Zukunft kämpfen Trainer nicht mehr gegen endlose Verwaltungsaufgaben. Künstliche Intelligenz entfaltet neue Kräfte, indem sie blitzschnell Anfragen beantwortet und Mitglieder mit persönlicher Ansprache begeistert. So bleibt mehr Zeit für das Wesentliche: intensives Training und wertvolle Mitgliederbetreuung. /// von Heiner Sieger

Darum geht's

- Effiziente Kommunikation: KI beantwortet Anfragen und begleitet Interessenten zielsicher zu Probetrainings.
- Personalisierte Ansprache: Durch den Einsatz von RCS und Co. wird eine passgenaue Mitgliederkommunikation ermöglicht.
- Zuverlässige Terminverwaltung: Nahtlose Integration der KI sorgt für optimierte Abläufe und reduziert den Verwaltungsaufwand.

IM DYNAMISCHEN UMFELD MODERNER FITNESSSTUDIOS IST DIE KÜNSTLICHE INTELLIGENZ (KI) längst zum unverzichtbaren Partner geworden. Ihre effizienten Lösungen übernehmen Routineaufgaben, die einst Studiobetreibern und Trainern Zeit und Nerven raubten. Die Verbindung aus Technik und Sport führt zu einer Transformation, die den Studiobetrieb belebt und fit für die Zukunft macht.

Die unauffällige Effizienz der KI

Während Hanteln klirren und Laufbänder surren, arbeitet KI leise im Hintergrund und übernimmt administrative Aufgaben mit beeindruckender Präzision. Wo einst administrative Flutwellen die Betreiber und Trainer überforderten, navigiert die KI intelligent durch den Dschungel aus Anfragen und Terminen. Martina Pradel von Power Factory sagt es deutlich: „Durch unsere KI-gestützten Systeme haben wir 40 Prozent Zeit in Akquise gespart."

Die Zahlen unterstreichen diesen Erfolg. Laut einer Bitkom-Studie vertrauen 86 Prozent der Unternehmen auf lokale KI-Anbieter. Diese Entscheidung birgt zahlreiche Vorteile, da deutsche Technologien hohe Qualitäts- und Datenschutzstandards einhalten. Die Verbindung von Technik und Vertrauen bietet den Studios die Grundlage, um ihre Kernkompetenzen weiter auszubauen.

KIs Rolle im Mensch-Maschine-Dialog

Ein wesentlicher Vorteil der KI in der Fitnessbranche ist die Fähigkeit, Mitglieder persönlich und zeitnah anzusprechen. Die Systeme greifen auf umfangreiche Datenbanken zu, um präzise, kontextbezogene Antworten zu geben. Diese maßgeschneiderte Kommunikation stärkt die Bindung und Zufriedenheit der Mitglieder. Die modernen Systeme erlauben eine effiziente Nutzung digitaler Kanäle wie WhatsApp und RCS, die als Zukunft der Mitgliederkommunikation gelten.

Laut einer weiteren Bitkom-Research-Umfrage nutzen 76 Prozent der deutschen Tech-Startups KI, was die Dynamik und den Drang unterstreicht, den Mehrwert moderner Technologien frühzeitig zu erkennen und zu implementieren. Der von der KI gewährte persönliche Touch wirkt ebenso effektiv wie motivierend, ein wesentlicher Erfolgsfaktor in einem zunehmend digitalisierten Studioumfeld.

Integration und Effizienz als Erfolgsfaktoren

Ein durchgängiger und nahtloser Übergang zwischen bestehender Mitgliederverwaltung und innovativen KI-Lösungen bildet das Rückgrat moderner Studios. Partnerschaften mit Technologieführern wie Magicline gewährleisten, dass Automatisierungsprozesse reibungslos ablaufen. Kein potenzieller Kunde geht verloren und

DER AUTOR
Heiner Sieger
ist Chefredakteur der Fachmagazine DIGITAL BUSINESS
und e-commerce Magazin.

jedes Mitglied wird optimal betreut. Diese strategische Ausrichtung eng mit technologischen Innovationen vermittelt den Studios Vertrauen und Sicherheit im Umgang mit Ressourcen.

Die Qualität dieser Integration zeigt sich in der positiven Resonanz seitens der Betreiber, die durchweg Effizienzsteigerungen und Optimierungen im Tagesgeschäft erleben. Automatisierte Terminmanagement-Tools sorgen für eine optimierte Gestaltung der Arbeitsabläufe und ermöglichen den Trainern, sich voll auf die Betreuung und Motivation ihrer Mitglieder zu konzentrieren.

Überzeugend und zukunftsorientiert

Das Vertrauen in die lokal entwickelte Technologie schafft ein sicheres Umfeld, in dem datenschutzkonforme Anwendungen aktiv zum Einsatz kommen. Die ständige Weiterentwicklung und Anpassung an spezifische Marktbedingungen zeichnen „KI Made in Germany" aus und festigen die Branche in der digitalen Zukunft. „Effizienz trifft Innovation – die ideale Kombination für die Fitnessbranche", betont Maximilian van der Mond, CEO der Stone Bridge GmbH, Betreiber der KI-Lösung Studio-Partner. Die kontinuierlich wachsende Zahl zufriedener Mitglieder und ihre positive Rückmeldung bestätigen die Richtigkeit dieser Entscheidungen. Sie schätzen den wertvollen Mix aus digitaler Effizienz und individueller Betreuung, der ihnen im Studioalltag geboten wird.

„Durch enge Partnerschaften mit Magicline, Aidoo und bald auch weiteren Mitgliederverwaltungen wird nicht nur eine reibungslose Terminvereinbarung ermöglicht, sondern auch die direkte Übertragung in die bestehende Mitgliederverwaltung", sagt Maximilian van der Mond. Termine und weitere Aktionen werden automatisch angelegt, sodass kein potenzieller Kunde verloren geht und der administrative Aufwand erheblich reduziert wird. „In enger Zusammenarbeit mit der Deutschen Telekom sind wir einer der Vorreiter im Bereich RCS – dem modernen Pendant zu SMS, und Alternative zu WhatsApp. Zudem arbeiten wir an einer Voice API, die noch in diesem Jahr auf den Markt kommen soll", so der Chef des Start-ups. Diese Innovation ermöglicht es, Telefonate mit einer KI zu führen, die weit über die herkömmlichen, oft unbefriedigenden Lösungen hinausgeht.

Eine Symbiose von Technologie und Fitness

Die Einführung künstlicher Intelligenz hat das Potenzial, auch den Fitnessstudiobetrieb nachhaltig zu verändern. Nicht nur die Verwaltung wird effizienter, auch die Mitgliederbindung wird durch personalisierte Kommunikation gestärkt. In diesem verschmelzenden Spannungsfeld können sich Trainer auf ihre Kernaufgaben konzentrieren und ihren Mitgliedern eine optimierte, persönliche Betreuung bieten.

Die Symbiose aus technischer Innovation und menschlichem Engagement katapultiert Fitnessstudios in eine neue, vielversprechende Ära, in der die Digitalisierung Raum für persönliches Wachstum und unmittelbare, effektive Mitgliedschaftspflege schafft. Genau hier zeigt die KI ihre Muskeln: Nicht in Form traditioneller Stärke, sondern durch die Schaffung einer effizienten, verbindenden und nachhaltigen Studiokultur. •

> „ Die Einführung künstlicher Intelligenz **hat das Potenzial,** auch den Betrieb von Fitnessstudios nachhaltig zu verändern – von der Verwaltung bis zur Mitgliederbindung durch personalisierte Kommunikation. *Heiner Sieger*

WENN KI ENTSCHEIDET:

Verantwortung wird jetzt zum Erfolgsfaktor

Bereits heute steuern, skalieren und optimieren KI-Agenten Prozesse eigenständig. Damit sind sie Teil operativer Wertschöpfung im Unternehmen. Ihre Entscheidungen wirken systemisch – und können sich entlang der gesamten Wertschöpfungskette verstärken. Das gilt sowohl für die Potenziale als auch für mögliche Risiken. /// von Maike Scholz

DIE FOLGENDEN HANDLUNGSEMPFEHLUNGEN helfen Unternehmen dabei, Agentensysteme verlässlich, nachvollziehbar und im Einklang mit gesellschaftlichen Erwartungen zu integrieren. Sie basieren auf den sechs Ethik-Prinzipien des BVDW für den Einsatz von KI:

1. Fairness: Unternehmen sollten vor dem Einsatz von KI-Agenten festlegen, was „fair" im jeweiligen Anwendungskontext (z. B. Recruiting, Pricing, Support) bedeutet. Das muss sich in allen Prozessen widerspiegeln, die mit einem Agentensystem zusammenhängen. Anwender*innen sollten zudem Kennzahlen und Verantwortlichkeiten für Monitoring und Korrekturen festlegen.

2. Transparenz: Es braucht klare Dokumentation, wofür ein Agent eingesetzt wird, auf welche Daten und Tools er zugreift sowie welche Entscheidungsbefugnisse er hat. Auch sollte klar erkennbar sein, wann Nutzer*innen mit einem Agenten interagieren. Um dies sicherzustellen, können Unternehmen eine sogenannte „Agent Card" einführen - eine standardisierte „Visitenkarte" für die Agenten.

3. Erklärbarkeit: Autonome Entscheidungen dürfen keine Black Box bleiben. Unternehmen sollten sicherstellen, dass Entscheidungswege protokolliert sind und stets verständlich erklärt werden können. So behalten Mitarbeitende die Oberhand, Entscheidungen zu prüfen – ein zentraler Hebel gegen Automatisierungsbias.

4. Datenschutz: Wenn Firmen personenbezogene Daten in Agentensystemen verwenden, müssen sie festlegen, wofür diese genutzt werden, wie lange sie gespeichert werden und welche Daten dafür wirklich notwendig sind. In Systemen mit mehreren Nutzern müssen Agenten-Rechte technisch von Nutzerrechten getrennt sein. Unternehmen sollten außerdem immer eine Datenschutz-Folgenabschätzung durchführen, um mögliche Risiken für die Rechte und Freiheiten betroffener Personen frühzeitig zu erkennen.

5. Sicherheit: Unternehmen sollten den Systemen eindeutige Kennungen zuweisen und festlegen, welche Aktionen das System durchführen darf – und unter welchen Umständen es abgeschaltet werden soll. So kann jeder Agent individuell identifiziert und überwacht werden, um frühzeitig auf mögliche Anomalien zu reagieren.

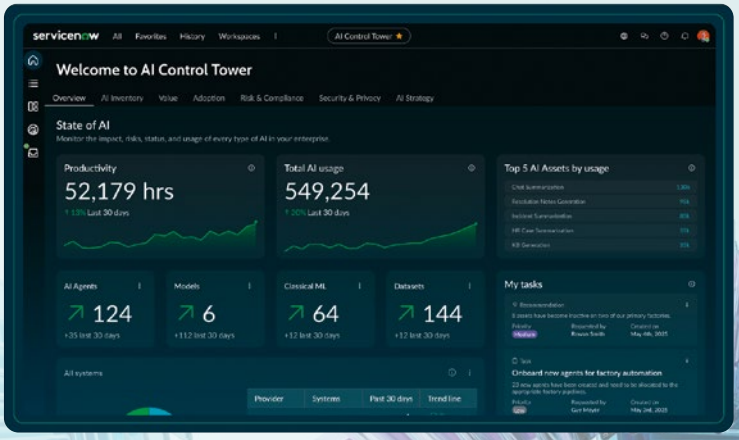
6. Robustheit: Die Widerstandsfähigkeit eines Systems wird durch die Antizipation möglicher Angriffe auf und Ausfälle von Agenten erhöht. Bevor ein KI-Agentensystem eingesetzt wird, müssen entsprechende Tests durchgeführt werden. Anschließend ist eine kontinuierliche Überwachung notwendig. Versionen von Agentenmodellen, Prompts, Daten und Zugriffsrechten sollten klar verwaltet werden. So ist es möglich, bei Problemen auf frühere Stände zurückzugehen und das System stabil zu betreiben.

KI-Agentensysteme werdenjetzt fester Bestandteil unternehmerischer Realität. Die Zukunft agentischer Systeme entscheidet sich nicht in den Algorithmen, sondern in strukturell verankerter Governance, die sie umgibt: Unternehmen, die ethische Prinzipien frühzeitig in ihre KI-Strategie integrieren, etablieren eine verlässliche Governance – und schaffen damit Transparenz, Kundenvertrauen und die Grundlage, agentische KI erfolgreich zu skalieren. •

DIE AUTORIN
Maike Scholz
ist Senior Compliance Expertin mit Schwerpunkt KI-Governance, digitale Ethik und Corporate Digital Responsibility (CDR) bei der Deutschen Telekom und verantwortet als Squad Lead für „Digital Ethics" die Implementierung des KI-Governance-Frameworks im Konzern. Im Bundesverband Digitale Wirtschaft (BVDW) e. V. ist sie stellvertretende Vorsitzende der Working Group Digital Responsibility.

KI Governance im Griff:

Innovation und Kontrolle vereinen



KI VERSPRICHT ENORME INNOVATIONSSPRÜNGE, DOCH VIELE UNTERNEHMEN STOSSEN AN EINE UNSICHTBARE GRENZE: FEHLENDE GOVERNANCE.

Ohne klare Regeln für Transparenz, Verantwortung und Kontrolle lassen sich KI-Initiativen zwar starten, aber nur schwer skalieren.

Der ServiceNow Enterprise AI Maturity Index zeigt: Der KI-Reifegrad stagniert vielerorts oder sinkt sogar, weil Governance und Steuerung nicht mit der technologischen Entwicklung Schritt halten. Gleichzeitig wird deutlich, wie entscheidend Governance für erfolgreiche KI-Initiativen ist: 63 % der Vorreiter verfügen bereits über KI-spezifische Richtlinien für Data Governance und Sicherheit – bei anderen Unternehmen sind es nur 42 %.

Mit dem EU AI Act existiert ein verbindlicher Rechtsrahmen für den Einsatz von KI. Systeme werden nach ihrem Risiko klassifiziert, Unternehmen müssen Transparenz herstellen, Risiken dokumentieren und Governance-Strukturen etablieren. Für Organisationen bedeutet das: Wer KI skalieren will, braucht mehr als innovative Modelle – nämlich klare Leitplanken.

Governance beginnt bei Daten und Use Cases

AI Governance beinhaltet die strategische Steuerung von KI-Initiativen, den verantwortungsvollen Umgang mit Daten sowie Richtlinien für Sicherheit und Ethik. Unternehmen müssen ihre relevanten KI-Use-Cases definieren und klären, welche Daten, Technologien und Investitionen dafür notwendig sind. Gleichzeitig gilt es, Datenschutz, Sicherheitsanforderungen und interne Richtlinien einzuhalten.

In der Praxis zeigt sich oft ein anderes Bild: KI-Projekte entstehen in einzelnen Fachbereichen, unterschiedliche Modelle werden parallel genutzt und der Überblick über Daten, Prompts oder Trainingsgrundlagen geht schnell verloren. Dadurch steigen Risiken und Compliance-Aufwand.

Transparenz über die gesamte KI-Landschaft

Genau hier setzt der ServiceNow AI Control Tower an. Als zentrale Steuerungsinstanz für KI in Unternehmen sorgt er für Transparenz über Systeme, Modelle und Daten. Unternehmen können Risiken identifizieren, Governance-Richtlinien durchsetzen und gleichzeitig den Nutzen von KI-Investitionen messen.

So kann mühelos die gesamte KI-Landschaft verwaltet werden – von Modellen und Datensätzen bis hin zu Workflows und KI-Agenten.

KI strategisch steuern und skalieren

Der AI Control Tower basiert auf der einheitlichen Datenarchitektur der ServiceNow AI Platform und integriert KI in bestehende Geschäftsprozesse. Unternehmen können sowohl intern entwickelte als auch externe KI-Systeme integrieren und erhalten eine konsolidierte Sicht auf ihre gesamte KI-Strategie.

Dadurch gewinnen CIOs und CTOs Transparenz über KI-Investitionen und deren Auswirkungen auf Geschäftsprozesse. Risiko- und Compliance-Verantwortliche können Governance-Vorgaben systematisch überwachen. Und Chief AI Officers erhalten belastbare Kennzahlen über den tatsächlichen Wert von KI-Initiativen.

Governance als Grundlage für erfolgreiche KI

Mit zunehmender Verbreitung von KI wird Governance zum zentralen Erfolgsfaktor. Unternehmen, die Transparenz über ihre KI-Landschaft schaffen, können Innovation schneller und verantwortungsvoll skalieren. Ein AI Control Tower liefert dafür die notwendige Grundlage und macht aus einzelnen KI-Projekten eine nachhaltige Unternehmensstrategie. •

DER AUTOR
Michael Wallner
AI GTM Lead EMEA Central bei ServiceNow

Kontakt:
ServiceNowDACH@servicenow.com

Open Source:

„Java ist zwar nicht hip, aber kritische Infrastruktur"

Java bildet das Rückgrat vieler geschäftskritische Anwendungen. Doch die Lizenzpolitik von Oracle treibt die Kosten in die Höhe. Im Gespräch mit Digital Business erläutert Ian Whiting, CRO bei Azul, welche Open-Source-Alternativen es gibt und warum sich der Umstieg für Unternehmen lohnt. /// von Stefan Girschner

Bei Java denken viele Menschen an eine veraltete Technologie. Herr Whiting, können Sie erklären, welche Rolle die Programmiersprache heute immer noch in Unternehmen spielt?
Ian Whiting | Java ist nach wie vor die populärste Programmiersprache der Welt. Laut Analysten wie Gartner laufen rund 70 Prozent aller Business-Anwendungen auf dieser Plattform. Große Unternehmen entwickeln damit individuelle Open-Source-Applikationen, die sich nicht mit Standardsoftware abbilden lassen – etwa in der Fertigung, im Finanzwesen, im Handel oder in der Logistik. Trading-Systeme, Enterprise-Industrie-Anwendungen oder Online-Retail-Systeme basieren zum Beispiel häufig auf Java. Viele Unternehmen wählen diese Programmiersprache, weil sie weit verbreitet ist und von einer riesigen, weltweiten Community unterstützt wird. So bietet Java eine außergewöhnlich große Auswahl an Bibliotheken und Frameworks, die Entwickler nutzen können.

Java ist Open Source. Warum zahlen Unternehmen trotzdem für eine kommerzielle Version?
IW | Open Source ist grundsätzlich ein großer Vorteil, weil Menschen auf der ganzen Welt zur Weiterentwicklung von Java beitragen. Das bringt aber auch Herausforderungen mit sich. Denn Unternehmen, die geschäftskritische Anwendungen betreiben, benötigen regelmäßige Security-Patches, Updates und langfristigen Support. Sie müssen sicher sein, dass ihre Applikationen stabil sind und effizient laufen. Daher entscheiden sich viele folgerichtig für eine kostenpflichtige Enterprise-Version. Ursprünglich wurde Java von Sun Microsystems erfunden. Oracle hat Sun dann 2010 übernommen und früh ein kommerzielles Modell aufgesetzt. Mittlerweile müssen Kunden aber viel Geld für Oracle Java SE bezahlen und immer wieder neue Lizenzbedingungen hinnehmen. Seit der letzten Änderung sind die Kosten bei den meisten Anwendern geradezu explodiert. Viele planen daher, zu einem anderen Java-Anbieter zu wechseln oder haben dies bereits getan.

Welche Alternativen haben Unternehmen, denen Oracle Java zu teuer geworden ist?
IW | Oracle Java basiert nach wie vor auf der Open-Source-Software OpenJDK. Im Grunde hat Oracle nichts Wesentliches am Quellcode geändert, verkauft Java SE jetzt aber als Closed Source. Es gibt zahlreiche andere Anbieter auf dem Markt, die ebenfalls OpenJDK-basierte Enterprise-Versionen von Java bereitstellen. Sofern diese TCK-zertifiziert sind, können sie Oracle Java eins zu eins ersetzen. TCK steht für Technology Compatibility Kit und bedeutet: Die Software ist zu 100 Prozent Java-Standard-Edition kompatibel. Unternehmen können also problemlos auf solche Java-Distributionen umsteigen. Azul bietet beispielsweise mit Platform Core eine sichere, stabile Oracle-Alternative, die im Vergleich zu Oracle 70 Prozent günstiger ist. Anders als Oracle wird die Software nämlich nicht nach der Anzahl der Mitarbeiter lizensiert, sondern nach tatsächlich vorhandenen Java-Nutzern.

Viele Unternehmen haben noch nie von Azul gehört. Wer verbirgt sich dahinter?
IW | Tatsächlich gibt es Azul schon seit über 20 Jahren. Wir sind das einzige Software-Unternehmen, das sich zu 100 Prozent auf Java spezialisiert hat, und beschäftigen rund 160 Java-Spezialisten. Ich sage gern scherzhaft, dass wir das bestgehütete Geheimnis im Enterprise-Software-Markt sind. Denn viele große Unternehmen setzen Produkte und Services von Azul im Hintergrund ein, reden aber nicht darüber. Unser primäres Geschäft besteht darin, Oracle Java zu ersetzen – mit günstigeren und flexibleren Lizenzbedingungen und starkem Support. Darüber hinaus wollen wir Java aber auch besser machen.

Wie können Unternehmen ihre Java-Umgebungen denn konkret optimieren?
IW | Ein wichtiger Bereich ist die Performance. Wenn Java-basierte Anwendungen schneller starten und mehr Vorgänge pro Sekunde verarbeiten, können Unternehmen ihre Produktivität steigern und die Customer Experience verbessern. Für einen Finanzdienstleister bedeutet ein performanteres Java zum Beispiel schnellere Trades und mehr Umsatz. Ein E-Commerce-Anbieter kann mehr Kunden in kürzere Zeit bedienen und kommt früher zum Abschluss. Java-Anwendungen lassen sich ganz einfach

beschleunigen, indem man eine leistungsfähigere JVM (Java Virtual Machine) einsetzt. Azul bietet dafür Platform Prime, seine High-Performance Java-Plattform. Unternehmen können damit zum Beispiel auch ihre Cloud-Kosten optimieren.

Welche Rolle spielt Java denn für die Cloud-Kosten?
IW | Unternehmen verlagern immer mehr Business-Anwendungen in die Cloud. Da ein Großteil dieser Applikationen auf Java basiert, wirkt sich die Java-Performance auch auf die Cloud-Kosten aus. Die Rechnung ist ganz einfach: Je schneller die Java-Anwendungen laufen, desto weniger vCPU-Leistung verbrauchen sie. Eine Studie von Azul hat gezeigt, dass die meisten Unternehmen ihre Cloud-Ressourcen überprovisionieren, weil sie Angst vor Performance-Engpässen haben. Denn bei geschäftskritischen Applikationen kann sich niemand Ruckler oder Störungen leisten. Um Lastspitzen abzufedern, zahlen sie also dauerhaft für Rechenleistung, die sie zum Großteil gar nicht benötigen.

Mit einer performanteren JVM lässt sich die Zahl der vCPUs deutlich reduzieren, ohne dass die Nutzererfahrung leidet. Dieser Use Case ist sehr wichtig, denn viele Unternehmen stellen nach der Migration fest, dass ihre Cloud-Ausgaben aus dem Ruder laufen. Sie suchen daher nach Möglichkeiten, um Kosten zu reduzieren.

Für welche Unternehmen lohnt sich der Einsatz von Azul Java?
IW | Vor allem Unternehmen mit großen Java-Entwicklungsumgebungen profitieren von unserer Plattform. Sie sparen durch den Umstieg und die Optimierungen am meisten. So gehören zu unserem Kundenstamm zum Beispiel 36 Prozent der Fortune-100-Unternehmen, die zehn größten Banken der Welt und weitere renommierte Weltkonzerne. Wir haben aber auch kleinere Kunden, die sehr kritische Workloads betreiben und daher hohe Anforderungen an Stabilität und Performance haben, wie etwa in der Finanzbranche.

Wie gelingt Unternehmen die Migration zu Azul Java?
IW | Wir arbeiten mit einigen großen Software Asset Management- und Software-Services-Partnern zusammen, die bei der Migration unterstützen. Außerdem stellen wir Tools und Best Practices bereit. In der Regel beginnt ein Projekt mit einer Bestandsaufnahme: Wo und wie setzt das Unternehmen Oracle Java ein? Wo liegen die Lizenzrisiken und welche Systeme sind davon betroffen? Technisch ist der Wechsel dann vergleichsweise unkompliziert, da Azul ja eine vollständig kompatible OpenJDK-Version anbietet, die Oracle-Java eins zu eins ersetzen kann. Kunden können außerdem selbst entscheiden, wo sie unsere Plattform betreiben – ob On Premises oder in einer Cloud ihrer Wahl.

Wird Java auch in Zukunft Bestand haben?
IW | Auf jeden Fall. Java wird kontinuierlich von der Open-Source-Community weiterentwickelt und wird auch künftig eine tragende Rolle im Bereich der Business-Anwendungen spielen. Ein bisschen lässt sich das mit den Rohren in einem Haus vergleichen: Java ist zwar nicht hip, aber kritische Infrastruktur. Der Bedarf an stabilen, sicheren und kosteneffizienten Alternativen zu Oracle Java SE ist daher groß. Das zeigt sich auch daran, dass Azul kontinuierlich wächst. Vor Kurzem ist mit Thoma Bravo eine der weltweit größten Private-Equity-Firmen als Mehrheits-Investor eingestiegen. Ein klares Zeichen dafür, welch strategisches Potenzial in Java weiterhin steckt. •

> „ Wir sind das **bestgehütete Geheimnis im Enterprise-Software-Markt**. Denn viele große Unternehmen setzen Produkte und Services von Azul im Hintergrund ein, reden aber nicht darüber. *Ian Whiting*

DER GESPRÄCHSPARTNER
Ian Whiting
ist Chief Revenue Officer bei Azul. Er ist für alle Aspekte der Einnahmen bei Azul verantwortlich, wie Vertrieb, Vorverkäufe, Vertriebspartnerschaften und Dienstleistungen. Whiting bringt eine langjährige Erfahrung in der Führung von Unternehmen mit.
Bild: Azul

ERP-Cloud-Migration ohne Stolpersteine

Viele ERP-Cloud-Projekte im Mittelstand scheitern nicht an der Technologie, sondern an der eigenen Systemrealität. Die Cloud löst keine Probleme – sie legt Strukturdefizite offen. Genau deshalb wird sie für viele Organisationen unbequem. Wer das versteht, erkennt: ERP-Cloud-Migration ist kein IT-Projekt. Sie ist eine strategische Neuaufstellung.

/// von Ulrich Zahner

Darum geht's
- Warum ERP-Cloud-Migration kein IT-, sondern ein Strukturprojekt ist
- Wo gewachsene Komplexität sichtbar wird
- Warum Klarheit zur eigentlichen Transformationsleistung wird

Die Cloud als Spiegel der Organisation

Seit Jahren sprechen wir über die Cloud. Collaboration-, CRM- oder HR-Lösungen sind längst selbstverständlich ausgelagert. Beim ERP-System, dem operativen Kern eines Unternehmens, ist die Diskussion grundsätzlicher. Eine ERP-Lösung ist nicht nur Software. Sie ist Prozessarchitektur, Datenbasis und Steuerungsinstrument zugleich. Über Jahre gewachsene Anpassungen, Sonderlogiken und Zusatzlösungen bilden die tatsächliche Organisationsstruktur ab. Und genau deshalb gilt:
Die Cloud löst keine Probleme – sie macht sie sichtbar.

Was vorher im Serverraum verborgen war, wird im Migrationsprojekt sichtbar. Gerade im Public-Cloud-SaaS-Modell entstehen kontinuierliche Updates, integrierte Innovationen, klare Sicherheitsstandards und planbare Kosten. Doch diese Vorteile entfalten ihre Wirkung nur dann, wenn die zugrunde liegende Struktur tragfähig ist. Ohne saubere Architektur kann die Cloud ihr Potenzial nicht entfalten.

Die fünf Strukturfelder, in denen die Cloud Klarheit schafft

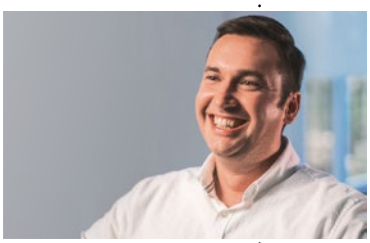
1. Architektur: Überindividualisierte Legacy-Systeme

In vielen mittelständischen Unternehmen sind ERP-Systeme über 15 bis 20 Jahre gewachsen. Jede neue Anforderung wurde individuell umgesetzt: Spezialfelder, Sonderauswertungen, eigene Schnittstellen. Diese Individualisierung spiegelt unternehmerische Entwicklung wider. Mit der Zeit entsteht jedoch eine hohe strukturelle Komplexität. Änderungen werden aufwendig, Abhängigkeiten schwer überschaubar. Die Migration in die Cloud bietet hier die Chance zur architektonischen Neuordnung. Sie macht transparent, welche Individualisierungen tatsächlich strategisch relevant sind und wo Standardisierung Stabilität und Effizienz erhöht. Statt historische Sonderwege fortzuschreiben, entsteht eine klar strukturierte, zukunftsfähige Systembasis.

2. (Eigen-)Betrieb: Ressourcenbindung statt Gestaltung

Der Eigenbetrieb eines ERP-Systems erfordert kontinuierliche Aufmerksamkeit: Wartung, Sicherheitsup-

DER AUTOR
Ulrich Zahner
ist Geschäftsführer der Allgeier inovar GmbH.



> „ Die Migration in die Cloud bietet hier die Chance zur architektonischen Neuordnung. Sie macht transparent, welche Individualisierungen tatsächlich strategisch relevant sind und wo Standardisierung **Stabilität und Effizienz** erhöht.
>
> *Ulrich Zahner*

dates, Backup-Strategien. Diese Aufgaben sind notwendig, binden jedoch Ressourcen. Im SaaS-Modell wird der technische Betrieb zur Serviceleistung. Updates erfolgen strukturiert, Sicherheitsstandards werden zentral umgesetzt. Dadurch verschiebt sich der Fokus der internen IT.

Statt Infrastruktur zu verwalten, entsteht Raum für Weiterentwicklung – etwa in der Prozessautomatisierung oder datenbasierter Steuerung. Die technische Basis bleibt stabil, während die Organisation an Innovationskraft gewinnt.

3. Steuerung: Intransparente Gesamtkosten

Im klassischen On-Premise-Modell verteilen sich Kosten auf viele Einzelpositionen: Hardware, Energie, Wartung, Personal. Eine ganzheitliche Betrachtung fällt dadurch schwer. Cloud-Modelle schaffen Transparenz. Laufende Kosten sind klar ausgewiesen, Investitionen planbar und skalierbar. Das ermöglicht eine strategische Steuerung der IT-Ausgaben und bessere Entscheidungsgrundlagen. Nicht die Frage nach „günstiger oder teurer" steht im Mittelpunkt, sondern die Fähigkeit, Kosten langfristig kalkulierbar und flexibel zu gestalten.

4. Innovation: Fehlende Anschlussfähigkeit an KI

Technologische Entwicklungen wie KI oder datengetriebene Automatisierung setzen flexible Architekturen voraus. In gewachsenen Systemlandschaften sind solche Erweiterungen oft mit erheblichem Aufwand verbunden. Cloud-ERP-Systeme entwickeln sich kontinuierlich weiter. Neue Funktionen stehen unmittelbar zur Verfügung. Innovation wird damit nicht zum Ausnahmeprojekt, sondern zum fortlaufenden Prozess. Unternehmen sichern sich so strukturelle Anschlussfähigkeit – ein entscheidender Faktor für Wettbewerbsfähigkeit in dynamischen Märkten.

5. Prozess: Fachkräftemangel trifft auf Fragmentierung

Parallel zur technologischen Entwicklung verschärft sich der Fachkräftemangel. Gleichzeitig arbeiten viele Organisationen mit historisch gewachsenen Insellösungen, Doppelpflege und manuellen Übertragungen. Eine integrierte Cloud-Architektur schafft die Grundlage für durchgängige Prozesse. Automatisierung reduziert Medienbrüche und Transparenz erhöht die Steuerungsfähigkeit. Das Ziel ist die wirksamere Nutzung vorhandener Kompetenz. Qualifizierte Mitarbeitende konzentrieren sich auf Analyse, Steuerung und Weiterentwicklung statt auf manuelle Routinetätigkeiten.

Von der Transparenz zur Transformation

Architektur, Betrieb, Wirtschaftlichkeit, Innovationsfähigkeit und Prozessorganisation greifen ineinander. In all diesen Feldern wirkt die Cloud wie ein Spiegel: Sie schafft Transparenz und macht gewachsene Komplexität sichtbar.

ERP-Cloud-Migration ohne Stolpersteine gelingt nicht durch Geschwindigkeit, sondern durch ein klares Zielbild. Wenn der Mittelstand sie als strukturelle Neuaufstellung versteht, gewinnt er damit nicht nur ein neues Betriebsmodell, sondern legt auch die Grundlage für seine Zukunftsfähigkeit. •

Datenmigration nach Unternehmenskauf:

So geht‘s

Datenmigration ist oft der problematischste Teil einer Firmenübernahme. Mit der richtigen Herangehensweise können Unternehmen Chaos, Stillstände und Datenverlust bei der Überführung komplexer Datenlandschaften vermeiden. /// von Max Giessler

Wenn Unternehmen fusionieren, stehen meist strategische Fragen, Synergien und Kosten im Fokus.
Doch in der Praxis entscheidet häufig ein anderes Thema über den Erfolg der Integration: die Datenmigration. Denn die Datenbestände beider Unternehmen sind kein Nebenprodukt der Transaktion, sondern ein strategisches Asset. Ihre Integration ist einer der komplexesten Schritte im Post-Merger-Prozess. Misslingt sie, drohen Betriebsunterbrechungen, Compliance-Probleme, finanzielle Schäden und Vertrauensverlust bei Kunden und Mitarbeitenden. Datenmigration ist kein rein technisches Thema, sondern ein organisatorisches und strategisches Integrationsprojekt.

DER AUTOR
Max Giessler
Max Giessler ist Geschäftsführer von Bitformer, ein IT-Beratungs- und Systemhaus mit Fokus auf IT-Interim-Management, Turnaround- /Kriseneinsätze und digitale Transformation.

Warum Datenmigration oft zum Problem wird
Bei einer Übernahme treffen meist zwei historisch gewachsene Systemlandschaften aufeinander – mit unterschiedlichen Datenmodellen, Stammdatenqualitäten und lückenhafter Dokumentation. Hinzu kommt erheblicher Zeitdruck, da Geschäftsbetrieb und Integration parallel laufen. Unvorbereitete „Big Bang“-Migrationen führen schnell zu Ausfällen, fehlerhaften Datensätzen oder Datenverlust.

Der größte Irrtum:
Migration ist ein IT-Projekt
Häufig wird Datenmigration als rein technische Aufgabe verstanden. Projekte scheitern selten an Tools, sondern an fehlender Abstimmung zwischen Management, Fachbereichen und IT. Erfolgreiche Integration beginnt mit einer klaren Regel: Daten gehören den Fachbereichen. Sie müssen von der Analyse bis zur Validierung aktiv eingebunden werden.

Data Due Diligence statt böser Überraschungen
Bereits in der Transaktionsphase sollte Klarheit herrschen: Welche Daten existieren? In welcher Qualität? Und welche Abhängigkeiten bestehen zwischen Systemen und Prozessen? Wer diese Fragen nicht vor dem Closing beantwortet, verschiebt Risiken lediglich in die Post-Merger-Phase.

Erst das Zielbild, dann die Migration
Bevor Daten bewegt werden, muss definiert sein, welche Systeme künftig bestehen, welche konsolidiert werden und welche Informationen tatsächlich benötigt werden. Oft sind mehr als 30 Prozent der Bestände veraltet oder redundant. Migration ohne Zielarchitektur bedeutet, Ineffizienzen einfach mitzunehmen.

Struktur schafft Sicherheit
Erfolgreiche Migration folgt keinem Zufall, sondern einem klar definierten Ablauf. Wer Daten als strategisches Asset versteht, braucht ein Vorgehen, das Transparenz schafft, Zielstrukturen definiert und Qualität messbar absichert. Genau hier setzt die ASSET-Methode an:

1. **Assess:** Dateninventur und Abhängigkeiten erfassen
2. **Shape:** Zielstruktur und Transformationslogik definieren
3. **Standardize:** Daten bereinigen und harmonisieren
4. **Execute:** Migration kontrolliert umsetzen
5. **Track:** Vollständigkeit, Konsistenz und Business-Fit validieren

Besonders die Standardisierungsphase wird häufig unterschätzt. Sie beginnt nicht erst vor der technischen Umstellung, sondern idealerweise bereits während der Due Diligence. Mangelhafte Datenqualität gefährdet selbst technisch einwandfreie Migrationen und damit den wirtschaftlichen Erfolg nach dem Closing.

Typische Fehler – und wie man sie vermeidet

1. **Datenqualität und -umfang werden unterschätzt**
   Unvollständige oder redundante Stammdaten führen zu Fehlern im Zielsystem und verlängern durch zusätzliche Testläufe die Projektlaufzeit. Wer Daten ungeprüft übernimmt, migriert auch Ineffizienzen. Frühzeitige Analyse und Bereinigung reduzieren Komplexität und Risiko erheblich.
2. **Fehlende Governance-Strukturen**
   Ohne klare Zuständigkeiten entstehen Brüche in der Datenpflege und Reibungsverluste in Prozessen. Nach dem Closing ist oft unklar, wer welche Daten verantwortet. Verbindliche Datenverantwortung in den Fachbereichen schafft Transparenz und sichert nachhaltige Qualität.
3. **Unzureichende Tests**
   Verkürzte oder rein technische Testläufe übersehen Performance-Probleme, Mapping-Fehler und Prozessbrüche. Mehrere Testzyklen mit produktionsnahen Szenarien sind notwendig, um Risiken vor dem Go-Live zu identifizieren.
4. **Unrealistische Zeitpläne und Erwartungshaltungen**
   Migration neben dem laufenden Betrieb „mitlaufen" zu lassen, führt zu überhasteten Entscheidungen und verkürzten Vorbereitungsphasen. Integration braucht realistische Zeitfenster, klare Prioritäten und abgestimmte Ressourcen.

FÜNF QUICK WINS FÜR EINE REIBUNGSLOSE DATENÜBERNAHME

1. **Frühzeitig Datenanalyse durchführen**
   Transparenz über Datenquellen, Systeme und Verantwortlichkeiten schafft Planungssicherheit.
2. **Kritische Daten priorisieren**
   Kunden-, Vertrags- und Finanzdaten zuerst migrieren und absichern.
3. **Dubletten bereinigen**
   Reduziert Datenvolumen und verbessert sofort die Qualität.
4. **Fachbereiche einbinden**
   Sie liefern Kontextwissen und erkennen Inkonsistenzen früh.
5. **Pilotmigration durchführen**
   Testläufe mit echten Daten identifizieren Risiken vor dem Go-Live.

Diese Maßnahmen schaffen schnell Klarheit, reduzieren Risiken und stabilisieren die Integrationsphase.

Fazit:
Integration entscheidet sich an den Daten

Strategische Logik und Synergieversprechen reichen nicht aus. Entscheidend ist, ob Daten strukturiert bewertet, bereinigt, migriert und validiert werden. Wer Migration frühzeitig entlang eines klaren Vorgehens plant - von der Analyse bis zur Qualitätssicherung - reduziert Risiken, beschleunigt Integration und schützt den Unternehmenswert.

Eine Transaktion endet nicht mit dem Closing. Sie endet, wenn aus zwei Datenbeständen eine belastbare Grundlage für das gemeinsame Geschäft geworden ist. •

> „ Bevor Daten bewegt werden, muss definiert sein, welche Systeme künftig bestehen, welche konsolidiert werden und welche Informationen tatsächlich benötigt werden. Oft sind mehr als 30 Prozent der Bestände veraltet oder redundant. **Migration ohne Zielarchitektur** bedeutet, Ineffizienzen einfach mitzunehmen.
>
> *Max Giessler*

Cloud-ERP:

Wie gelingt digitale Souveränität?

Um ein Enterprise Resource Planning (ERP) zur Steuerung und Optimierung der unternehmerischen und betrieblichen Abläufe kommt kaum ein Unternehmen herum. Und viele setzen hierfür auf die Cloud. Doch wie lässt sich eine digitale Souveränität im ERP-Bereich sicherstellen, ohne dass die Interoperabilität zu stark eingeschränkt wird?

/// von Konstantin Pfliegl

JENS SCHULTE

Prokurist Produktentwicklung bei ams.Solution

• ERP-Systeme steuern sämtliche Unternehmensprozesse zentral und sorgen so für Effizienz und Transparenz entlang der gesamten Wertschöpfungskette. Mit Blick auf die Sensibilität der Daten einerseits und dem Wunsch nach größtmöglicher Interoperabilität mit Dritt- und Cloudsystemen andererseits rückt die Frage nach digitaler Souveränität zunehmend in den Fokus – zumal der Faktor künstliche Intelligenz und die datentechnisch nicht risikolose Nutzung frei zugänglicher LLMs wie ChatGPT hinzukommt.

Datenhoheit behalten

Für ams.Solution bedeutet digitale Souveränität im ERP-Kontext die Wahrung der technischen und juristischen Datenhoheit. Dabei geht es zunächst um Governance- und Sicherheitsmaßnahmen. Dies darf jedoch nicht zu technologischen Abhängigkeiten und Einschränkungen führen. Vielmehr müssen die Anwender in der Lage sein, ihre Software flexibel durch die Anbindung von Drittsystemen und Cloud-Applikationen zu erweitern.

Der On-Premises-Betrieb bleibt für viele Kunden die bevorzugte und strategisch sinnvollste Option, weil er maximale Kontrolle über Daten, individuelle Anpassungen und Release-Zyklen ermöglicht. Insbesondere in regulierten Branchen oder bei sensiblen Produktions- und Betriebsdaten sprechen Compliance-Anforderungen, Sicherheitsaspekte und Performance-Vorteile für eine lokale Infrastruktur. Zudem lassen sich Investitions- und Betriebskosten langfristig planen. •

UDO HENSEN

Geschäftsführer der Gebra-IT

• Digitale Souveränität im ERP-Bereich bedeutet nicht, die Cloud grundsätzlich infrage zu stellen. Im Gegenteil: Cloud-Technologien bieten Unternehmen enorme Chancen in Bezug auf Skalierbarkeit, Verfügbarkeit und Geschwindigkeit. Entscheidend ist aber, dass Unternehmen nicht die Kontrolle über ihre eigenen Prozesse, Daten und Entwicklungsmöglichkeiten verlieren. Ein ERP-System darf nicht zur Black-Box werden, die zwar vieles kann, aber nur innerhalb eines starren Anbieter-Ökosystems funktioniert.

Digitale Souveränität entsteht dort, wo Unternehmen ihre Abläufe selbst gestalten, ihre Daten sicher und transparent nutzen und ihre Systemlandschaft flexibel weiterentwickeln können. Dafür braucht es offene Schnittstellen, verlässliche Integrationsmöglichkeiten und eine Architektur, die Interoperabilität nicht als Zusatzfunktion versteht, sondern als Grundprinzip.

Intelligente Vernetzung

Aus unserer Sicht ist genau das der richtige Weg: ein ERP, das als stabiles digitales Rückgrat funktioniert und gleichzeitig offen genug bleibt, um andere Systeme, Plattformen und Anwendungen nahtlos einzubinden – ob in der Cloud, hybrid oder in bestehenden Infrastrukturen. Denn kaum ein Unternehmen arbeitet heute noch in einer abgeschlossenen IT-Welt. Wer wettbewerbsfähig bleiben will, muss Finanzwesen, Logistik, Produktion, Einkauf, CRM, E-Commerce oder branchenspezifische Lösungen intelligent miteinander vernetzen können. •

v.l.: Jens Schulte (Bild: ams.Solution), Udo Hensen (Bild: Gebra-IT)

MORITZ LUKAS

VP Commercial bei Xentral

• Die Skepsis vieler Unternehmer gegenüber der Cloud ist sehr nachvollziehbar. Wer die Kernprozesse seines Betriebs digitalisiert, möchte nicht das Gefühl haben, die Fernbedienung für das eigene Unternehmen aus der Hand zu geben. Die Angst vor dem Vendor Lock-in – also der Gefangenschaft in einem starren System, das Innovationen bremst und Kosten unkontrollierbar macht – ist für viele Entscheider ein reales Wachstumshindernis. Doch echte digitale Souveränität bedeutet heute nicht mehr, eigene Server in den Kellerräumen zu warten. Für strategische Entscheider bedeutet Souveränität vor allem Handlungsfreiheit. Es geht darum, eine Software zu wählen, die sich den unternehmerischen Prozessen anpasst und nicht umgekehrt.

Zentrale Drehscheibe

Die Lösung für dieses Spannungsfeld liegt in der technologischen Offenheit. Ein modernes ERP muss als zentrale operationelle Drehscheibe fungieren, die über flexible Schnittstellen und smarte Middleware jederzeit erweiterbar bleibt. So behalten Unternehmen die volle Kontrolle über ihre Daten und ihre strategische Ausrichtung, während sie gleichzeitig die Skalierbarkeit und Sicherheit der Cloud nutzen. •

STEFAN ISSING

Presales Director DACH bei IFS

• Digitale Souveränität und Cloud schließen sich im ERP-Umfeld nicht aus. So sorgen klare Data-Residency-Modelle, transparente Rechenzentrumsstandorte und die Einhaltung regulatorischer Vorgaben dafür, dass Unternehmen die Datenhoheit behalten. Sie wissen jederzeit, wo ihre Daten liegen und welchen Rechtsräumen sie unterliegen.

Dadurch bleibt die Kontrolle über geschäftskritische Informationen gewahrt. Zudem gewährleisten Zero-Trust-Mechanismen und ein starkes Identity- und Access-Management, das Zugriffe strikt kontrolliert und Risiken minimiert, Datensicherheit.

Technologische Unabhängigkeit sichern

Auch beim Thema Innovationgeschwindigkeit behalten Unternehmen die Hoheit. Sie können Updates und neue KI-Funktionen im eigenen Tempo ausrollen und haben dadurch volle Kontrolle über ihre Transformationsprozesse. Durch standardnahe Implementierungen können sie außerdem Lock-in-Effekte vermeiden. Wenn sie auf individuelle Kernmodifikationen verzichten und Anpassungen stattdessen über klar definierte Erweiterungsschichten umsetzen, sichern sie sich technologische Unabhängigkeit. Einschränkungen bei der Interoperabilität müssen Unternehmen nicht in Kauf nahmen. Standardisierte APIs, offene Schnittstellen und sichere Integrationen ermöglichen es ihnen, Drittsysteme, Partnerlösungen und branchenspezifische Anwendungen flexibel anzubinden. •

THOMAS KNORR

Vice President Cloud Transformation bei Forterro

• Die Arbeit mit cloud-basierten Lösungen und Souveränität schließen sich nicht aus. Wer auf eine Architektur setzt, die Offenheit mit klar definierten Regeln, Strukturen und Prozessen verbindet, sichert seine Daten und kann so von den Vorteilen profitieren. Richtig umgesetzt erhöht die Cloud durch ihre Skalierbarkeit, Sicherheit und Innovationsgeschwindigkeit die strategische Handlungsfähigkeit.

Ein souveränes Cloud-ERP basiert auf drei Säulen: Erstens Datenkontrolle und Compliance. Unternehmen müssen jederzeit nachvollziehen können, wo ihre Daten verarbeitet werden und welchem Rechtsrahmen sie unterliegen. Zweitens eine offene Architektur. Ein ERP ist kein abgeschotteter Monolith, sondern agiert als orchestrierender Kern im digitalen Ökosystem. Drittens Portabilität und Exit-Fähigkeit: Strategische Abhängigkeiten gilt es von Anfang an zu vermeiden. Dabei helfen transparente Vertragsmodelle, standardisierte Datenformate und dokumentierte Exportmechanismen.

Kommandobrücke im Unternehmen

Die Interoperabilität moderner, cloud-basierter ERP-Systeme einzuschränken ist kein gangbarer Weg, weil man sie auf diese Weise ihrer großen Stärke beraubt. Als zentrale Kommandobrücke sind sie darauf angewiesen über gesicherte APIs mit anderen im Unternehmen eingesetzten Software-Lösungen Daten auszutauschen und zu kommunizieren. Dies ist kein „Nice-to-have“, sondern eine essenzielle Grundvoraussetzung. •



v.l.: Moritz Lukas (Bild: Xentral), Stefan Issing (Bild: IFS), Thomas Knorr (Bild: Forterro)

ERP in der Cloud: Die Freiheit, zu wählen

Ob hohe Anforderungen an die Verfügbarkeit, Herausforderungen durch verteilte Standorte oder schlicht der Wunsch nach weniger administrativem Aufwand: Der Bezug des ERP-Systems aus der Cloud kann viele Vorteile mit sich bringen. Und doch ist die Cloud nicht pauschal die Technologie für jedermann. Was Unternehmen für echte Zukunftsfähigkeit benötigen, ist die Freiheit, Betriebsmodelle flexibel und passgenau zu kombinieren.

/// von Ralf Bachthaler

INSBESONDERE IN DEN LETZTEN JAHREN HAT DIE CLOUD-TECHNOLOGIE EINE STEIGENDE NACHFRAGE ERFAHREN. Ein zentrales Argument für die Nutzung eines ERP-Systems aus der Cloud findet sich bereits auf finanzieller Seite: Da sich Unternehmen nicht länger selbst um den Betrieb und die Wartung der Lösung kümmern müssen, profitieren sie von größerer Flexibilität und – insbesondere bei volatilerem Geschäftsverlauf – durchaus auch von Kostenvorteilen. Auch im Kontext des anhaltenden Fachkräftemangels ist die Auslagerung des Betriebs eine attraktive Option: Wechselt Fachpersonal, das sich jahre- oder jahrzehntelang um die Wartung und Anpassung der ERP-Lösung gekümmert hat, in den Ruhestand, ist es oft nicht leicht, frei werdende Stellen nachzubesetzen.

Spiegelbildblich dazu ermöglicht es die Nutzung eines Cloud-Services, von der Expertise des Cloud-Anbieters zu profitieren. In der Regel verfügt dieser über hochgradig spezialisierte Teams, die sich zentralisiert um Aspekte wie Security, Datensicherheit oder Backups kümmern. Nicht selten lassen sich so Schutz- und Sicherheitsniveaus erreichen, die etwa ein klassischer Mittelständler ohne tiefgehendes Expertenwissen selbst nur schwer realisieren könnte.

Und schließlich ist auch das Thema Flexibilität ein wichtiges Argument für die Cloud. Cloud-Implementierungen lassen sich bei Bedarf sehr schnell skalieren. Insbesondere in wirtschaftlich volatilen Zeiten kann dies für Unternehmen einen entscheidenden Vorteil bedeuten, etwa wenn globale Veränderungen eine Expansion in neue Märkte erfordern. Neue Standorte – oder generell verteilte Standorte – lassen sich per Cloud-Technologie schnell und einfach anbinden: Es genügt ein Internetzugang und der Standort kann seinen Betrieb aufnehmen; ein Prozess, der im On-Premise-Szenario durch die erforderliche Anbindung an die jeweilige Netzwerkinfrastruktur meist deutlich komplexer ausfällt.

Kein Patentrezept

Die Nutzung eines ERP-Systems aus der Cloud bringt zahlreiche Vorteile mit sich – und doch ist das Betriebsmodell nicht für jedes Unternehmen geeignet. Nicht selten bestehen Hinderungsgründe, die eine Migration in die Cloud erschweren oder gar unmöglich machen. Compliance-Vorgaben etwa können hohe Hürden aufstellen, sensible Kunden- oder Firmendaten in externe Rechenzentren zu geben. Abhängig vom genutzten Service-Provider und

DER AUTOR
Ralph Bachthaler
Ralf Bachthaler ist Mitglied des Vorstands bei Asseco Solutions.
Bild: Asseco Solutions

den Standorten seiner Rechenzentren verlassen übertragene Daten gegebenenfalls den deutschen oder europäischen Rechtsraum und unterliegen dann der Gesetzgebung der Drittstaaten.

Ebenso verlangt die Nutzung einer Cloud-Lösung dem Unternehmen ein gewisses Maß an Anpassungsbereitschaft ab, denn umfassende Anpassungen oder Individualisierungen sind in der Cloud nicht möglich. Für Neugründungen oder Start-ups ist dies meist kein Problem, da sie in der Regel noch nicht über fest definierte Prozesse verfügen und sich daher leicht an den vorgegebenen Abläufen der Cloud-Lösung orientieren können. Für Unternehmen mit langjährig etablierten oder hochgradig spezialisierten Prozessen hingegen kann es schwierig sein, auf einen Standard-Ansatz zu migrieren.

Und schließlich gilt es zu bedenken: Zum reibungslosen Betrieb einer Cloud-ERP-Lösung ist eine stabile Internetverbindung mit hohen Bandbreiten zentral. Insbesondere in eher ländlichen Regionen ist dies jedoch auch heute noch immer keine Selbstverständlichkeit. Für Unternehmen aus Branchen wie der Automobil- und Zulieferindustrie oder der Serienfertigung, in denen Verzögerungen oder Ausfälle hohe Kosten zur Folge haben können, ist die Auslagerung kritischer Systeme dann keine Option.

Am Nutzen orientieren

Die Entscheidung, on-premises zu bleiben oder in die Cloud zu migrieren, sollte für Unternehmen kein „Entweder-oder" sein. Für ERP-Hersteller gilt es, Unternehmen einen sinnvollen Mittelweg aufzuzeigen, der die Möglichkeit bietet, die Vorteile beider Betriebsmodelle passgenau zu verbinden: Ein hybrider Ansatz etwa belässt zentrale Kernfunktionalitäten – wie zum Beispiel das Core-ERP, Materialwirtschaft oder Produktionsplanung – on-premises, während Funktionsbereiche, für die die Cloud einen echten Mehrwert bietet, aus der Cloud bezogen werden. Damit bei Bedarf auch spezifische Anforderungen in hybriden Szenarien passgenau abgedeckt werden können, sollten Hersteller weitreichende Customizing-Möglichkeiten zur Verfügung stellen, mit deren Hilfe Unternehmen Individualisierungen rein auf Konfigurationsebene im System umsetzen können.

KI erfordert meist eine Cloud

Besonders geeignet für eine Cloud-Nutzung ist etwa der CRM-Bereich. In vielen Fällen lassen sich die entsprechenden Funktionalitäten sehr gut im Standard nutzen, sodass die Cloud ihre Vorteile Einfachheit und Flexibilität bestmöglich ausspielen kann. Ähnlich geeignet sind zudem Funktionsbereiche, in denen User aus der Cloud zum Beispiel neue Dashboard- oder Funktionselemente für ihre Lösung beziehen – etwa auf Basis eine Kunden-Community – und dadurch ihre Lösung unabhängig von den Releasezyklen des Herstellers erweitern können.

Hochgradig empfehlenswert und oft sogar technisch unerlässlich ist die Nutzung von Cloud-Diensten schließlich für Funktionalitäten mit künstlicher Intelligenz. Generative KI oder Large Language Models der großen KI-Anbieter erfordern in den allermeisten Fällen ein gewisses Cloud-Element. Sowohl hier als auch im Kontext klassischer analytischer KI erleichtert die Cloud die Bereitstellung einer zentralisierten Datenbasis, die Informationen über verschiedene Standorte, Unternehmensbereiche oder Produktionsmaschinen hinweg beinhaltet.

> „ Die Nutzung eines ERP-Systems aus der Cloud bringt zahlreiche Vorteile mit sich – und doch ist das Betriebsmodell nicht für jedes Unternehmen geeignet. **Nicht selten bestehen Hinderungsgründe**, die eine Migration in die Cloud erschweren oder gar unmöglich machen.
>
> *Ralf Bachthaler*

Das Beste aus zwei Welten

Die Nutzung des ERP-Systems aus der Cloud bringt Vor- und Nachteile mit sich. Gerade im Kontext der heutigen Welt- und Wirtschaftslage sowie der technologischen Weiterentwicklungen kann sie mit Effizienz und Flexibilität punkten; der einzige Weg für eine solide Zukunftsfähigkeit ist sie jedoch nicht. Zielführender kann es sein, die Vorteile beider Betriebsmodelle passgenau in den Bereichen zu nutzen, in denen diese ihre jeweiligen Stärken tatsächlich ausspielen können.

Entscheidend ist die Wahlfreiheit: Wer flexibel selektieren kann, hat auch die Möglichkeit, das Beste aus zwei Welten sinnvoll miteinander zu verbinden. •

Ohne Budget keine Innovation:

Die Business-Strategie hinter hybriden Microsoft-Strukturen

Digitale Innovation steht auf der Agenda nahezu jedes mittelständischen Unternehmens. KI, Automatisierung und datengetriebene Geschäftsmodelle sind zentrale Hebel für Wachstum. Auf der anderen Seite binden steigende laufende Kosten einen immer größeren Teil der Budgets. Damit wichtige Modernisierungsprojekte nicht in der Cloud hängen bleiben, helfen hybride Strategien. /// von Björn Orth

NOCH VOR WENIGEN JAHREN GALT DIE MIGRATION IN DIE CLOUD als logischer nächster Schritt der Digitalisierung. Kollaboration, Mobilität und Skalierbarkeit sprachen dafür. Inzwischen zeigt sich jedoch eine weniger diskutierte Seite dieser Entwicklung: Die laufenden Kosten der Plattformen wachsen schneller als viele IT-Budgets.

Ein Grund sind regelmäßige Preisanpassungen. Ein weiterer, der auch 2026 wieder zum Tragen kommt:

Microsoft erweitert sein Portfolio kontinuierlich um neue Funktionspakete, Sicherheitsmodule und KI-Services. Viele davon erscheinen unter neuem Namen, als zusätzliche Lizenzbausteine oder kostenpflichtige Erweiterungen bestehender Pläne. Für Unternehmen wird es dadurch immer schwieriger, Leistungen zu vergleichen und ihre langfristigen IT-Kosten realistisch zu kalkulieren. Die Cloud ist technisch enorm leistungsfähig – wirtschaftlich wird sie aber zur Dauerinvestition. Wie stark das die Gesamtbudgets bindet, realisieren Organisationen oft erst nach einigen Jahren.

Finanzielle Spielräume schaffen

Die eigentliche strategische Herausforderung liegt deshalb nicht in der Technologie, sondern in der Budgetstruktur. Digitale Innovation entsteht selten aus laufenden Betriebskosten, sondern aus Investitionsspielräumen. Das zeigt sich besonders deutlich beim Thema künstliche Intelligenz.

Neue KI-Funktionen, Analyseplattformen oder Automatisierungs-Lösungen entstehen meist zusätzlich zur bestehenden IT-Landschaft – sie müssen also finanziert werden, ohne dass anderswo eingespart werden kann. Vor diesem Hintergrund eignen sich hybride Lizenzarchitekturen. Die Kombination aus M365-Diensten mit lokal betriebenen Microsoft-Anwendungen rechnet sich.Wir erstellen für unsere Kunden regelmäßig den Kostenvergleich: Cloud-only versus hybrid. Werden die On-Premises-Lizenzen, wie von uns empfohlen, gebraucht eingekauft, erzielen wir Einsparungen von 30 bis 40 Prozent.

Hybrid als strategischer Mittelweg

Kollaborations-Plattformen wie Microsoft Teams, Exchange oder Sharepoint entfalten ihre Vorteile klar in der Cloud. Gleichzeitig gibt es in jedem Betrieb eine Vielzahl von Anwendungsfällen, bei denen lokale Strukturen sinnvoller bleiben. Dazu gehören Office-Programme, Windows-Installationen oder Terminal-Server-Umgebungen, spezialisierte Fachanwendungen und Software, die über viele Jahre stabil genutzt wird. Auch bei sehr großen Datenmengen zeigt sich der Unterschied deutlich: Werden umfangreiche Projekt- oder Archivdaten dauerhaft in der Cloud gespeichert, sprengt das die laufenden Kosten.„So etwas gehört auf eigene Server. Hybride Modelle ermöglichen, Daten und Anwendungen gezielt dort zu betreiben, wo sie technisch und wirtschaftlich am besten aufgehoben sind.

Datensouveränität wird zum Innovationsfaktor

Neben der Kostenfrage gewinnt noch ein weiterer Aspekt an Bedeutung: die Kontrolle über Daten. Mit der zunehmenden Nutzung von KI und digitalen Geschäftsprozessen werden Unternehmensdaten zu einem zentralen strategischen Asset. Unsere Consultants raten un-

> „ Die Cloud ist technisch enorm leistungsfähig – **wirtschaftlich wird sie aber zur Dauerinvestition**. Wie stark das die Gesamtbudgets bindet, realisieren Organisationen oft erst nach einigen Jahren.
>
> *Björn Orth*

seren Kunden deshalb, bewusst zu entscheiden, wo sensible Daten liegen und wer darauf zugreifen kann. Hybride Infrastrukturen schaffen diese Wahlfreiheit: Kritische Informationen verbleiben im eigenen Rechenzentrum, während Cloud-Dienste für Kollaboration, Analyse oder KI genutzt werden. Hybrid bedeutet nicht raus aus der Cloud. Es bedeutet, Cloud bewusst dort einzusetzen, wo sie einen Mehrwert für ihren hohen Preis liefert.

Lizenzstrategie als Teil der Business-Strategie

Damit verschiebt sich auch die Rolle der Software-Lizenzierung. Früher ein reines Beschaffungsthema ist sie heute Teil der unternehmerischen Strategie. Denn sie entscheidet darüber, wie stabil Kostenstrukturen sind – und wie viel finanzieller Spielraum für Innovation bleibt. Hybride Microsoft-Modelle entfalten genau diesen Effekt: Ein Teil der IT-Kosten wird von laufenden Preisanpassungen entkoppelt. Für viele Unternehmen entsteht dadurch ein entscheidender Vorteil: Planungssicherheit. Digitale Innovation entsteht dort, wo Unternehmen ihre Plattform-IT so steuern, dass noch genug Budget für Neues übrig bleibt. •

DER AUTOR
Björn Orth
ist Geschäftsführer bei Vendosoft.
Bild: Vendosoft

TAKE-AWAYS FÜR UNTERNEHMEN

Bestandsaufnahme und Kostenklarheit schaffen:
Erfassen Sie alle genutzten Cloud-Dienste, Add-ons und KI-Module sowie deren laufende Kosten. Überlegen Sie, was tatsächlich gebraucht wird und was „Nice-to-have ist. Ziel: Transparenz über Ausgaben für die Cloud.

Hybrid-Szenario konkret durchrechnen:
Stellen Sie Cloud-only und Hybrid über drei bis fünf Jahre gegenüber. Beziehen Sie in die Kalkulation die wiederkehrenden Preisanpassungen sowie zusätzliche Microsoft-Module ein. Prüfen Sie den Einsatz gebrauchter On-Premises-Lizenzen für lokale Microsoft-Workloads.

Datensouveränität bewusst gestalten:
Entscheiden Sie, welche Daten sensibel sind, wo sie liegen und wer zugreift. Kritische Informationen bleiben im eigenen Unternehmen. Cloud-Dienste werden gezielt für Zusammenarbeit, Auswertung und KI genutzt. So behalten Sie Kontrolle – und schaffen gleichzeitig die Basis für neue digitale Prozesse.

Lizenzen als Business-Strategie:
Behandeln Sie Lizenzierung nicht als reinen Einkauf, sondern als Hebel für Planungssicherheit. Ein hybrides Modell entkoppelt einen Teil Ihrer IT-Kosten von laufenden Preiserhöhungen. Verankern Sie diese Entscheidungen im Budgetprozess, damit Investitionsspielräume für Innovation entstehen.

NEWS

INDUSTRIAL AI CLOUD: DEUTSCHE TELEKOM BAUT KI-FABRIK WEITER AUS

Anfang Februar hat die Deutsche Telekom die Industrial AI Cloud in Betrieb genommen – die erste ihrer Art in Europa. Jetzt baut der Konzern das angeschlossene KI-Ökosystem weiter aus. Dafür fungiert T-Systems ab sofort als „Sovereign Partner Cloud Provider" von ServiceNow. Damit baut die Deutsche Telekom die seit 2014 bestehende Partnerschaft mit ServiceNow in Deutschland weiter aus. So können deutsche Kunden insbesondere in hochregulierten Branchen ihre Workflows noch besser automatisieren und unstrukturierte Daten mit Hilfe von KI strukturieren und die Effizienz steigern unter Einhaltung strenger regulatorischer Anforderungen. Zudem unterstreicht die enge Kooperation das Engagement beider Unternehmen, eine sichere, KI-getriebene digitale Transformation in der Region zu ermöglichen. •

CYBERBEDROHUNGEN: ANGREIFER FAVORISIEREN EINLOGGEN STATT EINDRINGEN

Ein neuer Bericht von Cloudflare zu Cyberbedrohungen 2026 zeigt, dass sowohl nationalstaatliche Akteure als auch Cyberkriminelle ihren Fokus vom „Eindringen" zum „Einloggen" verlagern. Die Daten zeigen, dass Angreifer DDoS-Angriffe in einem noch nie dagewesenen Ausmaß nutzen, KI-Systeme einsetzen, um Schwachstellen auszunutzen, und weiterhin traditionelle Schwachstellen wie E-Mails angreifen, um Wege zu finden, sich anzumelden anstatt einzudringen.

KI beseitigt die technische Einstiegshürde für Angriffe: Bedrohungsakteure verwenden Large Language Models (LLMs), um Netzwerke in Echtzeit abzubilden, neue Exploits zu entwickeln und hyperrealistische Deepfakes zu erstellen. Und nordkoreanische Agenten nutzen KI-generierte Deepfakes und gefälschte Identitäten, um Einstellungsprozesse zu umgehen und staatlich unterstützte Kräfte direkt in die Gehaltslisten westlicher Unternehmen einzuschleusen. •

CYBERRESILIENZ: GEFÄHRLICHE LÜCKEN BEI DER DEUTSCHEN WIRTSCHAFT

Der neue Cyber Security Report 2026 von Schwarz Digits offenbart gefährliche Lücken bei der Cyberresilienz. Womöglich 48 Prozent der befragten Unternehmen gehen fälschlicherweise davon aus, nicht von der NIS-2-Richtlinie betroffen zu sein. Besonders gefährlich ist die Lage für umsatzstarke Kleinunternehmen: Obwohl sie mit 10 bis 49 Mitarbeitern eine geringe Personalstärke aufweisen, überschreiten sie die Umsatzgrenze von zehn Millionen Euro und werden damit regulierungspflichtig. In diesem Segment wiegen sich bis zu 92 Prozent in trügerischer Sicherheit und schließen eine Betroffenheit fälschlicherweise aus.

Dabei wächst die Kritik an der öffentlichen Hand: 62 Prozent der Unternehmen fühlen sich bei der NIS-2-Einführung von den Behörden unzureichend unterstützt. Auch die generelle digitale Handlungsfähigkeit des Staates wird abgestraft: Lediglich 21 Prozent der Firmen fühlen sich durch politische und verwaltungstechnische Maßnahmen ausreichend geschützt. •

QUANTENCOMPUTING: UNTERNEHMEN VERLASSEN SICH NICHT MEHR AUF VISIONEN

Eine Studie von QuEra Computing zeigt, wie pragmatisch Unternehmen Quantencomputing bewerten: 62 Prozent der Befragten mit relevanten Anwendungsfällen geben an, dass klassische Rechenverfahren bereits an ihre Grenzen kommen. Der Bedarf an Quantencomputing entsteht damit weniger aus technologischer Neugier als aus Leistungsgrenzen heutiger IT-Systeme. Gleichzeitig hat sich der Blick auf den Markt ernüchtert. Der Anteil der Befragten, die ihr Land als „sehr gut positioniert" im Bereich Quantencomputing einschätzen, ist gegenüber dem Vorjahr um zwanzig Prozentpunkte gesunken – von über 45 Prozent im Jahr 2025 auf 25 Prozent im Jahr 2026. Der anfängliche Optimismus weicht einer nun immer kritischeren Bewertung. •

SECURITY INSIGHT

Cyber Risk & Resilience

Cyber-Resilienz 2026:

Weckruf für KMU

Der Cyber Security Report 2026 (Schwarz Digits) zeigt gravierende Lücken: 48 Prozent verkennen NIS2-Pflichten, 54 Prozent unterschätzen KI-Risiken, 75 Prozent auditieren Partner nicht. Budgets steigen zwar auf 17 Prozent des IT-Budgets. Die Wirkung bleibt jedoch reaktiv. /// von Dr. Alexander Schellong

WECKRUF FÜR DIE DEUTSCHE WIRTSCHAFT: Der auf der Cyber Security Conference der Schwarz Gruppe in Heilbronn veröffentlichte Cyber Security Report 2026 von Schwarz Digits legt deutliche Resilienz-Lücken offen. Trotz geschätzter 202 Milliarden Euro jährlicher Schäden durch Cyberangriffe, steigen Security Budgets auf etwa auf 17 Prozent des Gesamt IT Budget. Viele Maßnahmen bleiben jedoch reaktiv und primär regulatorisch getrieben. Der Befund: Zwischen gefühlter Vorbereitung und tatsächlicher Widerstandskraft liegt eine Lücke die Risiken für einen Cybervorfall erhöhen kann.

NIS2: Betroffenheit wird häufig falsch eingeschätzt

Die Erhebung unter 1.001 Unternehmen zeigt ein kritisches Defizit bei der NIS2-Einordnung: Rund 48 Prozent der Befragten gehen davon aus, nicht betroffen zu sein – gerade bei umsatzstarken Kleinunternehmen: Betriebe mit 10 bis 49 Beschäftigten, die die Umsatzgrenze von 10 Millionen Euro überschreiten, sind regulierungspflichtig – in diesem Segment schließen bis zu 92 Prozent eine Betroffenheit fälschlicherweise aus.

Alle öffentlichen und privaten Organisationen sollten sich an den NIS2 Vorgaben orientieren. Nur so können wir die Abwehrkräfte des Gesamtsystems stärken.

Begrenzte staatliche Unterstützung, wachsende Frustration

62 Prozent der Unternehmen fühlen sich bei der Einführung von NIS2 von Behörden unzureichend unterstützt. Nur 21 Prozent sehen sich insgesamt durch politische und verwaltungstechnische Maßnahmen ausreichend geschützt. Besonders kritisch wird die Basis eingeschätzt: Lediglich 7 Prozent attestieren den Ländern eine gute Aufstellung gegen Cyberangriffe – Kommunen kommen auf 12 Prozent, der Bund auf 15 Prozent. Entgegen den politischen Debatten über Hackbacks, befürworten 79 der Unternehmen offensive staatliche Maßnahmen gegen Cyberangreifer.

KI: Beschleuniger von Angriffen – Governance-Druck für KMU

Künstliche Intelligenz wirkt 2026 als Beschleuniger und Skalierungsfaktor bestehender Angriffe. Gleichzeitig schätzt mit 54 Prozent mehr als die Hälfte der Unternehmen das zusätzliche Risiko durch KI als gering ein. Während 73 Prozent der großen Unternehmen klare Regeln für den KI-Einsatz eingeführt haben, besteht bei kleinen und mittleren Unternehmen deutlicher Nachholbedarf. Der Report skizziert Szenarien autonomer Angriffe und die gezielte Manipulation von KI-Entscheidungen in phy-

DER AUTOR
Dr. Alexander Schellong
ist Managing Director, Institutes, Accelerators & Security bei Schwarz Digits.

sischen Prozessen – ein Risiko, das Security-Architekturen adressieren müssen. Erforderlich sind unternehmensweite Richtlinien zum KI-Einsatz, Schutzmaßnahmen an Modellen und Schnittstellen, Monitoring von Eingaben und Ausgaben, Missbrauchs Abwehr sowie die Integration von KI-Aspekten in Bedrohungsanalysen und Incident-Playbooks.

Digitale Souveränität:
Strategie bekannt, Umsetzung dünn

Anspruch und Wirklichkeit driften auseinander: Nur 19 Prozent der Unternehmen verfügen über eine Strategie für digitale Souveränität. 42 Prozent wären bereit, für souveräne Lösungen mehr zu bezahlen. Dennoch investieren lediglich 13 Prozent gezielt in Ressourcen, um technologische Abhängigkeiten aktiv zu reduzieren.

Das im Report verwendete Software-Sovereignty-Framework bescheinigt EU-basierten Open-Source-Lösungen im Schnitt eine höhere Souveränität als proprietären Plattformen außerhalb der EU. Für Unternehmen bedeutet das: Abhängigkeiten systematisch inventarisieren, Exit-Strategien planen, Datenportabilität und offene Standards priorisieren, europäische Alternativen evaluieren – und Souveränitätskriterien in Beschaffung und Architektur fest verankern.

Lieferkette: Drittrisiken als Einfallstor

Die Vernetzung der Wertschöpfung wird zur zentralen Schwachstelle. Jedes zweite Unternehmen registrierte bereits Angriffe auf Zulieferer, drei von vier verzichten dennoch auf regelmäßige Audits ihrer Partner. Nur ein Drittel hat die Abhängigkeiten in der Lieferkette vollständig im Blick. Besonders verlustträchtig sind Vorfälle über IT-Dienstleister oder kompromittierte Software-Updates; die vollständige Wiederherstellung dauert im Ernstfall bis zu 30 Tage.

Ein belastbares Third-Party-Risk-Management ist damit Pflicht: Kritikalität von Lieferanten klassifizieren, Mindestkontrollen (z. B. Aufbau eines Informationssicherheitsmanagement (ISMS), kontinuierliche Penetrationstests, Systemhärtungen) vertraglich festlegen, Software-Stücklisten (SBOMs) einfordern, Remote-Zugriffe auf Zero-Trust-Basis absichern, kontinuierliches Monitoring etablieren und Audit- sowie Incident-Meldepflichten mit klaren SLAs verankern. Regelmäßige Übungen mit Schlüsselpartnern sollten die Wirksamkeit der eigenen Verteidigungsstrategien prüfen.

Von reaktiv zu wirksam:
Handlungsagenda für die nächsten 180 Tage

- Jährliche Durchführung einer strukturierten Risiko- und Schutzbedarfsanalyse, deren Ergebnisse in die Maßnahmenpläne für Technologie, Prozesse oder Personalaufbau fließen. Wichtig ist, dass man den eigenen Risikoentscheidungen traut und danach handelt.
- NIS2-Scoping und Governance: Betroffenheit prüfen, Verantwortlichkeiten bis auf Geschäftsführungsebene klären, Melde- und Krisenprozesse dokumentieren und üben.
- KI-Governance: Einsatzrichtlinien festlegen, Modell- und Schnittstellenschutz implementieren, Prompt-/Output-Monitoring einführen, Manipulationsrisiken in Threat Models und Playbooks integrieren.
- Lieferkette absichern: Kritische Drittparteien priorisieren, Mindestkontrollen und SBOM in Verträgen verankern, Update-Ketten härten, Rechte auf Audit und Notfalltests vereinbaren.
- Wirksamkeit messen: Security-KPIs (z. B. Mean Time to Detect/Respond, Patch-Laufzeiten, Testabdeckung) definieren, Red-Teaming/Tabletop-Exercises quartalsweise durchführen und Ergebnisse ins Risiko- und Budgetmanagement rückkoppeln.
- Souveränität als Sicherheitshebel: Architektur- und Anbieterabhängigkeiten bewerten, Portabilität sicherstellen, europäische und Open-Source-Optionen dort nutzen, wo sie Risiko und Compliance verbessern können.

> „ Die Vernetzung der Wertschöpfung wird zur **zentralen Schwachstelle**. Jedes zweite Unternehmen registrierte bereits Angriffe auf Zulieferer, drei von vier verzichten dennoch auf regelmäßige Audits ihrer Partner. *Dr. Alexander Schellong*

Quintessenz: Der Report 2026 macht deutlich: Resilienz entsteht nicht nur aus steigenden Budgets, sondern aus klarer Governance, geübten Prozessen und belastbaren Lieferketten. Wer NIS2, KI-Risiken und Souveränität als integrierte Steuerungsaufgabe versteht, reduziert Ausfälle, verkürzt Wiederanlaufzeiten und erhöht die Handlungsfähigkeit – gerade im Mittelstand. •

Wie sich Unternehmen vor Cyberangriffen schützen

Auch in diesem Jahr steht Cybersecurity ganz oben auf der Prioritätenlistevon Unternehmen. Die Anforderungen an die IT-Sicherheit verändern sich jedoch durch neue Technologien wie KI, Automatisierung oder Cloud-Dienste. Wir haben Experten ausgewählter Cybersecurity-Anbieter gefragt, mit welchem Ansatz Unternehmen den bestmöglichen Schutz vor Cyberangriffen und anderen Bedrohungen erreichen. /// von Stefan Girschner

TIZIAN KOHLER

Head of Security bei Adlon Intelligent Solutions GmbH

- **KI, Automatisierung und Cloud-Dienste verändern die Bedrohungslandschaft** insbesondere in zwei Richtungen: Während Unternehmen von neuen Technologien profitieren, nutzen Angreifer dieselben Werkzeuge für schnellere und gezieltere Attacken. Der wichtigste Paradigmenwechsel führt weg vom reaktiven Schutz hin zu kontinuierlicher Resilienz. Das bedeutet zunächst, dem Zero-Trust-Prinzip zu folgen, bei dem kein Nutzer oder Gerät als vertrauenswürdig eingestuft wird. Klingt streng, ist aber notwendig. Ein oft unterschätzter Einstieg für Unternehmen ist Multi-Faktor-Authentifizierung (MFA). Sie stellt sicher, dass gestohlene Zugangsdaten allein nicht ausreichen, um in Systeme einzudringen und gehört heute zur absoluten Mindestanforderung für Unternehmen.

Genauso wichtig ist es, Schwachstellen zu schließen, bevor Angreifer sie finden. Regelmäßige Risiko-analysen und konsequentes Schwachstellenmanagement müssen oberste Priorität haben. Sollte dies nicht möglich sein, ist die schnelle Erkennung von und Reaktion auf Angriffe umso kritischer. Beides funktioniert nur durch kontinuierliches Monitoring und klare Definition der internen Reaktionsmaßnahmen. Und dann ist da noch der Faktor Mensch. Phishing und Social Engineering sind nach wie vor die häufigsten Einfallstore. Technik allein schützt nicht, wenn Mitarbeitende nicht sensibilisiert sind. Cybersicherheit ist also kein Projekt, das man abhakt, sondern ein kontinuierlicher Prozess aus Strategie, Technologie und Sicherheitsbewusstsein.

HERMANN RAMACHER

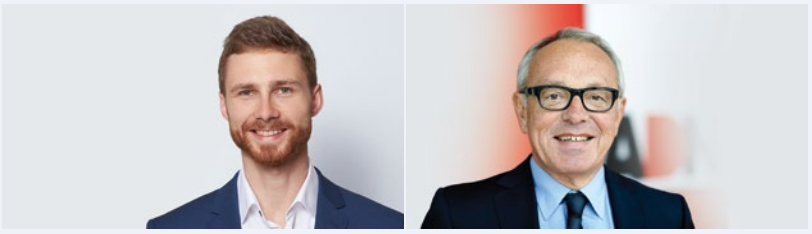
Geschäftsführer der ADN Distribution GmbH

- **Unternehmen stehen heute unter enormen Druck,** ihre Sicherheitsstrategien schneller weiterzuentwickeln, als sich die Methoden der Angreifer anpassen können. KI verschärft die Bedrohungslage, bietet aber gleichzeitig enorme Chancen für eine intelligentere Abwehr. Entscheidend ist daher ein ganzheitlicher Ansatz, der Prävention, Detektion und Reaktion verbindet.

Es empfiehlt sich, Sicherheitsarchitekturen konsequent nach Zero-Trust-Prinzipien auszurichten, Identitäten klar zu kontrollieren und Zugriffe engmaschig zu steuern. Moderne XDR- und KI-gestützte Mechanismen erhöhen die Resilienz, indem sie Anomalien früh erkennen und automatisiert reagieren. Ebenso wichtig ist die Absicherung hybrider und Multi-Cloud-Umgebungen durch zentral steuerbare, softwarebasierte Netzwerkansätze. Ein besonderes Augenmerk sollte auch auf der Backup-Resilienz liegen, da Ransomware zunehmend gezielt Sicherungen attackiert.

Um unseren Partnern das richtige Werkzeug zum effektiven Schutz an die Hand zu geben, haben wir unser Security-Portfolio kontinuierlich ausgebaut, etwa um Zero-Trust-Lösungen oder widerstandsfähige Datensicherung. Zusätzlich unterstützten wir als Value-Added-Distributor unsere Partner dabei, diese Entwicklungen greifbar zu machen – durch praxisorientiertes Enablement und Technologien, die reale Sicherheitslücken adressieren, ohne zusätzliche Hürden zu schaffen.

Cybersecurity ist heute kein Produkt mehr, sondern ein fortlaufender Transformationsprozess.



v.l.n.r.: Tizian Kohler (Bild: Adlon Intelligent Solutions), Hermann Ramacher (Bild: ADN Distribution)

v.l.n.r.: Tommy Grosche (Bild: Fortinet), Frank Schwaak (Bild: Rubrik)

TOMMY GROSCHE

Country Manager Germany bei Fortinet

• **Die Anforderungen an die Cybersicherheit** ändern sich aufgrund von Technologien wie KI, Automatisierung und Cloud-Diensten rasant. Regularien wie NIS2, CRA und AI Act transformieren Compliance von theoretischer Vorgabe zu operativer Notwendigkeit mit Nachweispflichten. Optimaler Schutz erfordert einen ganzheitlichen Ansatz, der diese Entwicklungen proaktiv adressiert. Hierbei ist es entscheidend, alle relevanten Vorschriften in ein konsistentes Betriebsprogramm zu integrieren.

Angesichts verstärkter Auditierung und Nachweispflichten ist eine lückenlose Dokumentation von Sicherheitskontrollen, Incident-Response-Prozessen und Lieferantenüberwachung für den Resilienz-Nachweis unerlässlich. Eine gestärkte Lieferantensteuerung ist ebenso wichtig. Die zunehmende Nutzung von KI erfordert außerdem eine integrierte KI-Governance.

FRANK SCHWAAK

Field CTO EMEA bei Rubrik

• **Automatisierung und KI-gesteuerte Schadsoftware** machen Angriffe schneller und anpassungsfähiger. Daher empfehle ich Unternehmen den Wechsel von vollständiger Abwehr hin zu messbarer Cyber-Resilienz. Die zentrale Kennzahl ist Time-to-Recovery (TTR): Wie schnell lässt sich der Betrieb wieder aufnehmen? Die Dauer der Wiederherstellung der Geschäftsfähigkeit nach einem Vorfall ist heute die entscheidende Kennzahl moderner Resilienz.

Grundlage ist eine „Assumed Breach"-Denkweise. TTR verbessert sich durch Routine, wie regelmäßige Recovery-Übungen, Simulationen oder automatisierte Wiederherstellungstests. Investitionen sollten auf kürzere Wiederanlaufzeiten zielen wie unveränderliche Backups oder automatisierte Restore-Prozesse. Ergänzend sollten Unternehmen proaktives Posture Management für Backup-Daten etablieren, um die Angriffsfläche gezielt zu reduzieren.

HEATHER CEYLAN

CISO bei Box

• **Cyberangriffe werden immer schneller, automatisierter und datengetriebener**. Daher müssen auch Sicherheitsstrategien weiterentwickelt werden. Wir bei Box denken, dass der effektivste Ansatz Zero-Trust-Prinzipien mit KI-gestützten Sicherheitsfunktionen kombiniert. Dies bedeutet, dass jeder Benutzer und jedes Gerät überprüft wird, während mithilfe von KI Datenmengen in Echtzeit analysiert werden, um ungewöhnliche Aktivitäten zu erkennen.

Gleichzeitig rückt der Schutz der Inhalte stärker in den Mittelpunkt. Da KI-Systeme zunehmend mit Firmendaten arbeiten, müssen Organisationen ihre Informationen automatisch klassifizieren, Zugriffe kontrollieren und Risiken überwachen. Entscheidend ist eine Sicherheitsstrategie, die Daten, Identitäten und KI-Workflows als Ganzes denkt. Unternehmen müssen Zugriffe konsequent kontrollieren und KI auch für die Sicherheitsprozesse nutzen.

DR. IRIS BRUNS

Geschäftsführung der ConSense GmbH

• **Angesichts von KI, Automatisierung und Cloud-Diensten** nimmt die Komplexität der IT-Landschaft rasant zu. Neue Technologien steigern die Effizienz in Unternehmen, erhöhen aber auch das Risiko von Datenverlust, Sabotage und Erpressung. Wir empfehlen Unternehmen, dieser vergrößerten Angriffsfläche mit einem strukturierten, ganzheitlichen Ansatz ihrer Schutzmaßnahmen zu begegnen.

Ein Informationssicherheits-Managementsystem (ISMS) definiert Prozesse und schafft Verantwortlichkeiten. Gleichzeitig verankert es ein systematisches Risikomanagement – von der Asset-Identifikation über die Risikobewertung bis hin zu Notfallplänen und regelmäßigen Audits. Statt punktueller Maßnahmen entsteht ein kontinuierlicher Verbesserungsprozess, der technische, organisatorische und personelle Aspekte verbindet. So werden Risiken frühzeitig erkannt, bewertet und gesteuert.

v.l.n.r.: Heather Ceylan (Bild: Box), Dr. Iris Bruns (Bild: ConSense)

Wie KMUs Sicherheit, Kosten und Compliance vereinen

Ab 2027 erzwingen Cyber Resilience Act und Maschinenverordnung Safe & Secure by Design – auch für KMUs. Bußgelder bis 15 Mio. € treffen Unternehmen, die Dokumentationschaos und fehlende Expertise ignorieren. clockworkX und CADFEM zeigen, wie strategisches Enablement aus Prozess-Know-how und qualifizierten Tools nachhaltige Compliance-Unabhängigkeit schafft. /// von Dres. Christian T. Geiss und Jan Seyfarth

DIE BISHERIGEN COMPLIANCE STRATEGIEN DER KMUS WERDEN NICHT MEHR GENÜGEN, denn die EU vollzieht mit dem Cyber Resilience Act (CRA) und der neu formulierten Maschinenverordnung (MVO) einen Paradigmenwechsel in Gesetzestext. Der Wandel geht von reaktiver Sicherheit zu „Secure by Design". Bisherige Standards wie ISO 9001 oder CE-Kennzeichnung fokussierten auf Produktqualität zum Zeitpunkt der Markteinführung. Die neuen Regularien fordern jedoch Lifecycle-Monitoring – von der Konzeptphase bis zur Stilllegung.

Hersteller vernetzter Produkte müssen nun TARA (Threat Analysis and Risk Assessment), kontinuierliches Vulnerability Management und dokumentierte Update-Prozesse nachweisen. „Secure by Default" bedeutet nämlich: Sicherheit ist kein nachträgliches Add-On, sondern Entwicklungsprinzip von Beginn an.

Die Konsequenz: Wer heute noch mit Excel arbeitet und keine Traceability zwischen Risikoanalyse und Produktdesign hat, kann in Zukunft bei Audits durchfallen.

Welche Produkte sind betroffen?

Der CRA erfasst alle „Produkte mit digitalen Elementen" – Software, Hardware, Firmware mit Netzwerkanbindung. Die Maschinenverordnung betrifft alle Maschinen, die ein CE-Kennzeichen tragen. Der Selbsttest für Ihr Unternehmen: Integrieren Sie Elektrisch/Elektronische Komponenten? Haben Ihre Produkte Remote-Zugriff oder IoT-Funktionen? Laufen Software-Updates über das Netzwerk? Wenn Sie auch nur die Möglichkeit bereitstellen, sind Sie CRA-pflichtig.

Wichtig: Es gibt keine Ausnahmen für KMUs. Die Unternehmensgröße spielt keine Rolle. Deshalb achten auch OEMs zunehmend auf Compliance innerhalb ihrer gesamten Zuliefererkette. Solche Unternehmen stecken heute schon in einer Zwangslage.

Non-Compliance als Business-Risiko

Für die Nichtbeachtung des CRA wurden empfindliche Strafen formuliert. Falsche oder unvollständige CE Kennzeichnung kostet bis zu 5 Millionen Euro oder 1% des welt-

DIE AUTOREN

Dr. Christian T. Geiss

Geschäftsführer clockworkX GmbH, TÜV Austria Gruppe.

Dr. Geiss hat im Bereich probabilistisches Risikomanagement an der TU München promoviert.Mit über 15 Jahren Erfahrung in ISO 21434, ISO 26262 und UN-ECE R155 begleitet er als TÜV-zertifizierter Auditor KMUs beim Aufbau von Cybersecurity Management Systemen (CSMS).

Dr. Jan Seyfarth

Business Development Manager Safe & Secure, CADFEM GmbH.

Dr. Seyfarth verantwortet bei CADFEM den Bereich Funktionale Sicherheit und Cybersecurity. Als Ansys Medini-Experte trainiert er Ingenieure in modellbasierter Sicherheits-Analysen und kümmert sich um die Prozess-Integration beim Kunden. CADFEM ist Ansys-Partner und betreut 2.300 KMUs in DACH mit einem 220-köpfigen Team.

weiten Jahresumsatzes. Dokumentationsmängel schlagen mit bis zu 10 Millionen Euro oder 2% zu Buche. Kernverstöße gegen Cybersecurity-Anforderungen werden mit bis zu 15 Millionen Euro oder 2,5% geahndet – je nachdem, welcher Betrag höher ist. Hinzu kommen Produktrückrufe und Verlust des EU-Marktzugangs. Bei kritischer Infrastruktur verschärft die NIS2-Richtlinie zusätzlich: Geschäftsführer haften persönlich! Die Realität ist – bisher wurden wenige Strafen verhängt, aber ab 2026 starten BSI-Audits. Frühe Compliance wird also zum Wettbewerbsvorteil gegenüber Nachzüglern.

KMUs stecken in der Klemme

Warum scheitern KMUs häufig an der praktischen Umsetzung? Aus der Erfahrung heraus finden sich drei Hauptbarrieren:

1. **Dokumentation:** es herrscht Chaos. Excel-FMEA oder -TARA hier, PDF-Risikoanalysen dort, CAD-Daten im dritten System. Es gibt keine durchgängige Traceability zwischen Anforderung und Testnachweisen. Bei Audits wird aber genau das gefordert.
2. **Ressourcen:** Sicherheits-Ingenieure – gerade mit Cybersecurity Expertise – sind Mangelware. Externe Berater kosten 1.500-2.000 Euro pro Tag. Die Kosten summieren sich für vollständige Projekte schnell in sechsstellige Höhen.
3. **Prozesse:** gerade in KMUs wird noch viel nach dem „Trial-and-Error"-Prinzip anstelle von systematischen und standardisierten Workflows gearbeitet. Dr. Christian Geiss von clockworkX: „Kunden ohne Governance auf Geschäftsführerebene scheitern – nicht an der Technik, sondern an der fehlenden Organisation."

Die Crux: Viele verstehen das Risiko des Nichthandelns nicht. „Risk of Inaction" übersteigt den „Return on Investment" bei Weitem!

Das Befähigungskonzept wird zum Schlüssel

Das „Selber-Machen" wird für KMUs den Erfolg bringen. Ein gutes Enablement orientiert sich an dem 3-Stufen-Modell:

- **Stufe 1 – Outsourcing:**
  Zunächst übernehmen externe Berater alles. Das sichert die derzeitige Situation ab. Diese Lösung ist schnell, aber auch teuer und nicht nachhaltig. Es entstehen starke Abhängigkeiten.
- **Stufe 2 – Enablement:**
  Hier entsteht ein Mix aus interner und externer Expertise. Über Training und Coaching fließt das Know-How ins Unternehmen. Tool-Integration und Prozessaufbau laufen parallel dazu. Die Basis wird geschaffen.
- **Stufe 3 – Unabhängigkeit:**
  Der Wissenstransfer ist abgeschlossen. Das Team kann eigenständig TARAs durchführen, FMEAs aktualisieren und sich auf Audits vorbereiten. Das Unternehmen agiert unabhängig, hat aber bei Problemen immer noch starke Partner im Rücken.

Der Kern von Enablement ist „selber machen". Beispiel: Eine TARA-Masterclass von clockworkX kombiniert mit der Medini-Tool-Schulung von CADFEM versetzt das Team in die Lage, selbstständig zu arbeiten.

Der Partnership-Vorteil: clockworkX baut die Governance-Struktur auf, CADFEM integriert das Tool in den Entwicklungsprozess. „More than Software" – ohne Prozess ist selbst das beste Tool nutzlos.

Wie sieht so ein Umsetzungs-Fahrplan ganz pragmatisch aus?

- **Phase 1 – Gap-Analyse** (4 Wochen)
  Es gilt zunächst, den IST-Zustand gegen die CRA/MVO-Anforderungen prüfen. Checkliste: Ist TARA vorhanden? Wird die SBOM (Software Bill of Materials) gepflegt? Sind Update-Prozesse dokumentiert?
- **Phase 2 – Quick-Wins** (2 Monate)
  Low-Hanging-Fruits identifizieren. Bestehende ISO 9001- oder ISO 27001-Prozesse um Cybersecurity erweitern. Das QM-System liefert meist bereits Grundgerüste für die Governance. Marktbarrieren absichern und die aktuelle Risikoanalyse (TARA) noch outsourcen – die Ergebnisse „Medini-Tool-ready" einfordern.
- **Phase 3 – Tooling** (3 Monate)
  Medini-Lizenz beschaffen – Team schulen, am besten gleich anhand der Medini TARA aus Phase 2. In einem weiteren Pilotprojekt ein Produkt komplett selber durchmodellieren. Lessons Learned dokumentieren.
- **Phase 4 – Prozess-Rollout** (6 Monate)
  Die TARA in den Entwicklungsprozess integrieren. Rollen definieren: Wer macht die Anaylse? Wer ist der Reviewer für die TARA? Wer pflegt Vulnerability-Datenbank und übernimmt das Monitoring?
- **Phase 5 – Pre-Audit** (ab Monat 9)
  clockworkX führt als externer Berater ein Mock-Audit durch. Schwachstellen können noch behoben werden, bevor das offizielle BSI-Audit kommt.
- **Realistisch planen:** 9-12 Monate bis audit-readyness sollten vorgehalten werden. Die Branchen-übergreifende Erfahrung zeigt: 6-9 Monate allein für den Prozessaufbau sind normal. •

MEHR ERFAHREN ...

Lesen Sie den gesamten umfassenden Beitrag auf der Webseite von DIGITAL BUSINESS.

Vom Patchen zur Risiko-Strategie:

Exposure Management als Grundlage moderner Cybersicherheit

Cybersicherheit steht an einem Wendepunkt: Isolierte Schwachstellenmeldungen allein helfen Unternehmen wenig, wenn der Bezug zum Geschäftsrisiko fehlt. Darum braucht es jetzt einen strategischen Perspektivwechsel, um Sicherheit konsequent an geschäftlichen Risiken auszurichten. /// von Roger Scheer

IN EINER ZEIT, IN DER DIGITALE GESCHÄFTSMODELLE IMMER STÄRKER VERNETZT UND KOMPLEXER WERDEN, reicht es nicht mehr aus, nur Schwachstellen zu erkennen und zu beheben. Klassische Schwachstellen-Scans liefern zwar wertvolle Daten, zeigen jedoch selten, welche Risiken für das Geschäftsmodell tatsächlich relevant sind. Moderne Cyberrisiken verlangen einen strategischen Blick auf die gesamte Risikolage eines Unternehmens – ein Ansatz, der als Exposure Management bezeichnet wird und weit über traditionelle Schwachstellenanalysen hinausgeht.

Die Grenzen klassischer Schwachstellenanalyse

Seit vielen Jahren folgen Sicherheitsprogramme einem eingespielten Zyklus: scannen, bewerten, patchen, wiederholen. Dieser Ansatz ist grundsätzlich sinnvoll, stößt jedoch zunehmend an Grenzen. Zum einen entstehen enorme Datenmengen, die kaum noch sinnvoll priorisiert werden können. Zum anderen werden Schwachstellen häufig isoliert betrachtet, ohne sie in den Kontext von Geschäftsprozessen, Angriffspfaden oder der tatsächlichen digitalen Infrastruktur einzuordnen.

In der Praxis führt dies nicht selten zu Alarmmüdigkeit. Sicherheitsteams arbeiten umfangreiche Listen technischer Einzelfunde ab, ohne sicherstellen zu können, dass damit die realen Risiken für das Unternehmen wirksam reduziert werden. Für Unternehmen, die ihre digitale Transformation konsequent vorantreiben, ist dieser Zustand kaum tragbar. Mit jeder neuen Cloud-Anwendung, jeder vernetzten Produktionsanlage und jeder zusätzlichen Schnittstelle wächst die Angriffsfläche – und damit die Komplexität der Risikosteuerung.

> **„ Punktuelle Schwachstellenscans reichen nicht mehr aus**, um die komplexen Abhängigkeiten moderner IT-Landschaften zu beherrschen.
>
> *Roger Scheer*

DER AUTOR
Roger Scheer
ist Regional Vice President Central Europe bei Tenable.
Bild: Tenanble

Ein Perspektivwechsel

Exposure Management setzt an einem anderen Punkt an. Statt ausschließlich zu fragen, welche Schwachstellen vorhanden sind, steht die Frage im Mittelpunkt, welche konkreten Risiken das Geschäftsmodell bedrohen und auf welchen Wegen Angreifer diese Risiken ausnutzen könnten. Dieser Perspektivwechsel verändert die Priorisierung grundlegend.

Ein solcher Ansatz erfordert zunächst Transparenz über sämtliche relevanten Assets – von klassischen IT-Systemen über Cloud-Dienste und Identitäten bis hin zu OT- und IoT-Umgebungen. Entscheidend ist jedoch nicht nur die Inventarisierung, sondern die intelligente Verknüpfung dieser Informationen. Schwachstellen, Fehlkonfigurationen, übermäßige Berechtigungen oder exponierte Zugangsdaten entfalten ihr tatsächliches Gefahrenpotenzial oft erst im Zusammenspiel. Gerade sogenannte „toxische Risikokombinationen" – etwa ein kompromittiertes Benutzerkonto mit weitreichenden Rechten auf einem verwundbaren System – lassen sich nur erkennen, wenn Datenquellen zusammengeführt und in Beziehung gesetzt werden.

Damit verschiebt sich der Fokus von einer reaktiven Abarbeitung technischer Mängel hin zu einer strategischen Bewertung tatsächlicher Risiken. Sicherheitsmaßnahmen werden nicht mehr primär nach Schweregrad einzelner Schwachstellen priorisiert, sondern nach ihrer Bedeutung für das Geschäftsrisiko.

Sichtbarkeit über Silos hinweg

Traditionelle Schwachstellenscanner betrachten häufig nur Teilbereiche der IT-Landschaft. Netzwerk, Server, Anwendungen oder Identitäten werden separat analysiert. In hochgradig vernetzten Umgebungen entsteht so jedoch ein fragmentiertes Bild der Sicherheitslage.

Exposure Management verfolgt einen integrierten Ansatz und schafft eine einheitliche Sicht auf das digitale Risikoökosystem. Erst durch die Zusammenführung verschiedener Perspektiven wird deutlich, welche Angriffspfade tatsächlich existieren. Ein Cloud-Dienst mag für sich genommen unkritisch erscheinen. Treffen jedoch eine unzureichende Netzwerkkonfiguration, weitreichende Zugriffsrechte und eine bekannte, aktiv ausnutzbare Schwachstelle aufeinander, kann daraus ein direkter Weg in sensible Kernsysteme entstehen. Die isolierte Betrachtung einzelner Komponenten würde dieses Szenario möglicherweise nicht erkennen.

Gerade in hybriden Infrastrukturen, in denen On-Premises-Systeme, Multi-Cloud-Architekturen und industrielle Steuerungstechnik ineinandergreifen, ist eine solche ganzheitliche Sicht Voraussetzung für wirksames Risikomanagement.

Vom Datenberg zur Entscheidungsgrundlage

Für Führungskräfte ist weniger die Anzahl entdeckter Schwachstellen entscheidend als die Frage, welche davon das Unternehmen tatsächlich gefährden. Exposure Management transformiert technische Detailinformationen in kontextbezogene Erkenntnisse über geschäftskritische Risiken. Dadurch wird es möglich, Ressourcen gezielt dort einzusetzen, wo sie den größten Effekt auf die Risikominimierung haben.

Sicherheitsberichte gewinnen so an strategischer Aussagekraft. Statt rein technischer Kennzahlen stehen belastbare Einschätzungen zur realen Gefährdungslage im Mittelpunkt. Das erleichtert die Kommunikation zwischen IT, Sicherheitsverantwortlichen und Geschäftsführung erheblich. Sicherheit wird damit nicht als Kostenfaktor oder Bremse wahrgenommen, sondern als integraler Bestandteil verantwortungsvoller Unternehmensführung.

Sicherheit als Bestandteil der Geschäftsstrategie

Mit zunehmender Digitalisierung steigt nicht nur die Innovationsgeschwindigkeit, sondern auch die regulatorische und operative Verantwortung. Anforderungen wie NIS-2 unterstreichen, dass Transparenz über Risiken und deren systematische Steuerung keine Option mehr ist, sondern zur unternehmerischen Pflicht wird.

Ein strategisch ausgerichtetes Exposure Management ermöglicht es, Angriffspfade frühzeitig zu erkennen, bevor sie ausgenutzt werden, begrenzte Sicherheitsressourcen auf die tatsächlich kritischen Bereiche zu konzentrieren und fundierte Entscheidungen auf Basis konsolidierter Risikoinformationen zu treffen. Damit entwickelt sich Cybersicherheit von einer rein technischen Disziplin zu einem zentralen Element des unternehmensweiten Risikomanagements.

Fazit

Für Unternehmen, die ihre digitale Agenda konsequent verfolgen, ist die Zeit reif für einen Paradigmenwechsel. Punktuelle Schwachstellenscans reichen nicht mehr aus, um die komplexen Abhängigkeiten moderner IT-Landschaften zu beherrschen. Gefragt ist eine umfassende, kontextbezogene Betrachtung der gesamten Risikolage. Exposure Management bietet hierfür den strategischen Rahmen – nicht als Ersatz bewährter Sicherheitsmechanismen, sondern als deren Weiterentwicklung hin zu einer risikoorientierten Gesamtperspektive. •

SECURITY INSIGHT

STRATEGISCHE ANSATZPUNKTE FÜR DIE PRAXIS

- Technische Einzelfunde konsequent in einen geschäftlichen Risikokontext einordnen
- Zusammenhänge zwischen Systemen, Identitäten und Konfigurationen transparent machen
- Sicherheitsprioritäten regelmäßig an der tatsächlichen Risikolage ausrichten

KLARHEIT SCHAFFEN:

Kommunikations-strategie für Geopolitik und Technologie

Digitale Souveränität ist vom Nischenthema zum festen Bestandteil politischer und medialer Debatten geworden. Allerdings variiert das Verständnis des Begriffs stark. Für Unternehmen wird es deshalb immer wichtiger, eine klare Definition zu finden und das Thema verständlich, konsistent und zielgruppengerecht zu kommunizieren. /// von Christoph Fabian

DIGITALE SOUVERÄNITÄT IST LÄNGST ZUM BUZZWORD GEWORDEN – in Medien ebenso wie in vielen Fachartikeln. Oft wird dabei vorausgesetzt, dass alle Beteiligten dasselbe Verständnis des Begriffs teilen. Genau hier beginnt jedoch das Problem: Die existierenden Definitionen unterscheiden sich teils erheblich. Während etwa der Digitalverband Bitkom das Konzept primär technisch und wirtschaftlich fasst, versteht das Bayerische Forschungsinstitut für Digitale Transformation digitale Souveränität deutlich breiter und bezieht auch staatliche und gesellschaftliche Dimensionen ein.

Dieser Beitrag legt keine „richtige" Definition fest. Wichtig ist vielmehr: Die jeweils zugrunde liegende Definition prägt maßgeblich, wie Unternehmen ihre eigene Position finden. Wer eine technische Lesart wählt, adressiert vor allem IT-Verantwortliche. Wer stärker politisch oder regulatorisch denkt, spricht eher Akteure aus dem öffentlichen Sektor an.

Vom Randthema zur Top-Priority

Damit digitale Souveränität überhaupt zum Buzzword werden konnte, musste viel passieren. Noch vor ein bis zwei Jahren war der Begriff quantitativ gesehen ein Nischenthema. Laut der Software-Plattform MuckRack gab es im Jahr 2023 nur rund 5.500 Erwähnungen des Begriffs „Digitale Souveränität", 2024 waren es 6.700. Im Jahr 2025 stieg die Zahl jedoch sprunghaft an: Von Januar bis Anfang Dezember wurden bereits 28.500 Erwähnungen gezählt. Allein im November entstanden fast 2.500 Artikel mehr als im September.

Auch qualitativ hat sich viel verändert. 2023 wurde digitale Souveränität überwiegend in Fach- und Expertenöffentlichkeiten diskutiert. Dazu gehörten etwa Studien, Thinktanks, IT-Fachmedien und spezialisierte Formate großer Qualitätszeitungen. In der breiten Berichterstattung spielte der Begriff dagegen eine eher untergeordnete Rolle und tauchte meist nur in Nischenrubriken auf. Spätestens seit 2025 ist digitale Souveränität deutlich stärker im politischen und medialen Mainstream angekommen – als Rahmenerzählung für Debatten über Cloud-Infrastruktur, KI, Rechenzentren und Europas technologische Unabhängigkeit.

Damit verschiebt sich auch die kommunikative Zielarchitektur: Unternehmen müssen digitale Souveränität heute nicht mehr nur für ein Fachpublikum, sondern zunehmend für Politik, Wirtschaftspresse und breite Öffentlichkeit attraktiv und verständlich machen.

Geopolitische Entwicklungen als Treiber der digitalen Souveränität

Dass digitale Souveränität zum politischen Topthema wurde, ist kein Zufall. Eine Reihe geopolitischer Entwicklungen hat das Konzept erheblich beschleunigt. Dazu zählt auch die Rückkehr von Donald Trump ins Amt Anfang 2025: Sie verstärkte in Europa die Debatte über Abhängigkeiten von US-Technologieanbietern, über den CLOUD Act und über potenzielle Datenzugriffe amerikanischer Behörden. Diese erhöhte Sensibilität fällt zeitlich mit dem starken Anstieg der Medienberichte zu digitaler Souveränität zusammen.

Parallel dazu rückten weitere Faktoren das Thema ins Zentrum der politischen Agenda: Der deutsch-französische Gipfel zur europäischen digitalen Souveränität, die laufenden Debatten zur KI-Regulierung sowie der zunehmende Fokus auf europäische Datenräume und unabhängige Cloud-Infrastrukturen. Das bedeutet für Unternehmen, dass sich die Geopolitik unmittelbar auf die kommunikativen Erwartungen auswirkt. Wer digitale Souveränität als zentralen Bestandteil seines Geschäftsmodells sieht, sollte solche politischen Wendepunkte aktiv begleiten und in der Kommunikation aufgreifen.

Best Practices: Wie Unternehmen digitale Souveränität wirksam kommunizieren

Je stärker digitale Souveränität auf politischen und medialen Agenden präsent ist, desto wichtiger wird eine

klare kommunikative Positionierung für Unternehmen. Das Thema eignet sich ideal, um zu zeigen, wie komplexe technologische und politische Konzepte verständlich vermittelt werden können.

Zentral ist eine konsistente Definition, an der sich alle Botschaften ausrichten. Nur so entsteht eine kohärente Storyline, die verhindert, dass digitale Souveränität zum inhaltsleeren Buzzword verkommt.

Darüber hinaus sollten Unternehmen das Thema positiv framen: Als Chance für Innovation, Wettbewerbsfähigkeit und Unabhängigkeit – nicht ausschließlich als Reaktion auf Risiken oder potenzielle Abhängigkeiten. Dieses Framing erlaubt es, die Vorteile souveräner Lösungen hervorzuheben, ohne andere Anbieter abzuwerten, von denen viele Organisationen weiterhin abhängig sind. Wer stärker polarisieren möchte, kann bewusst mutiger kommunizieren, sollte sich dabei jedoch der Aufmerksamkeit – und der Risiken – in der öffentlichen Debatte bewusst sein.

Wirksam ist zudem, gesellschaftliche Dimensionen wie demokratische Teilhabe, Bildung oder technologische Handlungsfähigkeit in die kommunikative Erzählung aufzunehmen. Ebenso wichtig ist der Hinweis, dass digitale Souveränität ein prozesshaftes Ziel ist – kein Zustand, den Unternehmen von heute auf morgen erreichen. Eine solche Perspektive hat den Vorteil, dass klare Fortschrittsnarrative möglich sind und realistische Erwartungen vermittelt werden.

Ausblick

Digitale Souveränität wird auch in den kommenden Jahren ein zentrales Thema für Politik, Wirtschaft und Gesellschaft bleiben. Für Unternehmen bedeutet das vor allem, die Entwicklungen kontinuierlich zu beobachten und ihre Kommunikationsstrategie flexibel anzupassen. Die Dynamik der vergangenen Jahre hat gezeigt, wie schnell sich die Relevanz bestimmter Narrative verschieben kann und wie wichtig es ist, auf neue politische, technologische und regulatorische Impulse zu reagieren.

Gleichzeitig wird der Diskurs durch die wachsende Bedeutung von künstlicher Intelligenz, Datenräumen und europäischer Regulierung weiter an Fahrt gewinnen. Unternehmen, die sich aktiv in diesen Dialog einbringen, prägen nicht nur die öffentliche Wahrnehmung, sondern leisten auch einen Beitrag dazu, dass digitale Souveränität langfristig als Standard verstanden wird – und nicht als kurzfristiger Trend. •

DER AUTOR

Christoph Fabian

ist Kommunikationsberater bei We.Communications mit Schwerpunkt auf Technologie-, und Digitalisierungsthemen. Er begleitet Unternehmen bei der strategischen Positionierung zu Cloud-Infrastruktur, Compliance, Cybersecurity und digitaler Souveränität.

DO'S & DON'TS
DER KOMMUNIKATION ZU DIGITALER SOUVERÄNITÄT

Do's

- Mit konkreten Use-Cases arbeiten: Praxisbeispiele aus Branchen oder Anwendungen machen digitale Souveränität verständlich und greifbar.
- Juristische Begriffe korrekt einsetzen: Präzise und kontextgerecht formulieren, um Kompetenz und Glaubwürdigkeit zu stärken.
- Positive Leitbilder nutzen: Visionen und Zukunftsbilder kommunizieren, die Orientierung geben und Chancen aufzeigen.
- Klare Begriffsabgrenzungen formulieren: Etwa um „Sovereignty Washing" verständlich und differenziert zu erklären.

Dont's

- Keine überzogenen Versprechen: Nur kommunizieren, was r ealistisch erreichbar ist; digitale Souveränität ist ein Prozess, kein kurzfristiges Ziel.
- Keine unbelegten Aussagen: Claims und Vorteile immer mit Daten, Beispielen oder externen Quellen untermauern.
- Nicht mit Technik-Jargon überfrachten: Zu viele technische Details schrecken Zielgruppen ab, die das Thema politisch, strategisch oder wirtschaftlich betrachten.
- Komplexität nicht übervereinfachen: Zu starke Vereinfachungen führen zu falschen Erwartungen und unpräzisen Botschaften. Das Thema braucht Klarheit – aber auch Genauigkeit.

Strategien für mehr Kontrolle Europas in der Cloud

Für europäische Unternehmen stellt sich dringlicher denn je die Frage nach digitaler Souveränität. Ein Gespräch mit Prof. Dr. Iris Lorscheid, Professorin für Digital Business und Data Science, über den US Cloud Act, strukturelle Abhängigkeiten und einen Cloud-Fahrplan für die digitale Souveränität für Europa. /// von Konstantin Pfliegl

DATEN SIND DAS RÜCKGRAT DER DIGITALEN WERTSCHÖPFUNG – UND SIE WANDERN IN RASANTEM TEMPO IN DIE CLOUD. Für europäische Unternehmen stellt sich damit die Frage nach digitaler Souveränität: Wie behalten wir die Kontrolle über sensible Informationen, kritische Geschäftsprozesse und Schlüsseltechnologien, ohne die Innovationsvorteile globaler Plattformen zu verlieren? Im Interview sprechen wir darüber mit Prof. Dr. Iris Lorscheid, Professorin für Digital Business und Data Science an der University of Europe for Applied Sciences (UE). Sie ordnet ein, wie Unternehmen Souveränität erreichen können. Wie viel Souveränität ist heute realistisch, was kostet sie, und wo liegt der Sweet Spot zwischen Regulierung, Risiko und Tempo der digitalen Transformation?

Frau Prof. Dr. Lorscheid, welche konkreten strukturellen Abhängigkeiten entstehen denn Ihrer Ansicht nach in globalen Cloud-Ökosystemen – also den großen Hyperscalern wie Amazon, Google oder Microsoft?

Prof. Dr. Iris Lorscheid | Daten von AWS, Google Cloud oder Microsoft Azure können zwar in Rechenzentren innerhalb der EU beziehungsweise Deutschlands liegen, unterliegen aber bei diesen US-Anbietern zusätzlich dem US-Recht, sodass US-Behörden unter bestimmten Bedingungen auch auf Daten in europäischen Rechenzentren zugreifen können. Damit können juristische Zugriffsmöglichkeiten entstehen, die mit europäischen Datenschutzlogiken kollidieren. Das bedeutet nicht automatisch Missbrauch – aber es verschiebt die letztliche Verfügungsmacht über Daten. Wenn zentrale Verwaltungsprozesse, Energieinfrastrukturen, Gesundheitsdaten oder KI-Trainingsumgebungen auf wenigen Plattformen laufen, entsteht eine systemische Konzentration. In stabilen Zeiten ist das effizient. In geopolitisch angespannten Situationen kann es jedoch die eigene Handlungsfähigkeit einschränken.

Bei der digitalen Souveränität Europas wird ja vor allem über den US Cloud Act diskutiert. Das US-Gesetz sagt doch schon einiges über die realen Machtverhältnisse im digitalen Raum aus, oder?

IL | Der US Cloud Act ist ein sichtbares Symptom der bestehenden Machtverhältnisse im digitalen Raum. Er macht deutlich, dass die großen Cloud-Anbieter global agieren, aber nationalem Recht unterliegen. Unternehmen wie Amazon, Google oder Microsoft sind privatwirtschaftliche Akteure – zugleich unterstehen sie der Rechtsordnung ihres Herkunftslandes.

Daraus ergibt sich eine strukturelle Spannung: Digitale Infrastrukturen sind global vernetzt, staatliche Souveränität bleibt jedoch territorial organisiert.

Der US Cloud Act verdeutlicht daher, dass wirtschaftliche Dominanz und rechtliche Zugriffsmöglichkeiten zusammenfallen können. Wer die zentralen Infrastrukturen betreibt, steht zugleich im Einflussbereich eines bestimmten Rechtssystems. Das ist kein ungewöhnliches Prinzip – jeder Staat beansprucht rechtliche Zuständigkeit für „seine“ Unternehmen.

DIE GESPRÄCHSPARTNERIN

Prof. Dr. Iris Lorscheid

ist Dekanin der Wirtschaftsfakultät und Professorin für Digital Business und Data Science an der University of Europe for Applied Sciences (UE).

Bild: University of Europe for Applied Sciences (UE)

Sichtbar wird hier jedoch die Asymmetrie: Europa nutzt in großem Umfang Infrastrukturen, die außerhalb seiner eigenen Rechtsordnung verankert sind. Der US Cloud Act ist daher ein Ausdruck dieser Konstellation. Er zeigt, dass digitale Souveränität nicht nur eine Datenschutzfrage ist, sondern eine Frage infrastruktureller und juristischer Verfügungsgewalt.

Aber ist Europa hier nicht schlicht schon viel zu weit abgehängt und ohne Regulierung funktioniert es nicht mehr?

IL | Europa ist technologisch nicht führend bei globalen Cloud-Plattformen – aber „abgehängt" impliziert Alternativlosigkeit. Und genau das halte ich für problematisch. Digitale Souveränität ist kein Zustand, den man entweder vollständig besitzt oder verloren hat. Sie ist ein kontinuierlicher Prozess zwischen Marktkräften, technologischer Entwicklung und Politik. Europa verfügt über erhebliche regulatorische Gestaltungsmacht, über starke industrielle Kerne, über Forschungskapazitäten und über einen großen Binnenmarkt. Das sind keine trivialen Ressourcen.

Was sollte Europa also tun?

IL | Regulierung ist in diesem Kontext notwendig – aber nicht hinreichend. Sie schafft Verlässlichkeit, Rechtssicherheit und Mindeststandards. Ohne Regulierung würde Europa seine normative und rechtliche Position verlieren. Aber Regulierung allein ersetzt keine eigene Infrastruktur, keine Investitionen in Halbleiter, keine leistungsfähigen Cloud-Alternativen und keine Skalierung von KI-Unternehmen. Es braucht also industriepolitische Maßnahmen, Kapitalzugang und technologische Kompetenz.

Die eigentliche Frage ist nicht, ob Europa „zu spät" ist, sondern ob es gelingt, seine Stärken erfolgreich strategisch zu bündeln. Souveränität entsteht nicht durch Rückzug aus globalen Märkten, sondern durch die Fähigkeit, in ihnen eigenständig gestaltend mitzuwirken.

Doch wenn es etwa um KI geht, dann kommt man um die Angebote der Großen aus den USA kaum herum. Wie soll Europa es schaffen, seine Abhängigkeiten zu reduzieren, ohne seine Innovationsfähigkeit zu verlieren?

IL | Es stimmt: Im Bereich KI sind die großen US-Cloud-Anbieter derzeit technologisch führend. Sie stellen nicht nur Rechenleistung bereit, sondern integrierte KI-Ökosysteme – von spezialisierten Chips über Trainingsinfrastruktur bis hin zu Foundation Models, Entwicklungsumgebungen und produktionsreifen APIs. Wer KI-Systeme heute skaliert einsetzen möchte, bewegt sich häufig innerhalb dieser integrierten Plattformarchitekturen. Diese Innovationsgeschwindigkeit kann Europa kurzfristig kaum replizieren. Gerade deshalb wäre eine vollständige Abkopplung zu diesem Zeitpunkt weder realistisch noch sinnvoll. Die Herausforderung besteht daher jetzt nicht darin, bestehende Infrastrukturen zu meiden, sondern die spezifischen Abhängigkeiten von KI-Systemen strategisch zu managen.

Wie würde Ihr Cloud-Fahrplan für digitale Souveränität aussehen? Welche konkreten Schritte sollte Europa in den kommenden fünf Jahren gehen?

IL | Mein Cloud-Fahrplan für die nächsten fünf Jahre umfasst drei Prioritäten:

1. **Infrastruktur konsequent aufbauen:** Europa braucht eigene, skalierbare Rechenzentrums- und KI-Kapazitäten. Dazu gehören leistungsfähige Rechenzentren, spezialisierte KI-Chips, Edge-Infrastrukturen und industrielle Cloud-Kapazitäten.
2. **Souveräne KI und industrielle Wertschöpfung stärken:** KI ist ein wichtiger Faktor in der Cloud-Abhängigkeit. Europa sollte gezielt in eigene Basismodelle, Trainingskapazitäten und industrielle KI-Anwendungen investieren – insbesondere für sicherheitskritische und wissensintensive Branchen. Der strategische Fokus sollte auf einer leistungsfähigen Industrial-AI-Cloud unter europäischem Recht liegen.
3. **Regulierung mit Skalierung verbinden:** Regeln allein schaffen keine Souveränität. Europa muss Regulierung innovationsfähig gestalten, bürokratische Hürden für KMU reduzieren und öffentliche Beschaffung gezielt als Hebel einsetzen, um europäischen Anbietern Marktzugang und Skalierung zu ermöglichen.

Europa muss nicht autark sein – aber in der Lage, Kooperationen aus einer Position eigener Stärke heraus zu gestalten und nicht vollständig von externen Entscheidungen abhängig zu sein. Souverän ist nicht, wer sich abschottet, sondern wer auch in globalen Abhängigkeiten selbstbestimmt handeln kann. •

„ Der US Cloud Act zeigt, dass **digitale Souveränität nicht nur eine Datenschutzfrage ist**, sondern eine Frage infrastruktureller und juristischer Verfügungsgewalt. *Prof. Dr. Iris Lorscheid*

MEHR ERFAHREN …

Lesen Sie das ausführliche Interview mit Prof. Dr. Iris Lorscheid auf der Webseite von DIGITAL BUSINESS.

Kommunikative Täuschung

Europa feiert Souveränität – und bleibt abhängig. Die AWS Sovereign Cloud in Brandenburg, die KI-Fabrik in München, das Google AI Center in Berlin: Was nach Aufbruch klingt, kommt aus den USA und unterliegt den dortigen Gesetzen. Bernd Korz, CEO von alugha, ordnet ein – und zeigt, wie Unternehmen echte digitale Resilienz aufbauen können.

/// von Bernd Korz

WENN DIE POLITIK DIGITALE SOUVERÄNITÄT FEIERT, LOHNT SICH EIN BLICK AUF DAS KLEINGEDRUCKTE. In Brandenburg entsteht die sogenannte Sovereign Cloud von Amazon Web Services. In München plant die Bundesregierung eine KI-Fabrik als Teil der europäischen KI-Offensive. Und Google eröffnet an der Museumsinsel in Berlin ein KI-Zentrum für Wissenschaft, Wirtschaft - und Politik. Das alles klingt nach Aufbruch – verdient aber vor allem eine ehrliche Einordnung.

Die AWS Sovereign Cloud wird auf deutschem Boden stehen. Betrieben wird sie von einem US-Konzern, der dem CLOUD Act unterliegt: US-Behörden können unter bestimmten Bedingungen Zugriff auf dort gespeicherte Daten verlangen – unabhängig davon, wo der Server physisch steht. Souverän ist daran vor allem das Label. Und in München? Die KI-Fabrik soll auf Nvidia-GPUs laufen. Die Wertschöpfung bei den entscheidenden Komponenten – Chips, Modelle, Trainingsdaten – findet außerhalb Europas statt. Was entsteht, ist ein Rechenzentrum. Was nicht entsteht, ist technologische Eigenständigkeit. Und Google? Sucht in Berlin noch einmal die Nähe zur Politik, mir scheint das allzu offensichtlich.

Das ist kein Vorwurf an die beteiligten Unternehmen. Es ist ein Vorwurf an eine politische Kommunikation, die Abhängigkeit als Souveränität verpackt – und hofft, dass niemand genauer hinschaut.

Wo die eigentliche Abhängigkeit liegt

Wer als Unternehmensentscheider verstehen will, wie exponiert die eigene IT-Infrastruktur tatsächlich ist, muss vier Dimensionen in den Blick nehmen.

- Erstens:
  Cloud-Infrastruktur. AWS, Microsoft Azure und Google Cloud dominieren den europäischen Markt. Wer dort Anwendungen aufbaut, bindet sich an proprietäre Schnittstellen, Datenformate und Preismodelle. Ein Anbieterwechsel ist theoretisch möglich – in der Praxis aber so aufwändig, dass er selten stattfindet. Das ist kein Zufall, sondern Geschäftsmodell.
- Zweitens:
  Hardware und Halbleiter. Die modernsten Chips kommen von TSMC, Samsung und Nvidia. Der European Chips Act soll Europas Fertigungskapazität stärken, doch selbst optimistische Szenarien sehen erste relevante Ergebnisse frühestens Ende dieses Jahrzehnts. Bis dahin bleibt Europa bei der zentralen Ressource der digitalen Wirtschaft auf Importe angewiesen.
- Drittens:
  Künstliche Intelligenz. Die dominierenden generativen KI-Modelle stammen von OpenAI, Google und Meta. Europa hat mit Mistral AI einen vielversprechenden Akteur, doch das Ökosystem ist noch überschaubar. Wer heute KI einsetzt, nutzt meist Technologie, deren

DER AUTOR
Bernd Korz
ist CEO von alugha.

Entwicklung und Governance außerhalb europäischer Jurisdiktion liegt.

- Viertens:
  Softwareplattformen. Von Microsoft 365 über Salesforce bis Slack – die digitalen Werkzeuge, mit denen europäische Unternehmen täglich arbeiten, stammen überwiegend aus den USA. Die Abhängigkeit ist oft so selbstverständlich geworden, dass sie gar nicht mehr als solche wahrgenommen wird.

Was die Politik tut – und was sie nicht tut

Brüssel hat das Problem erkannt. Der Digital Markets Act begrenzt Plattformmacht. Der AI Act reguliert den KI-Einsatz. Der Chips Act fördert Halbleiterproduktion. GAIA-X sollte europäische Cloud-Standards schaffen – und ist bisher weitgehend hinter den Erwartungen zurückgeblieben.

Das strukturelle Problem dahinter: Regulierung schafft Spielregeln, aber keine Spieler. Europa reguliert Technologie, die andere bauen. Das ist wichtig – reicht aber nicht. Solange industriepolitische Programme primär auf internationalen Technologien aufsetzen, entsteht bestenfalls kontrollierte Abhängigkeit. Keine Unabhängigkeit.

Berlin feiert jedes neue Rechenzentrum als Standorterfolg. Aber ein AWS-Rechenzentrum auf deutschem Boden macht Europa nicht souveräner – es macht den Standort attraktiver für den Anbieter. Das ist ein Unterschied, den die politische Kommunikation gerne verwischt. Und wenn im Behördenumfeld dann KI-Lösungen zum Einsatz kommen sollen, die auf genau diesen Infrastrukturen basieren, stellt sich die Frage: Wem dient das eigentlich – dem Bürger oder dem Anbieter?

Resilienz aufbauen:
Was Unternehmen konkret tun können

Die gute Nachricht: Unternehmen müssen nicht auf die nächste politische Initiative warten. Digitale Resilienz lässt sich heute aufbauen – pragmatisch, schrittweise und ohne ideologischen Überbau.

Der wichtigste Hebel ist die Architektur. Wer modulare Systeme mit standardisierten Schnittstellen und portablen Datenformaten baut, kann einzelne Komponenten austauschen, ohne das Gesamtsystem zu gefährden. Das klingt nach Lehrbuch – ist aber gelebte Praxis in Unternehmen, die ihre IT strategisch denken. So haben wir es bei alugha von Beginn an gemacht - und sind heute komplett unabhängig.

Multi-Cloud-Strategien verteilen Workloads auf mehrere Anbieter und senken das Lock-in-Risiko. Dabei sind europäische Alternativen längst keine Notlösung mehr: Hetzner, OVH oder Exoscale bieten technisch ausgereifte Infrastruktur mit echter DSGVO-Konformität – nicht die marketingtauglich verpackte Variante eines US-Anbieters mit Rechenzentrum in Frankfurt.

Bei KI gilt ein ähnliches Prinzip. Wer vollständig auf externe Modelle setzt, gibt Kontrolle über Daten und Prozesse ab. Der pragmatische Weg: externe Modelle für unkritische Anwendungen nutzen, europäische Alternativen wie Mistral AI einbeziehen und gleichzeitig eigene Kompetenz aufbauen. Bei alugha setzen wir bewusst auf einen vollständigen EU-Stack – von Hetzner über Exoscale bis Mistral AI. Nicht weil es der bequemste Weg ist, sondern weil wir unseren Kunden echte Datenhoheit bieten wollen, nicht nur ein Compliance-Versprechen.

Open Source spielt dabei eine Schlüsselrolle. Offene Datenbanken, containerbasierte Infrastrukturen und standardisierte Schnittstellen reduzieren Lock-in-Effekte und schaffen die Basis für technologische Beweglichkeit.

> ” Das strukturelle Problem: Regulierung schafft Spielregeln, aber keine Spieler. Europa reguliert Technologie, die andere bauen. Das ist wichtig – reicht aber nicht. Solange industriepolitische Programme primär auf internationalen Technologien aufsetzen, entsteht bestenfalls **kontrollierte Abhängigkeit**. Keine Unabhängigkeit.
>
> *Bernd Korz*

Souveränität ist eine Managementaufgabe

Digitale Souveränität entsteht nicht durch Pressemitteilungen aus Ministerien und nicht durch Rechenzentren mit dem richtigen Länderkürzel. Sie ist eine strategische Managementaufgabe – unbequem, komplex und ohne politischen Applaus.

Wer seine Abhängigkeiten kennt, kann sie steuern. Wer sie ignoriert, wird zum Spielball geopolitischer Verschiebungen. Die politische Bühne liefert dafür gerade ein lehrreiches Schauspiel: Souveränität wird versprochen, Abhängigkeit verwaltet. Unternehmen, die es ernst meinen, sollten nicht auf den nächsten Gipfel warten – sondern ihre digitale Resilienz als das behandeln, was sie ist: eine Überlebensfrage. •

Wer ohne KI auswählt, WÄHLT SCHLECHTER?

KI-optimierte Bewerbungen treffen auf manuelle Auswahlprozesse. Das muss kein Risiko sein – wenn Unternehmen Technologie gezielt als Unterstützung einsetzen. KI ist kein Ersatz für menschliche Entscheidungen, sondern ein Werkzeug, das Auswahl strukturierter, transparenter und nachvollziehbarer machen kann. /// von Gianluca Winkel

EIN FIKTIVES EXTREMBEISPIEL:
Auf eine Remote-Stelle im Marketing gehen 300 Bewerbungen in drei Tagen ein. Formal überzeugend, sauber strukturiert, präzise formuliert. Viele Profile wirken erstaunlich professionell. Der Grund ist offensichtlich: Bewerber nutzen heute KI.

So weit, so legitim. Das Problem beginnt bei der Frage, wie Unternehmen darauf reagieren. Wenn Bewerbungen KI-optimiert sind, während Auswahlprozesse rein manuell bleiben, entsteht eine technologische Asymmetrie: Auf Kandidatenseite werden Werkzeuge selbstverständlich genutzt, auf Unternehmensseite häufig nicht.

Doch daraus folgt kein Zwang zur Automatisierung um jeden Preis. Entscheidend ist vielmehr, KI bewusst als unterstützendes Instrument einzusetzen – dort, wo sie Struktur schafft, ohne Verantwortung zu übernehmen.

Recruiting leidet heute weniger unter Talentmangel als unter wachsender Komplexität. Auswahlarchitekturen, die für geringere Volumina entwickelt wurden, stoßen an Grenzen. Genau hier kann KI sinnvoll entlasten.

Technologische Asymmetrie

Wenn Bewerber KI zur Optimierung ihrer Unterlagennutzen, Unternehmen aber ausschließlich auf manuelle Sichtung setzen, entsteht ein Ungleichgewicht. KI kann helfen, diese Lücke zu schließen – nicht indem sie entscheidet, sondern indem sie Transparenz und Struktur schafft.

Das eigentliche Risiko ist Qualitätsverlust
Hohe Bewerbungszahlen sind kein Ärgernis, sondern Ausdruck eines offenen Marktes. Zum strategischen Risiko werden sie erst dann, wenn Auswahl unter Zeitdruck erfolgt und Vergleichbarkeit fehlt. Jede Verzögerung verlängert die Time-to-Hire. Jede Fehlentscheidung erhöht Fluktuationskosten. Jede Überforderung im Team kann die Entscheidungsqualität senken.

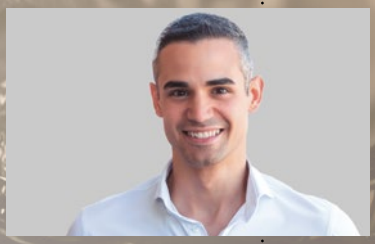
Recruiter arbeiten unter hohem Erwartungsdruck. Aufmerksamkeit wird zur knappen Ressource. Subjektive Eindrücke gewinnen an Gewicht, wenn strukturierte Vergleichsmaßstäbe fehlen. Das ist kein Vorwurf an HR, sondern ein Systemproblem.

Wenn Volumen steigt und Profile homogener werden, braucht Auswahl eine neue Logik. Nicht mehr Dokumente lesen, sondern Informationen strukturieren. Nicht mehr Keywords zählen, sondern Kompetenzen nachvollziehbar vergleichen. Genau hier kann KI produktiv unterstützen.

Fight Fire with Fire: Fünf Hebel zur Entlastung

1. **Unstrukturierte Daten in vergleichbare Profile überführen**
   KI kann Inhalte automatisch erfassen, vereinheitlichen und vergleichbar machen. Das reduziert manuelle Erfassungsarbeit und schafft eine belastbare Datengrundlage für weitere Schritte. Informationen aus CV, Anschreiben oder Profilen fließen konsistent in ein Gesamtbild ein. Recruiter gewinnen Zeit für qualitative Bewertung, Führungskräfte erhalten eine strukturierte Entscheidungsbasis.
2. **Kompetenzen statt Schlagworte bewerten**
   Keyword-Matching greift zu kurz. KI kann Inhalte semantisch analysieren und in Kompetenzmodelle überführen. Damit wird sichtbar, was jemand tatsächlich kann – auch wenn es anders formuliert ist als in der Stellenausschreibung.
   Wichtig ist dabei die bewusste Konfiguration: Anforderungen, Gewichtungen und Bewertungskriterien werden von Menschen definiert. KI übersetzt diese Kriterien in strukturierte Vergleichbarkeit. Das kann helfen, unbewusste Verzerrungen zu reduzieren, die bei rein subjektiver Sichtung entstehen.
3. **Priorisieren statt stapeln**
   KI kann Bewerbungen nach definierter Passung vorsortieren. Das bedeutet keine automatische Entscheidung, sondern eine strukturierte Reihenfolge für die Sichtung. Recruiter entscheiden weiterhin selbst, profitieren aber von einer nachvollziehbaren Priorisierung. Flexibilität ist entscheidend: Muss- und Kann-Kriterien lassen sich differenzieren, fachliche und ergänzende Aspekte getrennt betrachten. So entsteht eine dynamische Entscheidungsunterstützung statt eines starren Rankings.
4. **Entscheidungsgrundlagen transparent machen**
   Ein häufiger Vorbehalt gegenüber KI betrifft Bias und Intransparenz. Diese Sorge ist berechtigt, wenn Systeme unreflektiert eingesetzt werden. Moderne KI-Lösungen können jedoch offenlegen, welche Kriterien zu

DER AUTOR
Gianluca Winkel
ist Chief Technology Officer bei Rexx Systems und ein erfahrener Experte im Bereich Human Resources und Technologie.



einer Bewertung geführt haben. Bewertungen werden erklärbar, Abweichungen sichtbar.
Gerade Transparenz ist ein Hebel gegen Diskriminierung: Wenn Kriterien dokumentiert, überprüfbar und anpassbar sind, lassen sich Verzerrungen systematisch identifizieren und korrigieren. KI kann damit nicht nur Effizienz steigern, sondern auch zu mehr Nachvollziehbarkeit beitragen.

5. **Candidate Experience beschleunigen**
   Automatisierte Datenerfassung reduziert Hürden im Bewerbungsprozess. Bewerbende müssen Informationen nicht mehrfach eingeben, Prozesse werden klarer strukturiert. Schnellere Rückmeldungen und kürzere Durchlaufzeiten erhöhen Professionalität.
   Auch hier gilt: KI ersetzt keine Kommunikation. Sie schafft Freiräume, damit Recruiter sich stärker auf Dialog und Passung konzentrieren können.

Bias – Risiko und Chance

Algorithmen sind nicht per se neutral. Sie spiegeln die Daten und Kriterien wider, mit denen sie arbeiten. Der Unterschied: Während menschliche Vorurteile oft unbewusst bleiben, lassen sich algorithmische Kriterien prüfen, anpassen und auditieren. Richtig eingesetzt kann KI helfen, subjektive Verzerrungen zu reduzieren, statt sie zu verstärken.

Recruiting ist Infrastruktur

Unternehmen investieren selbstverständlich in Produktionssysteme, ERP, Marketingautomation oder Cybersecurity. Recruiting dagegen wird häufig noch als operative HR-Aufgabe betrachtet.

Dabei entscheidet die Qualität der Auswahl über Innovationskraft, Vertriebsstärke und Umsetzungsgeschwindigkeit. Eine überforderte Auswahl wirkt wie ein Engpass im gesamten Unternehmen. KI ist in diesem Kontext kein Zwang, sondern ein Werkzeug. Sie bringt Ordnung in Datenmengen, schafft Vergleichbarkeit und erhöht die Konsistenz von Entscheidungen. Sie ersetzt nicht die Menschen im Recruiting, sondern unterstützt sie dabei, fundierter und transparenter zu entscheiden.

Die zentrale Frage lautet daher nicht, ob KI Menschen ersetzt. Sondern wie sie so gestaltet wird, dass sie Menschen stärkt. •

» KI ist kein Zwang, sondern ein Werkzeug. Sie bringt Ordnung in Datenmengen, schafft Vergleichbarkeit und erhöht die Konsistenz von Entscheidungen. Sie ersetzt nicht die Menschen im Recruiting, sondern **unterstützt** sie dabei, fundierter und transparenter zu entscheiden.

Gianluca Winkel

Frauen EMPOWERN Frauen

Die IT-Welt wird noch immer von Männern dominiert. Frauen sehen sich insbesondere in solchen Branchen oft noch mit zahlreichen Karriere-Hindernissen konfrontiert. Sie brauchen eigenen Strategien zur Stärkung von Karriere und Netzwerken untereinander. /// von Barbara Liebermeister

IN DEN ZURÜCKLIEGENDEN JAHREN HAT SICH AUS FRAUENSICHT IM GROS DER UNTERNEHMEN VIELES ZUM POSITIVEN GEWANDELT. Trotzdem stehen Frauen im Berufsleben noch vor besonderen Herausforderungen. Insbesondere in männerdominierten Branchen und Berufen sowie auf höheren Führungsebenen erleben sie oft, dass sie sich stärker behaupten müssen als ihre männlichen Kollegen, um die gleiche Anerkennung zu erfahren und die dieselben Aufstiegschancen zu haben. Frauen, die es bereits geschafft haben und in ihren Unternehmen eine exponierte Position als Spezialistin oder Führungskraft innehaben, spielen beim Verändern dieser Situation eine zentrale Rolle, denn: Sie können andere Frauen bei ihrer Entwicklung unterstützen – fachlich, persönlich und strategisch.

Die Herausforderungen erkennen und benennen

Frauen sehen sich in der Arbeitswelt oft mit folgenden strukturellen und kulturellen Barrieren konfrontiert:

- Unbewusste Vorurteile (Unconscious Bias): Frauen werden häufig als weniger durchsetzungsstark sowie risiko- und technikaffin wahrgenommen (selbst, wenn sie einen Abschluss an einer technischen Universität erworben haben). Das wirkt sich negativ auf ihre Gestaltungsmöglichkeiten, ihren Karriereverlauf usw. aus.
- Fehlende Rollen-Vorbilder: In vielen Unternehmen fehlen sichtbare Frauen in Top-Positionen, die zum Beispiel jüngeren Kolleginnen als Vorbilder dienen können und ihre Zuversicht stärken „Auch ich schaffe es, wenn …".
- Vereinbarkeit von Beruf und Privatleben: In nicht wenigen Betrieben existieren zwar flexible Arbeitsmodelle und Work-Life-Balance-Konzepte auf dem Papier, ihre Wahrnehmung wird kulturell aber kaum unterstützt – insbesondere bei Personen, die in der Organisation Schlüsselpositionen innehaben.
- Netzwerkstrukturen: Viele informelle Netzwerke im Business-Bereich sind weiterhin männlich geprägt. Frauen haben deshalb oft nur einen eingeschränkten Zugang zu wichtigen Kontakten und Informationen.

Diese Hürden sollten Frauen in exponierten Positionen offen ansprechen, um in ihrem Umfeld ein Bewusstsein hierfür zu schaffen – auch damit ihre Kolleginnen die negativen Folgen hiervon nicht als eine Konsequenz persönlicher Defizite erfahren. Dies ist der erste Schritt in Richtung Veränderung.

Mentoring – gezielte Unterstützung und Empowerment

Ein wirksames Instrument, um Frauen zu empowern, ist Mentoring – also die unterstützende Begleitung von nachrückenden Fach- und Führungskräften durch erfahrene (Kollegen und) Kolleginnen.

Gute Mentorinnen

- teilen Wissen und Erfahrungen: Sie geben Einblicke in Unternehmensstrukturen, Entscheidungsprozesse und Karrierepfade.
- stärken das Selbstvertrauen: Gerade in herausfordernden Situationen hilft die Perspektive einer erfahrenen Mentorin oft, Rückschläge und Widerstände einzuordnen und sich neu zu fokussieren.
- öffnen Türen: Mentorinnen können Kontakte vermitteln, Empfehlungen aussprechen und Netzwerke zugänglich machen.

Außerdem stimulieren Mentoring-Beziehungen oft wechselseitige Lernprozesse, von denen auch die Mentorinnen profitieren – unter anderem, weil sich ihnen neue Perspektiven eröffnen, die ihren Horizont erweitern.

Digitalisierung als Chance zur Vernetzung und Sichtbarkeit

Die Digitalisierung eröffnet Frauen neue Möglichkeiten, sich zu vernetzen, zu lernen und sich zu positionieren:

- Online-Communities und Business-Plattformen wie LinkedIn und Xing ermöglichen den Austausch über Unternehmens- und Branchengrenzen hinweg. Frauen können dort ihre Expertise zeigen und sich wechselseitig sichtbar machen.
- Virtuelle Mentoring-Programme und Peer-Gruppen erlauben es, auch über Distanzen hinweg Wissen und Unterstützung zu teilen – besonders wertvoll ist dies in dezentral organisierten und internationalen Unternehmen.
- Digitale Weiterbildungsangebote erleichtern den Zugang zu neuem Know-how – beispielsweise zu den Themen Leadership, KI-Nutzung, Kommunikation und Selbstmanagement.

Durch eine aktive digitale Präsenz können Frauen sich gegenseitig stärken, gemeinsam Erfolge feiern und eine Kultur der wechselseitigen Wertschätzung in ihrem Umfeld etablieren.

DIE AUTORIN
Barbara Liebermeister
leitet das Institut für Führungskultur im digitalen Zeitalter (IFIDZ), Wiesbaden.

Frauenförderung als Teil der Unternehmenskultur

Individuelle Initiativen haben meist nicht die Kraft, Organisationen nachhaltig zu verändern, sofern sie nicht auf eine für Veränderungen offene Unternehmenskultur stoßen. Frauen in Führungspositionen können hier als Change-Agents bzw. -Treiber fungieren, indem sie

- Diversity-Programme mitgestalten und weiterentwickeln,
- transparente Beförderungs- und Vergütungsprozesse einfordern,
- eine inklusive Führung vorleben und
- Männer als Verbündete in dem Prozess gewinnen, Gleichstellung nicht als reines „Frauenthema", sondern als strategischer Erfolgsfaktor von Unternehmen zu begreifen.

Mehr Frauen-Power und Solidarität im Betrieb

Frauen, die in Unternehmen eine exponierte Position in Unternehmen innehaben und folglich auch Einfluss haben, tragen – nicht selten unbewusst und teils auch ungewollt – eine doppelte Verantwortung und zwar für den eigenen Erfolg und den Erfolg anderer Frauen in ihrer Organisation.

Indem sie sich mit diesen vernetzen und sich wechselseitig inspirieren und fördern, entsteht eine Bewegung, die Strukturen verändert:

- Die Digitalisierung bietet hierfür wertvolle Tools,
- das Mentoring schafft den erforderlichen persönlichen Rahmen und
- das aktive Networking die nötige Solidarität und emotionale Unterstützung.

Echte Gleichstellung kann man Organisationen nicht verordnen. Sie wächst durch das Engagement von Frauen für (sich selbst und für) andere Frauen – und die Bereitschaft von Männern sich ihrer „Unconscious Bias", also unbewussten Vorurteile bewusst zu werden, und ihre gewohnten Reiz-Reaktionsmuster zu verändern. •

SPONSORSHIP STATT NUR MENTORING

10 Moves, die Kolleginnen sofort sichtbarer machen

Mentoring berät, Sponsorship befördert: Sponsorinnen und Sponsoren nutzen aktiv ihren Einfluss, um Kolleginnen Chancen, Bühnen und Credits zu verschaffen.
Diese 10 Moves lassen sich sofort starten:

1. Echo mit Attribution:
Wiederholen Sie Beiträge von Kolleginnen im Meeting und nennen Sie explizit den Ursprung („Anknüpfend an den Punkt von Frau X …").

2. Sichtbarkeits-Slots teilen:
Geben Sie bei Präsentationen/Panel-Slots Co-Speakerinnen die Bühne – ideal: 5–10 Minuten Abschnitt mit klarer Verantwortlichkeit.

3. „Office Housework" umverteilen:
Protokoll, Orga, Care-Aufgaben rotieren – strategische Aufgaben (P&L, Architektur, KI-Piloten) gezielt an Kolleginnen vergeben.

4. Warm Intro pro Woche:
Stellen Sie Kolleginnen jede Woche aktiv einer Schlüsselperson vor (Kunde, Vorstand, Gremium) – mit kurzer, starker Positionierung.

5. Stretch Assignments absichern:
Vereinbaren Sie Ziel, Ressourcen, Schutz vor Ad-hoc-Tasks und eine Sponsor-Review nach 30/60 Tagen.

6. Credits sichtbar machen:
In Mails, Projektsteckbriefen und Townhalls: Leistung und Ownership namentlich zuordnen.

7. Diverse Shortlists erzwingen:
Für Rollen/Projekte konsequent mehr als eine qualifizierte Kandidatin shortlisten; Auswahlkriterien vorab schriftlich fixieren.

8. LinkedIn/Internes Netz boosten:
Mindestens zweimal pro Monat Beiträge oder Ergebnisse einer Kollegin fachlich kommentiert teilen.

9. Moderations- und Entscheidungsrollen rotieren:
Sitzungsleitung, Gremien-Stellvertretungen, Lenkungskreise turnusmäßig mit Kolleginnen besetzen.

10. Sponsorship-OKR setzen:
Zwei Kolleginnen 2–3 messbare Chancen eröffnen (z. B. Projektleitung, Kunden-Pitch, Konferenz-Slot); Wirkung tracken (Einladungen, Beförderung, NPS).

Studien zeigen, dass fehlende Fürsprache und „Broken Rung" (erste Beförderung) zentrale Hürden sind. Sponsorship schließt diese Lücke – „Mentors talk with you. Sponsors talk about you."

Künstliche Intelligenz in der Klinik:

Vom Datenstau zum Smart Hospital

Wie kommen Kliniken aus dem Digitalstau – und was bringt KI heute schon messbar? Zukunftsforscher Nils Müller von Trendone* erklärt, warum alles mit Datenqualität und Interoperabilität beginnt, welche Partnerschaften den Durchbruch ermöglichen und wie „Human-in-the-Loop" Ärzte und Pflege spürbar entlastet. /// von Heiner Sieger

Wie arbeitet ein Trendforscher eigentlich mit Kliniken zusammen, – und woran erkennt man belastbare Zukunftsbilder statt Hype?
Nils Müller | Trendforschung hat drei Ebenen. Erstens der inhaltliche Blick: Wir beobachten ein Trenduniversum aus 18 Megatrends und rund 120 Makrotrends. Zweitens die Methode, mit der Unternehmen Zukunft handhabbar machen – Foresight: Szenarien, Backcasting, Forecasting, Trendradars und Milestone Planning verankern Trends in Strategie- und Innovationsarbeit. Drittens die Future Literacy: die Fähigkeit, im Unternehmen über Zukunft sprechen, priorisieren und entscheiden zu können. Wer diese drei Ebenen zusammenführt, macht aus Hype konkrete Roadmaps. Das gilt für Kliniken genauso wie für Unternehmen.

Wo steht KI in deutschen Kliniken heute – und welches Missverständnis begegnet Ihnen am häufigsten?
NM | Es gibt Leuchttürme wie die Charité oder Häuser in NRW, Bayern, der Schweiz und Österreich. Aber der Mainstream ist stark hierarchisch und bürokratisch organisiert. Das sichert Ordnung, kostet aber Innovationskraft – und das ist gefährlich, weil träge Prozesse in der Versorgung reale Risiken erzeugen. Das häufigste Missverständnis: Man könne ohne solide Datenbasis „einfach KI einführen". Ohne integrierte, zugängliche Daten bleibt jede KI-Pilotierung Stückwerk.

Können Sie die Lücke zwischen Anspruch und Klinikalltag an einem Beispiel illustrieren?
NM | Nehmen wir einen zentralen Bereich, die Patient Journey: Menschen füllen dieselben Formulare mehrfach aus, Abteilungen drucken, scannen, übertragen. Es fehlt ein klinikweiter Data Lake, der Daten aus allen Bereichen vernetzt. Solange Informationen in Silos liegen, entstehen Medienbrüche, Fehler und Wartezeiten – für Patienten, Pflege und Ärzte frustrierend und teuer.

Wo liegen schnelle Hebel – was funktioniert heute schon besser?
NM | Ein echter Fortschritt ist, dass moderne Datenmodelle auch unstrukturierte Daten verarbeiten. In einem Data Lake können Bild-, Text-, Audio- oder Sensordaten gemeinsam nutzbar gemacht werden. Darauf lassen sich interoperable Anwendungen und KI-Modelle aufsetzen. Diese technische Basis macht fachliche Innovation erst möglich.

Auf Sicht von zehn Jahren: Welche technologischen, gesellschaftlichen und wirtschaftlichen Entwicklungen prägen das Gesundheitswesen am stärksten?
NM | Drei Bewegungen treiben den Wandel. Erstens Prävention: ganzheitliche, kontinuierliche Gesundheitsvorsorge statt reiner Akutmedizin. Zweitens Personalisierung: Diagnostik, Therapie und Services werden datengetrieben individuell. Drittens DIY-Healthcare: Patientinnen und Patienten nutzen verlässliche Informationen, Wearables und KI-Agenten zur Selbststeuerung – vor, während und nach einem Klinikaufenthalt. Der größte Effekt entsteht an den Schnittstellen: Wenn Systeme, Akteure und Daten übergreifend zusammenspielen.

Was bedeutet das konkret für Klinikverantwortliche?
NM | Vernetzung wird zur Kernkompetenz. Innovation entsteht nicht im Silo, sondern entlang der durchgängigen Patient Journey – von der Zuweisung über Diagnostik und Therapie bis Reha und Nachsorge. Wer diese Kette digital schließt, hebt Qualität,Tempo und Effizienz zugleich.

Welche drei Prioritäten gehören in den nächsten 12–24 Monaten ganz oben auf die Agenda, um KI wirksam und sicher nutzbar zu machen?
NM | Erstens Governance: Der CTO gehört ins Board. IT ist keine Serviceabteilung mehr, sondern strategischer Taktgeber und muss Investitionen und Prioritäten mitbestimmen. Zweitens Datenfundament: Interoperable Architektur, ein klinikweiter Data Lake, saubere Schnittstellen und klare Datenrechte. Drittens fokussierte Use Cases: Nicht „KI überall", sondern wenige, gut definierte Anwendungsfälle mit klinischem Nutzen, die Skalierung ermöglichen.

***DER GESPRÄCHSPARTNER**

Nils Müller

ist Gründer und CEO von TRENDONE, einem der führenden Institute für Trendforschung und Corporate Foresight im deutschsprachigen Raum. Er unterstützt Unternehmen dabei, technologische Entwicklungen früh zu erkennen und in umsetzbare Strategien zu übersetzen – als Berater und internationaler Keynote-Speaker mit Fokus auf KI, Healthcare und Smart Hospital.

> „Human-in-the-Loop" heißt, Menschen behalten die Entscheidungshoheit, KI entlastet von Routinen, steigert Qualität und gibt Zeit am Patientenbett zurück. Das spürt das Team schnell – wenn die ersten **Quick Wins** sichtbar sind. *Nils Müller*

Viele Kliniken schreiben rote Zahlen. Womit starten, wenn Ressourcen knapp sind?

NM | Mit Maßnahmen, die medizinischen Nutzen und Effizienz gleichzeitig liefern. Kurzfristig kostet das, mittelfristig amortisiert es sich. Die Digitalisierung von Patienten- und ÄrzteJourney, automatisierte Dokumentation, Termin- und Bettensteuerung oder Radiologie-Workflows sparen Zeit und Kosten – und verbessern die Versorgung.

Sie sagen: „Alles beginnt mit Daten." Welche ersten Schritte sichern deren saubere Erfassung am Point of Care?

NM | Drei Basics: erstens Standards und Schnittstellen definieren, zweitens Systemverträge so gestalten, dass die Klinik Daten rechtssicher nutzen darf, drittens möglichst viele relevante Datenquellen in den Data Lake integrieren – klinische, administrative und patientenseitige. Ohne diese Rechte- und Architekturarbeit blockieren Sie spätere KI-Projekte.

Stichwort „Build vs. Buy": Welche Rolle spielen Partnerschaften mit Start-ups und MedTech – und mit welchen Plattformen kommen Kliniken schneller voran?

NM | Hyperscaler wie Microsoft Azure oder AWS sind heute die Wachstumshubs für Health-Start-ups. Wer dort andockt, bekommt Zugang zu geprüften Lösungen, Security-Services und Skalierung. Viele Anbieter sind längst Scale-ups mit Tausenden Kunden – das reduziert Integrationsrisiken und Time-to-Value.

Wie finden Kliniken die richtigen Partner – und wie klappt die Zusammenarbeit?

NM | Starten sollten sie mit einem Use-Case-Portfolio: Wo sind die größten Pain Points? Wo ist der schnellste klinische und wirtschaftliche Return? Daraus ergeben sich Top-Cases – und die passenden Anbieter. Meine Empfehlung an Klinikverantwortliche:

Nutzen Sie die Ökosysteme Ihrer Cloud-Partner, beteiligen Sie sich an Health-Innovation-Hubs, schauen Sie auf Referenzen anderer Kliniken und sprechen Sie früh mit potenziellen Partnern über Integration, Datenrechte und Governance.

Wo bleibt der Mensch? Wie gewinnen Kliniken Ärztinnen, Ärzte und Pflege für KI?

NM | Indem KI als Assistenzsystem verstanden wird: Augmented Doctor und Augmented Nurse. „Human-in-the-Loop" heißt, Menschen behalten die Entscheidungshoheit, KI entlastet von Routinen, steigert Qualität und gibt Zeit am Patientenbett zurück. Das spürt das Team schnell – wenn die ersten Quick Wins sichtbar sind.

Welche Quick Wins und Weiterbildungsformate haben sich bewährt, ohne den Betrieb zu stören?

NM | Es gibt Hunderte erprobte Use Cases in eHealth, Smart Hospital, Radiologie, Chirurgie oder Pflege – von automatisierter Dokumentation über Triage bis zu Bildanalyse und Robotik. Für die Qualifizierung funktionieren modulare Online-Formate, zum Beispiel „Learning Snacks" von zwei bis drei Stunden, für unterschiedliche Berufsgruppen sehr gut. Optimal ist, wenn HR und Geschäftsführung das kuratieren; wo das fehlt, helfen berufsständische Angebote und Stiftungen – oft kostenfrei.

Blicken wir ins Jahr 2035: Woran erkennt man das Krankenhaus der Zukunft – und was sollten Kliniken schon morgen dafür starten?

NM | Das Krankenhaus der Zukunft ist Teil einer Ecosystem Economy. Es orchestriert Partnerschaften – von Zuweiser-Netzwerken über Telemedizin bis zu Reha- und Homecare-Services – und wirkt wie eine Plattform, die Patientinnen und Patienten mit den richtigen Services verbindet. Zweite Säule ist die Automatisierung: administrative, klinische und physische Prozesse laufen durchgängig digital unterstützt. Starten sollten Kliniken morgen mit Partnerschaftskompetenz, Governance, Einkaufs- und Datenmodellen dafür, einem robusten Datenfundament und zwei bis drei skalierbaren KI-Use-Cases mit klaren Outcome-Kennzahlen. •

Vom Wollen zum Tun:

Eine Agenda für digitale Gesundheit

Uwe Heckert, T-Systems COO Health, skizziert die Systemagenda hinter Tempo und Technik: Interoperabilität statt Insellösungen, nutzerfreundliche Identitäten in der TI 2.0, FHIR-basierte Datenräume, souveräne Cloud und erklärbare KI. Mit Modellregionen, klaren KPIs und Resilienz sollen in 12 Monaten messbare Entlastungen entstehen – für Personal und Patienten. /// von Heiner Sieger

Wie bringen Sie Ihre bisherige Erfahrung im Gesundheitswesen in Ihre neue Rolle als COO Healthcare bei T-Systems ein – und worauf fokussieren Sie sich als erstes?
Uwe Heckert | Ich bin seit Mitte Januar 2026 als COO Healthcare bei T-Systems an Bord. Unser Portfolio reicht von Netzen, Security, Cloud und Systemintegration bis zu Branchenlösungen wie dem KIS iMedOne. Diese werden von Ärzten, Pflegenden, Krankenhäusern, Krankenversicherungen, also nahezu allen Beteiligten im deutschen Gesundheitssystem und darüber hinaus in Ländern wie Österreich, Schweiz, Spanien, Singapur, Südafrika oder Nordamerika genutzt. Für mich stehen drei Schwerpunkte im Fokus. Erstens: Radikale Kundenorientierung, beginnend bei Patientinnen und Patienten, Ärzteschaft und Pflege. Zweitens: stabile, skalierbare und resiliente Systeme, die Vertrauen schaffen. Drittens: Innovationen konsequent operationalisieren – Interoperabilität und KI mit klarem Nutzen im Arbeitsalltag.

Wie bewerten Sie den Status quo der Digitalisierung im deutschen Gesundheitswesen – und wo helfen Technologien kurzfristig?
UH | Das deutsche System ist im internationalen Vergleich eher durchschnittlich und steht unter immensem Druck. Die größten Schmerzpunkte sind: Fachkräftemangel, überbordende Dokumentation und extrem fragmentierte IT. Große Kliniken betreiben oft 500 bis 1.000 Applikationen, zusätzlich getrennt nach Sektoren. Das bremst Effizienz. Kurzfristige Hebel sind verlässliche, nutzerfreundliche digitale Identitäten, strukturierte Datenflüsse auf Basis von HL7 FHIR, Automatisierung in der Dokumentation sowie sichere, souveräne Cloud-Infrastrukturen. Technologien sind vorhanden – nun zählt Umsetzung mit Disziplin.

Wie stellen Sie sicher, dass die User Experience künftig wirklich Zeit zurückgibt an alle Stakeholder?
UH | Durch Zuhören und Co-Creation mit Ärztinnen und Ärzten, Pflege, Kassen und Patientinnen und Patienten. Unsere Leitprinzipien dabei sind: weniger Klicks, weniger Reibung, Interoperabilität und konsequente Prozessintegration. Wir müssen weg von Formularhölle und Doppelerfassung, hin zu Vorbefüllung, smarter Suche und klaren Workflows. KI muss Assistenz sein – etwa durch strukturierende Vorschläge in der Dokumentation oder Leitlinien-Checks im Schockraum – nicht zusätzliche Kontrolle. Resilienz ist für mich integrierter Teil der Nutzererfahrung: Systeme müssen im Alltag und im Krisenfall laufen. Der Berliner Stromausfall war da ein Weckruf.

Die deutsche Gesundheitslandschaft hat eine große Achillesferse – sie ist sehr zerfasert. Wie holen Sie die vielen Akteure an einen Tisch – und beschleunigen sektorübergreifende Vorhaben?
UH | Die Einsicht ist grundsätzlich da: Wir geben in Deutschland weit mehr als 500 Milliarden Euro pro Jahr für das Gesundheitssystem aus. Das ist viel zu viel und gleichzeitig liegt die Lebenserwartung unter dem EU-Durchschnitt. Das muss sich ändern. Hebel sind Modellregionen mit klaren Use Cases, eindeutigen KPIs und einer starken Governance, die zu abgestimmten und damit kosteneffizienten und trotzdem leistungsfähigen Versorgungsangeboten führen. Länder wie Dänemark, Norwegen oder auch die baltischen Staaten zeigen, dass Standardisierung wirkt. Entscheidend ist die Haltung: Nicht alles kann besser werden, ohne irgendwo Abstriche zu machen. Die Telekom kann Sektoren verbinden und End-zu-End umsetzen – mit Partnern aus Versorgung, Kostenträgern, Industrie und Politik.

Was bedeutet das hochaktuelle und sensible Thema digitale Souveränität für Ihre Cloud- und Datenstrategie – auch mit Blick auf EHDS und Regulierung?
UH | Souveränität und Resilienz sind nicht verhandelbar. Europäische Cloud-Infrastrukturen, sichere Identitäten, Redundanz und technische Autonomie. Der EHDS ist eine große Chance, wenn Rollen, Interoperabilität und dezentrale Datenhaltung sauber geregelt sind. Beim EU AI Act braucht es Kohärenz mit der EU-Medizinprouktverordnung: Regulierung ja, aber ohne Doppelbelastung, die Zulassungen von ein bis zwei auf drei bis vier Jahre verlängert.

DER GESPRÄCHSPARTNER

Uwe Heckert

ist seit 16. Januar 2026 Chief Operating Officer Healthcare bei T-Systems (Deutsche Telekom). Zuvor verantwortete er bei Philips die DACH-Region und leitete europaweit Healthcare Informatics. Er kennt auch den europäischen Gesundheitsmarkt bestens als Vorsitzender des Health Executive Councils von Digitaleurope.

MEHR ERFAHREN ...

Lesen Sie das vollständige Interview und hören Sie den Podcast mit Uwe Heckert unter:

Vom Wollen zum Tun – eine Agenda für Digital Health

Sonst verlieren wir Tempo und Wettbewerbsfähigkeit. Unser Ziel ist, Sicherheit und Innovation zu verbinden – nicht gegeneinander auszuspielen.

Welche KI-Anwendungen sind im Gesundheitswesen heute sinnvoll – und wo ziehen Sie Grenzen?

UH | Bereits wirksam sind Dokumenten- und Reporting-Automatisierung, Entscheidungsunterstützung in Radiologie und auf Intensivstationen, Prognosen, Kapazitäts- und OP-Planung. Grenzen setzen wir bei vollautonomen Diagnosen und Therapien: Es fehlt zum einen oftmals eine durchgängige konsistente Datengrundlage. Zudem muss die finale Verantwortung immer beim Menschen bleiben. Wir bringen praxisnahe Assistenten in den Echtbetrieb – etwa für den Schockraum und Command-Center-Lösungen zur gezielten Patientensteuerung innerhalb einer Klinik. Ziel ist messbarer Zeitgewinn, nicht zusätzlicher Aufwand.

Security und Resilienz sind aber nach wie vor unterbelichtet. Was tun Sie konkret, um das zu ändern?

UH | Wir härten Infrastrukturen, indem wir Systeme konsolidieren und Redundanzen für eine stabile Systemlandschaft auch in kritischen Hochlastsituation aufbauen – inklusive souveräner Cloud-Set-ups. Wichtig sind durchgängige Sicherheitskonzepte, kontinuierliche Tests und klare Notfallprozesse. Es darf nicht vorkommen, dass Kliniken nach einem Cyber-Angriff zum Beispiel keine Operationen mehr durchführen können. Stabilität kommt zuerst, dann Skalierung – und immer mit Blick auf die Bedürfnisse der Kliniken. Unsere Industrial AI Cloud, die wir mit NVIDIA und Polarise aufgebaut in weniger als sechs Monaten aufgebraut haben, zeigt, dass wir schnell industrialisieren können – Tempo mit Qualität ist möglich.

Woran lassen Sie sich in zwölf Monaten messen – was wird konkret sichtbar sein?

UH | Erstens: Leuchtturmprojekte zur Daten- und Infrastrukturkonsolidierung – inklusive sicherer Cloud-Umgebungen. Zweitens: spürbare Fortschritte bei TI 2.0, vor allem nutzerfreundliche Identitätsplattformen mit weniger Supporttickets und höheren Nutzungsraten. Drittens: KI-Assistenten im Echtbetrieb – zum Beispiel Schockraum. Viertens: Projekte, die „digital vor ambulant vor stationär" in Modellregionen praktisch umsetzen. Fünftens: messbare Entlastungen bei Kosten und Zeit im Klinikalltag.

Zu guter Letzt: Was ist Ihnen persönlich am wichtigsten?

UH | Dass wir vom Wollen ins Tun kommen. Die Technologien sind reif, die Notwendigkeit ist offensichtlich. Standardisierung, Interoperabilität, Sicherheit – und der Mut, auch unbequeme Entscheidungen zu treffen. Nur so schaffen wir Tempo, echten Nutzen und Erleichterung für Patientinnen und Patienten, Ärzteschaft, Pflegende und Verwaltungsmitarbeitende. •

> „ Die Technologien sind reif, die Notwendigkeit ist offensichtlich. Standardisierung, Interoperabilität, Sicherheit – **und der Mut, auch unbequeme Entscheidungen zu treffen**.
>
> *Uwe Heckert*

Höchste Zeit für Post-Quantum-Kryptographie

Quantencomputer sind gleichermaßen Chance und Risiko für Datenschutz und Datensicherheit. Auch DSGVO und NIS2 zwingen Unternehmen, jetzt wirklich zu handeln. Drei Schritte führen zur Zukunftssicherheit: Krypto-Inventar erstellen, Risiken priorisieren und die Migration starten. /// von Sebastian Hausmann

CYBERKRIMINELLE NUTZEN BEREITS HEUTE DIE STRATEGIE „HARVEST NOW, DECRYPT LATER“: Das heißt, sie greifen bereits verschlüsselte Daten ab und lagern sie, um sie, sobald möglich, mit Quantencomputern zu entschlüsseln. Was nach Science-Fiction klingt, ist wissenschaftlich fundierte Realität: Eine aktuelle Studie rechnet damit, dass zwischen 2028 und 2033 Quantencomputer klassische Verschlüsselungsverfahren wie RSA oder ECC innerhalb von Tagen oder Wochen knacken können. Dieser Zeitpunkt wird als Q-Day bezeichnet – und er rückt schneller näher als gedacht.

Die Herausforderung für Unternehmen und Behörden: Viele sensible Informationen müssen Jahrzehnte lang vertraulich bleiben. Gesundheitsdaten, Forschungsergebnisse, Verträge, Produktdesigns – alle diese Daten sind bereits heute gefährdet. Gleichzeitig dauert die Umstellung auf quantensichere Verschlüsselung bei großen Unternehmen seine Zeit – zwölf bis 15 Jahre stehen im Raum. Die Rechnung ist einfach: Setzt man den erwarteten Q-Day in Relation zur voraussichtlichen Migrationsdauer – dann baut sich bereits heute enormer Handlungsdruck auf.

Compliance wird zur Pflicht

Die Lösung heißt Post-Quantum-Kryptographie (PQC): Diese neuen Verschlüsselungsverfahren basieren auf mathematischen Problemen, die auch Quantencomputer nicht in vertretbarer Zeit lösen können. Das US-amerikanische National Institute of Standards and Technology (NIST) hat 2024 drei PQC-Standards zertifiziert: FIPS 203, FIPS 204 und FIPS 205. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt diese Verfahren in der Technischen Richtlinie TR-02102-1 und fordert gemeinsam mit 21 europäischen Partnerbehörden Unternehmen auf, PQC bis spätestens 2030 zu etablieren. Um das zu erreichen, müssen deutsche Unternehmen noch Gas geben: Laut einer Studie zum „State of PQC readiness“ hinken 90 Prozent der Befragten noch hinterher. Im Februar 2026 hat die EU-Kommission vorgeschlagen, die PQC-Migration explizit auch in die NIS2-Richtlinie aufzunehmen.

DER AUTOR
Sebastian Hausmann
ist Senior Manager Solutions Engineering bei NetApp und unterstützt die Vertriebspartner bei technischen Themen. Er beschäftigt sich seit 20 Jahren mit Storage-Systemen, Servern und Rechenzentrumsbetrieb und ist auch im Channel aktiv.
Bild: NetApp

Die DSGVO verlangt bereits „dem Stand der Technik entsprechende" Datenschutzmaßnahmen – doch das ist immer auch Auslegungssache. PQC würde mit der Integration in NIS2 vom Nice-to-have zur Compliance-Pflicht. Für Unternehmen stellt sich nun – auch angesichts der drängenden Zeit – die Frage, wie konkret sie die Thematik angehen und Post-Quantum-Kryptographie etablieren sollen.

Zukunftssicherheit verspricht ein Vorgehen in drei Schritten:

Schritt 1:
Krypto-Inventar erstellen

Bevor Unternehmen handeln können, müssen sie wissen, wo sie überall Kryptographie einsetzen. Bei großen Organisationen kann diese Bestandsaufnahme mehrere Jahre dauern – ein Zeitfaktor, der einkalkuliert werden muss.

In der Praxis bildet eine zentrale Liste aller Systeme und Anwendungen die Grundlage: Erste Informationen liefern technische Dokumentationen und Sicherheitsrichtlinien, und auch Abteilungen wie IT, Entwicklung, HR und Einkauf verfügen über hilfreiches Detailwissen. Klare Zuständigkeiten und enge, crossfunktionale Zusammenarbeit beschleunigen Prozesse.

Schritt 2:
Risiken priorisieren

Nicht alle Daten sind gleich schutzbedürftig und gleichermaßen sensibel. Und nicht alle Systeme lassen sich gleichzeitig auf PQC umstellen. Unternehmen brauchen klare Prioritäten, damit sie ihre Aufwände richtig einteilen können. Ein Entscheidungskriterium ist die Schutzdauer: Wie lange müssen welche Daten vertraulich bleiben? Bei Gesundheitsdaten können das in Deutschland bis zu 30 Jahre sein, bei Verträgen zehn Jahre. Je länger die Schutzdauer, desto dringender ist die Migration auf PQC. Unterstützen kann ein PQC-Risikobewertungsmodell mit verschiedenen Kriterien, wie es die Finanzbranche entwickelt hat. Systeme mit langer Schutzdauer und hoher Kritikalität, aber niedrigem Migrationsaufwand sind zum Beispiel ideale Kandidaten für den Start.

Schritt 3:
Pilotprojekt im Storage starten

Der beste Einstieg in PQC ist ein Pilotprojekt im Speicherbereich. Hier lagern die meisten Unternehmensdaten, und moderne Storage-Systeme bieten bereits PQC-konforme Lösungen. Ein Pilotprojekt ermöglicht es, Erfahrungen zu sammeln, ohne die Produktion zu gefährden – und schnell sichtbare Resultate zu erzielen.

Verschlüsselung im Ruhezustand (data at rest) gilt als die letzte Verteidigungslinie. Selbst wenn Angreifer Netzwerk-Sicherheitsmaßnahmen überwinden, bleiben Daten im Storage geschützt. Hier hilft, dass es für die Erneuerung oder Aufrüstung von Storage-Systemen in praktisch allen Unternehmen etablierte Prozesse und Ansprechpartner gibt, im Zweifelsfall auf Partnerseite. Konkrete Schritte in diesem Zug können selbstverschlüsselnde Laufwerke mit PQC-Algorithmen sowie ein krypto-agiles Schlüsselmanagement sein. Ein überschaubares System für den PQC-Start – etwa ein internes Backup-System oder ein Datenarchiv – reduziert das Risiko. War das Pilotprojekt erfolgreich, lässt sich die Umstellung schrittweise auf andere Bereiche ausweiten.

Stolpersteine bei PQC vermeiden

Bei der Einführung von PQC lauern einige Fallen: Viele Unternehmen warten auf vermeintlich bessere Standards, obwohl die NIST-Standards bereits weltweit Anwendung finden. Weiter abzuwarten, erhöht das Risiko, denn dies verschiebt den Start der Migration nach hinten – Zeit, die am Ende fehlen wird. Eine weitere Fehlannahme ist, dass PQC nur ein IT-Projekt sei. Tatsächlich betrifft es das ganze Unternehmen. Datenschutz, Compliance, Einkauf und Fachabteilungen müssen von Anfang an eingebunden werden, sonst drohen Verzögerungen und Abstimmungsprobleme. PQC bedeutet mehr, als nur die Verschlüsselung auszutauschen. Es erfordert Anpassungen in Prozessen, Schulungen der Mitarbeiter und aktualisierte Notfallpläne.

Höchste Zeit, zu handeln

Die Umstellung auf Post-Quantum-Kryptographie ist eine strategische Notwendigkeit und Pflicht für Unternehmen, um sensible Daten langfristig zu schützen. Mit einem strukturierten Vorgehen in drei Schritten lässt sich die Herausforderung meistern: Krypto-Inventar erstellen, Risiken priorisieren und Pilotprojekt im Storage starten. Wer jetzt beginnt, gewinnt Zeit, vermeidet Hektik kurz vor dem Q-Day und sichert sich einen Wettbewerbsvorteil. Denn quantensichere IT wird künftig ein Qualitätsmerkmal sein, auf das Kunden, Partner und Aufsichtsbehörden achten werden. Die Bedrohung wartet nicht. Unternehmen sollten es auch nicht tun. •

„ PQC bedeutet mehr, als nur **die Verschlüsselung auszutauschen**. Es erfordert Anpassungen in Prozessen, Schulungen der Mitarbeiter und aktualisierte Notfallpläne.

Sebastian Hausmann

PQC: Der Countdown für Unternehmen läuft

Quantencomputer rücken immer näher – und die Gefahr für heutige IT-Verschlüsselungsalgorithmen wächst. Prof. Dr. Johannes Buchmann und Ismet Koyun zeigen, warum hybride Post-Quantum-Kryptografie jetzt zählt und skizzieren Wege zur Quantum-Readiness. /// von Konstantin Pfliegl

QUANTENCOMPUTER RÜCKEN IMMER NÄHER IN DEN PRAXISEINSATZ – mit deutlichen Folgen für die IT-Sicherheit. Viele gängige Verschlüsselungsverfahren werden dann angreifbar. Dazu kommt ein stilles Risiko: Daten können schon heute mitgeschnitten und später entschlüsselt werden – wenn Quantenrechner verfügbar sind, sogenannte HNDL-Angriffe (Harvest-now, decrypt-later). Die Antwort darauf heißt Post-Quantum-Kryptografie (PQC): neue Verfahren, die auch gegen Quantenangriffe schützen sollen.

Doch was heißt das konkret? DIGITAL BUSINESS spricht darüber mit Ismet Koyun und Prof. Dr. Johannes Buchmann. Ismet Koyun ist Gründer und CEO von Kobil, Prof. Dr. Buchmann ist ehemaliger Professor am Fachbereich Informatik der TU Darmstadt und einer der Begründer des Forschungsgebietes der Post-Quantum-Kryptographie.

Herr Koyun, Herr Prof. Dr. Buchmann, es ist nicht mehr die Frage ob, sondern wann Quantencomputing im großen Stil zur Verfügung steht. Wann schätzen Sie wird es soweit sein, dass herkömmliche Kryptografie-Methoden durch Quantencomputing im großen Stil gefährdet sind?
Prof. Dr. Johannes Buchmann | Eine konkrete Jahreszahl kann ich Ihnen nicht nennen, das wäre nicht seriös. Es gibt aber gerade in jüngerer Zeit technologische Fortschritte, die uns Quantencomputing näherbringen.
Ismet Koyun | Ein genaues Datum ist aktuell auch gar nicht so entscheidend. Sicher ist: Der Q-Day wird kommen.

Was sind denn aktuell die häufigsten Missverständnisse über PQC in Unternehmen? Sind sich Unternehmen der Gefahr und dem Handlungsdruck überhaupt bewusst?
Ismet Koyun | IT-Landschaften, die über Jahre oder Jahrzehnte gewachsen sind, lassen sich nicht auf Knopfdruck umbauen. Sorgfältige, strategische Planung ist wichtiger als überstürztes Handeln. Das Problem ist nur: Viele Organisationen wissen gar nicht genau, wo sie welche Kryptographieverfahren einsetzen. Kryptographie wird an allen möglichen Punkten benötigt. Zum Beispiel in Kommunikationsprotokollen, Cloud-Schnittstellen, mobilen Apps, Hardware-Sicherheitsmodulen, Identitätsabfragen oder in Public-Key-Infrastrukturen. Dazu kommen noch Komponenten von Partnern und Drittanbietern. Abhängigkeiten lassen sich nicht so einfach auflösen, vor allem nicht im laufenden Betrieb.

Für Unternehmen geht es zunächst also weniger darum, einzelne neue Algorithmen einzuführen. Quantum-Readiness beginnt stattdessen damit, die eigene Systemlandschaft inklusive Kryptographie vollständig zu erfassen und zu analysieren. Erst dann ist es möglich, Anpassungen vorausschauend einzuplanen, die sich in Zukunft ergeben können.

Welche PQC-Methoden gelten 2026 als solide Basis und welche Bereiche sollte man unbedingt schützen?
Prof. Dr. Johannes Buchmann | Geschützt werden müssen als erstes die Verbindungen, über die langfristig sensible Daten laufen und die sehr lange Wartungs- und Update-Intervalle haben. Die aktuell verbreiteten Verschlüsselungsverfahren wie RSA oder ECC stützen sich auf mathematische Aufgaben wie Primfaktorzerlegung und diskrete Logarithmen. Quantencomputer werden solche Aufgaben mithilfe des sogenannten Shor-Algorithmus effizient lösen können, das gilt in der Forschung als gesichert. Post-Quanten-Verfahren machen nichts grundlegend anderes. Sie verwenden aber mathematische Probleme, für die nach jetzigem Stand keine effizienten Lösungen bekannt sind, auch nicht mit Quantencomputern. Eine vielversprechende Variante ist beispielsweise die gitterbasierte Kryptographie.

Es gilt aber zu betonen: Post-Quantum-Kryptografie ist noch jung. Außerdem müssen wir Kompatibilität gewährleisten. Deshalb spricht viel für einen hybriden Ansatz, der neue quantensichere Methoden mit bewährten klassischen Verfahren kombiniert.

Wie stabil und ausgereift sind denn PQC-Standards inzwischen für den breiten Einsatz?

MEHR ERFAHREN ...

Lesen Sie das ausführliche Interview mit Ismet Koyun und Prof. Dr. Johannes Buchmann auf der Webseite von DIGITAL BUSINESS.

DIE GESPRÄCHSPARTNER

Ismet Koyun (l.)
ist Gründer und CEO von Kobil. Koyun setzt sich für die digitale Souveränität Europas ein.
Bild: Kobil Gruppe

Prof. Dr. Dr. h.c. Johannes Buchmann
ist Informatiker und Mathematiker sowie ehemaliger Professor am Fachbereich Informatik der TU Darmstadt. Er ist einer der Begründer des Forschungsgebietes der Post-Quantum-Kryptographie.
Bild: Katrin Binner Fotografie

Prof. Dr. Johannes Buchmann | 2024 hat das amerikanische National Institute of Standards and Technology (NIST) Standards für die Post-Quantum-Kryptographie veröffentlicht. Diese geben eine wichtige Orientierung. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezieht sie in die Entwicklung eigener Empfehlungen ein. Es existieren somit standardisierte Post-Quantum-Algorithmen, etwa für den Schlüsselaustausch und für digitale Signaturen. Bei Standards für Public-Key-Infrastrukturen und Protokolle gibt es Ansätze.

Herr Koyun, Ihr Unternehmen Kobil hat bekannt gegeben, dass es nun Quantum-ready ist. Wann war Ihnen klar, dass Sie dieses Thema unbedingt in Angriff nehmen müssen und wie lange dauerte die Umstellung?
Ismet Koyun | Wir haben den Handlungsbedarf schon früh erkannt. Nicht nur für uns selbst, sondern für alle Unternehmen, die langfristig sicheren Datenaustausch garantieren wollen. Als Anbieter von vielfach bewährten Sicherheitslösungen können und wollen wir bei der Quantenresistenz vorangehen. An unseren Erfahrungen mit der PQC-Einführung können sich andere Unternehmen orientieren. Und sie können bei Bedarf unsere Sicherheitsarchitektur als Basis ihrer Lösungen nutzen.

Die Umstellung konnten wir in vergleichsweiser kurzer Zeit realisieren. Das liegt zum einen daran, dass wir auf eine strukturierte und modulare Code-Basis zurückgreifen. Etwas, das für Quantum-Readiness unverzichtbar ist. Zum anderen wird auch deutlich, dass die standardisierten Algorithmen auf NIST-Basis mittlerweile so stabil sind, dass sie in realen Produkten eingesetzt werden können.

Kobil setzt auf einen hybriden Ansatz: Anstatt bestehende kryptografische Verfahren vollständig zu ersetzen, werden beim Verbindungsaufbau parallel klassische kryptografische Verfahren und Post-Quantum-Algorithmen eingesetzt. Welche Vorteile hat diese Lösung?
Prof. Dr. Johannes Buchmann | Der hybride Ansatz vereint beide Welten: jahrzehntelang bewährte Verschlüsselungsverfahren und die neuartigen PQC-Methoden. Innerhalb desselben kryptografischen Prozesses kommen beide Verfahren parallel zum Einsatz und tragen zum Beispiel zur Ableitung eines gemeinsamen Sitzungsschlüssels bei. Nur wenn beide Anteile gebrochen werden, ist der Schlüssel kompromittierbar. Das heißt: Der PQC-Anteil schützt vor Angriffen durch Quantencomputer. Sollte sich aber herausstellen, dass einzelne PQC-Verfahren schwächer sind als angenommen – was angesichts der fehlenden Erfahrungswerte durchaus passieren kann –, dann bleibt die klassische Kryptografie als zusätzlicher Sicherheitsanker erhalten.

Aber wie sicher ist eigentlich Post-Quantum-Kryptografie? Wie wahrscheinlich ist es, dass neue Angriffe einzelne Verfahren schwächen – und wie bleibt man flexibel?
Prof. Dr. Johannes Buchmann | Die Wahrheit ist: Wir wissen es nicht mit Sicherheit. Es ist nicht auszuschließen, dass Quantenrechner irgendwann mathematische Probleme lösen, die aktuell als nicht effizient lösbar gelten. PQC ist ein vergleichsweise junges Forschungsfeld. Ich gehe aber davon aus, dass die standardisierten Algorithmen auf absehbare Zeit Schutz bieten, weil sie international von vielen Forschungsgruppen untersucht wurden. •

Änderungen beim Omnibus der EU

Mehrheit der Unternehmen setzt Nachhaltigkeits-berichterstattung fort

Eine neue Studie von osapiens hat den Umgang europäischer Unternehmen mit den Änderungen beim Nachhaltigkeits-Omnibus untersucht. Demnach wollen 90 Prozent der Unternehmen in Europa, die künftig nicht mehr unter die Pflicht zur Nachhaltigkeits-berichterstattung fallen, dennoch weiterhin berichten. /// von Stefan Girschner

UNTERNEHMEN IN EUROPA ENTSCHEIDEN SICH MEHRHEITLICH DAFÜR, IHRE NACHHALTIGKEITSBERICHTERSTATTUNG FORTZUSETZEN – und das, obwohl sie durch das Omnibus-Vereinfachungspaket der EU von den verbindlichen Anforderungen befreit wurden. Laut der neuen Studie „Beyond Compliance: Sustainability Reporting After the Omnibus" von osapiens beabsichtigen 90 Prozent der Unternehmen, die von den CSRD-Berichtspflichten ausgenommen wurden, ihre Nachhaltigkeitsberichterstattung beizubehalten oder sogar auszuweiten. Die Ergebnisse deuten darauf hin, dass sich die Berichterstattung für viele Unternehmen von einer regulatorischen Verpflichtung zu einer grundlegenden Geschäftsfunktion entwickelt hat.

Von der Compliance zum Wettbewerbsvorteil

Nach dem Vereinfachungspaket Omnibus I der EU wurden viele Unternehmen aus dem unmittelbaren Anwendungsbereich formaler Berichtspflichten, etwa im Rahmen der Corporate Sustainability Reporting Directive (CSRD), ausgenommen. Doch auch wenn das Omnibus-Paket neu definiert, wer berichten muss, ändert es nichts daran, dass Nachhaltigkeitsrisiken gesteuert werden müssen.

Die Ergebnisse zeigen klar: Nachhaltigkeitsberichterstattung wird längst nicht mehr nur als regulatorische Pflicht verstanden. Sie ist vielmehr zu einem festen Bestandteil geworden, wie Organisationen Risiken managen, Kapital einsetzen und mit Investoren, Kunden und Partnern zusammenarbeiten.

Hier die wichtigsten Ergebnisse der Studie im Überblick:

- 90 Prozent der Unternehmen, die vom Geltungsbereich der CSRD ausgenommen sind, beabsichtigen, ihre Nachhaltigkeitsberichterstattung beizubehalten oder sogar auszuweiten.
- 86 Prozent der Unternehmen sind weiterhin zuversichtlich, dass sie Berichte erstellen können, die den CSRD-Standards entsprechen.
- 89 Prozent gehen davon aus, dass sie in den nächsten zwölf Monaten ihre Investitionen in Tools und Automatisierung für die Nachhaltigkeitsberichterstattung erhöhen werden.
- 90 Prozent geben an, dass die Nachhaltigkeitsberichterstattung bereits teilweise oder vollständig in die Finanzberichterstattungsprozesse integriert ist.

Alberto Zamora
ist Mitgründer und Co-CEO von osapiens.
Das Unternehmen bietet die Hyperscaler-Plattform HUB für Zusammenarbeit und KI-Automatisierung an, die über 25 Lösungen in den Kategorien Transparenz und Effizienz enthält.

> „ Unternehmen haben erkannt, dass **die Berichterstattung nicht mehr nur eine Compliance-Maßnahme ist**, sondern Teil ihres Verständnisses von Risiken, ihrer Kapitalallokation und eines nachhaltigen Wachstums. *Alberto Zamora*

Trotz dem Omnibus-Vereinfachungspaket der EU wollen 90 Prozent der befragten Unternehmen ihre Nachhaltigkeitsberichterstattung fortsetzen.

Die Unternehmen beziehen Nachhaltigkeitsdaten proaktiv bei folgenden Geschäftsentscheidungen ein: Betriebs- und Ressourcenplanung (53 Prozent), Innovation und Prozessgestaltung (48 Prozent), Finanzplanung und Investitionsentscheidungen (38 Prozent) sowie Risikobewertung der Lieferkette (38 Prozent). Jedes zweite befragte Unternehmen nannte die verbesserte Transparenz in Bezug auf Klima-, Lieferketten- und Betriebsrisiken als den wichtigsten Vorteil der Nachhaltigkeitsberichterstattung. Als weitere Vorteile wurden ein stärkeres Vertrauen der Investoren durch überprüfbare Informationen, die Erfüllung der Berichts- und Prüfungsanforderungen von Kunden und Partnern sowie eine bessere Integration von Finanz- und Nachhaltigkeitsentscheidungen genannt.

Das Paradoxon der Nachhaltigkeitsberichterstattung

Während 90 Prozent der befragten Unternehmen beabsichtigen, weiterhin zu berichten, erwarten 84,5 Prozent, dass die reduzierte Kontrolle der Behörden letztendlich dazu führen wird, dass weniger interne Ressourcen für die Nachhaltigkeitsberichterstattung bereitgestellt werden. Budgetbeschränkungen (43 Prozent), fragmentierte Datensysteme (41 Prozent), mangelhafte Technologie-/Systemintegration (31 Prozent) und unklare Zuständigkeiten (29 Prozent) wurden als die wichtigsten internen Hindernisse für die Aufrechterhaltung einer strukturierten Berichterstattung identifiziert.

Dies führt zu einem „Nachhaltigkeitsparadoxon", also einer hohen strategischen Anerkennung des Wertes der Berichterstattung bei gleichzeitig sinkender Ressourcenunterstützung. Die Ergebnisse deuten darauf hin, dass Automatisierung und zentralisiertes Datenmanagement für Unternehmen, die die Qualität ihrer Berichterstattung aufrechterhalten und gleichzeitig mit Ressourcenengpässen umgehen müssen, von entscheidender Bedeutung sein werden. Dies gilt umso mehr, als die regulatorische Fragmentierung im Rahmen der freiwilligen Berichterstattung zunimmt und Unternehmen sich mit mehreren Rahmenwerken wie VSME, CCF, GRI und ISSB auseinandersetzen müssen.

Präferenz für die Kontinuität der Berichterstattung

Andreas Rasche, Professor an der Copenhagen Business School, erläutert: „Die Ergebnisse zeigen eine klare Präferenz für die Kontinuität der Berichterstattung bei größeren Unternehmen, die im Rahmen des Omnibus-I-Pakets von der Berichtspflicht befreit wurden. Diese Entwicklung rückt freiwillige Berichterstattung und Strategien, die über die Compliance hinausgehen, fest in den Vordergrund der zukünftigen Nachhaltigkeitsagenda."

Alberto Zamora, Mitgründer und Co-CEO von osapiens, ergänzt: „In den letzten Jahren war die regulatorische Entwicklung weitgehend einseitig: mehr Anforderungen und mehr Unternehmen im Geltungsbereich. Das Omnibus-Paket hat diese Richtung geändert. Unsere Daten zeigen jedoch, dass Unternehmen nicht zurückweichen, wenn die Verpflichtung aufgehoben wird. Sie haben erkannt, dass die Berichterstattung nicht mehr nur eine Compliance-Maßnahme ist, sondern Teil ihres Verständnisses von Risiken, ihrer Kapitalallokation und ihres nachhaltigen Wachstums."

Zentrale Rolle für das Risikomanagement

Die Studie „Beyond Compliance: Sustainability Reporting After the Omnibus" von osapiens zeigt, dass die Nachhaltigkeitsberichterstattung auch bei geringem regulatorischem Druck weiterhin eine zentrale Rolle für das Risikomanagement und die Glaubwürdigkeit von Unternehmen spielt.

Die Berichterstattung wird zunehmend genutzt, um Finanzierungen zu sichern, Kunden- und Lieferkettenanforderungen zu erfüllen und Investitionen und Betriebsabläufe mit zuverlässigen Daten zu steuern – und wird damit zu einer Markterwartung und einem Wettbewerbsfaktor. •

Der unsichtbare Datenmarkt:

Unternehmen sollten ihre Datenstrategien überdenken

Datenbroker sammeln, verknüpfen und verkaufen Daten – aber kaum nachvollziehbar. Für Unternehmen heißt das: Jetzt hinschauen, bevor die Aufsicht es tut. Woher stammen zugekaufte Datensätze? /// von Melanie Ludolph

UNTERNEHMEN SPRECHEN HEUTE VIEL ÜBER DATENSTRATEGIEN: über First-Party-Data, KI-Training und datengetriebene Geschäftsmodelle. Die zentrale Frage lautet meist: Welche Daten haben wir – und wie können wir sie besser nutzen? Eine neue Studie des Europäischen Datenschutzausschusses lenkt den Blick auf eine andere Perspektive: den Markt der Datenbroker. Gemeint sind Unternehmen, die personenbezogene Daten aus unterschiedlichen Quellen sammeln, zusammenführen und weiterverkaufen. Der spannende Punkt der Studie liegt jedoch weniger in dieser Beobachtung. Dass es Datenbroker gibt, ist seit Jahren bekannt. Interessant ist vielmehr, warum sich die europäischen Datenschutzbehörden jetzt intensiver mit diesem Markt beschäftigen.

Ein Markt, den Regulierung erst verstehen muss

Der Markt für Datenbroker funktioniert anders als klassische Datenverarbeitung. Daten stammen aus unterschiedlichen Quellen, werden aggregiert, angereichert und mehrfach weitergegeben.

Für Außenstehende und häufig auch für die ursprünglichen Datensammler ist kaum nachvollziehbar, wo Informationen letztlich landen. Genau hier setzt die Studie an. Sie versucht nicht in erster Linie, rechtliche Antworten zu geben. Ihr Ziel ist es vielmehr, den Markt besser zu verstehen: Akteure zu identifizieren, Geschäftsmodelle zu analysieren und Datenflüsse sichtbar zu machen. Mit anderen Worten: Die Aufsichtsbehörden versuchen zunächst, eine Landkarte dieses Marktes zu zeichnen.

Vom Verständnis zum Enforcement

Solche Marktanalysen sind selten Selbstzweck. Wer einen Markt verstehen will, will ihn in der Regel auch regulieren können. Für Datenschutzbehörden bedeutet das: Erst wenn klar ist, welche Akteure beteiligt sind und wie Daten tatsächlich zirkulieren, lassen sich gezielte Untersuchungen oder koordinierte Verfahren führen. Die Studie könnte daher ein Hinweis darauf sein, dass Datenbroker künftig stärker in den Fokus der Aufsicht rücken. Der unsichtbare Datenmarkt zeigt damit ein typisches Muster der digitalen Wirtschaft: Daten werden längst gehandelt wie eine eigene Ressource – während Regulierung erst beginnt zu verstehen, wie dieser Markt tatsächlich funktioniert.

Warum Unternehmen das interessieren sollte

Für Unternehmen ist das mehr als eine akademische Debatte. Sie bewegen sich bewusst oder unbewusst bereits in diesem Ökosystem. Sie kaufen Marketingdaten ein, nutzen angereicherte Datensätze oder arbeiten mit Dienstleistern, die selbst Daten aus unterschiedlichen Quellen zusammenführen. Der Datenbroker-Markt ist damit längst Teil der digitalen Infrastruktur geworden. Die Studie deutet an, dass Datenschutzbehörden diesen Markt künftig genauer in den Blick nehmen könnten. Für Unternehmen bedeutet das vor allem eines: Datenstrategien enden selten an der eigenen Systemgrenze. Wer Daten einkauft oder mit externen Datensätzen arbeitet, bewegt sich immer auch in einem größeren Datenökosystem. Gerade deshalb lohnt sich ein genauerer Blick auf die Herkunft solcher Daten. •

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 Privatpersonen 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.

xSuite Group GmbH
Hamburger Str. 12
22926 Ahrensburg
+49 4102 88380
info@xsuite.com
www.xsuite.com

xSuite Group entwickelt und vermarktet Anwendungen zur Automatisierung dokumentenbasierter Geschäftsprozesse und ist Experte für die **Rechnungsverarbeitung mit SAP**, inkl. E-Invoicing, Auftragsmanagement und durchgängige **P2P-Prozesse**. Über 300.000 User verarbeiten mit xSuite mehr als 80 Mio. Dokumente pro Jahr. Die Lösungen werden in der Cloud und hybrid betrieben und sind für alle SAP-Umgebungen zertifiziert (ECC-Systeme, SAP S/4HANA, SAP S/4HANA Cloud, SAP Clean Core). Managed Services ergänzen das Angebot.

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
02

DIGITAL BUSINESS

03 2026

/// **Cyber Risk & Resilience**
Bedrohungslage
Im Bereich Business Email Compromise nehmen die Angriffe zu.Welche Defense-Mechanismen Unternehmen jetzt einsetzen müssen.

/// **Digital Health**
Rückstand
Viele deutsche Kliniken arbeiten noch immer mit fragmentierten Einzellösungen und hauseigenen Serverräumen.

/// **Tech & Future Systems**
Geschwindigkeit
Die Low-Code-„Programmierung“ etabliert sich als Innovationstreiber. Weniger komplexe Anwendungen lassen sich deutlich schneller generieren.

/// **Business Strategy & Innovation**
Zeitfresser
Wachsende Dokumentationspflichten (NIS2, ESG, CSRD) zwingen Unternehmen, Prozesse lückenlos nachzuweisen – ein riesiger Aufwand.

Die nächste Ausgabe erscheint am 10.06.2026

Erwähnte Unternehmen in dieser Ausgabe

Adlon, ADN Distribution, Allgeier Innovar, ams.Solution, Asseco Solutions, Azul, Bitfoemer, Box, BVDW, CADFEM, Cloudflare, ConSense GmbH, Deutsche Telekom, Fieldfisher, Forterro, Fortinet, Freshworks, Gebra-IT, IFIDZ, IFS, Kobil, NetApp, Osapiens, QuEra Computing, Rexx Systems, Rubrik, Schwarz Digits, ServiceNow, Telekom, Tenable, Trendone, T-Systems, TÜV Austria Gruppe, University of Europe for Applied Sciences, Vendosoft, Vier, WeCommunications, Wipro, Xentral

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:
Ralph Bachthaler, Ivana Bartoletti, Dr. Iris Bruns, Prof. Dr. Johannes Buchmann, Heather Ceylan, Christian Fabian, Carsten Fiegler, Dr. Christian T. Geiss, Max Giessler, Tommy Grosche, Sebastian Hausmann, Simon Hayward, Udo Hensen, Stefan Issing, Thomas Knorr, Tizian Kohler, Ismet Koyun, Barbara Liebermeister, Prof. Dr. Iris Lorscheid, Moritz Lukas, Melanie Ludolph, Björn Orth, Hermann Ramacher, Roger Scheer, Dr. Alexander Schellong, Maike Scholz, Jens Schulte, Frank Schwaak, Dr. Jan Seyfarth, Bennet Vogel, Ian Whiting, Gianlucca Winkel, Ulrich Zahner

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)

Abonnentenservice 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

Ausgabe: 02/2026
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, PlastXnow

Junior Mediaberater (m/w/d) gesucht – Gestalten Sie die Zukunft der Medien mit!
Unser Verlagshaus zählt zu den Pionieren und führenden Anbietern im Bereich der digitalen Transformation. Mit innovativen B2B-Medienmarken, die in ihren jeweiligen Branchen zur Spitzengruppe gehören, setzen wir Maßstäbe.

Zur Verstärkung unseres Teams suchen wir engagierte **Junior Mediaberater** (m/w/d) in Voll- oder Teilzeit.

Sie möchten Ihre Kreativität einbringen und aktiv zum Erfolg unserer Medienmarken beitragen? Dann freuen wir uns darauf, Sie kennenzulernen!

Wir freuen uns auf Ihre aussagekräftige Bewerbung unter
https://win-verlag.de/karriere/

WIN VERLAG


SCHWARZ
Souveräne digitale Lösungen schaffen,
statt auf andere zu warten.
Voraushandeln
www.voraushandeln.schwarz