03/2026 /// 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.: 203

SECURITY INSIGHT

COMPOSABLE ENTERPRISE

Bausteine statt Bollwerk

Wie Unternehmen den Umbau vom geschlossenen System zum offenen Ökosystem meistern

INTELLIGENT ENTERPRISE

KI in Geschäftsprozessen: Warum viele Initiativen scheitern und was Unternehmen anders machen müssen.

TECH & FUTURE SYSTEMS

Nach der technologischen Expansion stellt sich die Frage, ob Firmen ihre digitalen Ökosysteme noch beherrschen.

WORK & PEOPLE

Warum und wie Urteilskraft für Unternehmer und Entscheider zur wichtigsten Zukunftskompetenz wird.

Hier geht's zur aktuellen Ausgabe

Die nächste Ausgabe

Sonderheft Security

erscheint am 30. September 2026

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

EDITORIAL

Liebe Leserin, lieber Leser

• es gibt Momente, in denen sich gleich mehrere Entwicklungen so verdichten, dass aus einzelnen Trends ein Paradigmenwechsel wird. Genau an einem solchen Punkt stehen wir derzeit. Die Frage, wie Unternehmen ihre digitale Architektur aufstellen, ist keine rein technische mehr – sie entscheidet über Innovationsfähigkeit, Regulierungsfestigkeit und am Ende über Souveränität.

Monolithische Plattformen waren lange Zeit das Versprechen von Stabilität. Heute werden sie immer öfter zum Bollwerk gegen Veränderung. Wenn Prozesse, Daten und Entscheidungslogiken in proprietären Systemen verborgen bleiben, wird Transparenz teuer – und mit dem EU AI Act sogar zum Compliance-Risiko. Das **Composable Enterprise** dreht dieses Prinzip um: Statt geschlossener Festungen entstehen interoperable Bausteine aus Daten, Modellen, Agenten, Governance- und Orchestrierungsebenen. Erst diese Modularität schafft die Voraussetzung für verantwortungsvolle KI – ergänzt um den operativen Kontext, den **Process Intelligence** liefert. Denn ohne das Verständnis dafür, wie ein Unternehmen tatsächlich funktioniert, bleibt selbst die beste KI generisch. Responsible AI beginnt eben nicht bei Dokumentationspflichten, sondern bei der Architektur.

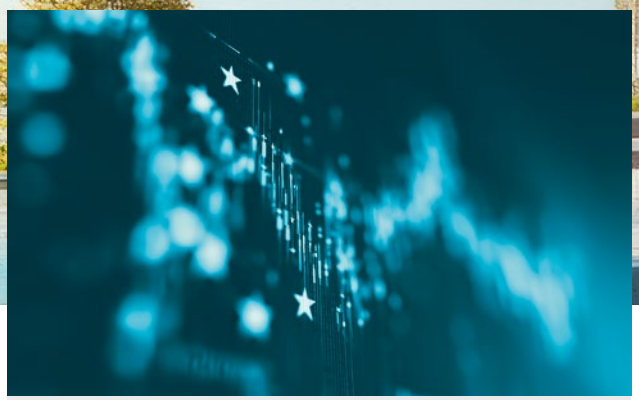
Dass diese Architekturfrage längst auch eine **geopolitische Dimension** hat, zeigt unser zweiter Schwerpunkt: **Digitale Souveränität.** Pandemie, gestörte Lieferketten und der Krieg in der Ukraine haben uns vor Augen geführt, wie verletzlich europäische Strukturen sind. Sieben der zehn wertvollsten Unternehmen der Welt sind KI-Firmen – Europa spielt darin faktisch keine wesentliche Rolle. Unsere Autorin Prof. Feiyu Xu plädiert deshalb für einen klaren **„Winning Plan“** statt risikofokussierter Defensive: hochkonzentrierte Investitionen in strategische Projekte nach dem Vorbild Airbus, eine ausbalancierte Make-Buy-Partner-Strategie und eine echte europäische Datenkultur.

Wie schwierig der Weg dorthin ist, beschreibt Prof. Michael Berthold mit erfrischender Nüchternheit: Vollständig souveräne Software ist in global verwobenen Open-Source-Ökosystemen kaum realisierbar. Die wirkliche **Alarmstufe Rot gilt den Daten** – Forschungsergebnisse, Archive, Trainingsdaten –, die im Ernstfall unwiederbringlich verloren gehen können. Souveränität muss also fallbasiert und differenziert gedacht werden.

Was das für Unternehmen konkret heißt, bringt Martin Merz von SAP auf den Punkt: Es reicht nicht, Server in Europa aufzustellen. Souveränität entsteht erst im Zusammenspiel von Daten-, Betriebs-, technischer und juristischer Ebene – über den gesamten Stack hinweg. Und sie braucht **Kooperation statt Abschottung.**

Was alle Beiträge eint: Die Zukunft gehört nicht den Festungen, sondern den anschlussfähigen Architekturen. Wer heute auf Bausteine setzt – technologisch wie geopolitisch –, schafft die Grundlage dafür, **im Ernstfall handlungsfähig zu bleiben**. Bollwerke schützen kurz. Bausteine tragen lang. •

Viel Spaß bei der Lektüre,
Ihr
HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS
heiner.sieger@win-verlag.de



SECURITY INSIGHT

DIGITAL BUSINESS

03 2026

Baukasten als Beschleuniger

Starres ERP bremst den Mittelstand. Was Microsoft Dynamics 365 als modularer Baukasten anders macht und worauf Entscheider dabei achten müssen. /// von Andreas Schneider-Lenhof

DER AUTOR
Armin Schneider-Lenhof
leitet das Marketing des Microsoft-Partners KUMAVISION AG.

> Eine gemeinsame Datenbasis reduziert den Integrationsaufwand strukturell, weil aufwändiges Datenmapping zwischen herstellerfremden Systemen entfällt. Insbesondere mittelständische Unternehmen können damit die Vorteile eines **modularen ERP-Systems** nutzen und die vier oben genannten Projektrisiken minimieren.
>
> *Armin Schneider-Lenhof*

Wenn das ERP zur Bremse wird

Um dem Investitionsstopp von Unternehmen entgegenzutreten, will ein mittelständischer Maschinenbauer sein Geschäftsmodell auf „Pay per Use" umstellen und parallel die Field Service-Dienstleistungen ausbauen. Die ERP-Software ist seit acht Jahren im Einsatz und stark individuell angepasst. Das Ergebnis: Jede Änderung kostet Monate, jedes Update wird zum Risikoprojekt, Pläne für die längst überfällige Migration in die Cloud liegen seit Jahren in der Schublade.

Dieses Szenario ist kein Einzelfall. In vielen mittelständischen Unternehmen ist die ERP-Landschaft zur Bremse geworden, ausgerechnet in einer Phase, in der dynamische Märkte, instabile Lieferketten, neue Wettbewerber und KI-gestützte Prozesse ein hohes Maß an Agilität und Anpassungsfähigkeit verlangen.

Composable ERP ist die strategische Antwort auf dieses Szenario: Statt eines monolithischen Gesamtsystems entsteht eine Architektur aus austauschbaren Bausteinen. Jede zentrale Geschäftsfunktion ist eine eigenständige Komponente, verbunden über standardisierte Schnittstellen. Die IT folgt der Strategie und nicht umgekehrt.

Wo scheitert Composable ERP im Mittelstand?

Der Composable-Ansatz eröffnet Vorteile wie mehr Flexibilität und kurze Reaktionszeiten, er ist allerdings nicht ohne Risiken. Unternehmen sollten diese vier Herausforderungen bei der Entscheidungsfindung berücksichtigen:

- **Integrationsaufwand:** Eine verfügbare API bedeutet noch keinen integrierten Prozess. Datenmapping, Fehlerhandling und Monitoring kosten Zeit und Know-how, Aufgaben, die in der Projektplanung regelmäßig unterschätzt werden.

MICROSOFT DYNAMICS 365:

Die pragmatische Composable ERP-Strategie für den Mittelstand

Composable ERP ist kein Selbstzweck, es ist die Antwort auf wachsenden Veränderungsdruck. Für den Mittelstand bietet Microsoft Dynamics 365 Business Central einen pragmatischen Einstieg: einen stabilen Kern, der modular wächst, ohne die Komplexität einer vollständig fragmentierten IT-Landschaft zu erzeugen. Der Weg dahin führt über klare Prinzipien: Standard nutzen, Erweiterungen bewusst auswählen, Daten konsequent zentrieren. Wer das konsequent umsetzt, gewinnt die erforderliche Agilität und Anpassungsfähigkeit.

WAS ENTSCHEIDET ÜBER DEN ERFOLG BEI DER EINFÜHRUNG EINES COMPOSABLE ERP?

Aus Projekterfahrung von KUMAVISION sind drei Faktoren für eine erfolgreiche Einführung von Microsoft Dynamics 365 ausschlaggebend:

Standard-first-Mindset:
Jede individuelle Code-Anpassung ist ein potenzielles Risiko bei künftigen Updates. Die Faustregel lautet: erst konfigurieren, dann Apps und Anwendungen nutzen, zuletzt entwickeln.

Klare Governance:
Wer verantwortet Schnittstellen, Stammdaten und App-Auswahl? Ohne definierte Zuständigkeiten entsteht eine Schatten-IT, auch mit einer Plattformlösung.

Automatisierte Tests:
Automatisierte End-to-End-Softwaretests sind kein Nice-to-Have, sondern Pflicht. Nur so bleibt eine Composable-Landschaft bei monatlichen Updates stabil. Bekommt eine Shopify-Integration ein Update, darf das weder die Zollabwicklung noch den Zahlungsprozess beeinträchtigen.

- **App-Wildwuchs:** Wer zu viele Drittanbieter-Apps kombiniert, erhöht Abhängigkeiten und Updaterisiken erheblich. Ohne aktives Abhängigkeitsmanagement wird die Composable-Landschaft selbst zum Stabilitätsproblem.
- **Stammdaten-Governance:** Ohne klare Datenverantwortung entstehen Silos zwischen den einzelnen Systemen. Die Frage „Wer pflegt welche Stammdaten und welches System ist führend?" muss vor der Implementierung beantwortet sein.
- **Updatefähigkeit:** Das Cloud-basierte Betreibermodell Software-as-a-Service (SaaS) mit monatlichen oder zumindest regelmäßigen Updates ist heute Standard. Ohne automatisierte Software- und Integrationstest wird jedes Update zum Risiko.

Wie setzt Microsoft Dynamics 365 diesen Composable Ansatz um? Und was macht Microsoft anders?
Microsoft stellt mit Business Central kein isoliertes ERP-System bereit, sondern die Technologieplattform Dynamics 365, die zahlreiche Bausteine für ein Composable ERP beinhaltet. Eine gemeinsame Datenbasis reduziert den Integrationsaufwand strukturell, weil aufwändiges Datenmapping zwischen herstellerfremden Systemen entfällt. Insbesondere mittelständische Unternehmen können damit die Vorteile eines modularen ERP-Systems nutzen und die vier oben genannten Projektrisiken minimieren.

Die ERP-Software Microsoft Dynamics 365 Business Central übernimmt dabei die Rolle des „Digital Core": Sie deckt die wesentlichen Kernprozesse – Finanzwesen, Einkauf, Lager und Logistik – in einem System ab und ist gleichzeitig offen für modulare Erweiterungen.

Q&A:

DIE HÄUFIGSTEN FRAGEN ZU COMPOSABLE ERP

Welche Anforderungen muss der Microsoft-Partner mitbringen?
Ein geeigneter Partner bringt mehr mit als reines ERP-Customizing. Entscheidend ist die Fähigkeit, eine belastbare Zielarchitektur für einen „Digital Core" plus Erweiterungen zu entwerfen und dauerhaft zu betreiben. Dazu gehören: Erfahrung mit Business Central sowie eine umfassende Kenntnis des Dynamics 365-Ökosystems in der Breite wie in der Tiefe. Zu den zentralen Anforderungen zählen Integrationskompetenz (APIs, Konnektoren, Fehlerhandling/Monitoring), Datenkompetenz (Dataverse-/Datenmodell-Verständnis, Stammdaten-Governance) sowie ein „Evergreen"-Betriebsansatz mit automatisierten Softwaretests. Ebenso wichtig: Beratungs- und Change-Kompetenz, um Fachbereiche auf Standardprozesse und Governance-Regeln auszurichten.

Was ist der Microsoft AppSource?
Der Microsoft AppSource ist der zentrale Marktplatz für Geschäftsanwendungen von Microsoft und zertifizierten Partnern. Man kann ihn sich wie einen „App Store" für Unternehmen vorstellen. Anstatt individuelle Anpassungen (Customizing) mühsam programmieren zu lassen, können Unternehmen hier vorgefertigte Erweiterungen (Apps) suchen, testen und direkt in ihre Business Central Umgebung integrieren. Die Bandbreite reicht von spezialisierten Branchenlösungen bis hin zu kleinen Tools für die automatisierte Rechnungsverarbeitung oder Anbindung von Versanddienstleistern.

Warum sind automatisierte Softwaretest unverzichtbar?
Ein Composable ERP besteht aus zahlreichen Modulen, die möglichst reibungslos ineinander greifen. Da Microsoft und Drittanbieter in kurzen Zyklen kontinuierliche Updates einspielen, ist eine manuelle Prüfung zeitlich nicht mehr leistbar. Eine Zahl aus der Praxis: Die ERP-Branchenlösungen von KUMAVISION durchlaufen bis zu 40.000 automatisierte Tests pro Tag. Automatisierte Softwaretests stellen sicher, dass Updates die Stabilität der Kernprozesse nicht beeinträchtigen. Besonders wichtig ist dabei, dass nicht einzelne Funktionalitäten, sondern End-to-End-Prozesse getestet werden,

die mehrere Anwendungen einbeziehen, beispielsweise Auftrag im Online-Shop, Verarbeitung im ERP, Auslieferung über Versanddienstleister, Versandstatus im CRM.

Welche Einschränkungen ergeben sich durch die Entscheidung für die Microsoft-Plattform?
Die Festlegung auf die Microsoft-Plattform bedeutet oft den Verzicht auf die absolute „Best-of-Breed"-Lösung in jeder Einzeldisziplin, da spezialisierte Nischenanbieter punktuell oft tiefere oder innovativere Funktionen bieten. Der Analyst Gartner positioniert Microsoft zwar als Leader (Cloud ERP for Product-Centric bzw. Service-Centric-Enterprises sowie Analytics and Business Intelligence Platforms), doch der wahre funktionale Vorteil liegt nicht zwingend in der Überlegenheit jeder einzelnen Funktion, sondern in der Synergie des gesamten Ökosystems.

Für den Mittelstand erweist sich dieser „Plattform-Kompromiss" meist als die wirtschaftlich naheliegende Wahl: Der Aufwand für die Integration und Wartung einer externen Drittlösung mit punktuell tieferen Spezialfunktionen, steht oft in keinem Verhältnis zum Nutzen. In einem integrierten Szenario entfallen komplexe Schnittstellenprobleme, Datenbrüche und zusätzliche Schulungsaufwände, was besonders im laufenden Betrieb zu einer höheren Gesamteffizienz führt. Die funktionale Einschränkung im Detail wird somit durch die Stabilität und Durchgängigkeit des Gesamtpakets von ERP über CRM bis hin zu Office mehr als kompensiert.

Besteht bei der Entscheidung für Microsoft ein „Vendor Lock-in"?
Die Sorge vor einer zu starken Abhängigkeit von einem einzelnen Anbieter (Vendor Lock-in) ist berechtigt, wird jedoch durch die offene Architektur der Microsoft-Plattform entschärft. Microsoft verfolgt keine geschlossene Welt, sondern setzt auf Offenheit durch Konnektoren und APIs.
In der Praxis zeigt sich diese Offenheit durch die Koexistenz mit anderen Marktführern: So gehören Integrationen zu Salesforce (für CRM-Prozesse) oder die Anbindung an SAP- und Oracle-Umgebungen (beispielsweise in Two-Tier-ERP-Szenarien wie Konzern/Landesgesellschaft) zum technologischen Standard. Das Risiko, dass der Anbieter ein Produkt einstellt oder Funktionalitäten streicht, besteht wie bei jedem Software-Anbieter. Angesichts von über 50.000 Unternehmen, die weltweit Business Central nutzen, ist dieses Risiko als gering zu betrachten.

Erweiterungsweg 1: ERP-Branchenlösungen
ERP-Anbieter wie bieten branchenspezifische ERP-Lösungen auf Basis von Microsoft Dynamics 365, die maßgeschneiderte Prozesse, Vorlagen und Auswertungen für unterschiedliche Branchen mitbringen. Dieser Best-Practice-Ansatz liefert letztlich ein vorkonfiguriertes Composable ERP, was die Einführungsdauer (Time-To-Value) verkürzt.

Erweiterungsweg 2: Apps aus Microsoft AppSource
Der Microsoft AppSource bietet vergleichbar mit dem Apple App Store bereits fertige Lösungen für zahlreiche Spezialanforderungen: Zollabwicklung, Shopify-Anbindung, Reisekostenmanagement, Zahlungsdienstleister, Sanktionslistenprüfung, Qualitätsmanagement und einige mehr. Diese Apps liegen technisch „neben" dem Kern. Das entschärft das Updaterisiko strukturell. Gleichzeitig können Fachbereiche Erweiterungen schnell und einfach testen.

Erweiterungsweg 3: Microsoft-Anwendungen
Das Dynamics 365-Ökosystem enthält zahlreiche Business-Anwendungen. Von CRM-Lösungen für Vertrieb, Marketing, Customer Service und Field Service über Business-Intelligence bis zu Teams, Outlook und Office sowie Künstlicher Intelligenz steht alles auf einer Plattform mit einer einheitlichen Datenbasis und einer einheitlichen Benutzeroberfläche bereit.

Erweiterungsweg 4: Power Platform als Integrationslayer
Power Automate verbindet Business Central mit externen Systemen, ohne dass dazu eine aufwändige Programmierung erforderlich wird. Ein typisches Szenario sieht so aus: Wird ein neuer Kunde im Business Central angelegt, erstellt Power Automate automatisch einen SharePoint-Ordner und sendet dann eine Teams-Benachrichtigung. Für Power Automate sind mehr als 1.400 vordefinierte, zertifizierte Konnektoren verfügbar, einschließlich ERP- und CRM-Systeme wie Dynamics 365, SAP und Salesforce.

Erweiterungsweg 5: Standard-APIs und Dataverse
Business Central liefert über 100 vorgefertigte REST-API-Endpunkte mit. Externe Systeme wie E-Commerce-Plattformen oder andere Business-Anwendungen lassen sich damit strukturiert anbinden. Über das Dataverse stehen ERP-Daten auch anderen Dynamics-365-Anwendungen wie Sales oder Field Service in Echtzeit zur Verfügung. Dataverse löst das Stammdaten-Problem an der Wurzel: Eine gemeinsame Datenbasis statt mühsam synchronisierter Silos. •

> „ Statt eines monolithischen Gesamtsystems entsteht eine **Architektur aus austauschbaren Bausteinen**. Jede zentrale Geschäftsfunktion ist eine eigenständige Komponente, verbunden über standardisierte Schnittstellen. Die IT folgt der Strategie und nicht umgekehrt. *A. Schneider-Lenhof*

Die teuerste Standardantwort in der IT? „Alles in die Cloud.“

Dass Microsoft im Juli die nächste Preiserhöhung für M365-Pläne durchführt, lässt viele CIOs nur müde nicken. Wieder teurer. Wieder neue Bundles. Wieder zusätzliche Funktionen, die mitbezahlt werden müssen – oder bisher enthaltene, die nun extra kosten. Dabei wäre jetzt ein guter Zeitpunkt, die eigene Microsoft-Strategie kritisch zu hinterfragen.
Es gibt schließlich Alternativen...

FELIX REICHLMAIR IST HEAD OF SALES BEIM MICROSOFT-DISTRIBUTOR MRM. Sein Team berät IT-Systemhäuser, die für ihre Kunden die beste Lizenzierung anfragen. Klassische Produktionsunternehmen jeder Größe, Gesundheitswesen und kommunale Einrichtungen sind typische Organisationen, für die MRM Distribution Microsoft-Alternativen durchrechnet, Empfehlungen ausspricht und gebrauchte Lizenzen vermittelt. Das darin enthaltene Sparpotenziale ist seiner Ansicht nach mit dem Cloud-Hype in Vergessenheit geraten „Die meisten Anwendungen erzeugen lokal betrieben deutlich geringere Gesamtkosten. Vor allem, wenn der Bedarf mit gebrauchten Microsoft-Lizenzen gedeckt wird“, erklärt der Lizenzmanager. Er hält große Stücke auf Software vom Zweitmarkt. „Einfach, weil das viel Geld spart und keinen Nachteil hat!“

Tatsächlich denken immer mehr Unternehmen um, seit klar ist: Preiserhöhungen sind bei M365 die Regel, nicht die Ausnahme. Die Möglichkeiten, die sie haben, wenn Vernetzung, Kollaboration oder remote Work eine zentrale Rolle spielen, fasst der Begriff „hybrides Microsoft-Modell“ zusammen. Eine breite Spielwiese, bei der ausgewählte Cloud-Dienste weiterhin über Microsoft 365 laufen. Für ressourcenintensive Fachanwendungen, Datenbanken oder klassische Serverstrukturen empfiehlt MRM dagegen, sie im eigenen Rechenzentrum zu belassen. In produzierenden Unternehmen betrifft das häufig lokal betriebene Windows-Server, SQL-Server oder Remote-Desktop-Umgebungen, die eng mit Maschinensteuerung, Warenwirtschaft oder Spezialsoftware verzahnt sind. In Kliniken und kommunalen Einrichtungen sind es eher Office, Exchange-, Datei- oder Archivserver – weil Mitarbeitende nicht in die Cloud müssen, weil die Systeme zuverlässig funktionieren und über Jahre kalkulierbar bleiben. In diesen und vielen weiteren Szenarien rechnen sich gebrauchte Microsoft-Lizenzen und längere Nutzungszyklen deutlich besser als permanente Subscription-Modelle.

„Deshalb“, betont Felix Reichlmair, „lohnt sich die Frage, die Unternehmen ihren IT-Dienstleistern bislang zu selten stellen: Warum eigentlich alles in die Cloud? Zwischen kompletter Migration und On-Prem-only existieren jede Menge wirtschaftlich sinnvollere Alternativen, die Kosten stabilisieren, Investitionen planbarer machen und moderne Zusammenarbeit ermöglichen. •

Mehr unter: mrm-distribution.com

Kontaktdaten

MRM Distribution GmbH & Co.KG |
info@mrm-distribution.com |
Tel: +49.89.2488 369-0

> „Unternehmen sollten Ihre IT-Dienstleister viel öfter nach den Alternativen zur Microsoft-Cloud fragen. Hybride Szenarien sparen einfach so viel Geld!
>
> *Felix Reichlmair, Head of Sales bei der MRM Distribution GmbH*

Bild/Copyright: @MRM Distribution

Composability: Basis für transparente KI

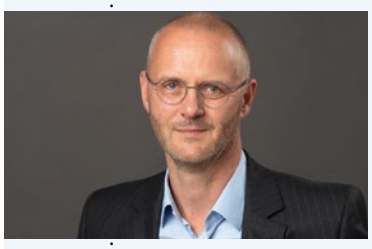
Mit dem EU AI Act wird die Diskussion um künstliche Intelligenz konkreter. Nach Jahren voller Visionen, Leitlinien und Experimente rückt nun eine deutlich pragmatischere Frage in den Mittelpunkt: Wie können Unternehmen KI so einsetzen, dass Entscheidungen nachvollziehbar, kontrollierbar und regulatorisch belastbar bleiben? /// von Rudy Kuhn

Darum geht's:

- Der EU AI Act zwingt Unternehmen, ihre KI-Systeme transparent und nachvollziehbar zu gestalten.
- Monolithische Systeme scheitern daran strukturell – nicht erst bei der Compliance, sondern bereits in der Architektur.
- Die Antwort: modulare (composable) KI-Systeme, ergänzt durch Process Intelligence als operativen Kontext.

GERADE IN EUROPA STEIGT DER DRUCK, MEHR TRANSPARENZ ÜBER KI-SYSTEME HERZUSTELLEN. Unternehmen müssen nachvollziehen können, welche Daten in automatisierte Entscheidungen einfließen, welche Systeme daran beteiligt sind und welche Auswirkungen diese Art der Entscheidungsfindung auf Kunden, Mitarbeitende oder Geschäftsprozesse hat. Mit dem EU AI Act wird dieser Transparenzgedanke nun zu einer gesetzlichen Anforderung.

Was auf den ersten Blick wie eine Compliance-Frage erscheint, ist bei genauerer Betrachtung eine Frage der Architektur.



DER AUTOR
Rudy Kuhn
ist Lead Evangelist bei Celonis.

Wenn Architektur zum Problem wird

Viele Unternehmen arbeiten entweder in fragmentierten IT-Landschaften, die durch Datensilos und redundante Strukturen gekennzeichnet sind, oder sie nutzen monolithische Plattformen. Dabei handelt es sich klassischerweise um Systeme oder Anwendungen, die als in sich geschlossene Einheit entwickelt und bereitgestellt werden. Zugehörige Komponenten wie Benutzeroberfläche und Datenbankzugriff sind dadurch eng miteinander verbunden, was das Deployment erleichtert, das Datenmanagement vereinfacht und Latenzzeiten reduziert.

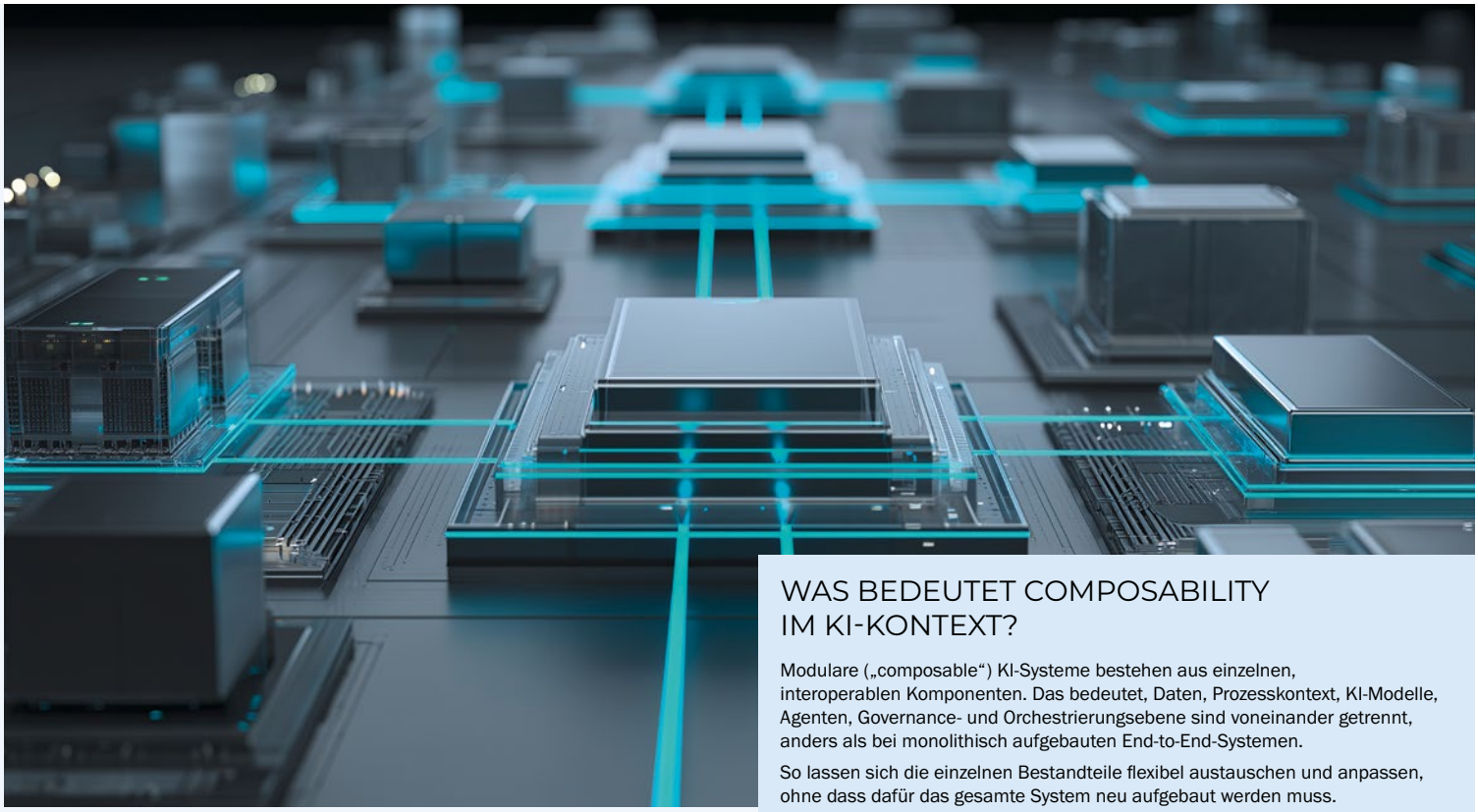
Zugleich entstehen dadurch neue Abhängigkeiten: Denn wenn Prozesse, Daten und Entscheidungslogiken in proprietären Systemen verborgen bleiben, wird Transparenz schwierig und Anpassungsfähigkeit teuer. Mit Blick auf die im AI Act definierten Transparenzanforderungen wird Compliance damit zu einer Frage architektonischer Entscheidungen.

Hinzu kommt der technologische und wirtschaftliche Veränderungsdruck: Unternehmen müssen neue KI-Anwendungen schneller integrieren, auf Marktveränderungen reagieren und bestehende Prozesse laufend anpassen können. Starre Architekturen werden in diesem Umfeld zunehmend zum Risiko, da sie Innovation verlangsamen und regulatorische Anpassungen erschweren.

Warum Composability an Bedeutung gewinnt

Genau hier wird Composability relevant. Dahinter steckt die Idee, technologische Fähigkeiten nicht in einer geschlossenen Plattform zu bündeln, sondern in klar getrennte, interoperable Bausteine aufzuteilen. Im KI-Kontext können diese aus Datenquellen, Kontextsystemen, Modellen, Agenten, Governance-Komponenten und Orchestrierung bestehen. Der Vorteil: Unternehmen können die einzelnen Teile flexibel austauschen oder erweitern, ohne jedes Mal das gesamte System neu aufbauen zu müssen.

> „ Process Intelligence schafft eine Informationsschicht, die alle Systeme und Ebenen eines Unternehmens miteinander verbindet. Auf diese Weise wird **sichtbar, wie Prozesse in der Realität tatsächlich ablaufen**, einschließlich Schwachstellen und potenziellen Engpässen. *Rudy Kuhn*



WAS BEDEUTET COMPOSABILITY IM KI-KONTEXT?

Modulare („composable“) KI-Systeme bestehen aus einzelnen, interoperablen Komponenten. Das bedeutet, Daten, Prozesskontext, KI-Modelle, Agenten, Governance- und Orchestrierungsebene sind voneinander getrennt, anders als bei monolithisch aufgebauten End-to-End-Systemen.

So lassen sich die einzelnen Bestandteile flexibel austauschen und anpassen, ohne dass dafür das gesamte System neu aufgebaut werden muss.
Eine zentrale Rolle spielt dabei die Orchestrierung: Auf dieser Ebene werden Regeln, Richtlinien, Identitäten und KPIs verankert, die sicherstellen, dass KI-Systeme kontrollierbar und regelkonform agieren.

Im Unterschied zu starren, integrierten Systemen ermöglicht ein modular aufgebautes System eine höhere Anpassungsfähigkeit an technologische und regulatorische Anforderungen. Governance wird dabei strukturell verankert und nicht nachgelagert ergänzt.

Eine Schlüsselrolle spielt dabei die Orchestrierungsebene, in der Regeln, Restriktionen, Identitäten, Eskalationsmechanismen und KPIs festgeschrieben werden. Diese Vorgaben stellen sicher, dass KI-Systeme nicht isoliert handeln, sondern sich innerhalb klar definierter Leitplanken bewegen. Die strukturelle Verankerung dieser Aspekte in der Systemarchitektur macht Entscheidungen der KI nachvollziehbar und transparent.

Warum KI ohne Kontext scheitert

Doch eine modulare Architektur allein löst noch nicht das zentrale Problem vieler KI-Initiativen: fehlender Geschäftskontext. Denn mit dem Verständnis dafür, wie ein Unternehmen tatsächlich funktioniert, steht und fällt der Erfolg jedes KI-Projekts. So können beispielsweise Sprachmodelle eigenständig fehlerfreie Inhalte generieren und zeitaufwendige Aufgaben automatisieren. Allerdings sind ihre Ergebnisse oft generisch, unvollständig oder nicht belastbar. In der Praxis liegt genau hier eine zentrale Schwachstelle: Relevante Informationen sind häufig über diverse Systeme und Abteilungen verteilt und nicht ausreichend miteinander verknüpft. Daher stehen sie KI-Anwendungen nicht in der notwendigen Qualität, Aktualität oder Einordnung zur Verfügung.

Process Intelligence schließt diese Lücke. Basierend auf der Technologie des Process Minings analysiert sie digitale Spuren aus ERP-, CRM-, Supply-Chain- oder Service-Systemen und reichert die Daten mit unternehmensspezifischem Kontext an. Dies können etwa Business-KPIs, Benchmarks oder bestimmte Policies sein. So schafft Process Intelligence eine Informationsschicht, die alle Systeme und Ebenen eines Unternehmens miteinander verbindet. Auf diese Weise wird sichtbar, wie Prozesse in der Realität tatsächlich ablaufen, einschließlich Schwachstellen und potenziellen Engpässen. Gleichzeitig verschafft Process Intelligence KI dadurch Zugriff auf den operativen Kontext, den sie braucht, um relevante Ergebnisse zu erzielen.

Zahlreiche internationale Studien zeigen, dass ein erheblicher Teil aller KI-Projekte daran scheitert, echten Mehrwert zu erzeugen oder über Pilotphasen hinaus zu skalieren. Forrester prognostizierte in seinen Predictions 2026 bereits im November 2025, dass Process Intelligence rund 30 Prozent dieser gescheiterten Projekte retten könnte.

Verantwortungsvoller KI-Einsatz beginnt bei der Architektur

Unternehmen sollten deshalb auf offene Schnittstellen, eine klare Trennung von Modellen, Kontext und Governance sowie eine starke Orchestrierung setzen. Process Intelligence ergänzt diese Architektur um den operativen Kontext, der für belastbare und nachvollziehbare KI-Ergebnisse erforderlich ist. Der EU AI Act macht die Herausforderungen, vor denen Unternehmen mit Blick auf den Einsatz verantwortungsvoller KI stehen, sichtbarer. Das eigentliche Problem existierte jedoch schon vorher.

Denn Responsible AI beginnt nicht erst bei Dokumentationspflichten, sondern bei der Architektur. Unternehmen, die heute auf modulare Systeme und echten Prozesskontext setzen, schaffen die Basis, um KI langfristig skalierbar, kontrollierbar und wirtschaftlich sinnvoll einzusetzen. •

Digital Experience Monitoring

als strategisches Steuerungsinstrument

Observability macht sichtbar, wie technische Störungen Nutzererlebnisse und Geschäftsprozesse beeinflussen. Mithilfe von Digital Experience Monitoring werden technische Daten mit Geschäftsprozessen verbunden, zugleich wird die Nutzererfahrung verbessert.

/// von Roman Spitzbart

WENN EINE BUCHUNG ABBRICHT, EINE ZAHLUNG HÄNGEN BLEIBT oder ein Self-Service-Portal langsam reagiert, ist das selten nur ein technisches Detail. Für Nutzerinnen und Nutzer zählt nicht, ob ein Microservice überlastet ist, ein API-Call fehlschlägt oder eine Datenbank zu langsam antwortet. Sie erleben einen digitalen Service, der nicht funktioniert. Mangelnde Digital Experience hat für Unternehmen negative Folgen: Umsatz geht verloren, Supportkosten steigen, Service-Level-Agreements geraten unter Druck und Vertrauen wird beschädigt.

Genau deshalb hat sich Digital Experience zu einer Business-Kennzahl entwickelt. Sie beschreibt, wie zuverlässig, schnell und nachvollziehbar digitale Interaktionen funktionieren. Das betrifft Kunden im E-Commerce oder beim Online-Banking, Bürger bei der der Nutzung von Verwaltungsportalen, Gäste bei Hotelbuchungen oder Versicherte in digitalen Serviceprogrammen. In allen Fällen entscheidet die digitale Erfahrung darüber, ob ein Geschäftsprozess erfolgreich abgeschlossen wird.

Warum reicht klassisches Monitoring nicht mehr aus?

Klassisches Monitoring zeigt meist, ob bekannte Systeme innerhalb definierter Grenzwerte laufen. Das bleibt wichtig, beantwortet aber nur einen Teil der Frage. In Cloud-nativen Architekturen entstehen Probleme häufig über mehrere Ebenen hinweg. Ein langsamer Check-out kann im Browser beginnen, durch einen fehlerhaften API-Aufruf verstärkt werden und seine Ursache in einer nachgelagerten Datenbank oder einem Drittanbieter-Service haben.

Digital Experience Monitoring (DEM) betrachtet deshalb nicht nur einzelne technische Komponenten. Es verbindet die Perspektive der Nutzer mit Signalen aus Anwendungen, Infrastruktur, Netzwerken, Logs, Metriken und Traces. Entscheidend ist der Zusammenhang: Welche technische Störung betrifft welchen Geschäftsprozess? Welche Nutzergruppe ist betroffen? Welche Transaktionen schlagen fehl? Und welche Auswirkung hat das auf Umsatz, Servicequalität oder operative Effizienz?

Aus technischen Signalen wird ein Business-Kontext

Der zentrale Schritt besteht darin, technische Telemetriedaten mit Geschäftsprozessen zu verbinden. Für sich genommen liefern diese Daten nur Ausschnitte. Erst ihre

DER AUTOR
Roman Spitzbart
ist VP Solutions Engineering EMEA bei Dynatrace.
Bild: Dynatrace

> „ Digital Experience Monitoring (DEM) **verbindet die Perspektive der Nutzer mit Signalen** aus Anwendungen, Infrastruktur, Netzwerken, Logs, Metriken und Traces.
>
> *Roman Spitzbart*

WAS IST DIGITAL EXPERIENCE MONITORING?

Digital Experience Monitoring (DEM) misst die tatsächliche Nutzererfahrung digitaler Services, etwa bei Login, Checkout oder Buchung. Es zeigt, wo Störungen entstehen, welche Nutzer betroffen sind und welche Auswirkungen sie auf Geschäftsprozesse haben.

Korrelation zeigt, wie ein Problem entsteht, wie es sich durch die Systemlandschaft bewegt und welche digitale Interaktion dadurch beeinträchtigt wird.

Ein Beispiel aus dem E-Commerce: Eine steigende Fehlerrate im Warenkorb ist zunächst ein technisches Signal. Kritisch wird es, wenn klar wird, dass die Fehlerrate vor allem mobile Nutzer betrifft, dass der Fehler während einer Rabattaktion auftritt und dass dadurch abgeschlossene Bestellungen zurückgehen. DEM macht diesen Zusammenhang sichtbar. Teams erkennen, dass ein Fehler vorliegt, welche Priorität er hat und welche geschäftlichen Folgen drohen.

In der Praxis verkürzt dieser Kontext die Zeit zwischen Erkennung und Lösung. So konnte in einem Fall durch die Kombination aus Observability, Automatisierung und AIOps die Mean-Time-to-Resolution um bis zu 80 Prozent reduziert werden. Während Spitzenzeiten wie Black Friday sanken kritische Incidents um 60 Prozent. Der geschäftliche Nutzen liegt dabei nicht allein in schnellerer Fehlerbehebung, sondern in stabileren digitalen Kaufprozessen.

KI-gestützte Observability als Voraussetzung

Eine KI-gestützte Observability hilft, aus großen Mengen an Telemetriedaten präzise Antworten abzuleiten. In komplexen IT-Umgebungen entstehen pro Sekunde enorme Datenmengen. Manuelle Analyse stößt hier schnell an Grenzen, weil Teams zwar viele Signale sehen, aber nicht zuverlässig erkennen, welche davon zusammengehören.

Kausale KI analysiert Abhängigkeiten zwischen Systemkomponenten und ordnet Ereignisse nach Ursache und Wirkung. Dadurch unterscheidet sie zwischen Symptomen und tatsächlichen Ursachen. Für IT-Teams ist das entscheidend: Sie müssen nicht mehrere Dashboards vergleichen, Hypothesen testen und Teams nacheinander einbinden. Stattdessen erhalten sie eine priorisierte Erklärung, wo ein Problem entstanden ist und welche Services oder Nutzer betroffen sind.

Diese Form der automatisierten Root-Cause-Analysis entlastet IT-Betrieb, SREs, DevOps und Support. Sie reduziert manuelle Sucharbeit, beschleunigt Eskalationen und schafft eine gemeinsame Entscheidungsgrundlage. Gerade in hybriden und Multi-Cloud-Umgebungen ist das wichtig, weil Fehler selten an Organisationsgrenzen haltmachen.

Digital Experience Monitoring benötigt gemeinsamen Datenkontext

Digitale Services werden von vielen Teams verantwortet. Entwicklungsteams optimieren Code, Plattformteams betreiben Infrastruktur, Security-Teams prüfen Risiken, Support-Teams reagieren auf Nutzeranfragen und Business-Verantwortliche betrachten Conversion, Verfügbarkeit oder Servicequalität. Wenn jedes Team mit eigenen Tools und Daten arbeitet, entstehen Teilwahrheiten.

Ein gemeinsamer Datenkontext schafft eine konsistente Sicht auf digitale Abläufe. Alle Beteiligten sehen dieselben Ereignisse, aber aus ihrer jeweiligen Perspektive. Der Support erkennt, welche Nutzer betroffen sind. DevOps sieht, welcher Service reagiert. Das Business ver-

steht, welcher Prozess gefährdet ist. Security kann prüfen, ob Auffälligkeiten mit Risiken zusammenhängen. In einem Fall fehlte beispielsweise die Transparenz darüber, wie Kunden digitale Angebote tatsächlich nutzten. Probleme wurden häufig erst über das Contact Center sichtbar. Mit End-to-End-Transparenz konnten 25 Prozent mehr Incidents identifiziert, 20 Prozent schneller reagiert und Infrastrukturkosten um bis zu 45 Prozent gesenkt werden. Gleichzeitig gingen kundenrelevante Störungen um mehr als 60 Prozent zurück.

Wie profitieren regulierte und servicekritische Branchen?
In regulierten Branchen ist Digital Experience eng mit Resilienz, Nachvollziehbarkeit und Compliance verbunden. Banken, Versicherungen und Behörden müssen digitale Services nicht nur verfügbar halten, sondern Störungen auch transparent erkennen, priorisieren und dokumentieren. DEM verbindet technische Ereignisse mit konkreten Serviceauswirkungen. Praxisbeispiele zeigen, dass Organisationen Probleme früher erkenenen, Releases effizienter steuern und Partner schneller integrieren. Entscheidend ist die Bewertung technischer Signale im Kontext des jeweiligen Serviceprozesses.

Welche Kennzahlen erfordert Digital Experience Monitoring
DEM sollte technische und geschäftliche Kennzahlen zusammenführen. Reine Infrastrukturmetriken reichen dafür nicht aus. Relevant sind Kennzahlen, die Nutzererlebnis, Servicequalität und Geschäftsauswirkung verbinden. Dazu zählen Ladezeiten, Fehlerraten, Abbruchquoten, erfolgreiche Transaktionen, betroffene Nutzergruppen, Incident-Dauer, Mean-Time-to-Identify, Mean-Time-to-Resolve und Auswirkungen auf definierte Geschäftsprozesse. Wichtig ist, diese Kennzahlen nicht isoliert zu betrachten. Eine leicht erhöhte Antwortzeit kann unkritisch sein, wenn sie einen internen Nebenprozess betrifft. Sie kann geschäftskritisch werden, wenn sie den Check-out, eine Zahlungsfreigabe oder einen Terminbuchungsprozess beeinflusst.

Wie der Einstieg in Digital Experience Monitoring gelingt
Unternehmen sollten zunächst die digitalen Journeys identifizieren, die für ihr Geschäft oder ihren öffentlichen Auftrag besonders relevant sind. Dazu gehören Kaufabschlüsse, Kontoeröffnungen, Schadenmeldungen, Buchungen, Antragsstrecken oder interne Self-Service-Prozesse. Im zweiten Schritt sollten Teams die wichtigsten Telemetriedaten zusammenführen. Dazu gehören unter anderem Real-User-Monitoring, synthetische Tests, Logs, Metriken, Traces und Topologie-Informationen. Eine Observability-Plattform sollte Abhängigkeiten automatisch erkennen, Ursachen analysieren und Auswirkungen auf Nutzer und Geschäftsprozesse sichtbar machen. Drittens erfordert es genau definierte Verantwortlichkeiten. DEM ist eine gemeinsame Aufgabe von IT, DevOps, SRE, Support und Business. Nur wenn alle Teams mit einem gemeinsamen Datenkontext arbeiten, lassen sich Probleme schneller priorisieren und beheben.

Digital Experience als Führungsaufgabe
Digitale Erlebnisse sind heute ein messbarer Teil der Unternehmensleistung. Sie beeinflussen Umsatz, Effizienz, Kundenbindung, Servicequalität und Resilienz. Wer digitale Services nur technisch überwacht, erkennt Probleme oft zu spät oder ohne ausreichenden Kontext. Digital Experience Monitoring schafft die Verbindung zwischen Nutzerperspektive, Systemzustand und Geschäftsauswirkung. In Kombination mit AI-driven Observability und automatisierter Ursachenanalyse wird daraus ein strategisches Steuerungsinstrument. Das Ziel ist nicht mehr nur, Störungen schneller zu beheben, sondern digitale Services so zu betreiben und weiterzuentwickeln, dass sie zuverlässig Geschäftswert liefern. •

> „ Regulierte Branchen wie Banken, Versicherungen und Behörden müssen **digitale Services nicht nur verfügbar halten**, sondern Störungen auch transparent erkennen, priorisieren und dokumentieren.
>
> *Roman Spitzbart*

Und ewig erhöht Microsoft die Preise...

WEGE AUS DER ABO-SPIRALE

DIE NÄCHSTE PREISRUNDE KOMMT NICHT ÜBERRASCHEND – ABER SIE TRIFFT. Wenn Microsoft zum 1. Juli 2026 erneut seine M365-Pläne verteuert, geht es um mehr als ein paar Prozentpunkte. Es geht um die Frage, wie viel Kontrolle Unternehmen über ihre IT-Kosten überhaupt noch haben. Denn was als flexibles Subscription-Modell begann, reißt heute immer tiefere Löcher in die IT-Budgets von Unternehmen.

Cloud-first verliert seinen Automatismus

CIOs in Betrieben jeder Größe lösen sich deshalb zunehmend von der Idee, dass „Cloud-first" automatisch wirtschaftlich ist. Stattdessen rückt die deutlich pragmatischere Architektur der hybriden Microsoft-Lizenzierung in den Fokus: die gezielte Kombination aus Cloud-Diensten und lokal betriebenen Systemen. Ihr Vorteil liegt auf der Hand: Nicht jede Anwendung braucht die Cloud. Klar, Kollaboration, Identity-Management und manche Security-Services spielen ihre Stärken online aus. Andere Workloads hingegen – darunter stabile Fachanwendungen, Produktionssysteme, klassische Office-Umgebungen und Microsoft Server – laufen lokal einfach günstiger und planbarer. Unternehmen entkoppeln mit Hybrid weite Teile ihrer IT von monatlich steigenden Abo-Kosten und gewinnen ein Stück finanzieller Steuerbarkeit zurück.

Nicht jede Anwendung gehört in die Cloud

Hinzu kommt ein Faktor, der lange unterschätzt wurde: Datensouveränität. Die Frage, wo geschäftskritische Informationen liegen und wer im Zweifel darauf zugreifen kann, ist längst nicht mehr nur ein Thema für Datenschutzbeauftragte. Sie ist strategisch. Hybride Modelle erlauben es, genau zu definieren, welche Daten und Prozesse in der Cloud sinnvoll sind – und welche bewusst im eigenen Einflussbereich bleiben.

Warum hybride Modelle wirtschaftlich attraktiv sind

Auch wirtschaftlich rechnet sich dieser Ansatz schneller als viele erwarten. Gerade in bestehenden IT-Landschaften können lokal betriebene Systeme über Jahre stabil genutzt werden. In Kombination mit gebrauchten Lizenzen entstehen so Kostenstrukturen, die sich deutlich von reinen Cloud-Modellen abheben – ohne auf moderne Funktionen verzichten zu müssen.

Der entscheidende Punkt:

Hybrid ist kein Rückschritt, sondern eine bewusste Steuerungsentscheidung. Unternehmen nutzen die Cloud dort, wo sie echten Mehrwert liefert – und vermeiden sie dort, wo sie vor allem Kosten erzeugt.

Der Microsoft Solutions Partner VENDOSOFT begleitet genau diesen Schritt: mit der Analyse bestehender Lizenzumgebungen, der Identifikation hoher Einsparpotenziale und der Entwicklung hybrider Lizenzstrategien, die sensible Daten schützen helfen. •

www.vendosoft.de/hybride-cloud | info@vendosoft.de

DIESE MICROSOFT 365 PLÄNE SIND VON DER PREISERHÖHUNG BETROFFEN

Plan	Preis vor 01.07.2026	Preis ab 01.07.2026	Steigerung
Microsoft 365 Business Basic	6,00 $	7,00 $	+16 %
(ohne Teams)	4,40 $	5,40 $	+23 %
Microsoft 365 Business Standard	12,50 $	14,00 $	+12 %
(ohne Teams)	9,29 $	10,79 $	+16 %
Microsoft 365 Business Premium	22,00 $	22,00 $	0 %
Office 365 E1	10,00 $	10,00 $	0 %
Office 365 E3	23,00 $	26,00 $	+13 %
(ohne Teams)	14,45 $	17,45 $	+14 %
Office 365 E5	38,00 $	41,00 $	+8 %
(ohne Teams)	29,45 $	32,45 $	+10 %
Microsoft 365 E3	36,00 $	39,00 $	+8 %
(ohne Teams)	27,45 $	30,45 $	+11 %
Microsoft 365 E5	57,00 $	60,00 $	+5 %
(ohne Teams)	48,45 $	51,45 $	+6 %
Microsoft 365 F1 (Frontline)	2,25 $	3,00 $	+33 %
(ohne Teams)	1,75 $	2,50 $	+43 %
Microsoft 365 F3 (Frontline)	8,00 $	10,00 $	+25 %
(ohne Teams)	6,93 $	8,93 $	+29 %

(Quelle: Microsoft 365 Pricing and Packaging Updates 16.02.26)

VENDOSOFT
Strategische Lizenzberatung

No-Code-Apps: Tempo für Compliance

Gesetzliche Vorgaben zwingen Unternehmen, Prozesse lückenlos nachzuweisen – ein riesiger Aufwand. Wie Unternehmen ihre Dokumentation jetzt in den Griff bekommen und sich auditfest aufstellen. /// von Sven Zuschlag

NIS2, ESG, CSRD. Die Liste regulatorischer Anforderungen wächst stetig und mit ihr der Druck, Sicherheits- bzw. Umweltmaßnahmen zu ergreifen und diese auch belegen zu können. Oft mangelt es an Geschwindigkeit und Struktur. Statt Lösungen entsteht ein Geflecht aus Tools, Abstimmungsschwierigkeiten und uneinheitlicher Dokumentation. Mit entsprechender Mehrarbeit. Dabei gibt es einen überraschend einfachen und pragmatischen Ansatz, der viele dieser Probleme gleichzeitig adressiert: No Code.

Gewachsene Prozesse, fehlende Struktur

In vielen Unternehmen ist die Dokumentation historisch gewachsen. Excel-Tabellen, PDFs, E-Mails oder papierbasierte Prozesse existieren parallel und ohne einheitliche Struktur. Daten werden mehrfach erfasst, sind über verschiedene Systeme verteilt und oft nicht eindeutig versioniert. Unter normalen Bedingungen mag dieses Vorgehen funktionieren. Unter Audit-Anforderungen wird es jedoch schnell zur Compliance-Falle. Fehlende Konsistenz und unvollständige Datensätze erschweren die Nachweisfähigkeit erheblich. Der klassische Reflex besteht häufig darin, neue Software einzuführen oder ein IT-Projekt zu starten. Doch individuelle Entwicklungen brauchen Zeit, Standardlösungen passen selten exakt und die nötige Reaktionsgeschwindigkeit bleibt aus. Währenddessen bleibt das eigentliche Defizit bestehen: Prozesse werden nur verzögert oder inkonsistent umgesetzt.

Der entscheidende Hebel: Prozesse mit No Code digitalisieren

Genau an diesem Punkt setzen No-Code-Plattformen an. Sie ermöglichen es Fachbereichen, ihre Prozesse selbst zu digitalisieren. Aus der Praxis heraus und ganz ohne Programmierkenntnisse. Denn niemand kennt die Anforderungen und Abläufe so gut wie diejenigen, die täglich damit arbeiten. Per Drag & Drop oder Prompt bauen die Mitarbeitenden No-Code-Apps, mit denen sie Daten strukturiert, vollständig und auditierbar erfassen. Direkt dort, wo sie entstehen: im Feld, in der Produktion, im Lager oder am Schreibtisch. Jederzeit im Einklang mit NIS2, CSRD oder weiteren Richtlinien. Um die Daten sicher und vollständig zu erheben, braucht es lediglich ein Tablet oder Mobiltelefon.

Compliance wird dabei direkt im Prozess mitgedacht. Pflichtfelder, klare Datenstrukturen und nachvollziehbare Änderungen sorgen für prüfbare Ergebnisse, während Rollen- und Berechtigungskonzepte den Zugriff absichern. Typische Zeitfresser wie manuelle Dateneingaben, doppelte Dokumentation oder das Nachpflegen von Informationen entfallen so komplett.

Von fragmentierten Abläufen zu effizienten Lösungen

Gerade im Kontext wachsender regulatorischer Anforderungen entstehen zahlreiche konkrete Einsatzmöglichkeiten, etwa im Gerätemanagement. Ein Prozess, der oft noch über Excel-Listen, E-Mails und einzelne Ticketsysteme abläuft. Dabei werden Geräte manuell zugeordnet, Statusänderungen nur teilweise erfasst und insgesamt mehr Zeit aufgewendet als notwendig. Mit No Code wird das Gerätemanagement deutlich vereinfacht. Jede Gerätebewegung wird direkt digital erfasst, eindeutig zugeordnet und automatisch dokumentiert. Der gesamte Lebenszyklus ist jederzeit nachvollziehbar. So entsteht ein transparenter, auditierbarer Prozess, der Compliance sichert und den operativen Aufwand spürbar reduziert.

> „ No-Code-Plattformen ermöglichen es Fachbereichen, ihre **Prozesse selbst zu digitalisieren**. Aus der Praxis heraus und ganz ohne Programmierkenntnisse. Denn niemand kennt die Anforderungen und Abläufe so gut wie diejenigen, die täglich damit arbeiten.
>
> *Sven Zuschlag*

Weitere Anwendungsbeispiele für No Code aus der Praxis:

Im NIS2-Umfeld:

- Lieferantenwechsel, neue Tools und Dienstleister, z. B. Auswahlprozesse, Bewertungen, Vertrags- und Freigabestatus

- Berechtigungsänderungen bei Eintritten, Rollenwechseln und Austritten, z. B. Mitarbeiter steigt ein oder scheidet aus, Abteilungswechsel, Adminrechte
- Schulungen und Awareness-Nachweise, z. B. Teilnahme, Inhalte, Zeitpunkte und Wissensstände

Im CSRD-Umfeld:

- Erfassung von Energieverbrauch auf Anlagenebene, z. B. Strom-, Gas-, Wärmeverbrauche einzelner Maschinen oder Strandorte
- Tracking von Fuhrparkaktivitäten, z. B. gefahrene Kilometer, Fahrzeugtypen, eingesetzte Kraftstoffe
- Dokumentation von Materialeinsatz und Ressourcenverbrauch, z. B. Mengen, Herkunft und Effizienz der Ressourcen

Klare Rollen, klare Regeln:
So lassen sich No-Code und Governance vereinbaren

Diese Anwendungsfälle zeigen, dass viele dokumentationspflichtig Prozesse sich tief im operativen Kern von Unternehmen befinden. Genau dort, wo Daten und Compliance unmittelbar zusammenlaufen. Umso wichtiger ist ein klar definierter Governance-Rahmen. Er stellt sicher, dass Anwendungen nicht unkontrolliert entstehen, sondern Standards eingehalten und Sicherheitsanforderungen zuverlässig erfüllt werden. In der Praxis hat sich dabei eine klare Aufgabenteilung bewährt: Die IT verantwortet Sicherheit, Governance und Integration in bestehende Systeme. Die Fachbereiche hingegen gestalten ihre Prozesse selbst und erfassen alle relevanten Daten nachweisbar direkt im Prozess. So entsteht schrittweise eine belastbare operative Struktur, in der Compliance nicht nachgelagert dokumentiert wird, sondern integraler Bestandteil der täglichen Arbeit ist.

Daraus ergeben sich mehrere Vorteile:

- Kontinuierliche Compliance statt punktueller Audit-Vorbereitung
- Höhere Datenqualität durch standardisierte und vollständige Erfassung
- Reduzierter Aufwand durch den Wegfall manueller und redundanter Tätigkeiten
- Erhöhte Transparenz durch klar definierte und nachvollziehbare Prozesse
- Zentrale Datenverfügbarkeit für Audits, Reportings und Analysen

Vor allem aber verschiebt sich die Wahrnehmung. Dokumentation ist kein notwendiges Übel mehr, sondern ein natürlicher Bestandteil des Prozesses, der nicht viel Zeit kosten muss.

Compliance als Treiber statt Bremse

Regulatorische Anforderungen werden nicht verschwinden. Im Gegenteil. Sie werden komplexer, dichter, selbstverständlicher. Unternehmen haben zwei Möglichkeiten: Sie versuchen, steigende Dokumentationspflichten mit bestehenden Strukturen zu bewältigen oder sie nutzen den Druck als Impuls, ihre Prozesse grundlegend zu überdenken. No Code ist dabei nicht nur ein weiteres Tool, sondern ein pragmatischer Enabler, der Unternehmen in die Lage versetzt, operative Prozesse selbstständig, schnell und kontrolliert weiterzuentwickeln.

Richtig eingesetzt wird so aus Pflicht plötzlich Potenzial und aus Dokumentation ein Motor für Tempo, Effizienz und Zukunftsfähigkeit. •

DER AUTOR
Sven Zuschlag
ist CEO und Mitgründer der smapOne AG und verantwortet die Bereiche Strategie, Märkte und Mitarbeiter.

INFOKASTEN NIS2

Die NIS2-Richtlinie ist eine EU-weite Vorgabe zur Stärkung der Cybersicherheit. Sie verpflichtet Unternehmen, Risiken systematisch zu managen, Sicherheitsvorfälle zu melden und Maßnahmen nachvollziehbar zu dokumentieren.

INFOKASTEN CSRD

Die CSRD ist eine EU-Richtlinie zur verpflichtenden Nachhaltigkeitsberichterstattung. Unternehmen müssen ESG-Kennzahlen (Umwelt, Soziales, Governance) strukturiert erfassen, dokumentieren und offenlegen.

Vom Monolithen zur kombinierbaren Wertschöpfung

Märkte verändern sich schneller als Planungszyklen. Wer resilient wachsen will, muss Angebot, Erlös und Betrieb als Bausteine denken. Modulare Geschäftsmodelle machen Unternehmen composable – verkürzen die Time-to-Market, verbessern Margen und öffnen den Weg in Partner-Ökosysteme. /// von Heiner Sieger

Warum Modularität jetzt strategisch wird

Der Druck auf Unternehmen, schneller zu lernen und häufiger zu liefern, ist in den vergangenen Jahren kontinuierlich gestiegen. Kunden erwarten Varianten, Bundles und Service-Erweiterungen, ohne dass Preise oder Lieferzeiten aus dem Ruder laufen. Gleichzeitig werden Wertschöpfungsketten zu Netzwerken: Partner ergänzen Leistungen, digitale Marktplätze erschließen neue Kanäle, Daten werden zum verbindenden Rohstoff.

In diesem Umfeld stoßen monolithische Geschäfts- und IT-Modelle an Grenzen. Wer jedes neue Angebot als Sonderanfertigung bauen muss, verliert Tempo, treibt Kosten und erhöht Risiken. Modulare Geschäftsmodelle setzen an der Wurzel an: Sie strukturieren Angebot, Erlösmechanik und Betriebslogik in wiederverwendbare Bausteine – standardisiert, klar beschrieben und über definierte Schnittstellen kombinierbar. Damit wird die Organisation in die Lage versetzt, neue Wertversprechen aus bestehenden Komponenten zu montieren, statt sie jedes Mal neu zu erfinden.

Vom Baukasten zur Betriebslogik

Modularität beginnt nicht in der IT, sondern im Wertversprechen. Produkte und Services lassen sich als Kernleistung mit ergänzenden Modulen denken: Ein Grundangebot, das durch Add-ons wie Premium-Support, Datenanalysen oder Garantien erweitert wird. Die Preis- und Erlöslogik folgt demselben Prinzip: Abonnements, nutzungsabhängige Tarife, Einmalkomponenten oder erfolgsabhängige Gebühren können so konfiguriert werden, dass sie je Segment oder Kanal passgenau wirken.

Entscheidend ist, dass diese Module nicht nur vertrieblich, sondern auch operativ eigenständig geführt werden. In der Sprache der Unternehmensarchitektur sind dies Geschäftsfähigkeiten – stabile Beschreibungen dessen, „was" das Unternehmen tut, unabhängig davon, „wie" es organisiert ist. Eine Fähigkeit wie „Order-to-Cash" oder „Identity & Consent" erhält klare Ziele, Budgets, Messgrößen und Ownership. Auf der Technologieebene wird diese Struktur durch kombinierbare Softwarebausteine abgebildet, die fachlich erkennbar sind, eigene Datenmodelle und Services besitzen und über APIs sowie Ereignisse interagieren. Unter Begriffen wie Packaged Business Capabilities und einer MACH-orientierten Architektur (Microservices, API-first, Cloud-native, Headless) hat sich in den vergangenen Jahren ein Repertoire bewährt, das die Wiederverwendung in der Praxis möglich macht. Doch Technik allein genügt nicht: Erst wenn Angebots-, Erlös- und Betriebsbausteine konsistent definiert und von funktionsübergreifenden Teams verantwortet werden, entsteht echte Beweglichkeit.

Nutzen messbar machen

Der Mehrwert modularer Geschäftsmodelle zeigt sich vor allem in Geschwindigkeit, Skalierung und Transparenz. Neue Angebote lassen sich als Kombination vorhandener Bausteine schneller testen und ausrollen; erfolgreiche Varianten werden skaliert, weniger überzeugende verworfen – ohne hohe Vorlaufkosten. Unternehmen, die Modularität ernst nehmen, beobachten spürbar kürzere Durchlaufzeiten von der Idee bis zum Marktstart und einen steigenden Anteil an Projekten, die auf bereits vorhandene Komponenten zurückgreifen. Gleichzeitig verbessert sich die Steuerbarkeit: Wenn Kosten, Qualität und Risiken je Baustein gemessen werden, wird sichtbar, welche Module Wert schaffen, wo Engpässe liegen und welche Partnerschaften

" Modularität beginnt nicht in der IT, sondern im **Wertversprechen**. Produkte und Services lassen sich als Kernleistung mit ergänzenden Modulen denken: Ein Grundangebot, das durch Add-ons wie Premium-Support, Datenanalysen oder Garantien erweitert wird.

Heiner Sieger

sich lohnen. Das ist besonders für mittelständische Unternehmen relevant, die Innovationen finanziell diszipliniert umsetzen müssen. Transparente Unit Economics pro Modul erleichtern die Priorisierung. Auch die Resilienz steigt: Änderungen in einem Modul – etwa ein neues Preismodell oder eine geänderte Compliance-Anforderung – müssen nicht das Gesamtsystem destabilisieren, solange Schnittstellen und Verantwortlichkeiten sauber definiert sind. Ein anonymisiertes Beispiel aus dem industriellen B2B-Umfeld illustriert dies: Ein Hersteller trennte Ersatzteilverkauf, Wartung und Remote-Services in eigenständige Module, standardisierte die Angebots- und Preislogik und öffnete über APIs den Zugang für Installations- und Finanzierungspartner. Innerhalb eines Jahres beschleunigten sich Einführungen regionaler Varianten deutlich, der Serviceanteil am Umsatz stieg zweistellig – bei stabiler Änderungsqualität.

So gelingt der Umbau

Der Weg zur Modularität beginnt mit einer ehrlichen Standortbestimmung. Eine kompakte Karte der Geschäftsfähigkeiten – fünf bis neun Domänen auf oberster Ebene, darunter weiter verfeinert – liefert das gemeinsame Vokabular für Management, Fachbereiche und IT. Auf dieser Basis werden Angebots- und Erlösbausteine systematisch gegenübergestellt: Was ist Kern, was ist Add-on, was kann entbündelt werden, wo lohnt sich ein nutzungsabhängiges Modell? Parallel dazu wird die technische Umsetzung vorbereitet: Schnittstellenstandards, Ereignisse, Datenmodelle und Versionierung werden festgelegt, um die Austauschbarkeit der Bausteine zu sichern.

Wichtig ist das passende Operating Model: End-to-End-Verantwortung je Fähigkeit, ein klarer Katalog der verfügbaren Module, einheitliche Qualitäts- und Sicherheitskriterien, definierte Lebenszyklen von der Einführung bis zur Stilllegung. Governance ist dabei kein Selbstzweck, sondern Voraussetzung für Tempo: Wer weiß, wo ein Baustein verankert ist, wem er gehört und wie er verändert werden darf, entscheidet schneller und risikobewusster. Das gilt auch für Compliance: Mehr Komponenten bedeuten mehr Prüfpfade. Sicherheits- und Datenschutzanforderungen müssen pro Modul nachweisbar erfüllt, Datenbegriffe unternehmensweit konsistent geführt und Ausstiegsoptionen gegen Lock-in vorgeplant sein. Ein pragmatisches Vorgehen zahlt sich aus: mit zwei bis drei priorisierten Modulen starten, in einem überschaubaren Kundensegment testen, Kennzahlen konsequent auswerten, dann skalieren.

Fallstricke und Ausblick

Die häufigste Falle ist Pseudo-Modularität. Wer ohne klare Architektur- und Datenprinzipien einfach mehr Tools einführt, produziert Integrationsspaghetti statt Flexibilität. Ebenso wirkungslos bleibt Modularität, wenn die Preis- und Erlösmechanik unverändert am Monolithen festhält: Was intern entkoppelt ist, muss sich auch am Markt variabel kombinieren lassen. Schließlich scheitern viele Vorhaben an unklarer Ownership. Ohne eindeutige Verantwortungen je Baustein – inklusive Budget, Backlog und Servicelevels – bleiben Abhängigkeiten diffus und Entscheidungen langsam.

Richtig umgesetzt, ist Modularität keine modische Architekturidee, sondern eine Managementdisziplin. Sie schafft die Grundlage, neue Wachstumschancen in Ökosystemen zu nutzen und technologische Sprünge – etwa KI-gestützte Funktionen entlang des Lebenszyklus – dort zu verankern, wo sie wirtschaftlich Sinn stiften. •

Der Beitrag wurde erstellt mit Unterstützung unseres KI-Assistenten

DER AUTOR
Heiner Sieger
ist im WIN-Verlag Chefredakteur von Digital Business und e-commerce-Magazin.

KI in Geschäftsprozessen: Das müssen Unternehmen anders machen

Viele KI-Initiativen scheitern an isolierter Umsetzung statt fehlender Technologie. Statt Effizienz entsteht neue Komplexität. Der Schlüssel liegt nicht in mehr Automatisierung, sondern in durchgängiger Prozessintegration, Transparenz und Kontrolle.

/// von Dr. Rafael Arto-Haumacher

KÜNSTLICHE INTELLIGENZ IST IN UNTERNEHMEN ANGEKOMMEN. Pilotprojekte werden umgesetzt, Use Cases identifiziert, Budgets freigegeben. Auf dem Papier schreitet die Transformation voran. In der Realität zeigt sich jedoch ein anderes Bild. Viele KI-Initiativen bleiben isoliert, skalieren nicht und liefern keinen messbaren Beitrag zum Geschäftserfolg. Statt Klarheit entsteht neue Komplexität. Statt Effizienz wächst der Steuerungsaufwand.

Das eigentliche Problem ist dabei selten die Technologie. Es ist die Art und Weise, wie KI in Prozesse integriert wird. Die entscheidende Frage lautet heute nicht mehr, ob Unternehmen KI einsetzen sollten, sondern warum so viele Initiativen trotz hoher Investitionen nicht den erwarteten Mehrwert liefern.

Das eigentliche Problem: KI ohne Prozesskontext

Ein zentraler Grund für das Scheitern vieler KI-Initiativen liegt in ihrer isolierten Einführung. Lösungen werden häufig punktuell implementiert, etwa zur automatischen Belegerkennung oder zur Priorisierung von Kundenanfragen. Was auf den ersten Blick effizient wirkt, erzeugt in der Praxis neue Brüche. Daten werden mehrfach verarbeitet oder bleiben in Silos. Entscheidungen sind nicht durchgängig nachvollziehbar. Prozesse enden an Systemgrenzen statt entlang des tatsächlichen Geschäftsablaufs. Im Ergebnis führt die punktuelle Automatisierung zu einem Transparenz- und Kontrollverlust über den Gesamtprozess. Gerade im DACH-Markt wird dieses Spannungsfeld zunehmend kritisch bewertet. Hier stehen nicht nur Effizienzgewinne im Fokus, sondern vor allem Transparenz, Nachvollziehbarkeit und Governance. KI darf nicht zur Black Box werden, insbesondere in finanznahen oder compliance-relevanten Prozessen.

Wenn Automatisierung zum Risiko wird

Diese Aussage könnte man gegebenenfalls noch mehr schärfen, beispielsweise: Mehr Automatisierung führt nicht automatisch zu mehr Kontrolle. Aktuelle Studien der Unternehmensberatung Deloitte beschreiben vielmehr ein wiederkehrendes Muster: Wo Automatisierung punktuell eingeführt wird, ohne in Prozesse und Governance eingebettet zu sein, steigt der Integrationsaufwand. Verantwortlichkeiten verschwimmen, Transparenz geht verloren – und Steuerung wird aufwendiger statt einfacher.

Je mehr isolierte Lösungen im Einsatz sind, desto größer wird die Komplexität. Unterschiedliche Logiken und Datenmodelle erschweren die Abstimmung. IT-Abteilungen verlieren den Überblick über Integrationen und Abhängigkeiten. Fachbereiche schaffen sich Workarounds außerhalb der Systeme. Gleichzeitig steigt das Risiko im Umgang mit KI-gestützten Entscheidungen. Wenn nicht klar ist, wie Ergebnisse zustande kommen, wird es schwierig, diese gegenüber internen Stakeholdern oder externen Prüfern zu rechtfertigen. Die Folge ist ein schleichender Vertrauensverlust, der eine skalierbare Nutzung von KI verhindert.

Der Perspektivwechsel: Von Automatisierung zu Orchestrierung

Führende Unternehmen beginnen daher umzudenken. Der Fokus verschiebt sich weg von isolierten KI-Funktionen hin zu einer ganzheitlichen Betrachtung von Geschäftsprozessen. Im Mittelpunkt steht eine einfache, aber oft unterschätzte Erkenntnis: Der Wert von KI entsteht nicht im einzelnen Anwendungsfall, sondern im Zusammenspiel von Prozessen, Daten und Entscheidungen.

Statt weitere Einzellösungen zu implementieren, setzen Organisationen zunehmend auf integrierte Platt-

> „ Das eigentliche Problem ist selten die Technologie. Es ist die Art und Weise, **wie künstliche Intelligenz in Prozesse integriert wird.**
>
> *Dr. Rafael Arto-Haumacher*

DER AUTOR
Dr. Rafael Arto-Haumacher
ist Managing Director DACH bei Esker.
Bild: Esker

> „ Ein zentraler Grund für das Scheitern vieler KI-Initiativen **liegt in ihrer isolierten Einführung**.
>
> *Dr. Rafael Arto-Haumacher*

formansätze, die Prozesse durchgängig abbilden, Daten konsistent verfügbar machen und Entscheidungen im jeweiligen Kontext treffen. KI wird in diesem Modell nicht als zusätzliche Technologie verstanden, sondern als eingebettete Intelligenz, die Prozesse aktiv steuert, priorisiert und unterstützt.

Erklärbare KI als Voraussetzung für Skalierung

Ein entscheidender Erfolgsfaktor ist dabei die Fähigkeit, KI-gestützte Entscheidungen transparent zu machen. Nur wenn nachvollziehbar ist, warum ein System eine bestimmte Handlung empfiehlt oder ausführt, kann Vertrauen entstehen. Das gilt sowohl für Anwender als auch für Compliance- und Audit-Anforderungen. Entscheidungen müssen dokumentiert und rückverfolgbar sein. Modelle und Regeln müssen in bestehende Governance-Strukturen eingebettet werden. Fachbereiche müssen in der Lage sein, Ergebnisse zu interpretieren und aktiv zu steuern. Erst unter diesen Voraussetzungen wird KI von einem Experimentierfeld zu einem belastbaren Bestandteil operativer Prozesse.

Integration statt Insellösungen: Die Rolle der IT

Für IT-Organisationen ergibt sich daraus eine klare Aufgabe. Sie müssen den Rahmen schaffen, in dem KI kontrolliert und integriert eingesetzt werden kann. Dazu gehört die Reduktion von Tool-Landschaften zugunsten konsistenter Plattformen ebenso wie die Sicherstellung von Datenqualität und die Etablierung klarer Governance- und Sicherheitsmechanismen. Gleichzeitig wächst die Bedeutung der Zusammenarbeit zwischen IT und Fachbereichen. KI ist längst kein isoliertes Innovationsthema mehr, sondern ein integraler Bestandteil der operativen Wertschöpfung.

Fazit: KI wird erst durch Kontrolle wertvoll

Die nächste Phase der Digitalisierung wird nicht durch mehr KI entschieden, sondern durch bessere Integration. Unternehmen stehen vor einer klaren Wahl: Entweder sie erweitern ihre bestehenden Landschaften um weitere isolierte KI-Funktionen und erhöhen damit Komplexität, Risiko und Steuerungsaufwand. Oder sie schaffen die Grundlage für durchgängige, kontrollierbare Prozesse, in denen KI gezielt und nachvollziehbar wirkt.

Der Unterschied liegt nicht in der Technologie, sondern im Betriebsmodell. Wer KI als isoliertes Werkzeug betrachtet, wird ihren Nutzen begrenzen. Wer sie als integralen Bestandteil der Prozesssteuerung versteht, erschließt ihren tatsächlichen Wert. Am Ende entscheidet nicht die Innovationsgeschwindigkeit über den Erfolg, sondern die Fähigkeit, Komplexität zu beherrschen und Wirkung messbar zu machen. •

„KI made in Europe“: Wie die Industrie wieder Tempo gewinnt

Ferri Abolhassan*, Mitglied des Vorstands der Telekom und CEO von T-Systems, über die KI-Fabrik München, Large Industry Models und warum Deutschland bei physischer KI zum Zugpferd Europas werden kann – effizient, grün und mit klarer B2B-Fokussierung. /// von Heiner Sieger

DER GESPRÄCHSPARTNER
Dr. Ferri Abolhassan
ist seit 1. Januar 2024 Vorstand der Deutschen Telekom AG und CEO der T-Systems International GmbH. Er ist Mitglied im Aufsichtsrat des DFKI, Mitglied der Expertenkommission „Wettbewerb & KI“ des Bundeswirtschaftsministeriums, acatech-Senator und engagiert bei Max-Planck-Gesellschaft und Bitkom.

> „ Der Stack ist offen, interoperabel und auf **Co-Creation** ausgelegt. Wir integrieren bestehende Systeme, schaffen **standardisierte Schnittstellen** und entwickeln gemeinsam mit Kunden und Technologiepartnern die Large Industry Models, die Europa braucht.
>
> *Dr. Ferri Abolhassan*

Wie lautet der Kernauftrag der KI-Fabrik – und welches Problem der deutschen Industrie lösen Sie konkret?
Ferri Abolhassan | Die KI-Fabrik ist für uns mehr als ein Technologieprojekt. Sie steht für „KI made in Europe“ und „made for Germany“ – sicher, offen und souverän. Wir liefern einen kompletten Stack von Konnektivität und Security über Cloud und Plattform bis hin zu smarten Business-Anwendungen. Im Zentrum stehen Large Industry Models: Modelle, die unstrukturierte Industriedaten in messbare, produktionsnahe Lösungen übersetzen. Genau hier liegen die größten Hebel für Produktivität und Automatisierung. Deutschland ist ein Industrieland. Wir haben einen enormen Bestand hochwertiger Prozess- und Fertigungsdaten. Was bisher fehlte, war eine Infrastruktur, um dieses Potenzial stärker zu nutzen, ohne die Hoheit über diese Daten aus der Hand zu geben. Mit unserer Industrial AI Cloud bieten wir hierfür eine souveräne Lösung. Wir reden nicht nur, wir handeln: Wir sind im Februar gestartet und sehen bereits eine Auslastung von rund 50 Prozent.

Woran zeigt sich der Nutzen bereits heute – können Sie konkrete Beispiele nennen?
FA | Ein prominentes Beispiel ist Siemens. Mit dem Digital Twin Composer lassen sich Fabriken oder Rechenzentren virtuell planen und simulieren; Pepsi nutzt das bereits. Was früher Zeichnungen, CAD, Simulationen und viel Planungsarbeit erforderte, gelingt mit digitalen Zwillingen schneller, transparenter und flexibler. Planung, Abstimmung und Änderungsschleifen verkürzen sich, und Qualität sowie Nachvollziehbarkeit steigen.

Gibt es Kennzahlen, an denen Unternehmen den Effekt messen?
FA | KPIs unterscheiden sich je nach Branche und Reifegrad. Typisch sind weniger Personal- und Planungsaufwand, kürzere Time-to-Design und Time-to-Factory, höhere First-Time-Right-Quoten sowie sinkende Nacharbeits- oder Ausschussraten. Die Firmen, die auf Automatisierung setzen, quantifizieren diese Effekte für ihr Business – und skalieren dann.

Welche Leuchtturmprojekte können Sie bereits nennen?
FA | SOOFI zum Beispiel ist ein souveränes europäisches Sprachmodell, das speziell für Unternehmens- und Industrieanwendungen entwickelt wird – mit Fokus auf Datensouveränität, Compliance und Mehrsprachigkeit. Wir als Deutsche Telekom bzw. T-Systems treiben SOOFI gemeinsam mit Partnern voran: Wir stellten dafür die souveräne

Infrastruktur und das Hosting in unserer KI-Fabrik bereit, übernehmen Betrieb, Sicherheit und Compliance und integrieren das Modell in konkrete B2B-Use-Cases. Zweites Beispiel ist Agile Robots, hier adressieren wir KI-gestützte Robotikfertigung. Denken Sie zum Beispiel an die Textilindustrie. Hier ist Europa nur mit Robotik plus KI wettbewerbsfähig: Designs, Größen, Farben und Sortimente werden in Echtzeit in Produktionsaufträge übersetzt, die Roboter zuverlässig umsetzen. Unsere KI-Fabrik liefert dafür Daten, Modelle und Rechenleistung. Drittes Beispiel: Noxtua im Rechtsbereich. Das Unternehmen erschließt mit Hilfe unserer Industrial AI Cloud Millionen von Fällen, um in großen Foundation-Modellen präzisere Beratungen zu ermöglichen.

Ist die KI-Fabrik vor allem etwas für Konzerne – oder senken Sie damit auch Einstiegshürden für den Mittelstand?
FA | Wir adressieren Mittelständler ganzheitlich. Häufig beginnt es mit einem konkreten Problem, etwa Predictive Maintenance bei Klimaanlagen oder Kompressoren. Unstrukturierte Daten – zum Beispiel Geräuschprofile – erlauben Rückschlüsse auf den „Gesundheitszustand" von Maschinen. Wir hören den Kunden zu, schärfen den Use Case und verbinden Konnektivität, Cloud, Plattform und Anwendung zu einer Lösung. So reduzieren wir Komplexität, machen hohe Vorabinvestitionen überflüssig und liefern schnell Ergebnisse.

Wie sieht das Onboarding aus – und wie schnell geht es?
FA | Das hängt vom Reifegrad ab. Großunternehmen wie Siemens verfügen über starke Expertenteams und starten zügig. Mittelständler benötigen in der Regel mehr Unterstützung. Wir bieten strukturierte Beratung, klare Meilensteine und frühe Prototypen, damit der Nutzen rasch sichtbar wird. Schnelligkeit, Pragmatismus und Ganzheitlichkeit sind unser USP.

Welche Rolle spielt Green AI – Energieeffizienz und CO2?
FA | Eine zentrale. Unsere KI-Fabrik läuft zu 100 Prozent mit grünem Strom und erreicht einen PUE von 1,2 – das ist sehr effizient. Gekühlt wird mit Wasser aus dem Münchner Eisbach; über einen Wärmetauscher erhitzen wir das Wasser nicht, sondern nutzen die Abwärme zum Heizen des Tucher-Parks. Effizienz, Nachhaltigkeit und regionale Wertschöpfung greifen hier ineinander.

Wie stärken Sie mit dem Standort die digitale Souveränität – auch im Lichte des EU AI Act?
FA | Unsere KI-Fabrik ist souverän – aus deutscher und europäischer Hand, mit einer notwendigen Ausnahme: den NVIDIA-Chips, weil es in Europa derzeit keine gleichwertige Alternative gibt. Alles andere – von Steckverbindern über Verkabelung bis zur Plattform – ist deutsch bzw. europäisch. Damit bieten wir Transparenz, Sicherheit und Governance vom Datenzugang bis zum Modellbetrieb.

Was unterscheidet die Large Industry Models von reinen Sprachmodellen?
FA | LLMs sind stark bei Text. Die Industrie braucht jedoch Modelle, die physische Prozesse, Maschinendaten und Produktionskontexte verstehen. Large Industry Models verbinden Domänenwissen, Sensordaten und Betriebsdaten zu konkreten Anwendungen – von Planung und Qualität über Instandhaltung bis zur Supply-Chain-Optimierung. Das ist unser Fokus: B2B statt Consumer.

Wie offen ist Ihr Technologie-Stack – und welche Rolle spielen Partner?
FA | Der Stack ist offen, interoperabel und auf Co-Creation ausgelegt. Wir integrieren bestehende Systeme wie die Business Technology Plattform von SAP oder den Digital Twin Composer von Siemens, schaffen standardisierte Schnittstellen und entwickeln gemeinsam mit Kunden und Technologiepartnern die Large Industry Models, die Europa braucht. So entsteht Tempo – ohne Vendor-Lock-in.

Plant Europa ein Netzwerk von AI Gigafactories – und welche Rolle könnte Deutschland übernehmen?
FA | Die EU bereitet eine Ausschreibung für AI-Gigafactories vor. Wir haben Interesse bekundet, warten aber nicht auf Fördergelder, sondern lernen bereits im laufenden Betrieb. Wird die Ausschreibung konkret, prüfen wir die Fördermechanik, die Rolle des Staates als Ankerkunde – etwa 30 Prozent wurden diskutiert – sowie wettbewerbsrelevante Faktoren wie Strompreise. Um gegen die Nordics oder Frankreich zu bestehen, brauchen wir industriellen Grünstrom zu vergleichbaren Konditionen und klare Standortzusagen.

Mit welcher Ambition geht T-Systems in dieses mögliche Netzwerk?
FA | In industrieller, physischer KI sind wir heute schon Zugpferd. Während die USA stark auf Consumer-orientierte Sprachmodelle setzen, fokussieren wir Industrie und Mittelstand im B2B. Wir wollen nicht mit den größten LLMs konkurrieren, sondern dort führen, wo Deutschland stark ist: bei produktionsnaher, sicherer und souveräner KI.

Was erwarten Sie von der Politik, damit das skaliert?
FA | Erstens: Strom als Grundressource der Daten- und KI-Industrie begreifen – und als Industriestrom fördern. Zweitens: Der Staat sollte als Ankerkunde die Auslastung stützen und eigene Anforderungen auf der KI-Fabrik aufsetzen. Drittens: Beschaffungs- und Förderlogik vereinfachen. Die Telekom braucht keine AI Gigafactory. Deutschland braucht eine AI Gigafactory. Wir können unsere KI-Fabrik am Tucher-Park kurzfristig um 50 Prozent erweitern und über einen zweiten Standort in München die Rechenkapazitäten sogar verdoppeln. Für eine nationale Gigafactory braucht es daher gemeinsame Prioritäten von Bund, Ländern und öffentlicher Hand.

Ihr Blick nach vorn: Woran messen Sie Erfolg in den nächsten 12 bis 24 Monaten?
FA | An skalierenden Use Cases mit klarem Businessnutzen: mehr Digitale Zwillinge in der Planung, produktive Robotik-Workflows, präzisere KI-Modelle im Recht, dazu breitere Mittelstandsprogramme. Wenn Partnernetz, Energieeffizienz und Souveränität zusammenspielen und Kunden schneller liefern, planen und warten, sind wir auf Kurs. •

Empathie und Kontext für bessere Geschäftsentscheidungen

Emotionen KI und Humane KI markieren die nächste Entwicklungsstufe der Business Intelligence. Während Emotionen KI emotionale Signale aus Daten, Sprache, Mimik, Gestik und Verhalten erkennt, bringt Humane KI Empathie, Kontextverständnis und Mensch-Maschine-Kooperation ein. /// von Dr. Anna Maria Rostomyan

UNTERNEHMEN VERFÜGEN HEUTE ÜBER ENORME DATENMENGEN. Dennoch bleiben viele Entscheidungen unvollständig, weil ein zentraler Faktor oft fehlt: Emotionen. Kunden kaufen nicht nur rational – sie reagieren emotional auf Marken, Produkte und Erlebnisse

Darüber hinaus, viele geschäftliche Entscheidungen entstehen nicht allein aus rationalen Überlegungen. Kaufentscheidungen, Markenbindung oder Mitarbeitermotivation werden maßgeblich von Emotionen beeinflusst. Genau hier setzt eine neue Generation von Technologien an: Emotionen-KI und Humane KI. Genau hier setzt eine neue Generation von Technologien an: Emotionen-KI und Humane KI. Sie erweitern klassische Business-Analytics um eine Dimension, die lange schwer messbar war – die emotionale Reaktion von Menschen. Diese Technologien erweitern klassische Business Intelligence um eine Dimension, die bislang nur schwer messbar war – die emotionale Reaktion von Menschen. Für Unternehmen eröffnet das neue Möglichkeiten: von präziserem Marketing über bessere Personalentscheidungen bis hin zu empathischeren digitalen Services.

Emotionen erkennen und darauf zu reagieren: Die Rolle der Emotionen-KI

Emotionen-KI – häufig auch als Affective Computing bezeichnet – nutzt künstliche Intelligenz, um emotionale Signale aus unterschiedlichen Datenquellen zu analysieren. Dazu gehören beispielsweise:

- Sprachmuster, Stimmlage und Tonfall,
- Gesichtsausdrücke und Mikroreaktionen,
- Körpersprache und Verhalten,
- Textanalysen aus Kundenfeedback oder Social Media (SM).

Die Systeme erkennen emotionale Muster wie Frustration, Zufriedenheit oder Interesse. Für Unternehmen entstehen dadurch neue Möglichkeiten, emotionale Reaktionen systematisch zu messen und zu verstehen.

Diese Informationen liefern wertvolle Hinweise darauf, wie Produkte wahrgenommen werden, wie Kunden auf Marketing reagieren oder wie Mitarbeitende ihre Arbeitsumgebung erleben.

Von Emotionen-KI zu Humaner KI

Während Emotionen-KI vor allem Emotionen erkennt und interpretiert und darauf reagiert (Rostomyan, 2023b), geht Humane KI einen Schritt weiter.

Sie kombiniert emotionale Analyse mit Kontextverständnis, Empathie und kooperativer Interaktion zwischen Mensch und Maschine.

Das Ziel ist nicht nur, Emotionen zu messen, sondern sie sinnvoll in Entscheidungsprozesse einzubeziehen. Dadurch entstehen Systeme, die:

- menschliche Bedürfnisse besser verstehen
- situativ angemessener reagieren
- Entscheidungsprozesse unterstützen, statt sie zu ersetzen

Humane KI wird damit zu einer Art emotional intelligenter Entscheidungsassistenz, wo wir über Mensch-Maschine kooperativen Interaktionen sprechen.

Business-Anwendungen mit unmittelbarem Mehrwert

Immer mehr Organisationen beginnen, emotionale Daten in ihre Geschäftsprozesse zu integrieren. Einige typische Anwendungsfelder zeigen das Potenzial:

- Marketing und Customer Experience
  Emotionserkennung ermöglicht Firmen zu analysieren, wie Kunden tatsächlich auf Produkte, Werbung, Farben oder Preise reagieren. Dadurch lassen sich Kampagnen, Unternehmen, Markenbotschaften und Produktdesign deutlich präziser optimieren.
- Retail und Point-of-Sale-Analysen
  Intelligente Kamerasysteme können emotionale Reaktionen von Kunden auf Displays, Produkte oder Ladenlayouts messen. Händler gewinnen so Echtzeit-Feedback, das unmittelbar in Sortiments- und Preisentscheidungen einfließen kann.
- Human Resources und Recruiting
  Im Personalmanagement kann Emotionen-KI helfen,

Stimmungslagen, Engagement oder Stressindikatoren in Teams besser zu verstehen. Dies unterstützt Führungskräfte dabei, Arbeitsumgebungen produktiver und gesünder zu gestalten.

- Kundenservice im Banking-Bereich
  Digitale Assistenten und Chatbots können mithilfe von Emotionen-KI erkennen, ob ein Kunde beispielsweise frustriert, unsicher oder zufrieden ist. Die Systeme passen ihre Antworten entsprechend an und können komplexe Anliegen an menschliche Berater weiterleiten. Diese Erkenntnisse helfen, Kunden proaktiv und empathisch passende Finanzlösungen anzubieten.
- Digitale Kundeninteraktion
  Chatbots, virtuelle Assistenten und Serviceplattformen werden zunehmend empathischer. Sie erkennen beispielsweise Frustration oder Unsicherheit im Gespräch und passen ihre Antworten entsprechend an. Dadurch entsteht eine persönlichere und effizientere Kundenkommunikation.
- Risikomanagement und Betrugserkennung
  Emotionale Analyse kann auch im Bereich Compliance und Sicherheit eingesetzt werden. Auffällige Stress- oder Unsicherheitsmuster in Gesprächen oder Interaktionen können Hinweise auf potenziellen Betrug oder ungewöhnliche Transaktionen liefern und zusätzliche Prüfungen auslösen.
- Beratung mit emotionaler Intelligenz
  In der Vermögensberatung kann Emotionen-KI unterstützen, indem sie emotionale Reaktionen auf Marktbewegungen oder Anlageentscheidungen analysiert. Berater erhalten dadurch zusätzliche Hinweise auf die Risikowahrnehmung ihrer Kunden und können ihre Empfehlungen entsprechend anpassen.

Warum emotionale Daten strategisch werden

Mit der zunehmenden Digitalisierung entsteht ein neuer Wettbewerbsvorteil: emotionale Intelligenz in datengetriebenen Entscheidungen.

Unternehmen, die emotionale Signale verstehen, können:

- Kundenbedürfnisse präziser erkennen,
- Kommunikationsstrategien verbessern,
- Kundenbindung und Empathie stärken,
- innovationsfähigere Organisationen aufbauen.

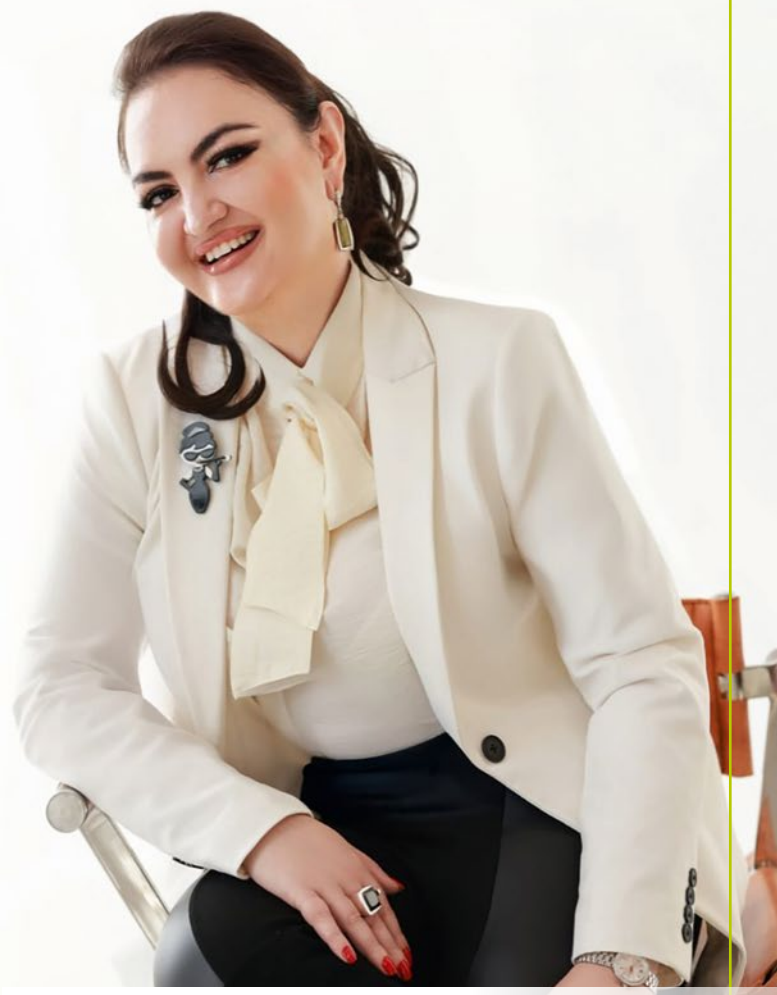
Emotionale Daten ergänzen also damit klassische Kennzahlen um eine Perspektive, die für nachhaltige Geschäftsentscheidungen entscheidend sein.

Eine gestärkte Empathie ist einer der Eckpfeiler der menschlichen KI, wenn es darum geht, dass KI menschliche Emotionen versteht und einfühlsam darauf reagiert. Hier können wir von drei Hauptarten von Empathie sprechen, nämlich 1) kognitiver Empathie, dem Verstehen menschlicher Emotionen, 2) emotionaler Empathie, dem emotionalen Teilen der Emotionen anderer, 3) und mitfühlender Empathie, bei der es nicht nur um Verstehen und Teilen geht, sondern auch darum, Hilfe anzubieten. Somit können wir feststellen, dass wir im Falle der menschlichen KI die erste und die dritte Art von Empathie haben in der Mensch-Maschine Interaktion.

Die Zukunft der Business Intelligence

Emotionen-KI und Humane KI markieren einen wichtigen Entwicklungsschritt in der Nutzung von KI im Business. Sie verbinden analytische Datenverarbeitung mit einem tieferen Verständnis menschlicher Reaktionen und Bedürfnisse. Für Firmen bedeutet das eine neue Qualität von Entscheidungsgrundlagen: Daten werden nicht nur analysiert, sondern auch emotional interpretiert mit relevanten Antworten mit einer emotionalen Wirkung.

Organisationen, die diese Technologien strategisch einsetzen, können Produkte, Dienstleistungen und Kommunikation stärker an den tatsächlichen Erfahrungen ihrer Kunden und Mitarbeitenden ausrichten. Die nächste Generation der Business Intelligence wird deshalb nicht nur datengetrieben sein – sondern emotional intelligent und human. •



DIE AUTORIN

Dr. Anna Maria Rostomyan

ist Freiberufliche Dozentin an der Fachhochschule des Mittelstandes (FHM) & NBS Northern Business School (Deutschland), internationale Autorin und Forscherin im Bereich Mensch-Maschine-Kommunikation und Emotionen-KI.

Governance
ist die Grundlage jeder KI-Strategie

Alle reden über Datensouveränität – doch kaum jemand meint dasselbe. Während Politik, Wirtschaft und Technik um Definitionen ringen, verlieren Unternehmen wertvolle Zeit. Dabei zeigt sich: Souveränität beginnt nicht beim Server-Standort, sondern bei der internen Governance. Wer hier nicht handelt, bleibt abhängig – egal, wo die Daten liegen. /// von Sven Selle

DATENSOUVERÄNITÄT IST DAS WORT DER STUNDE. Genau darin besteht auch die aktuelle Herausforderung, denn der Begriff wird in politischen Debatten, Unternehmensstrategien und Technologiediskussionen gleichermaßen verwendet, ohne dass man sich über ein gemeinsames Verständnis einig wäre. Doch die eigentliche Frage ist nicht: „Welche Definition von Datensouveränität ist die richtige?", sondern vielmehr: „Worauf muss jedes Unternehmen unabhängig von der laufenden Debatte eine Antwort haben?"

Souveränität ist eine Fähigkeit

„Datensouveränität lässt sich kaufen" ist ein weitverbreiteter Irrtum. Unternehmen investieren Jahre und Millionen in Migrationsprojekte, verlagern Daten in europäische Rechenzentren, wechseln Cloud-Anbieter oder bauen eigene Infrastrukturen, um fortan als souverän zu gelten. Doch das greift zu kurz. Denn was nützt es, wenn die Daten physisch in Frankfurt liegen, aber niemand im Unternehmen genau weiß, wer auf welche Daten zugreifen darf, woher sie stammen und wie sie verarbeitet werden?

Echte Souveränität beginnt intern. Sie entsteht durch klare Eigentumsverhältnisse, transparente Zugriffsrechte und nachvollziehbare Datenflüsse. Kurz: durch technische Data Governance. Wer diese Grundlage nicht gelegt hat, bleibt souverän auf dem Papier und abhängig in der Praxis. Das wird besonders deutlich, wenn man sich vor Augen führt, was in den meisten Unternehmen tatsächlich passiert. Daten liegen verteilt über Dutzende von Systemen, Teams entwickeln eigene Analyseumgebungen, und niemand hat einen vollständigen Überblick über den Gesamtzustand der Datenwelt. In dieser Realität ist die Frage nach dem Serverstandort zweitrangig.

Technische Governance

Wenn von Governance die Rede ist, denken viele sofort an Compliance-Abteilungen, DSGVO-Berater oder den EU AI Act. Diese regulatorische Dimension ist real und wichtig, doch ist sie nicht das Thema, das den Unterschied zwischen einer handlungsfähigen und einer gelähmten Organisation ausmacht. Entscheidend ist die technische Governance.

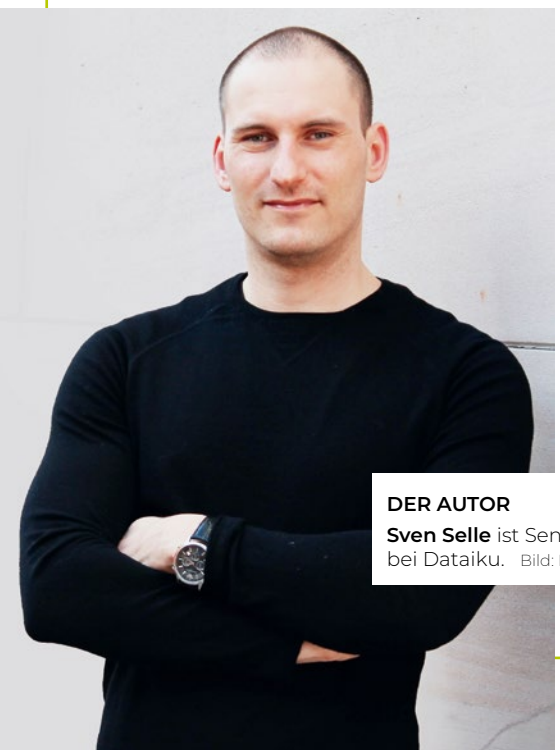
Neben dem Datenzugriff selbst müssen weitere Komponenten berücksichtigt werden, die im Kern vier Dimensionen umfassen:

- Dateneigentum und Zugriffsrechte: Wer darf welche Daten sehen oder weitergeben? Ohne klare Verantwortlichkeiten entstehen Sicherheitslücken, die innerhalb der Verwendung von KI-Agenten, die eigenständig auf Datenquellen zugreifen, fatale Folgen haben können. Sensible Informationen könnten unbeabsichtigt an LLM-Betreiber oder andere Dritte weitergegeben werden.

- Datenherkunft und Nachvollziehbarkeit: Woher stammen die Daten, die in ein Modell fließen? Welche Transformationen haben sie durchlaufen? Ohne Lineage-Tracking ist keine verlässliche Qualitätssicherung möglich.

- Dokumentation: Daten, Modelle und Workflows müssen gemeinsam verwaltet und reproduzierbar dokumentiert werden. Nur so lassen sich Änderungen nachverfolgen und Fehler auch identifizieren.

- Monitoring und Kontrolle von KI-Systemen: Gerade mit dem Aufstieg agentischer KI-Systeme wächst die Notwendigkeit, einen zentralen Überblick darüber zu haben, welche Agenten im Unternehmen aktiv sind, was sie tun und ob sie korrekt funktionieren. Agentic AI ohne Governance ist buchstäblich unkontrolliert. •



DER AUTOR
Sven Selle ist Senior Director Field Engineering EMEA bei Dataiku. Bild: Dataiku

Vertragsmanagement – mehr als „Verwaltung“

UNTERNEHMEN STEUERN LIEFERKETTEN MIT KI, VERHANDELN DEALS IN ECHTZEIT RUND UM DEN GLOBUS – und managen ihre Verträge in Excel. Was wie eine Pointe klingt, ist kein Ausnahmefall. Die Studie „Smartes Vertragsmanagement: Wo Unternehmen heute stehen” von techconsult und Ceyoniq zeigt: Fast jedes zweite Unternehmen verwaltet seine Verträge in Excel – obwohl jedes der befragten Unternehmen mindestens 100 aktive Verträge im Portfolio hat. Die Konsequenz: Kündigungsfristen laufen ab, Verträge verlängern sich automatisch, Zahlungsfristen werden verpasst. Wer heute sein Vertragsmanagement auf eine tragfähige Grundlage stellen will, braucht mehr als Zeilen und Spalten.

Vom Ablagesystem zur intelligenten Prozessplattform

Laut der techconsult-Studie haben über 40 Prozent der befragten Unternehmen in den vergangenen zwei Jahren finanzielle Schäden durch schlechtes Vertragsmanagement erlitten. Das ist kein Versagen einzelner Mitarbeitenden, sondern ein strukturelles Problem. Wer Vertragsdaten in Silos verwaltet, verliert den Überblick. Modernes Contract Lifecycle Management (CLM) denkt dieses Problem grundlegend anders. Statt Verträge lediglich zu archivieren, begleitet ein CLM-System jeden Vertrag über seinen gesamten Lebenszyklus: von der Anforderung über Verhandlung, Prüfung, Freigabe bis zur Unterzeichnung, laufenden Überwachung und schließlich der Kündigung. Mit **nscale CLM** hat Ceyoniq dazu eine Lösung entwickelt, die konsequent aus der Nutzerperspektive gedacht ist. Eine zentrale Plattform für alle Vertragsprozesse inklusive automatisierter Fristenüberwachung, revisionssicherer Ablage und KI-gestützter Dokumentenanalyse.

Souveränität beginnt bei den Vertragsdaten

Gerade weil Verträge sensible Daten eines Unternehmens enthalten, stellt sich bei der Wahl einer CLM-Plattform die entscheidende Frage: Wo liegen die Daten und wer hat darauf Zugriff? **nscale CLM** ist ein Cloud-Service, dessen Rechenzentren ausschließlich in Deutschland betrieben werden. Die nscale-Plattform ist zudem so konzipiert, dass sie vollständig ohne Microsoft-Technologie betrieben werden kann – ein klarer Vorteil für Unternehmen, die digitale Souveränität nicht nur als Schlagwort, sondern als strategische Anforderung verstehen.

Compliance und Datenschutz: Verträge als Haftungsrisiko

Verträge dokumentieren nicht nur Geschäftsbeziehungen, sondern sind Nachweis gegenüber Prüfern, Behörden und Geschäftspartnern. Wer im Audit-Fall nicht belegen kann, welche Vertragsversion zu welchem Zeitpunkt gültig war, hat ein Problem. Gleiches gilt für den Datenschutz: Vertragsunterlagen enthalten in der Regel personenbezogene Daten. Liegen sie unkontrolliert auf Fileservern oder in Posteingängen, ist eine revisionssichere Nachverfolgung schlicht nicht möglich.

Einfacher arbeiten, mehr kontrollieren

Statt CLM-Anforderungen in ein bestehendes DMS abzubilden, ist die Fachlösung **nscale CLM** konsequent auf solche Anwendungsfälle zugeschnitten. Zudem ist **nscale CLM** so intuitiv bedienbar, dass die Akzeptanz in der Belegschaft ganz natürlich entsteht. •

Mehr Informationen:
ceyoniq.com/vertragsmanagement

CEYONIQ Technology
A KYOCERA GROUP COMPANY

Agentic AI und Legacy-Systeme: Warum sie füreinander geschaffen sind

Unternehmensverantwortliche stehen heute unter enormem Druck. Sie sollen KI-Innovationen vorantreiben und gleichzeitig veraltete, störanfällige Systeme stabil halten – und das bei sinkenden Budgets und immer weniger verfügbaren Fachkräften. /// von Luis Blando

AUF DEN ERSTEN BLICK PASST DAS KAUM ZUSAMMEN. Das eine richtet den Blick nach vorn auf agentische KI und autonome Systeme, das andere zurück auf COBOL, Mainframes und gewachsene Altlasten. Viele sehen darin einen Widerspruch, tatsächlich steckt darin jedoch eine Chance.

Legacy-Systeme gelten oft als Hindernis für KI-Innovationen. Dabei bergen sie einen wertvollen Schatz an Wissen und Prozesslogik, denn in ihnen stecken Jahrzehnte an Geschäftsregeln, die kein Dokument vollständig erfasst. In Verbindung mit einer einheitlichen Plattform kann agentische KI dieses Wissen erschließen und gezielt nutzbar machen. Es geht also nicht darum, das Alte abzuschaffen, sondern es zu sichern und weiterzuentwickeln. Die vielen tausend Entwicklungsstunden, die in diese Systeme geflossen sind, sollen auch künftig Wert schaffen.

Agentische KI ist bereit, die Architektur oft nicht

Systeme, die mit möglichst wenig menschlichem Input denken, planen und handeln, sind längst keine Zukunftsvision mehr. Eine aktuelle Umfrage von OutSystems bei rund 550 Softwareverantwortlichen zeigt, dass in Europa bislang 40 Prozent der Organisationen agentische KI integriert haben, noch mehr sind es in Nordamerika (50 Prozent) und Asien (60 Prozent). Global gesehen hat fast die Hälfte der Unternehmen agentische KI fest in Anwendungen und Geschäftsabläufe eingebunden. Dennoch geraten zahlreiche Projekte ins Stocken. Ein Grund liegt in regulatorischen Vorgaben wie dem europäischen AI Act. Hinzu kommt ein zweiter Faktor, der besonders Unternehmen mit Legacy-IT betrifft. Bestehende Systeme lassen sich oft nur schwer anbinden, überwachen und automatisieren. Das Problem ist also nicht, dass die KI noch nicht ausgereift ist, sondern dass die bestehende IT-Architektur nicht für autonome Systeme ausgelegt wurde.

Legacy ist kein Ballast, sondern Potenzial

In den meisten Unternehmen bilden Altsysteme weiterhin das Rückgrat des Geschäfts. Sie rechnen Gehälter ab, steuern Lieferketten, bearbeiten Schadensfälle und schließen Finanzabschlüsse. Über Jahre hinweg haben sie komplexe Abläufe und Regeländerungen aufgenommen. Jede Codezeile entstand, weil im Geschäft etwas konkret geregelt werden musste. Genau hier kann nun agentische KI ansetzen.

Ein Beispiel aus dem Versicherungsbereich: Ein KI-Agent kann hier auf Vertragsdaten aus einem Mainframe zugreifen, zusätzliche Informationen wie Bildanalysen prüfen und den Schadenfall schließlich über eine moderne Zahlungs-API genehmigen.

DER AUTOR
Luis Blando ist CPTO bei OutSystems.
Bild: OutSystems

> „ Die Workbench schafft **Transparenz über Systemzustände** und ermöglicht Tests unter geschützten Bedingungen, bevor KI-Agenten produktiv eingesetzt werden. *Luis Blando*

Dafür sind weder ein vollständiger Umbau der bestehenden Systeme noch ein riskanter Neustart nötig, stattdessen passt sich die KI an die bereits vorhandene komplexe Logik an. Das Altsystem bleibt dabei die zentrale Datenbasis, während der KI-Agent die nötigen Schritte anstößt und moderne Abläufe auf Grundlage der verfügbaren Informationen koordiniert.

Das bedeutet, Unternehmen müssen ihre Systeme nicht vollständig ersetzen. Sie brauchen vielmehr eine Möglichkeit, agentische KI mit den Daten und Funktionen der bestehenden Plattformen zu verbinden und Abläufe über alte wie neue Systeme hinweg kontrolliert zu steuern. Hier setzt das Prinzip einer Agent Workbench an. In dieser Testumgebung können Teams KI-Agenten entwerfen, anbinden und verwalten, unabhängig davon, ob sie mit modernen oder älteren Systemen arbeiten.

Statt vieler einzelner Skripte entsteht so eine verlässliche Grundlage für die Integration und den Betrieb von KI-Agenten. Wiederverwendbare Schnittstellen ersetzen fragile Direktanbindungen, und standardisierte Abläufe sorgen für Konsistenz. Gleichzeitig definiert die Workbench klare Regeln für Zugriffe und Zuständigkeiten. Sie schafft Transparenz über Systemzustände und ermöglicht Tests unter geschützten Bedingungen, bevor KI-Agenten produktiv eingesetzt werden. Sie legt fest, wie diese reagieren dürfen und wann eine Übergabe an Menschen vorgesehen ist. Sicherheits- und Governance-Anforderungen sind dabei integriert.

Agenten als digitale Wartungsteams

Doch die Verbindung von Agenten und Legacy-Systemen ist nicht nur eine technische Herausforderung – sie ist auch eine Frage der verfügbaren Fachkräfte. Weltweit fällt es Unternehmen schwer, Entwickler mit Kenntnissen in älteren Sprachen und Plattformen zu finden und zu halten. Gleichzeitig müssen diese Systeme immer häufiger angepasst werden. Ohne entsprechendes Know-how wirkt jedoch jede Änderung riskant.

Mit der passenden Plattform kann agentische KI diese Lücke schließen. Während Entwickler die Systeme im Blick behalten sowie Änderungen prüfen und freigeben, können KI-Agenten die Rolle digitaler Wartungsteams übernehmen: Sie überwachen Systemzustände, analysieren Protokolle und melden Auffälligkeiten. Zudem können sie Patches vorschlagen und Code-Änderungen erzeugen, die Menschen anschließend freigeben. Darüber hinaus automatisieren sie wiederkehrende Aufgaben wie Regressionstests, Konfigurationsvergleiche oder Abhängigkeits-Updates. Damit entlasten sie Teams von zeitintensiven Tätigkeiten.

Das senkt auch die Hürde für jüngere Entwickler: In Low-Code-Umgebungen können sie mithilfe agentischer Werkzeuge an der Pflege und Weiterentwicklung von Altsystemen mitarbeiten. Sie können Fragen in natürlicher Sprache stellen, Änderungen erzeugen und sich darauf verlassen, dass die Plattform Regeln durchsetzt und Prüfungen anstößt.

Das führt schließlich auch zu einem neuen Rollenbild. 69 Prozent der Softwareverantwortlichen erwarten laut der Umfrage von OutSystems neue, spezialisierte Jobprofile durch den Einsatz von KI. 63 Prozent rechnen mit umfangreichen Weiterbildungsmaßnahmen. KI hilft damit, dem Fachkräftemangel zu begegnen und zugleich Teams aufzubauen, die sicher und kompetent mit der Technologie arbeiten.

Zwei Herausforderungen, eine Strategie

Viele IT-Verantwortliche haben lange getrennt gedacht. Einerseits stand die Modernisierung von Legacy-IT, andererseits die Einführung von KI-Anwendungen. Beide Vorhaben konkurrierten um Budget, Fachkräfte und Aufmerksamkeit. In Wirklichkeit gehören sie zusammen. Ohne KI lässt sich der Kern der IT kaum in der Geschwindigkeit erneuern, die das Geschäft verlangt. Und KI, die den Kern ignoriert, bleibt nur an der Oberfläche. •

Trends im IT-Management:
Steuern statt verwalten

Die IT-Infrastruktur in Unternehmen hat sich von einem Kostenfaktor zum Business-Enabler entwickelt. Das verändert die Rolle des IT-Managements und macht es zur neuen Schaltzentrale. /// von Marius Dunker

TECHNOLOGIE-ENTSCHEIDUNGEN BEEINFLUSSEN IN DER HEUTIGEN ZEIT UNMITTELBAR MARGEN, Time-to-Market, Compliance, Wettbewerbsfähigkeit und Entscheidungsfähigkeit. IT-Verantwortliche sind nicht länger reine Systemverwalter, sondern zugleich Innovations- und Risikomanager, Finanzplaner und Vermittler zwischen Business und Technologie. Fünf wichtige Trends zeigen, worauf es im IT-Management jetzt ankommt.

Trend 1: Geschäftswert statt Einkaufspreis

Die Enterprise-IT sucht nach einer neuen Definition von Erfolg: weg vom Fokus auf Kostensenkung, hin zu Kennzahlen, die ROI, Produktivität, Risiken und Nutzen messbar machen. Laut dem „State of the Cloud Report" von Flexera setzen 49 Prozent der IT-Teams auf Unit Economics und brechen Kosten auf Services, Workloads und Anwendungen herunter. Der Trend ist klar: Das IT-Management „verwaltet" nicht mehr nur. Es muss Kosten, Risiken und Nutzen transparent machen – und trägt Mitverantwortung für Unternehmenserfolg.

Trend 2: Die neue Ökonomie von KI

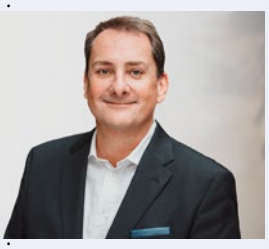
Die Geschwindigkeit der KI-Adoption übertrifft alle Prognosen. Ein Blick in den „AI Pulse Report 2026" von Flexera zeigt: 94 Prozent der IT-Entscheider suchen momentan nach neuen Wegen, KI in ihren Technologie-Stack zu integrieren. Es geht längst nicht mehr nur um einzelne KI-Modelle. Analytics-Plattformen, Datenpipelines sowie Speicher- und Rechenkapazitäten rücken ins Zentrum vieler Enterprise-AI-Roadmaps – und treiben den Kostendruck massiv nach oben.

Die finanzielle Sprengkraft von KI legt die Grenzen klassischer Kostensteuerung schonungslos offen. Das neue Finanzmodell von KI braucht neue Disziplinen, mehr Transparenz und eine Governance, die eng am tatsächlichen Nutzungs- und Kostenverhalten ausgerichtet ist. Das wiederum funktioniert nur, wenn die KI-Initiativen auf vertrauenswürdigen und konsistenten IT-Daten aufbauen. Bei dieser Aufgabe wandelt sich das IT Asset Management (ITAM) zum Enabler für KI-Governance und AI Value Management.

Trend 3: Cloud-Reife statt Cloud-Wachstum

In den letzten Jahren ist die Cloud größer, aber nicht zwangsläufig erwachsen geworden. SaaS-Sprawl, KI-Boom, Hybrid- und Multi-Cloud haben modernen IT-Landschaften einen Wachstumsschub verpasst: mehr Services, mehr Workloads, mehr Schnittstellen, mehr Anbieter, mehr Verbrauchsmodelle. Diese Komplexität trifft oft auf Cloud Governance, die zu wenig Steuerbarkeit bietet.

In Sachen Betrieb, Kostensteuerung und Verwaltung zeichnet sich daher eine Neuausrichtung ab: Nach Jahren aggressiver Cloud-Migration geht es künftig darum, Workloads dort zu platzieren, wo sie technisch, wirtschaftlich oder regulatorisch am sinnvollsten laufen. Cloud Repatriation gewinnt an Bedeutung: Anwendun-



DER AUTOR
Marius Dunker
verantwortet als Regional Vice President Enterprise Sales DACH bei Flexera das Geschäft in Deutschland, Österreich und der Schweiz.
Bild: Flexera

> „Unternehmen brauchen keine weitere Tool-Schicht, sondern eine Daten- und Steuerungsebene für ITAM, FinOps, SaaS, Cloud und KI. *Marius Dunker*

gen, Workloads und Daten wandern zurück. Das ist kein Rückzug aus der Cloud, sondern eine Verschiebung des Fokus – von maximaler Cloud-Expansion und Cloud-Only-Strategie hin zu Hybrid-Cloud-Modellen und effizienterer Architektur-, Kosten- und Betriebssteuerung.

Trend 4: Neue Definition von FinOps

FinOps begann als Cloud-fokussierte Disziplin für das Kostenmanagement: Engineering-, Finance- und Business-Teams sollten gemeinsam den geschäftlichen Wert der Cloud steuern. Angesichts der Dynamik rund um KI, SaaS und Cloud stößt dieser enge Cloud-Fokus jedoch an Grenzen. Mittlerweile versteht sich FinOps als mehr als nur Cloud-Kostenmanagement. Es geht um die Steuerung des gesamten Technologieportfolios. Die neue Grundausrichtung der FinOps Foundation bringt es auf den Punkt: „Advancing the People who manage the Value of Technology" statt „Advancing the People who manage the Value of Cloud". Damit positioniert sich FinOps als ganzheitlicher Managementansatz, der nicht nur auf Einsparungen blickt, sondern Technologieausgaben konsequent mit Nutzen koppelt.

Trend 5: Digitale Souveränität

Mit AI Act, strengeren Vorgaben zur Datennutzung und DORA gelten in Europa andere IT-Regeln. Das fordert vom IT-Management mehr Compliance, Transparenz und Verantwortung im Umgang mit Technologien. Was auf den ersten Blick wie regulatorische Gängelei wirkt, kann jedoch ein strategischer Vorteil sein: Wer nachvollziehbare Prozesse, klare Datenführung und belastbare Entscheidungen vorweisen kann, stärkt Resilienz und Vertrauen.

Digitale Souveränität ist dabei immer auch eine Cloud-Frage: Wo liegen meine Daten, wer kontrolliert Zugriff und Betrieb – und wie abhängig bin ich von einzelnen Anbietern? Die Zukunfts- und Innovationsfähigkeit europäischer Unternehmen entsteht nicht durch Abschottung. Wichtiger werden Kontrolle, Transparenz und echte Handlungsfähigkeit in komplexen Cloud-Umgebungen.

Trend 6: Plattformisierung statt Tool-Landschaften

Kostenkontrolle scheitert heute selten an zu wenigen Daten, sondern daran, dass sie über zu viele Systeme verteilt sind. Lizenzen liegen im ITAM, Cloud-Verbrauch im FinOps, SaaS-Kosten in Fachbereichen, KI-Nutzung oft irgendwo dazwischen. So entsteht keine Transparenz, sondern blinde Flecken.

Genau deshalb wird Plattformisierung zum nächsten Reifeschritt im IT-Management. Unternehmen brauchen keine weitere Tool-Schicht, sondern eine gemeinsame Daten- und Steuerungsebene für ITAM, FinOps, SaaS, Cloud und KI. Erst wenn Nutzung, Kosten, Risiken und Verantwortung zusammenlaufen, werden Technologieportfolios steuerbar.•

Low-Code für Fachabteilungen: Gamechanger für die Automatisierung

Die Low-Code-„Entwicklung“ etabliert sich zusehends als Innovationstreiber. Weniger komplexe Anwendungen lassen sich so deutlich schneller erstellen – ganz ohne tiefgreifende Programmierkenntnisse. Grafische Konfigurationsoberflächen machen es möglich. Die IT stellt deren Validität sicher und verantwortet weiterhin ambitioniertes Coden. /// von Dirk Hennig

DIE KONFIGURATION AUF LOW-CODE-BASIS HAT DIE SOFTWAREENTWICKLUNG sozusagen revolutioniert. Denn das klassische Programmieren von Applikationen war vor der Low-Code-Ära eine zeitaufwändige sowie personalintensive Angelegenheit – und es brauchte Spezialisten mit fundiertem Wissen. In Zeiten von Fachkräftemangel und/oder angespannter Wirtschaftslage kam die Low-Code-Technologie also zur rechten Zeit.

DER AUTOR
Dirk Hennig
ist Director of Product Experience bei der ELO Digital Office GmbH.

> „ Die Low-Code-Plattform basiert auf intuitiven Schnittstellen, mit Hilfe derer sich fachliche Lösungen durch Auswählen und Konfigurieren visueller Elemente erzeugen lassen. Zum Einsatz kommen **wiederverwendbare Komponenten**: Sie bieten vordefinierte Elemente, die angepasst und kombiniert werden können.
>
> *Dirk Henning*

Der Low-Code-Ansatz ist die ideale Mitte zwischen klassischem Coding und einer funktional doch wesentlich eingeschränkteren No-Code-Konfiguration. Dabei lässt sich auf eine Art Baukasten aus standardisierten und wiederverwendbaren Konfigurationsmodulen zugreifen. Dieser bietet zusätzlichen Spielraum für tiefergehende Erweiterungen in kontrollierten Bereichen, die – neben der Wartbarkeit der Lösung – auch eine hohe Sicherheitsstufe und Grundperformance gewährleisten. Der Mehrwert zeigt sich in einer höheren Stabilität der Lösung. Um die Anwendungen anforderungsgerecht zu generieren, stehen den Nutzern intuitive und visuelle Komponenten zur Modellierung zur Verfügung. Damit erfolgt das Entwickeln, Anpassen oder Erweitern von Lösungen in einem Bruchteil der Zeit und somit eindeutig kostengünstiger. Der große Vorteil: Technisch versierte Mitarbeiter der Fachbereiche, sogenannte Citizen Developer, sind in der Lage, selbst einen großen Anteil der Aufgabe zu übernehmen – und aktiv an der Gestaltung ihrer Prozesse mitzuwirken. So können sie dank ihres Prozesswissens fachliche Anforderungen schnell und präzise umsetzen.

Wiederkehrende Abläufe mit Low-Code automatisieren

Geschäftsprozesse zu optimieren und zu automatisieren, ist eine ureigene Domäne des Informationsmanagements. Ging es im ersten Schritt um die Digitalisierung der firmeneigenen Dokumente, so folgten im nächsten

die Geschäftsprozesse – als Grundlage einer sukzessiven Automatisierung und eines Abbaus manueller Arbeitsschritte. Hier spielt die nahtlose Integration aller Business-Anwendungen eine tragende Rolle. Denn nur so lassen sich Medienbrüche zugunsten einer durchgängigen Arbeitswelt vermeiden. ELO Digital Office hat daher seine Digitalisierungsplattform ELO ECM Suite mit vollumfänglichen Low-Code-Möglichkeiten ausgestattet – ebenso wie seine Business Solutions für Rechnungs- und Vertragsmanagement. Die Low-Code-Plattform basiert auf intuitiven Schnittstellen, mit Hilfe derer sich fachliche Lösungen durch Auswählen und Konfigurieren visueller Elemente erzeugen lassen.

Zum Einsatz kommen wiederverwendbare Komponenten: Sie bieten vordefinierte Elemente, die angepasst und kombiniert werden können. Dank Aufgabenautomatisierung lassen sich Prozesse wie das Versenden von Benachrichtigungen, die Verzahnung mit anderen Plattformen oder das Verfassen von Berichten optimieren. Erhebliche Unterstützung erwächst aus der Integration in externe Dienste wie Datenbanken, Programmierschnittstellen (APIs) oder Cloud-Dienste. Auch Verknüpfungen mit Drittsystemen beispielsweise für Enterprise-Resource-Planning (ERP) oder Customer-Relationship-Management (CRM) sind so rasch konfiguriert – und in fachliche Lösungen integriert. Eingebettete Sicherheit gewährleisten Mechanismen zur Authentifizierung, Zugriffskontrolle und Datenverschlüsselung.

Optimierte Prozesse dank Kombination mit KI

Aus der Kombination mit Künstlicher Intelligenz (KI) resultieren deutlich optimierte Prozesse. In der Folge entsteht ein skalierbares System, das mit den jeweiligen Anforderungen wächst – schnell, intelligent und zukunftssicher. Dabei kommen zwei Aspekte zum Tragen: Zum einen die leichte Anbindbarkeit beliebiger KI-Modelle an die Low-Code-Plattform. Zum anderen das einfache Einziehen von Sicherheitsmechanismen als Schutz vor zunehmenden Bedrohungsszenarien.

Der Anwender kann die Grenzen der KI klar definieren und die Lösung so absichern. Beispielsweise lassen sich sogenannte Pseudonymiser als zusätzliche Sicherungsschicht vorschalten, um personenbezogene Daten zu schützen.

Mehrwert für Fachbereiche

(Fach)Anwendern kommen nahtlos ineinandergreifende Prozesse, höhere Skalierbarkeit, Produktivität und Kosteneffizienz zugute. Manuelle Arbeitsschritte werden auf ein Minimum zurückgefahren. Weitere Pluspunkte sind die Kompatibilität mit Drittsystemen und nicht zuletzt ein geringerer Bedarf an Entwicklerressourcen. Hochkompetente Software-Ingenieure können sich strategischer ausrichten.

Wie sich das in der Praxis auswirkt, zeigt folgendes Beispiel aus dem Finanzwesen:

Soll eine Rechnung freigegeben und gleichzeitig der passenden Vertragsakte zugeordnet werden, können die Fachanwender mit Hilfe vorgefertigter Bausteine einen automatisierten Workflow erstellen. Die Low-Code-Plattform nutzt die verfügbaren Metadaten, wie Rechnungsaussteller und Auftragsnummer, als Grundlage dafür. Über konfigurierbare Bausteine lassen sich Regeln und Bedingungen definieren, um die Schritte bei der Rechnungsbearbeitung festzulegen. Abhängig von den Metadaten steuert der Workflow automatisch die Freigabeprüfung an. Nach erfolgter Freigabe gelangt die Rechnung automatisiert in die zugehörige Vertragsakte. Routineaufgaben laufen so im Hintergrund ab, ganz ohne manuelle Intervention.

Win-win-Situation dank perfektem Zusammenspiel von Fachbereich und IT

Low-Code-Technologie senkt die Eintrittshürden für die Automatisierung, verkürzt die Projektdauer und lässt wertvolles Wissen aus den Fachbereichen direkt in die Prozessgestaltung einfließen. Unternehmen können schneller reagieren, Abläufe stabilisieren und das Potenzial ihrer IT-Systeme besser ausschöpfen.

Automatisierte Workflows verarbeiten hohe Mengen an Informationen zuverlässig und prompt. Low-Code-Technologie steht für Skalierbarkeit und verbessert als strategisches Instrument nicht nur operative Prozesse, sondern fördert auch Innovationen. Unternehmen können neue Abläufe rascher testen, etwa durch Prototypen oder MVPs (Minimal Viable Products). Dies stärkt ihre Innovationskraft und verkürzt die Time-to-Market. Daraus resultieren langfristig echte Wettbewerbsvorteile. •

LOW-CODE TECHNOLOGIE

ANSATZ UND MEHRWERT IM ÜBERBLICK

Der Ansatz

Low-Code bildet die Mitte zwischen klassischem Coding und No-Code. Über grafische Oberflächen und wiederverwendbare Module entstehen Anwendungen in kürzester Zeit, ohne tiefe Programmierkenntnisse. Die IT sichert Validität, Performance und Wartbarkeit weiterhin ab.

Der Mehrwert

Citizen Developer setzen ihr Prozesswissen direkt in Anwendungen um. Es resultieren nahtlose Prozesse, Skalierbarkeit und Kosteneffizienz. Manuelle Arbeitsschritte werden minimiert, Drittsysteme wie ERP oder CRM lassen sich rasch anbinden. Hochqualifizierte Software-Ingenieure können sich dadurch deutlich strategischer ausrichten.

Patientendaten in der Cloud: So sehen sichere Lösungen aus

Seit 2024 dürfen Kliniken Patientendaten auch in der Cloud verarbeiten. Doch welche Infrastruktur erfüllt die strengen Vorgaben und schützt gleichzeitig vor fremdem Zugriff? /// von Thomas Chudo

PATIENTENDATEN DURFTEN BIS VOR KURZEM NICHT IN CLOUD-UMGEBUNGEN VERARBEITET WERDEN. Seit Verabschiedung des DigiG im Frühjahr 2024 öffnen sich die Rahmenbedingungen. § 393 SGB V schafft erstmals einen Erlaubnistatbestand für die Cloud-Verarbeitung von Gesundheitsdaten – geknüpft an das BSI-C5-Testat Typ 2.

Cybersicherheit: Healthcare im Visier

Wie dringend der Schritt in professionelle Infrastrukturen ist, verdeutlicht die Bedrohungslage. Ransomware-Angriffe auf Kliniken gehen weit über finanzielle Schäden hinaus. Es braucht forensische Kompetenz und ein Security Operations Center, das Vorfälle rund um die Uhr überwacht. Doch in welche Cloud sollen sensible Gesundheitsdaten wandern?

Der US Cloud Act ermöglicht amerikanischen Behörden den Zugriff auf Daten bei US-Anbietern – unabhängig davon, ob die Server in Europa stehen. Die Konsequenz sind souveräne Infrastrukturen, betrieben auf deutschem Boden, unter deutschem Recht, ohne Hintertüren für fremde Jurisdiktionen.

Souveräne Cloud als Antwort: Offenheit statt Abhängigkeit

An dieser Schnittstelle setzt zum Beispiel die Noris Sovereign Cloud (nSC) an. Die Plattform basiert auf den offenen Standards des Sovereign Cloud Stack – ohne proprietäre Abhängigkeiten und ohne Vendor Lock-in.

Betrieben in deutschen Hochsicherheitsrechenzentren, zertifiziert nach EN 50600, ist sie DSGVO- und KRITIS-konform sowie nach BSI C5 testiert. Damit lassen sich Patientendaten in einer Cloud verarbeiten, die BSI-Anforderungen und die Vorgaben des Krankenhauszukunftsgesetzes erfüllt.

Fazit: Der Weg ist vorgezeichnet

Der Gesundheitssektor muss das Rad nicht neu erfinden. Datenschutz, Hochverfügbarkeit, Compliance, Schutz vor Cyberangriffen sind in regulierten Branchen wie dem Finanzwesen seit Jahren Alltag. •

FAQ: CLOUD-NUTZUNG IN KLINIKEN

Was ist das BSI-C5-Testat?

Das BSI-C5-Testat definiert Mindestanforderungen an sicheres Cloud Computing. Es wird von unabhängigen Wirtschaftsprüfern nach BSI-Regeln vergeben. Bei Typ 1 wird geprüft, ob eine Plattform die Sicherheitsanforderungen grundsätzlich erfüllen kann. Bei Typ 2 wird nach mindestens einem Jahr Betrieb überprüft, ob die Maßnahmen tatsächlich gelebt werden. Für die Verarbeitung von Patientendaten ist Typ 2 zwingend erforderlich.

Warum sind US-Hyperscaler bei Patientendaten problematisch?

Der US Cloud Act ermöglicht amerikanischen Behörden den Zugriff auf Daten bei US-Anbietern – auch wenn die Server in Europa stehen. Bei Gesundheitsdaten ist dieses Risiko besonders gravierend, da sie zur Erpressung, Diskriminierung oder Benachteiligung bei Versicherungen missbraucht werden können.

Was ist der Sovereign Cloud Stack?

Der Sovereign Cloud Stack (SCS) ist ein Open-Source-Standard der Open Source Business Alliance. Er bildet die technische Grundlage für souveräne Cloud-Plattformen, die ohne proprietäre Abhängigkeiten von US-Hyperscalern auskommen und vollständig im EU-Rechtsraum betrieben werden können.

DER AUTOR
Thomas Chudo
ist Senior Manager Public/Health bei Noris Network.
Bild: Noris Network

Cyber Risk & Resilience

Business Email Compromise: So stoppen KMU die neue Phishing-Generation

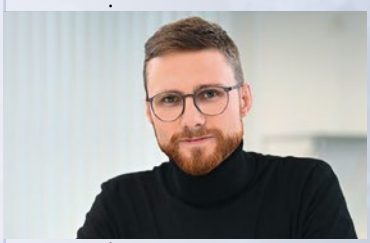
Tizian Kohler, Head of Security bei Adlon Intelligent Solutions erklärt im Gespräch, warum Identitätsschutz, genau definierte Prozesse und SOC-Erkennungen von Business Email Compromise entscheidend sind – und welche drei Schritte Mittelständler sofort angehen sollten. /// von Heiner Sieger

Wie ist die aktuelle Bedrohungslage rund um Business Email Compromise (BEC) – und wo gelingt Angreifern noch der Erstzugang?
Tizian Kohler | Die Lage ist konstant hoch. Angreifer passen sich Verteidigungsmechanismen schnell an, nutzen KI für authentische Sprache und täuschend echte Layouts und verlagern ihre Taktiken zunehmend außerhalb der „Schutzzone" des Unternehmens. Der Erstzugang erfolgt meist über Phishing – besonders dort, wo Multifaktor-Authentifizierung (MFA) fehlt oder nur für Administratoren aktiviert ist. Ohne robuste Identitätssicherung werden kompromittierte Konten zur Drehscheibe für weitere Schritte.

Können Sie ein anonymisiertes Beispiel skizzieren – vom initialen Phishing bis zur gefälschten Rechnung?
TK | Typisch ist Massenversand. Ein Klick führt auf eine täuschend echte Microsoft-Login-Seite. Nach der Eingabe von Anmeldedaten – teils inklusive zweitem Faktor – übernehmen die Täter das Postfach, lesen mit, kartieren Zahlungs- und Projektkommunikation und richten Weiterleitungsregeln ein. Antworten von Dritten verschwinden in Unterordnern; das Opfer merkt die Parallelkommunikation nicht. Im passenden Moment verschicken die Täter manipulierte Rechnungen im Namen des Opfers. Fehlen technische und organisatorische Kontrollen, werden diese bezahlt – vom Start-up bis zum Konzern.

Wie oft sehen Sie diese Abläufe?
TK | Phishing täglich. Bis zur erfolgreichen Rechnungsmanipulation braucht es mehrere Schritte, doch ohne wirksame Abwehr ist das weiterhin häufig. Professionalisiert wird vor allem die Vorbereitung: besseres Social Engineering, präzisere Timing-Fenster, mehr Gedud beim Ausspähen.

Was sind Ihre Sofortmaßnahmen für KMU – die Must-haves und ein pragmatischer Start?
TK | Erstens: MFA für alle Konten, nicht nur für Administratoren. Identitäten sind das primäre Einfallstor. Zweitens: kontinuierliche Sensibilisierung – kurze, wiederkehrende Trainings, simulierte Phishing-Kampagnen, klare Meldewege. Drittens: ein E-Mail-Security-Gateway bzw. Microsoft Defender for Office 365, das Phishing früh abfängt. Viertens: klare Reaktionsverantwortung – wer prüft Alarme, wer entscheidet, wer informiert? Diese Basis senkt das Risiko drastisch und ist schnell umsetzbar.



DER GESPRÄCHSPARTNER
Tizian Kohler
ist Head of Security bei ADLON Intelligent Solutions.
Zuvor war er Cyber-Ermittler bei der Polizei sowie Leiter von Security Operations Center und Cloud Security in verschiedenen Unternehmen.

Wie erkennen und stoppen Sie mehrstufige Phishing-Strecken in einem Managed SOC?
TK | Wir kombinieren Telemetrie aus Microsoft-Sicherheitsprodukten mit kundenspezifischen Erkennungsregeln. Beispiel: Eine E-Mail mit auffälligem Betreff enthält einen Link zu legitimen Diensten wie OneDrive oder Dropbox. Klickt der Nutzer binnen kurzer Zeit, korrelieren wir Betreff, Linkziel, User-Kontext und weitere Log-Muster. Trifft die UND-Verknüpfung zu, wird alarmiert und automatisiert eingedämmt – etwa durch Session-Invalidierung oder Blockieren der Regelanlage im Postfach. Eigene Use-Cases bringen uns vor die reinen Standarderkennungen.

Und was können Unternehmen ohne eigenes SOC realistisch tun?
TK | Ein E-Mail-Security-Gateway ist Pflicht, um Phishing vor Zustellung zu filtern. Nutzen Sie das integrierte Alerting konsequent: Benennen Sie Verantwortliche, die Alarme zeitnah bewerten, Playbooks anwenden und Maßnahmen auslösen. Kombiniert mit flächendeckender MFA, Basishärtung und Schulungen ist das für kleine Unternehmen ein wirksamer und bezahlbarer Ansatz.

SECURITY INSIGHT

MEHR ERFAHREN ...
Hören Sie auch den ausführlichen Podcast zum Thema mit Tizian Kohler.

> **„ Ein E-Mail-Security-Gateway ist Pflicht**, um Phishing vor Zustellung zu filtern. Nutzen Sie das integrierte Alerting konsequent: Benennen Sie Verantwortliche, die Alarme zeitnah bewerten, Playbooks anwenden und Maßnahmen auslösen.
>
> *Tizian Kohler*

Reicht Technik aus – oder braucht es mehr Organisation in der Rechnungsprüfung?
TK | Es braucht das Dreieck aus Technik, Mensch und Prozess. Technik blockiert viel, aber Prozesse sichern den „letzten Meter": Vier-Augen-Prinzip ab definierten Betragsschwellen, Rückruf beim bekannten Ansprechpartner unter verifizierter Nummer, Abgleich sauber geführter Lieferantenstammdaten (Empfänger, IBAN, Zahlungsadresse). Bei Änderungen gilt: keine Freigabe ohne unabhängige Verifikation. So werden selbst gut gemachte BEC-Ketten ausgebremst.

Viele BEC-Kampagnen spielen auf Microsoft-Ökosysteme. Was bedeutet „Identitäten zuerst" konkret?
TK | Konsequente MFA, Schutz riskanter Legacy-Protokolle, bedingter Zugriff nach Risiko, strenge Richtlinien für Regelanlagen im Postfach, Logging und Alarme für ungewöhnliche Sign-in-Muster, Schutz vor Weiterleitungsregeln nach extern und ein E-Mail-Schutz, der Links und Anhänge dynamisch prüft. Identität ist die neue Perimeter – alles ordnet sich darum.

Warum setzen Sie im Schwachstellenmanagement auf Risiko statt nur CVSS?
TK | CVSS bewertet die generelle Schwere, aber nicht die Relevanz im Unternehmenskontext. Wir gewichten zusätzlich Asset-Kritikalität (zum Beispiel Domain Controller vs. Testsystem) und Ausnutzungswahrscheinlichkeit (vorhandene Exploits, aktive Ausnutzung, Hersteller-Telemetrie). So kann eine CVSS-5-Lücke auf einem kritischen System dringender sein als eine CVSS-9-Lücke auf einem Rand-Asset. Das erhöht Wirkung pro investierter Stunde.

Welche KPIs helfen Mittelständlern, wirksam zu bleiben?
TK | Drei Kennzahlen haben sich bewährt: 1) Anzahl kritischer Findings über Zeitraum X – mit Trend möglichst abnehmend. 2) Patch-Quote kritischer Lücken innerhalb von 14/30 Tagen. 3) Time to Remediate (TTR) je Kritikalität. Diese Trias misst Tempo, Disziplin und Priorisierung. Wichtig: Zuständigkeiten, Fristen und Ausnahmen dokumentieren.

Welche Meldepflichten gelten nach Vorfällen?
TK | DSGVO: Sind personenbezogene Daten betroffen, binnen 72 Stunden an die Aufsichtsbehörde melden – mit Erstbewertung, betroffenen Datenkategorien und Sofortmaßnahmen. NIS2: Für betroffene, sektorrelevante Unternehmen gilt eine Erstmeldung binnen 24 Stunden und eine Detailmeldung nach 72 Stunden. Grundlage sind belastbare Logs, klare Verantwortlichkeiten und vorbereitete Vorlagen.

Und was droht, wenn Unternehmen nicht melden?
TK | Bußgelder, Auflagen und – unter NIS2 – verbindliche Umsetzungspläne mit Fristen. In gravierenden Fällen drohen Haftungsrisiken für Geschäftsleiter.

Wer transparent meldet, sauber dokumentiert und zügig Maßnahmen ergreift, steht deutlich besser da – fachlich wie regulatorisch. •

Wie Unternehmen ihre Cyberresilienz stärken können

Das neue Lagebild Cybercrime 2025 des BKA zeigt einen deutlichen Anstieg von DDoS-Angriffen. Zugleich weist die aktuelle IT-Sicherheitsumfrage des eco e.V. auf große Lücken bei der Notfallvorsorge in vielen Unternehmen hin. Wie können Krisenpläne für Cyberangriffe und moderne Sicherheitsarchitekturen zur Stärkung der Cyberresilienz in Unternehmen beitragen? /// von Stefan Girschner

HERMANN RAMACHER (Bild: ADN Distrubution)

Geschäftsführer der ADN Distribution GmbH

Steigende DDoS-Zahlen und immer professionellere, oft KI-gestützte Angriffe zeigen: Cyberresilienz ist kein Einzelprodukt mehr, sondern ein Zusammenspiel aus Architektur, Prozessen und Reaktionsfähigkeit. Für unsere Partner im Channel heißt das: Weg von punktuellen Sicherheitslösungen, hin zu integrierten Security-Stacks. Moderne Architekturen folgen konsequent Zero Trust, setzen auf saubere Identitäten, durchgängige Zugriffskontrollen und volle Transparenz über alle Ebenen hinweg. Nur so lassen sich Angriffe früh erkennen, automatisiert abwehren und vor allem in ihrer Ausbreitung begrenzen.

Genauso entscheidend ist aber die operative Ebene: Im Ernstfall zählt nicht die Theorie, sondern die Reaktionsgeschwindigkeit. Genau hier setzen belastbare Krisenpläne an. Sie geben klare Leitplanken vor: Wer handelt wann, wer entscheidet, wie wird kommuniziert. Das reduziert Komplexität, vermeidet Stillstand und verkürzt Reaktionszeiten signifikant.

Für Reseller ergibt sich daraus eine große Chance: Kunden brauchen heute keine isolierten Tools mehr, sondern ganzheitliche Sicherheitskonzepte – inklusive Notfallplanung und regelmäßiger Tests. Genau hier liegt der Mehrwert. Als VAD sehen wir unsere Rolle darin, Partnern nicht nur Technologien bereitzustellen, sondern sie zu befähigen, diese ganzheitlich zu verkaufen und umzusetzen. Denn am Ende gewinnt der, der Security nicht nur liefert, sondern operationalisierbar macht. •

MICHAEL SCHRÖDER (Bild: Eset)

Head of Product Marketing bei der Eset Deutschland GmbH

Krisenpläne und moderne Sicherheitsarchitekturen sind zwei Seiten derselben Resilienz-Medaille. Die Architektur senkt Eintrittswahrscheinlichkeit und Schaden. Der Krisenplan sorgt dafür, dass im Ernstfall nicht gesucht, sondern entschieden wird. Das BKA-Lagebild Cybercrime 2025 zeigt, warum das nötig ist: 2025 wurden unter anderem 1.041 Ransomware-Angriffe und 36.706 DDoS-Fälle registriert. Das Dunkelfeld dürfte deutlich größer sein.

Hier setzt Eset mit einem Zero-Trust-orientierten Sicherheitsmodell an. Vertrauen wird nicht vorausgesetzt, sondern laufend überprüft. Dazu gehören gehärtete Geräte, abgesicherte Identitäten durch Multi-Faktor-Authentifizierung, verschlüsselte Daten, geschlossene Schwachstellen sowie Schutz für E-Mail- und Cloud-Umgebungen. Der Erfolgsgarant ist aber das Zusammenspiel. Aus einzelnen Sicherheitsmaßnahmen muss eine Kette werden: vom Endpoint über Erkennung und Reaktion bis zur Wiederherstellung verschlüsselter Daten durch Ransomware Remediation von Eset. Gleichzeitig bleibt Cyberresilienz mehr als Technologie. Kein Produkt ersetzt Notfallorganisation, Kommunikation, Rechtsbewertung, Wiederanlaufkonzepte oder regelmäßige Übungen. Richtig integriert liefert Eset dafür zentrale Bausteine: weniger Einfallstore, kleinere Angriffsflächen, schnellere Entscheidungen und weniger Betriebsunterbrechung. Cyberresilienz heißt nicht, unverwundbar zu sein. Sie bedeutet, auch im Fall eines Incidents handlungsfähig zu bleiben. •

von oben links:

Hermann Ramacher,
Michael Schröder, Richard Werner,
Tommy Grosche

SECURITY INSIGHT

RICHARD WERNER (Bild: Trend Micro)

Security Advisor bei TrendAI, ein Geschäftsbereich von Trend Micro

Organisationen fehlt häufig der Überblick über ihre Infrastruktur und deren spezifische Herausforderungen. Dadurch lässt sich die Gefahrenlage nur schwer bestimmen. Oft wird zudem nur punktuell verteidigt wird und die Koordination der einzelnen Maßnahmen damit zu einer organisatorischen Herausforderung. Kommt es zum Angriff werden zuvor übersehene Probleme zur sprichwörtlichen Achillesverse. Um sich auf den Ernstfall vorzubereiten, sollten Unternehmen mögliche blinde Flecken identifizieren und automatisiert die Cyber-Risikosituation überwachen. Moderne Sicherheitsarchitekturen und -Plattformen sind in der Lage, solche Informationen zu erfassen, zu zentralisieren und damit die genannten organisatorischen Hürden zu überwinden.

Krisenpläne müssen Hand in Hand mit der Sicherheitsarchitektur interagieren und ergänzen in Ausnahmesituationen die regulären Maßnahmen. Dazu zählt auch, auf den Worst Case vorbereitet zu sein. Alle Prozesse, technologisch wie organisatorisch, sollten zudem regelmäßig geprüft werden, beispielsweise durch „Red Teaming". Künstliche Intelligenz erhöht die Dynamik in der Cybersicherheit weiter.

Doch sie macht nicht nur Angriffe effizienter. Richtig eingesetzt wird die KI zum entscheidenden Verbündeten der Verteidigung: Sie kann alle relevanten Prozesse deutlich beschleunigen, nicht nur auf technischer Ebene, sondern auch bei der Entscheidungsfindung der Verantwortlichen. •

TOMMY GROSCHE (Bild: Fortinet)

Country Manager Germany bei Fortinet

Das BKA warnt eindringlich vor der Zunahme von DDoS-Angriffen, und die Notfallvorsorge in deutschen Unternehmen weist weiterhin erhebliche Mängel auf. Detaillierte Krisenpläne und moderne Sicherheitsarchitekturen sind unerlässlich, um die Cyberresilienz zu stärken. Ein wirksamer Krisenplan ist die Grundlage: Er muss präzise Abläufe für Erkennung, Eindämmung und Wiederherstellung definieren. Wesentliche Bestandteile sind Incident-Response-Playbooks, klare Kommunikation und Schulungen zur Stärkung der „menschlichen Firewall". KI-gestützte Automatisierung beschleunigt die Reaktion zusätzlich und minimiert Ausfallzeiten.

Parallel dazu müssen Unternehmen ihre Sicherheitsarchitekturen aufwerten. Statt isolierter Lösungen ist eine einheitliche Sicherheitsplattform erforderlich, die Transparenz über die gesamte Angriffsfläche bietet und eine konsistente Richtliniendurchsetzung ermöglicht. Dies reduziert die Komplexität drastisch und optimiert die Effizienz. Solche modernen Architekturen umfassen eine Threat-Informed Defense, die Taktiken, Techniken und Vorgehensweisen der Angreifer proaktiv abwehrt. Außerdem Zero-Trust-Prinzipien mit Zugriffsüberprüfung, Netzwerksegmentierung zur Isolierung kritischer Systeme und KI-gestützte Sicherheit zur Automatisierung von Routineaufgaben, Anomalieerkennung und proaktive Abwehr (SOAR, EDR/XDR). Diese Symbiose aus Krisenplänen und adaptiven Architekturen minimiert die Angriffsfläche und gewährleistet die Betriebsfähigkeit bei Cyberangriffen. •

GERALD EID (Bild: Getronics)

Regional Managing Director DACH bei Getronics

Ein Notfallplan in der Schublade schützt keinen Betrieb. Dennoch beobachten wir genau das viel zu oft: Frameworks werden aufgesetzt, Dokumente abgelegt, und wenn es dann wirklich brennt, weiß niemand was zu tun ist. Die Absicherung entpuppt sich als leere Hülle. Cyberresilienz funktioniert nur als lebendiger Prozess. Ransomware und ähnliche Bedrohungen erfordern einen Framework-basierten Ansatz, der dann im Unternehmen „gelebt" wird. Das Problem ist dabei oft, dass viele Unternehmen das intern nicht stemmen können, weder personell noch fachlich.

Wenn sich ein Unternehmen eingesteht, Cybersicherheit nicht allein leisten zu können, ist schon ein wichtiger Schritt getan. Wenn Sicherheitsexperten nicht als einmalige Dienstleister verstanden werden, sondern als Partner in einem kontinuierlichen Prozess, dann kann auch eine Sicherheitsarchitektur entstehen, die von den Mitarbeitern angenommen und umgesetzt wird. Zudem leisten externe Security Operation Center einen Mammutdienst. Diese sind oft im Vorteil, was die Einschätzung der Bedrohungslage angeht und stehen als professionelle Schutzinstanz 24/7 bereit. Am Ende dürfen wir uns nichts vormachen: KI senkt die Einstiegshürde für Angreifer und wer keinen Partner hat, dies versteht, verliert diesen Wettlauf. •

STEFAN TIEFEL (Bild: noris network AG)

Senior Market Development Manager bei noris network

Die Bedrohungslage im digitalen Raum verschärft sich weiter. Laut dem BKA-Bundeslagebild Cybercrime 2025 stieg die Zahl der DDoS-Angriffe um 25 Prozent auf rund 37.000 Fälle, während die Ransomware-Vorfälle um zehn Prozent auf etwa 1.040 angezeigte Delikte zunahmen. Doch während Angreifer aufrüsten, hinkt die Verteidigung hinterher: Die eco-IT-Sicherheitsumfrage 2026 zeigt, dass lediglich 17 Prozent der Unternehmen über vollständig geprüfte Incident-Response-Pläne verfügen.

Eine zukunftsfähige Sicherheitsarchitektur beginnt bei der Frage: Was tun, wenn es brennt? Folgende drei Maßnahmen sollten umgesetzt werden: 1. Formulierung, Erprobung und Verankerung von Krisenplänen. 2. Schaffung der erforderlichen Strukturen wie Eskalationswege, proaktive Übungsszenarien und eine lückenlose Dokumentation. 3. Einrichtung einer mehrschichtigen Abwehr zum Erkennen von Anomalien in Echtzeit.

Widerstandsfähigkeit entsteht dort, wo Prävention, Detektion und Reaktionsfähigkeit als Einheit begriffen werden. noris network vereint technische Abwehr (SOC-Betrieb, Incident Response und forensische Analysen) mit strategischer Beratung zu Risikomanagement und Notfallplanung in zertifizierten deutschen Rechenzentren. •

THOMAS MIERSCHKE (Bild: Proofpoint)

Area Vice President DACH bei Proofpoint

Eine moderne Sicherheitsarchitektur muss den jüngsten Veränderungen in der Bedrohungslandschaft Rechnung tragen. Dies bedeutet: Während der Schutz von Menschen nach wie vor unverzichtbar ist, muss die Architektur nun auch agentische KI-Systeme absichern. KI-Agenten fungieren wie Mitarbeiter. Sie können durch bösartige Prompts manipuliert werden, dem „Data Drift" zum Opfer fallen, Privilegien missbrauchen oder Informationen preisgeben. Unser Report „AI and Human Risk Landscape" bestätigt, dass die Einführung von KI-Technologien den Ausbau der Sicherheitsmaßnahmen bei Weitem hinter sich lässt. 56 Prozent der deutschen Unternehmen sehen sich mit ihren Sicherheitsmaßnahmen in einem Aufholwettlauf begriffen oder betrachten diese als inkonsistent oder rein reaktiv.

Die Antwort liegt nicht darin, KI als neuartige Bedrohungskategorie zu behandeln, sondern bewährte Kontrollen konsequent auf alles anzuwenden, was KI berührt und ausführt. Unternehmen, die diese Basis frühzeitig legen, können ihren KI-Einsatz ruhigen Gewissens ausbreiten. Krisenpläne müssen regelmäßig aktualisiert und getestet werden. Unternehmen benötigen eine Sicherheitsplattform, die in der Lage ist, KI und KI-Agenten ebenso zu verwalten wie menschliche Mitarbeiter. Zudem müssen sie absichtsbasierte Handlungen analysieren können. •

FRANK SCHWAAK (Bild: Rubrik)

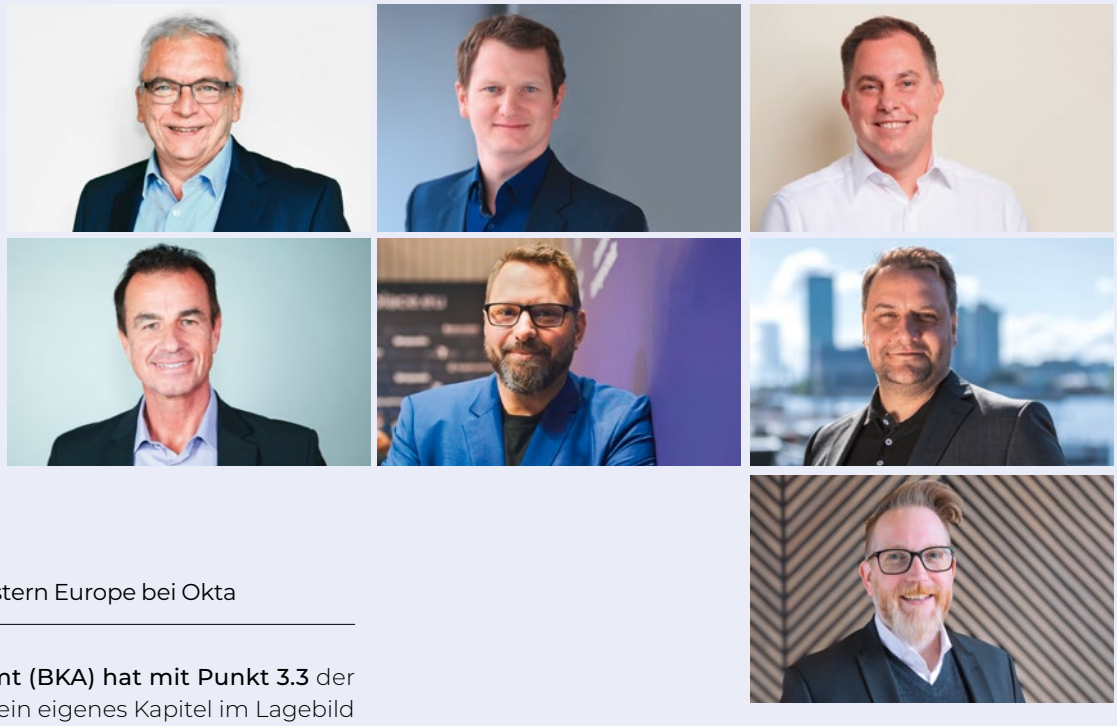
Field CTO EMEA bei Rubrik

Moderne Angriffe, ob automatisierte DDoS, Ransomware oder identitätsbasierte Vorfälle, zeigen deutlich: Vollständige Prävention ist keine realistische Zielgröße mehr und viele Unternehmen sind auf den Ernstfall wenig vorbereitet. Dabei ist die entscheidende Kennzahl heute Time-to-Recovery: Wie schnell kann ein Betrieb nach einem Vorfall einen verifizierten, sauberen Betriebszustand wiederherstellen? Nur wer das misst, kann gezielt diese Zeit verkürzen. Krisenpläne entfalten ihren Wert erst, wenn sie regelmäßig erprobt werden, durch Simulationen, automatisierte Wiederherstellungstests und klare Verantwortlichkeiten über IT und Fachbereiche hinweg. Ergänzt werden muss das durch eine Architektur, die auf „Assumed Breach" ausgelegt ist: Backups, isolierte Wiederherstellungsumgebungen und ein konsequentes Least-Privilege-Prinzip für alle Identitäten, menschliche wie maschinelle.

Denn Angreifer brechen heute nicht mehr ein, sie melden sich einfach an. Gekaperte Identitäten sind das neue Einfallstor, und der Kreis der Gefährdeten wächst: Laut Rubrik Zero Labs haben nur 21 Prozent der deutschen Unternehmen die Transparenz über die aktiven Agenten, oftmals sind sie eine „Shadow Workforce". Für echte Cyberresilienz gilt daher: Identitätsschutz muss als eigene Resilienzschicht in die Sicherheitsarchitektur integriert werden. •

von oben links:

Gerald Eid, Stefan Tiefel, Sven Kniest, Thomas Mierschke, Frank Schwaak, Stephan Schulz, Henning Dittmer



SVEN KNIEST (Bild: Okta)

VP Central Europe & Eastern Europe bei Okta

Das Bundeskriminalamt (BKA) hat mit Punkt 3.3 der künstlichen Intelligenz ein eigenes Kapitel im Lagebild Cybercrime 2025 gewidmet. Zurecht, denn die KI ist der Produktivitäts- und Innovationstreiber unserer Tage, wird aber von Cyberkriminellen für deren Zwecke missbraucht. Besonders KI-Agenten steigern in Unternehmen die Effizienz. Um unseren Kunden bei der Stärkung ihrer Cyberresilienz zu helfen, liefern wir mit unserer Blaupause für sichere KI-Agenten ein fachlich fundiertes Rahmenwerk.

Es geht also vor allem darum, Schatten-KI aufzudecken und zu vermeiden, zentralisierte Kontrolle über die Verbindungswege der KI-Agenten zu erlangen, sowie eine feingranulare Autorisierung für KI-Agenten einzuführen, um einerseits den Zugriff genau definieren und andererseits jederzeit im Notfall entziehen zu können.•

STEPHAN SCHULZ (Bild: F5)

Senior Principal Solutions Engineer, Strategic Accounts bei F5

Cyberresilienz erfordert heute mehr als klassische Perimetersicherheit. Da geschäftskritische Anwendungen und APIs über Rechenzentren, Clouds und Edge-Umgebungen verteilt sind, müssen Unternehmen ihre Sicherheitsarchitektur konsequent an diesen verteilten Realitäten ausrichten. Entscheidend sind zentrale Transparenz, konsistente Sicherheitsrichtlinien und die Fähigkeit, Angriffe in Echtzeit zu erkennen und abzuwehren.

Krisenpläne leisten dabei einen wesentlichen Beitrag, weil sie technische und organisatorische Abläufe im Ernstfall verbindlich festlegen: Wer reagiert wann, welche Anwendungen haben Priorität, wie wird bei DDoS-Angriffen, kompromittierten Zugängen oder API-basierten Angriffen eskaliert, und wie bleibt der Betrieb kritischer Services aufrechterhalten? Moderne Sicherheitsarchitekturen stärken diese Resilienz, wenn sie Schutz für Anwendungen, APIs und Identitäten mit Monitoring, intelligenter Traffic-Steuerung und automatisierter Abwehr verbinden. Gerade bei DDoS-Angriffen oder Bot-basierten Attacken kommt es darauf an, schädlichen Traffic früh zu erkennen, zu filtern und Dienste verfügbar zu halten. Cyberresilienz entsteht so aus dem Zusammenspiel von Vorbereitung, Echtzeit-Transparenz und anwendungsnaher Sicherheit. •

HENNING DITTMER (Bild: Ping Identity)

RVP DACH bei Ping Identity

Identitätsbasierte Angriffe haben klassische Infrastrukturangriffe längst überholt. In Gesprächen über Cyberrisiken taucht häufig noch das Bild kompromittierter IoT-Geräte auf, die als Ausgangspunkt für DDoS-Angriffe dienen. Solche Szenarien existieren – sie greifen heute jedoch zu kurz. Die größere Herausforderung liegt anderswo: Angreifer brechen nicht mehr ein – sie loggen sich ein. Kompromittierte Identitäten, schwache BYOD-Strategien und wiederverwendete Zugangsdaten ermöglichen Zugriff auf Ressourcen, ohne Sicherheitsmechanismen auszulösen. Phishing und Credential-Diebstahl machen keinen Unterschied, wie stark die Perimetersicherheit ist. Ist eine Identität kompromittiert, bewegen sich Angreifer unbemerkt durch Systeme und eskalieren ihre Rechte erst später.

Resilienz beginnt daher nicht beim Krisenplan, sondern bei der Architektur. Phishing-resistente Authentifizierung, Identity- und Access-Management und Verifikation von Zugriffsmustern schaffen die Grundlage, Risiken frühzeitig zu erkennen und einzugrenzen. Moderne Sicherheitsmodelle bewerten nicht nur die Anmeldung, sondern auch Kontext, Gerätezustand und Session-Risiken in Echtzeit. Auf dieser Basis kann ein Krisenplan greifen – weil er auf erkannte Risiken reagiert, bevor sie zum Vorfall werden. •

Der blinde Fleck: ein neues Compliance-Risiko

Autonome KI bei Lieferanten schafft neue Haftungs- und Auditrisiken. Unternehmen müssen digitale Entscheidungen kontrollieren – bevor Aufsicht und Prüfer belastbare Nachweise verlangen.

/// von Simon Jaehnig

VIELE UNTERNEHMEN HABEN IN DEN VERGANGENEN JAHREN GELERNT, Lieferketten anhand von Kennzahlen zu steuern: Emissionen, Zertifikate, Sorgfaltspflichten, Selbstauskünfte. Was dabei lange kaum im Fokus stand, ist eine andere Dimension: Wie entstehen Entscheidungen in der Lieferkette – und wer trifft sie eigentlich?

Diese Frage gewinnt jetzt massiv an Bedeutung. Denn Künstliche Intelligenz ist längst nicht mehr auf Pilotprojekte oder Innovationsabteilungen beschränkt. Lieferanten setzen KI ein, um Bestände zu optimieren, Aufträge zu priorisieren, Liefertermine zu disponieren, Risiken zu bewerten oder Eskalationen vorzubereiten – teilweise automatisiert, teilweise autonom.

Damit verschiebt sich die Verantwortung. Wenn ein KI-System bei einem Lieferanten Fehlentscheidungen trifft, Verzerrungen erzeugt oder Sicherheitsprobleme verursacht, bleiben die Folgen selten dort stehen, wo sie entstehen. Sie schlagen sich nieder in Lieferausfällen, Vertragsverstößen, Reputationsschäden oder regulatorischen Fragen – und landen damit beim Auftraggeber.

Die zentrale Frage lautet daher nicht mehr: Setzt ein Lieferant KI ein? Sondern: Welche Entscheidungen beeinflusst diese KI – und unter welchen Kontrollen?

Warum daraus ein Risk- und Compliance-Thema wird

Die meisten ESG- und Third-Party-Risk-Frameworks stammen aus einer Zeit, in der Entscheidungen klar menschlich getroffen wurden. Sie erfassen Prozesse, Richtlinien und Kennzahlen – nicht aber algorithmische Entscheidungslogiken oder den Grad von Autonomie. In der Praxis führt das zu Lücken. Bei KI wird dieser Ansatz nicht ausreichen.

Mit zunehmender KI-Regulierung verschiebt sich der Anspruch von Transparenz hin zu Nachweisbarkeit. Regulatoren, Wirtschaftsprüfer, Kunden und Aufsichtsgremien werden weniger danach fragen, ob Unternehmen „Prinzipien“ definiert haben, sondern ob sie wirksame Kontrollen umgesetzt haben – auch bei Dritten.

Konkret bedeutet das:
Unternehmen müssen erklären können,

- wo KI im Lieferantennetzwerk eingesetzt wird,
- welche Entscheidungen dadurch beeinflusst oder ausgelöst werden,
- wie menschliche Kontrolle sichergestellt ist,
- und wie Entscheidungen im Nachhinein nachvollzogen werden können.

Das ist klassische Compliance-Logik. Und sie endet nicht an der eigenen Organisationsgrenze. Besonders relevant ist das in komplexen Branchen wie der diskreten Fertigung. Hier treffen Systeme permanent Entscheidungen über Mengen, Prioritäten oder Lieferzeitpunkte. Je stärker automatisiert wird, desto größer ist der Einfluss von KI – und desto wichtiger wird ihre Governance.

Vom ESG-Projekt zur neuen Grunddisziplin

Damit wird Lieferanten-KI zu einem festen Bestandteil des Third-Party-Risk-Managements. Ähnlich wie Cybersecurity oder Sanktionen entwickelt sich ein neues Mindestniveau an Erwartungen: klar definierte Verantwortlichkeiten, dokumentierte Prozesse, Eskalationsmechanismen und Audit-Fähigkeit.

Unternehmen, die hier früh Strukturen schaffen, sind im Vorteil. Sie müssen Governance nicht unter regulatorischem Druck nachziehen, sondern können Standards selbst setzen – und KI in der Lieferkette nutzen, ohne Kontrolle abzugeben.

SECURITY INSIGHT

DER AUTOR
Simon Jaehnig
ist Mitgründer von IntegrityNext sowie Chief Strategy and Innovation Officer und President IntegrityNext Inc.

Fünf Schritte, um Lieferanten-KI beherrschbar zu machen
Damit Governance nicht abstrakt bleibt, lassen sich fünf pragmatische Schritte ableiten, die Unternehmen schon heute umsetzen können:

- KI sichtbar machen:
  Erstellen Sie eine Übersicht, wo Lieferanten KI einsetzen und welche Prozesse betroffen sind. Besonders relevant sind Entscheidungen mit Einfluss auf Kosten, Qualität, Lieferfähigkeit oder Vertragsbeziehungen.
- Entscheidungsrechte definieren:
  Trennen Sie klar zwischen KI als Empfehlungssystem und KI als Entscheidungsinstanz. Legen Sie fest, wo menschliche Freigaben verpflichtend sind – etwa bei Ausnahmen, Eskalationen oder hochvolumigen Transaktionen.
- Governance vertraglich verankern:
  Verankern Sie KI-Governance in Lieferantenverträgen und Codes of Conduct. Dazu gehören Anforderungen an Human-in-the-Loop, Eskalationspflichten und Mindeststandards für Dokumentation.
- Audit- und Incident-Fähigkeit sicherstellen:
  Governance heißt auch: Entscheidungen erklärbar machen. Logs, Versionsstände, Change-Dokumentation und definierte Incident-Prozesse sind Voraussetzung dafür, im Prüf- oder Krisenfall handlungsfähig zu bleiben.
- Verantwortung organisatorisch bündeln:
  Lieferanten-KI ist kein Thema für eine einzelne Abteilung. Procurement, Compliance, Legal, IT-Security und Risikomanagement brauchen gemeinsame Standards und klare Zuständigkeiten.

„Shadow AI" nicht unterschätzen
Zusätzlichen Druck erzeugt die Verbreitung sogenannter Shadow-AI-Tools – Anwendungen, die ohne formale Freigabe eingesetzt werden. Gerade in mehrstufigen Lieferketten bleiben solche Tools oft lange unentdeckt.

Das Risiko liegt weniger in der Technologie selbst als in der fehlenden Steuerung: unklare Datennutzung, keine Dokumentation, keine Eskalationspfade. Spätestens im Audit wird daraus ein Problem.

Jetzt Strukturen schaffen – bevor sie vorgegeben werden
Lieferanten-KI ist heute ein relevantes Risiko- und Compliance-Thema. Mit zunehmender Regulierung wird sich dieser Trend verstärken – und Anforderungen werden deutlich konkreter und strenger ausfallen, als viele es aus ESG kennen. Unternehmen, die Transparenz, klare Entscheidungsregeln und auditfähige Governance aufbauen, verschaffen sich Spielräume. Sie sichern Compliance, stärken ihre Lieferketten-Resilienz und behalten Kontrolle über digitale Entscheidungsprozesse. KI in der Lieferkette ist kein Argument gegen Automatisierung – sondern ein Anlass, Governance neu zu denken: operativ, belastbar und zukunftsfest. •

LIEFERANTEN-KI: DER NEUE COMPLIANCE-BRENNPUNKT

Risiko: Autonome Entscheidungen bei Dritten führen zu Haftungs-, Audit- und Reputationsrisiken.

Regulierung: Von Transparenz zu Nachweisbarkeit; Kontrollen und Logs werden prüfpflichtig – strenger als ESG.

4 Leitfragen: Wo wirkt KI? Welche Entscheidungen? Welche Freigaben? Wie wird dokumentiert?

5 Schritte: 1) KI-Landkarte der Lieferanten. 2) Entscheidungsrechte/ Human-in-the-Loop. 3) Governance vertraglich fixieren. 4) Audit-/Incident-Fähigkeit (Logs, Versionen). 5) Zuständigkeiten bündeln (Procurement, Compliance, Legal, IT-Sec, Risk).

Shadow AI: Unkontrollierte Tools früh identifizieren.

Effekt: Compliance sichern, Resilienz stärken, Steuerbarkeit erhöhen.

HR-Tech: Wie sieht das Personalmanagement von morgen aus?

HR-Tech – von KI-gestütztem Recruiting über People Analytics bis hin zu digitalen Employee-Experience-Plattformen – ist längst mehr als nur ein Effizienz-Booster für die Personalabteilung. Wir fragen bei Experten nach: „Wie verändert HR-Tech grundlegend die Art und Weise, wie wir über Personalmanagement denken?“ /// von Konstantin Pfliegl

SIMON RUSSIN

Vice President Enterprise Applications bei Cancom

• Noch immer wird HR in vielen Unternehmen über Tickets, Formulare und manuelle Prozesse definiert. Dabei entscheidet moderne HR Tech längst darüber, ob das Resort HR eine Verwaltungseinheit bleibt oder zur strategischen Steuerungsinstanz wird. Die HR-Tech-Revolution verändert das Personalwesen grundlegend – nicht durch einzelne Tools, sondern durch integrierte Plattformen, die fragmentierte Altsysteme ablösen und alle HR Prozesse in einem durchgängigen digitalen Workflow bündeln.

Entlastung für die HR-Abteilung

Wenn Onboarding, Vertragsdokumente oder Stammdatenpflege automatisiert ablaufen, gewinnt HR nicht nur Effizienz, sondern vor allem Handlungsspielraum. KI-gestützte Self-Service-Portale und Chatbots beantworten Alltagsfragen – ohne Ticket, ohne Warteschleife. HR-Teams werden spürbar entlastet und können sich auf das konzentrieren, was echten Mehrwert schafft.

Weg von isolierten Einzellösungen, hin zu skalierbaren Plattformen. Weg von reiner Administration, hin zu aktiver Unternehmensgestaltung. Die zentrale Frage ist nicht mehr, ob HR technologiegetrieben arbeitet, sondern wie lange sich Unternehmen leisten können, darauf zu verzichten. •

MARKUS KAMMERMEIER

Lead Strategic Advisor bei Workday

• HR-Tech wandelt die Perspektive auf Personalmanagement fundamental: HR wird von einer oft administrativen Funktion zum strategischen Partner für Transformation, Führung und Wachstum. KI unterstützt Entscheidungsprozesse, automatisiert wiederholende Tätigkeiten und unterstützt die Orientierung.

Skill Management für den Geschäftserfolg

Mit Blick auf Fachkräftemangel und demografischen Wandel reicht externe Rekrutierung nicht mehr. Oft wird unterschätzt, dass viele künftig benötigte Kompetenzen in den Organisationen bereits vorhanden sind. Entscheidend ist, sie sichtbar zu machen, gezielt weiterzuentwickeln und Mitarbeitern neue Perspektiven innerhalb des Unternehmens zu eröffnen. Dabei unterstützt HR-Tech, indem sie Skills erfasst, verknüpft und zur zentralen Währung eines zukunftsfähigen Talentmanagements macht.

Klar ist: Der Erfolg von HR-Tech ist keine reine Technologiefrage. Der Umgang mit Personendaten braucht Transparenz, klare Governance und nachvollziehbare Entscheidungen. KI kann HR wirksamer und vorausschauender machen – wenn sie Menschen stärkt. Genau darin liegt der Wandel: Personalmanagement wird datenbasierter, strategischer und zugleich menschlicher. •

Bild: Cancom

Bild: Workday

OLIVER ROZIC

Vice President Product Management bei Sage

• HR-Tech, insbesondere der Einsatz von KI, verändert das Personalmanagement grundlegend. Er ermöglicht es HR-Abteilungen, ihr Versprechen einzulösen und einen deutlich stärkeren strategischen Beitrag zum Unternehmenserfolg zu leisten. Denn bislang binden repetitive, administrative Aufgaben einen Großteil der Ressourcen – oft zulasten strategischer Initiativen. Dazu zählen etwa das Sichten von Lebensläufen, die Erstellung standardisierter Dokumente oder die Beantwortung wiederkehrender Anfragen.

Zeitgewinn für strategische Aufgaben

Mit KI-gestützter HR-Tech verschiebt sich dieses Verhältnis spürbar. Intelligente Systeme übernehmen die Vorqualifizierung von Kandidaten, analysieren Lebensläufe in kurzer Zeit und identifizieren relevante Qualifikationen präzise. Chatbots und automatisierte Antwortsysteme beantworten Anfragen von Bewerbern und Mitarbeitern rund um die Uhr – schnell, konsistent und zuverlässig. Das reduziert die Kommunikationslast für HR-Teams und verbessert zugleich die Candidate Experience. Vor allem aber gewinnt HR seine wertvollste Ressource zurück: Zeit für strategische Aufgaben wie Talententwicklung, Kulturgestaltung und die Unterstützung des Geschäftswachstums.

Gleichzeitig erfordert diese Entwicklung ein neues Verständnis von Verantwortung. Der Einsatz von KI in HR-Prozessen zwingt Unternehmen, sich intensiv mit Fragen der Ethik, Fairness und des Datenschutzes auseinanderzusetzen. HR-Verantwortliche müssen kritisch prüfen, auf welchen Daten Systeme basieren und ob ihre Ergebnisse nachvollziehbar und vertrauenswürdig sind.

Richtig eingesetzt macht KI die Personalabteilung zu einem strategischen Kernbereich des Unternehmens, denn sie gestaltet und entwickelt das wichtigste Kapital: die Menschen. •

KATHARINA HOLZAPFEL

Workforce Transformation Lead bei PwC Deutschland

• Die größte Wirkung von HR Tech liegt für mich nicht in der Technologie – sondern darin, dass sie eine Brücke zwischen HR und dem Business schlägt. Wir bei PwC sehen in Transformationsprojekten immer wieder: Wenn Quality of Hire, interne Mobilität, Skills Deckung und Pay Equity messbar werden, schafft das eine neue Gesprächsebene zwischen HR und der Geschäftsführung.

Neue Rollen

Das verlangt neue Kompetenzen. Die wichtigsten sind für mich Datenverständnis und Produktdenken, eine experimentierfreudige Grundhaltung, souveränes Arbeiten mit KI-Tools und die Fähigkeit, Workflows zu automatisieren. Damit verändern sich auch die Rollen: Wer früher CVs sichtete, gestaltet heute Prompts und Funnels, definiert Auswahlkriterien, strukturiert Evidenzen, testet Varianten durch und erklärt, warum das verwendete System wie entschieden hat. HR-Business-Partner stärken ihre Rolle als datenstarke Sparringspartner, L&D-Teams avancieren zu Learning Experience Designer.

Der regulatorische Rahmen ist dabei unserer Erfahrung nach kein Hindernis, sondern Qualitätsmerkmal: HR-KI gilt nach dem EU AI Act als Hochrisiko-Anwendung. DSGVO, Mitbestimmung und Erklärbarkeit gehören für uns damit in die Produktlogik, wir sehen sie nicht als nachgelagerte Compliance-Aufgabe.

Enabler sind die Mittel, nicht der Zweck: eine hohe Datenqualität mit sauberen Stammdaten, eindeutigen IDs und gepflegten Skill Profilen; zudem eine moderne Cloudarchitektur mit integrierten Systemen sowie KI-Copilots für Text, Matching und Empfehlungen.

Startpunkt muss deshalb immer das Geschäftsproblem sein, kein Tool: klein pilotieren, sauber messen, skalieren. Das sind die wesentlichen Schritte zum erfolgreichen Einsatz. Menschlich bleibt HR durch Kontext, Empathie, faire Urteilsfähigkeit. Gerade die Kombination aus Tech und menschlichen Skills macht HR schneller, fairer – und liefert messbare Wettbewerbsvorteile. •

Bild: Sage

Bild: PwC

Treffen wir noch eigene Entscheidungen?

KI liefert Antworten in Sekunden, aber ersetzt sie menschliche Entscheidungen? Für Unternehmer und Entscheider zeigt dieser Beitrag, warum Urteilskraft zur wichtigsten Zukunftskompetenz wird. /// von Slatko Sterzenbach

DER AUTOR

Slatco Sterzenbach hat 17 Ironman erfolgreich absolviert, ist Spiegel-Bestsellerautor und Experte für mentale und physische Peak Performance für Unternehmer.

Warum fällt es Menschen trotz mehr Daten schwerer zu entscheiden?
Mehr Informationen führen nicht automatisch zu besseren Entscheidungen. Oft passiert das Gegenteil. Studien zeigen, dass Menschen täglich rund 35.000 Entscheidungen treffen, viele davon unbewusst. Führungskräfte treffen hunderte relevante Mikro-Entscheidungen pro Tag. Gleichzeitig wächst durch Digitalisierung die Zahl der Optionen permanent.

Das Problem ist nicht Informationsmangel, sondern Überlastung.

Je mehr Optionen Menschen haben, desto mehr mentale Energie fließt in Auswahl statt in Klarheit. In der Verhaltenspsychologie nennt man das Decision Fatigue. Genau deshalb fühlen sich viele trotz technischer Unterstützung heute weniger entscheidungssicher als früher.

Künstliche Intelligenz scheint dafür die perfekte Lösung zu sein. Sie filtert, priorisiert und empfiehlt. Doch genau hier beginnt die kritische Frage: Hilft sie uns besser zu entscheiden – oder gewöhnen wir uns daran, Entscheidungen auszulagern?

Kann KI echte Entscheidungen treffen?
Kurz gesagt: Nein. KI kann berechnen, Muster erkennen und Wahrscheinlichkeiten ausgeben. Aber eine echte Entscheidung enthält mehr als Daten. Sie beinhaltet Risiko, Verantwortung, Wertorientierung und oft Intuition.

Ein Unternehmer entscheidet beispielsweise nicht nur auf Basis eines Marktmodells, ob er einen neuen Weg geht. Er entscheidet mit Erfahrung, Menschenkenntnis und manchmal gegen statistische Logik. Genau darin liegt der Unterschied zwischen Auswahl und Entscheidung.

Eine KI kann:
- Optionen analysieren
- Risiken berechnen
- Szenarien simulieren
- Wahrscheinlichkeiten optimieren

Eine KI kann nicht:
- Verantwortung tragen
- ethisch abwägen
- Sinn bewerten
- Haltung entwickeln

Maschinen können Antworten liefern. Aber Bedeutung entsteht beim Menschen.

Werden wir durch KI in Entscheidungen manipuliert?
Manipulation ist ein hartes Wort. Aber Vorselektion ist real. Jede KI filtert Antworten. Sie zeigt nicht alle Möglichkeiten, sondern eine priorisierte Auswahl. Das Problem daran: Was nicht gezeigt wird, wird selten hinterfragt.

Gerade darin liegt eine unterschätzte Gefahr. Wenn Menschen sich dauerhaft an vorgefilterte Lösungen gewöhnen, verengt sich ihr Denkraum. Dann treffen sie nicht unbedingt falsche Entscheidungen, aber oft nur noch innerhalb eines Rahmens, den sie selbst nie definiert haben. Diese „torselektierten Antworten" verändern subtil Urteilskraft. Und das ist gerade für Unternehmer relevant. Denn Innovation entsteht oft dort, wo jemand bewusst außerhalb naheliegender Optionen denkt.

Was passiert mit Urteilskraft, wenn wir Entscheidungen auslagern?
Urteilskraft funktioniert wie ein Muskel. Wird sie nicht genutzt, baut sie ab. Neurowissenschaftliche Studien zeigen, dass wiederholte kognitive Auslagerung Denkautonomie reduzieren kann. Ähnlich wie Navigationssysteme langfristig Orientierungssinn schwächen können, kann

permanente algorithmische Führung unabhängiges Denken schwächen. Besonders problematisch wird das unter Druck. Eine McKinsey-Untersuchung zeigt, dass in Unternehmen bis zu 70 Prozent strategischer Fehlentscheidungen nicht aus mangelnden Daten entstehen, sondern aus kognitischen Verzerrungen und schlechter Urteilsqualität.

Mehr Daten lösen dieses Problem nicht automatisch. Sie können es sogar verstärken. Denn Komplexität ohne Klarheit produziert selten bessere Führung.

Wie behalten Unternehmer in einer KI-Welt Entscheidungshoheit?
Die Antwort lautet: durch bewusste Selbstführung. Technologie nutzen, ohne ihr inneres Steuer zu überlassen.

Dafür braucht es mentale Prinzipien:

1. Entscheidungen nicht nur datenbasiert, sondern wertebasiert prüfen
   Nicht nur fragen: Was ist effizient? Sondern auch: Was ist richtig?
2. Entscheidungsräume bewusst erweitern
   Vor jeder wichtigen Entscheidung mindestens eine Option suchen, die außerhalb des offensichtlichen Spektrums liegt.
3. Intuition als Erfahrungsintelligenz trainieren
   Nicht als Bauchgefühl missverstehen, sondern als verdichtete Mustererkennung.
4. Digitale Reizreduktion praktizieren
   Wer permanent Input konsumiert, verliert Fokus. Weniger Optionen erhöhen oft Entscheidungsqualität.
5. Reflexionsräume schaffen
   Viele Top-Performer treffen gute Entscheidungen nicht schneller, sondern bewusster.

DENKFEHLER STATT DATENMANGEL

- 85 % aller Managemententscheidungen basieren laut Studien zumindest teilweise auf unvollständigen Informationen.
- 35.000 Entscheidungen trifft ein Mensch täglich.
- Bis 70 % strategischer Fehler entstehen durch Denkfehler, nicht Datenmangel.
- Mehr Technologie erhöht häufig Geschwindigkeit – nicht automatisch Urteilskraft.

> „Unternehmer und Entscheider sollten sich nicht fragen: Welche Antwort liefert mir das System? Die Frage sollte lauten: Treffe ich diese Entscheidung wirklich selbst? Denn Zukunft gehört nicht denen mit den besten Tools. Sondern denen, die trotz **Tools bewusst führen**.
>
> *Slatko Sterzenbach*

Gerade Coaching wirkt hier oft nicht als Wissensquelle, sondern als Spiegel für blinde Flecken – und genau darin liegt sein Wert.

Ist Entscheidungskraft die eigentliche Zukunftskompetenz?
Vieles spricht dafür. Früher war Wissen Macht. Heute ist Wissen Commodity. Was knapp wird, ist Orientierung. Nicht der Informierteste gewinnt künftig. Sondern oft derjenige, der trotz Unsicherheit klar handelt.

Genau deshalb wird mentale Stärke wichtiger, nicht unwichtiger, je intelligenter Systeme werden, denn in einer Welt voller Antworten wird die Qualität der Fragen zum Unterschied. Und vielleicht ist genau das die neue Elite-Kompetenz: Nicht mehr wissen, sondern besser entscheiden.

Fazit: Wer nicht selbst entscheidet, wird entschieden
Die eigentliche Gefahr von KI ist nicht, dass Maschinen irgendwann Menschen ersetzen, sondern dass Menschen unbemerkt Verantwortung abgeben. Technologie kann enorm unterstützen. Aber Führung, Urteilskraft und Haltung bleiben menschliche Aufgaben.

Gerade Unternehmer und Entscheider sollten sich deshalb nicht fragen: Welche Antwort liefert mir das System? Die Frage sollte lauten: Treffe ich diese Entscheidung wirklich selbst? Denn Zukunft gehört nicht denen mit den besten Tools. Sondern denen, die trotz Tools bewusst führen.

Handlungsimpuls:
Prüfen Sie bei Ihrer nächsten wichtigen Entscheidung bewusst, welche Optionen Ihnen vielleicht gar nicht gezeigt wurden. Genau dort beginnt oft echte Freiheit. •

Wenn HR digitalisiert. Nur nicht sich selbst.

Employer Branding ist noch analog – während Vertrieb, Produktion und Controlling längst digitalisiert sind. Ein KI-System schließt diese Lücke. /// von Jörg Schleburg

WARUM SCHEITERT EMPLOYER BRANDING IM MITTELSTAND? Wer heute ein mittelständisches Unternehmen besucht, findet in der Regel digitalisierte Prozesse: ERP-Systeme steuern die Produktion, CRM-Plattformen verwalten Kundenbeziehungen, Controlling-Dashboards liefern Echtzeit-Kennzahlen.

Nur nicht im Employer Branding.
Dort läuft vieles noch so wie vor zwanzig Jahren. Das Arbeitgeberprofil existiert als PowerPoint auf einem Laufwerk. Stellenanzeigen werden von wechselnden Personen in wechselnden Tonlagen verfasst. Social-Media-Posts entstehen situativ, wenn jemand Zeit hat. Kampagnen werden mit externen Agenturen entwickelt, dauern Monate, kosten fünfstellige Beträge – und versanden, sobald der externe Druck wegfällt.

Das ist keine Nachlässigkeit. Es ist eine strukturelle Lücke, die sich viele Unternehmen lange leisten konnten. Heute nicht mehr. Mittelständische Unternehmen konkurrieren im Arbeitsmarkt auf zwei Seiten: mit Konzernen, die spezialisierte Teams, große Budgets und jahrelang aufgebaute Arbeitgebermarken haben – und mit agilen Startups, die punkten, womit Mittelständler schwer mithalten können: maximale Flexibilität, flache Hierarchien, viel Eigenverantwortung. Zudem: Im Mittelstand verantwortet Employer Branding oft eine einzelne Person – neben zehn anderen Aufgaben. Besonders unterschätzt wird die interne Dimension. Eine starke Arbeitgebermarke entsteht, wenn Mitarbeitende das Versprechen selbst tragen. Die entscheidende Frage lautet: Was hat die Belegschaft davon – und wie werden aus Mitarbeitenden Multiplikatoren? Wer das nicht klärt, hat einen Claim. Aber keine Marke.

Was kostet eine schwache Arbeitgebermarke?
Laut einer Analyse der StepStone Group entstehen Unternehmen pro unbesetzter Stelle durchschnittlich 29.000 Euro Kosten – bei Unternehmen mit über 250 Mitarbeitenden steigen diese auf über 73.000 Euro. Entgangene Umsätze, verzögerte Projekte und Teamüberlastung sind dabei noch nicht eingerechnet. Employer Branding, das funktioniert, ist keine Kreativleistung. Es ist eine betriebswirtschaftliche Investition mit direkter Wirkung auf Produktivität und Wettbewerbsfähigkeit.

Employer Branding mit KI – wie geht das?
Hier liegt der eigentliche Sprung – nicht KI als Hype, sondern KI als Hebel für Prozesse, die bislang zu aufwendig, zu teuer oder zu abhängig von externem Know-how waren.

Arbeitgeberpositionierung entwickeln. Vorher: Tiefeninterviews, Workshops, Agenturprojekt. Zeitaufwand: Monate. Kosten: fünfstellig. Ergebnis: ein Dokument, das im Schrank verstaubt. Mit System: Ein geführter Prozess ermittelt systematisch Stärken, Werte und Positionierung. Das Ergebnis ist versioniert, jederzeit abrufbar und Grundlage für alle weiteren Maßnahmen – Stellenanzeigen, Karriereseite, interne Kommunikation.

DER AUTOR
Jörg Schleburg
ist Gründer der Employer Branding Agentur VonVorteil und Kopf hinter ASANTIAL. Er begleitet seit über 15 Jahren mittelständische Unternehmen im Employer Branding und hat mehr als 100 Projekte verantwortet.

> „ Wer als Arbeitgeber nicht systematisch sichtbar ist, **verliert den Wettbewerb um Talente** – messbar in längeren Vakanzen, höherer Fluktuation, steigendem Recruiting-Aufwand.
>
> *Jörg Schleburg*

Stellenanzeigen erstellen. Vorher: Jede Stelle wird von einer anderen Person getextet – mal HR, mal Fachbereich, mal Agentur. Kein einheitlicher Ton, kein Markenbezug, kein Archiv. Mit System: Stellenanzeigen werden auf Basis des hinterlegten Arbeitgeberprofils generiert – markenkonsistent, zielgruppengerecht, in Minuten statt Tagen.

Interne Kommunikation gestalten. Vorher: Mitarbeitende erfahren von Employer Branding Initiativen zufällig oder gar nicht. Niemand fragt: Was hat die Belegschaft davon? Wer soll was wann kommunizieren? Wie werden aus Mitarbeitenden Markenbotschafter? Mit System: Auf Basis der Arbeitgeberpositionierung werden interne Zielgruppen definiert und gezielt angesprochen – mit dem richtigen Wording, zum richtigen Zeitpunkt. Das Versprechen nach außen wird nach innen erlebbar.

Wettbewerb analysieren. Vorher: Wettbewerbsanalysen im Employer Branding sind aufwendig und teuer. Was Konkurrenten kommunizieren, wie sie sich positionieren – das bleibt oft im Dunkeln. Mit System: KI analysiert, wie sich Wettbewerber als Arbeitgeber positionieren. Das schafft Entscheidungsgrundlagen, die früher nur mit Beratungsbudget möglich waren.

Und das Entscheidende: Was jede Maßnahme bringt, wird in Kennzahlen abgebildet – von der Bewerbungsrate bis zur Reichweite. HR kann der Geschäftsführung erklären, was Employer Branding dem Unternehmen konkret bringt.

Employer Branding ohne Agentur – geht das?
Die Frage ist berechtigt – denn lange galt: Externe Perspektive ist unverzichtbar. Zu Recht. Agenturen sehen Lücken zwischen Wunschbild und Wirklichkeit, die Unternehmen selbst nicht sehen. Und woher sollen HR-Verantwortliche Markenaufbau und Positionierungsstrategie können? Früher war Agentur-Support schlicht ein Muss.

Nur endet der Beitrag einer Agentur, wenn das Projekt endet. Das Wissen geht mit. HR steht wieder allein – ohne Prozesse, ohne Entscheidungsgrundlage. Heute löst ein Betriebssystem genau das – aber nur, weil 15 Jahre Expertise darin stecken.

Viele Unternehmen kompensieren das heute mit generischen KI-Tools: ChatGPT für Stellenanzeigen, KI-Assistenten für Posts. Das hilft, aber es löst das eigentliche Problem nicht. Wer ohne klares Arbeitgeberprofil als Grundlage schnell Inhalte produziert, produziert schnell inkonsistente Inhalte. Der Unterschied liegt in der Einbettung: Ein spezialisiertes System kennt das Arbeitgeberprofil, die Zielgruppen, die Positionierung. Es baut Entscheidungen aufeinander auf. Und es sichert Wissen – auch wenn Mitarbeitende wechseln, erkranken oder im Urlaub sind.

Was bringt Employer Branding – konkret und messbar?
Vakanzzeit, Bewerbungsrate, Fluktuation, Reichweite – das sind die Kennzahlen, an denen sich Employer Branding messen lassen muss. Ein System, das diese Daten liefert, gibt HR endlich die Sprache, die Geschäftsführungen verstehen.

- **Schnellere Besetzung** – Ein klares Arbeitgeberprofil zieht passendere Bewerbungen an und verkürzt Vakanzzeiten messbar.
- **Interne Steuerung statt Agenturabhängigkeit** – Alle Maßnahmen laufen auf derselben Grundlage, konsistent und ohne externen Anschub.
- **Erklärbare Wirkung gegenüber der Geschäftsführung** – HR zeigt in Kennzahlen, was Employer Branding bringt – nicht in Aktivitäten.
- **Wissen bleibt im Unternehmen** – Nicht bei Einzelpersonen oder Agenturen, sondern im System. Auch bei Personalwechsel.
- **Wettbewerbsfähigkeit im Talentmarkt** – Wer als Arbeitgeber sichtbar und klar positioniert ist, gewinnt gegen größere Wettbewerber – auch ohne deren Budgets.

Fazit: Employer Branding:
die analoge Lücke im digitalen Unternehmen
Unternehmen haben enorme Energie in Digitalisierung investiert – Vertrieb, Produktion, Controlling laufen heute auf digitalen Plattformen, mit Echtzeitdaten, mit messbarer Wirkung. Employer Branding nicht.

Das ist die eigentliche Lücke. Und sie hat Konsequenzen: wer als Arbeitgeber nicht systematisch sichtbar ist, verliert den Wettbewerb um Talente – messbar in längeren Vakanzen, höherer Fluktuation, steigendem Recruiting-Aufwand.

KI schließt diese Lücke – nicht als Abkürzung, sondern als Fundament. Als System, das Employer Branding von der analogen Projektarbeit in eine digitale, steuerbare Unternehmensfunktion überführt. Mit bezifferbarem Beitrag zur Wertschöpfung. Mit Kontinuität. Mit Wirkung. •

„Auf Sieg spielen“: Europas Masterplan für KI und digitale Infrastrukturen

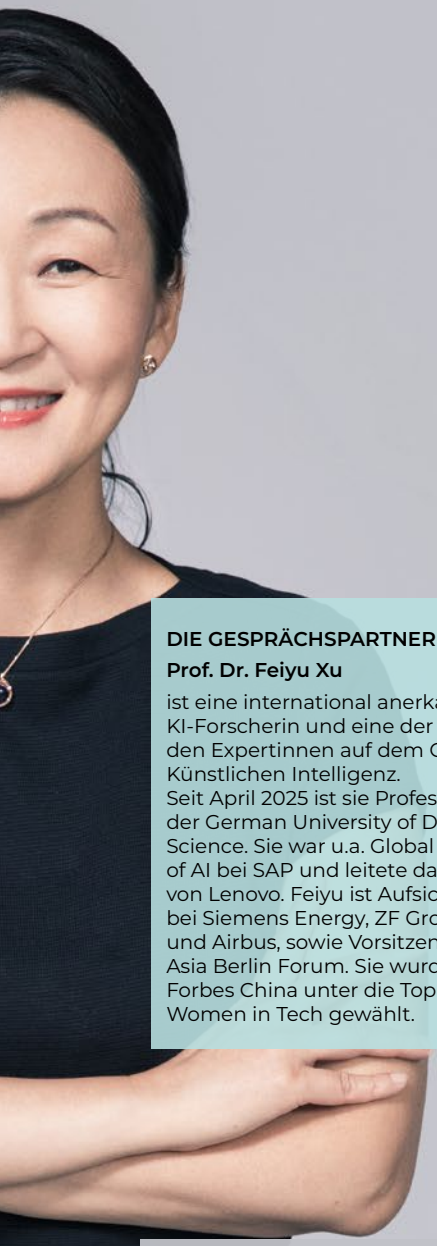
Prof. Dr. Feiyu Xu, Univ.-Professorin of Industry AI at German University of Digital Science, Board Member und Senior Advisor, zeigt auf wie eigene Cloud-, Satelliten- und KI-Plattformen technologische Unabhängigkeit sichern und industrielle Innovationen beschleunigen /// von Heiner Sieger

Warum ist es gerade jetzt so wichtig, das Thema digitale Souveränität ernst zu nehmen und Initiativen zu ergreifen?
Prof. Dr. Feiyu Xu | Zu lange haben wir uns auf unseren wirtschaftlichen Erfolgen ausgeruht. Klassische Geschäftsmodelle der Kernindustrie Europas waren enorm profitabel, nicht zuletzt aufgrund historisch günstiger Energiepreise und des riesigen, aufnahmefähigen Marktes in China. Dabei wurde jedoch übersehen, dass sich die globale Wirtschaft beginnend bereits vor zehn bis 15 Jahren grundlegend verändert hat. Plattform-Ökosysteme und serviceorientierte Modelle haben kontinuierlich an Bedeutung gewonnen, doch diese neuen Geschäftsmodelle erfordern zwingend eine eigene, starke Cloud-Infrastruktur. Die Veränderungen kamen schleichend und nicht abrupt, weshalb die Notwendigkeit zum Handeln lange ignoriert wurde. Erst die Pandemie, der plötzliche Boom der virtuellen Zusammenarbeit, gestörte Lieferketten und schließlich der Krieg zwischen Russland und der Ukraine haben uns schmerzhaft vor Augen geführt, wie verletzlich wir in unseren industriellen Strukturen in Europa eigentlich sind.

Wo stehen wir aktuell im internationalen Vergleich, wenn es um KI und digitale Ökosysteme geht?
Prof. Dr. Feiyu Xu | Die Zahlen sprechen eine eindeutige Sprache. Unter den zehn nach Marktkapitalisierung wertvollsten börsennotierten Unternehmen der Welt finden sich mindestens sieben KI-Firmen, darunter der AI-Chipdesigner Nvidia, Chip-Hersteller TSMC, große Hyperscaler und Plattformen wie Google, AWS, Microsoft und Meta. Diese Unternehmen bilden längst eine eigenständige, hochprofitable Zukunftsindustrie. Europa spielt in diesem digitalen KI-Ökosystem faktisch keine wesentliche Rolle. Stattdessen haben europäische Firmen in China bereitwillig die dortigen Hyperscaler genutzt und im Rest der Welt blind auf amerikanische Infrastruktur vertraut. Wir haben diese Technologien wie selbstverständlich konsumiert, ähnlich wie Strom oder Wasser aus der Leitung, ohne zu begreifen, dass sie die absolute Voraussetzung für das Überleben unserer eigenen Demokratie, unserer Industrie und unseres Alltags sind. Ein Beispiel dazu: Um die europäische Verteidigungsfähigkeit abzusichern, ist zwingend eine eigene Defense Cloud erforderlich. Wenn wir in diesem Zukunftsmarkt nicht sofort aktiv mitspielen, verlieren wir massiv an Wettbewerbsfähigkeit.

Bedeutet digitale Souveränität im Umkehrschluss, dass wir uns vollständig von den USA und Asien abkoppeln müssen?
Prof. Dr. Feiyu Xu | Eine komplette Abschottung ist weder realistisch noch erstrebenswert. Schließlich profitieren Staaten enorm von globaler Zusammenarbeit, dem Austausch von Gütern und dem Transfer von Technologien. Es geht vielmehr um eine strategische Neuausrichtung. Bisher verfolgte Europa fast ausschließlich ei-

> „ Wir sollten messerscharf identifizieren, welche kritischen Technologien wir **zwingend selbst entwickeln** müssen, den sogenannten Make-Teil. Als Voraussetzung brauchen wir eine systematische Datenspeicherung und müssen eine **Datenkultur aufbauen**, die das Teilen von Industriedaten aktiv fördert.
>
> *Prof. Dr. Feiyu Xu*



DIE GESPRÄCHSPARTNERIN

Prof. Dr. Feiyu Xu

ist eine international anerkannte KI-Forscherin und eine der führenden Expertinnen auf dem Gebiet der Künstlichen Intelligenz.
Seit April 2025 ist sie Professorin an der German University of Digital Science. Sie war u.a. Global Head of AI bei SAP und leitete das AI Lab von Lenovo. Feiyu ist Aufsichtsrätin bei Siemens Energy, ZF Group und Airbus, sowie Vorsitzende des Asia Berlin Forum. Sie wurde von Forbes China unter die Top 50 Women in Tech gewählt.

ne reine Partnerstrategie. Wir haben uns schlichtweg zu stark auf andere verlassen und zu wenig selbst entwickelt. Stattdessen ist eine ausbalancierte Make-Buy-Partner-Strategie erforderlich. Das bedeutet konkret, wir sollten messerscharf identifizieren, welche kritischen Technologien wir zwingend selbst entwickeln müssen, den sogenannten Make-Teil. Als Voraussetzung brauchen wir eine systematische Datenspeicherung und müssen eine Datenkultur aufbauen, die das Teilen von Industriedaten aktiv fördert. Gleichzeitig sollten wir definieren, welche sensiblen Daten auf keinen Fall in die Hände ausländischer Hyperscaler geraten dürfen und zwingend unter europäischer Kontrolle bleiben müssen.

Datensouveränität bedeutet, bewusste, strategische Entscheidungen zu treffen, nicht einfach nur Server in Europa aufzustellen.

Was sind aus Ihrer Sicht die aktuell drängendsten Handlungsfelder für Europa?

Prof. Dr. Feiyu Xu | Wir haben ein massives Defizit über die gesamte technologische Wertschöpfungskette hinweg. Nehmen wir die Chipindustrie als Beispiel. US-amerikanische Firmen dominieren das komplexe Chipdesign. In Europa gibt es zwar exzellente Unternehmen wie ASML, die erfolgskritische Lithographie-Technologien anbieten, aber in der gesamten Wertschöpfungskette machen sie vielleicht zehn Prozent aus. Etwa 40 Prozent der Wertschöpfung liegen in den USA und gewaltige 60 Prozent der Chipproduktion finden in Asien statt, wobei Taiwan eine absolut kritische Rolle für Hochleistungschips spielt. Daher stellt sich die Frage, ob diese fatale Abhängigkeit bei Chips, die nicht nur für unsere Autoindustrie existenziell sind, weiter akzeptabel ist. Ähnlich prekär sieht es bei den großen Sprachmodellen aus. Zwar bestehen in Europa ambitionierte Ansätze, aber im direkten Vergleich mit dominanten Akteuren wie OpenAI, Anthropic, DeepSeek oder Tencent hinken die heimischen Akteure deutlich hinterher. Uns fehlt somit die elementare KI-Lieferkette: Es sind schlichtweg zu wenig eigene Rechenzentren vorhanden, zugleich steht Europa vor enormen Herausforderungen bei der Bereitstellung stabiler und bezahlbarer Energie.

Die europäische Politik versucht gegenzusteuern, beispielsweise mit dem AI Act oder dem Data Act. Reicht das aus, um den Markt zu beruhigen und in geordnete Bahnen zu lenken?

Prof. Dr. Feiyu Xu | Der Data Act ist prinzipiell ein guter Schritt, um Unternehmen in die Richtung zu bewegen, Daten effektiver und zugleich sicher miteinander zu teilen. Doch diese Maßnahmen kommen eigentlich schon zu spät. Das weitaus größere Problem ist unsere politische Grundhaltung. Die europäische Regulierung ist stark risikofokussiert. Anders gesagt: Ziele werden bisher primär über die Minimierung von Risiken definiert. In den USA herrscht eine völlig andere Mentalität. Dort lautet das vom Weißen Haus erklärte Ziel KI-Leadership, direkt verbunden mit dem Abbau von technologischen und bürokratischen Barrieren. Anders gesagt: Die USA verfügen über einen klaren Winning Plan. Wenn man gewinnen will, ordnet man alle Aktionen diesem Ziel unter und strebt nach maximalen autonomen Fähigkeiten. Europa und Deutschland fehlt ein solcher holistischer Businessplan für die digitale Zukunft. Risikomanagement ist zwar wichtig, darf aber immer nur ein untergeordneter Teilbereich eines übergeordneten Wachstumsplans sein.

Wie lässt sich so ein Wachstumsplan angesichts der bisweilen schwerfälligen Strukturen in Europa finanzieren und organisieren? Müssen das die großen Konzerne richten oder ist der Staat gefordert?

Prof. Dr. Feiyu Xu | Digitale Infrastruktur ist aus meiner Sicht ein zentraler Bestandteil von kritischer Infrastruktur. Bei Projekten wie dem Bahnnetz oder Autobahnen hat sich gezeigt, dass kritische Infrastruktur durch mutige staatliche Planung in kluger Kombination mit privatwirtschaftlichen Geschäftsmodellen erfolgreich aufgebaut oder erweitert werden können. Das mit Abstand beste Beispiel für eine erfolgreiche europäische Zusammenarbeit ist meines Erachtens Airbus – ein Projekt, das Jahrzehnte nach Boeing startete und dennoch zur Weltspitze wurde. Allerdings sollte sich Europa vom dysfunktionalen Gießkannenprinzip lösen, bei dem Geld ziellos und ineffizient in die Breite verteilt wird. Für erfolgskritische, teure Technologien sind hochkonzentrierte Investitionen in zentrale strategische Projekte erforderlich, ausgestattet mit den absolut besten Köpfen und optimalen Rahmenbedingungen. Dazu gehört auch, aktiv Talente und Top-Experten anzuziehen, die derzeit für amerikanische Hyperscaler arbeiten. Viele dieser Spezialisten sind selbst Europäer, die sehr gerne zurückkehren würden, wenn sie in Europa eine adäquate Vergütung, ein förderliches regulatorisches Umfeld und exzellente Standortbedingungen vorfinden würden. •

Ohne digitale Souveränität keine Verteidigungsfähigkeit: Europas entscheidende Sicherheitsfrage

Für Unternehmen wird digitale Souveränität zur Sicherheitsfrage: Wer in einer Cloud und KIgeprägten Welt Daten, Systeme und Prozesse souverän kontrolliert, sichert Europas Resilienz – technisch, operativ und rechtlich. /// Von Martin Merz

Europas unterschätzte Verteidigungsfrage

Europa diskutiert über Verteidigungsbudgets, Abschreckung und industrielle Kapazitäten. Das ist zwar notwendig, aber eine entscheidende Sicherheitsfrage wird noch immer unterschätzt: Wer kontrolliert die digitale Infrastruktur, auf der moderne Verteidigung, Verwaltung und kritische Industrien laufen?

Genau dort beginnt heute Resilienz. In Krisen entscheidet nämlich nicht nur die Verfügbarkeit von Material über Handlungsfähigkeit, sondern ebenso die Hoheit über Daten, Systeme und Prozesse. Wer seine digitalen Grundlagen nicht eigenständig betreiben und absichern kann, ist im Ernstfall in seiner Reaktions- und Entscheidungsfähigkeit eingeschränkt.

Für Unternehmen und Behörden existiert diese Diskussion schon länger. In Zeiten stetiger geopolitischen Veränderungen wird es immer wichtiger, digitale Abhängigkeiten bewusst zu steuern. Die Risiken sind konkret und real. Manipulationen in der Produktion, Datendiebstahl oder Störungen operativer Abläufe können erhebliche Auswirkungen auf reale Wertschöpfung und Versorgungssicherheit haben. In der Industrie kann das die Resilienz von Produktionsketten schwächen, in der Logistik Versorgung unterbrechen, in sicherheitskritischen Szenarien sogar dazu führen, dass notwendige Updates für Systeme ausfallen.

Ganzheitliche Souveränität

Eine oft genannte Fehlannahme in der Debatte ist, dass es reicht, einzelne Komponenten zu schützen oder Daten nur im Land zu speichern. Dabei ist es entscheidend, Souveränität bereits auf Systemebene mitzudenken. Digitale Einsatzfähigkeit entsteht erst dann, wenn der gesamte Stack souverän betrieben wird, vom Rechenzentrum über Plattformen bis hin zu den Software-Applikationen. Dafür braucht es zudem klare Zuständigkeiten, technische

DER AUTOR
Martin Merz ist President Sovereign Cloud bei SAP.

> „ Eine oft genannte Fehlannahme in der Debatte ist, dass es reicht, einzelne Komponenten zu schützen oder Daten nur im Land zu speichern. Dabei ist es entscheidend, Souveränität bereits auf **Systemebene** mitzudenken. *Martin Merz*

DIE DEFINITION VON DIGITALER SOUVERÄNITÄT

Für digitale Souveränität reichen Datenschutz und der Standort eines Rechenzentrums nicht aus. Um souveräne Handlungsfähigkeit zu ermöglichen, müssen vier Ebenen als Fundament gewährleistet sein:

- **Datensouveränität** bedeutet, dass Daten innerhalb des nationalen oder europäischen Rechtsraums gespeichert und verarbeitet werden und vor unbefugtem Zugriff geschützt sind.
- **Betriebliche Souveränität** heißt, dass der Betrieb durch qualifiziertes, sicherheitsüberprüftes und haftbares Personal erfolgt, das dem jeweiligen nationalen Recht unterliegt.
- **Technische Souveränität** verlangt Systeme, die auch im Krisenfall stabil und funktionsfähig bleiben.
- **Juristische Souveränität** setzt voraus, dass Betreiber und Infrastrukturen klar definierten nationalen oder europäischen Gerichtsbarkeiten unterliegen und durch lokale Governance, rechtliche Zuständigkeiten und Kontrollmechanismen geschützt werden.

und organisatorische Absicherungen, verlässliche Kommunikationswege und Notfallprotokolle, die auch unter Druck funktionieren. Nur dann entsteht aus Souveränität tatsächlich auch Resilienz.

Konflikte werden in der heutigen Zeit längst nicht mehr nur physisch ausgetragen. Cyberangriffe destabilisieren Energieversorgung sowie innere und äußere Sicherheit, sie alle zielen darauf, Entscheidungsfähigkeit zu untergraben. Fehlt in solchen Fällen der souveräne Zugriff auf Systeme, Daten und Prozesse, nehmen Abhängigkeiten und Risiken zu: operativ, wirtschaftlich und strategisch.

Es geht auch ohne Abschottung

In der großen Diskussion um digitale Souveränität wird oft auf die Abhängigkeit von US-Hyperscalern hingewiesen und eine komplette Abschottung gefordert. Es greift jedoch zu kurz zu glauben, dass sich diese Herausforderungen allein durch Abschottung lösen lassen.

Europa kann nicht alle bereits vorhandenen Technologien neu erfinden, und das muss es auch nicht. Europa muss wissen, welche Systeme und Fähigkeiten unverzichtbar sind, und sie gemeinsam entwickeln, schützen und betreiben. Wo Kooperation sinnvoll ist, können europäische Partner Lösungen schaffen, die den eigenen Werten und Sicherheitsanforderungen entsprechen.

Auf diese Weise wird Sicherheit gewährleistet, ohne dabei in Sachen Innovation den Anschluss zu verlieren. Denn niemand kann sagen, wie die Welt morgen aussehen wird. Dafür sind die geopolitischen Entwicklungen zu schnell und erfordern stetige Anpassbarkeit, die bei einer Abschottung gebremst wird.

Was muss Europa jetzt tun?

1. Priorisierung
   Nicht alle Daten und Systeme sind gleich relevant. Europa muss definieren, welche Bereiche für Verteidigung, Versorgung und Entscheidungsfähigkeit kritisch sind und wo Offenheit möglich bleibt. Auf diese Weise lassen sich Schutzmaßnahmen dort konzentrieren, wo sie strategisch am meisten bewirken, ohne Innovationen oder Partnerschaften unnötig zu begrenzen.
2. Souveräner Umgang mit Daten
   Europa muss verstehen, welche Informationen seine digitalen Kronjuwelen sind: die Daten, die für Funktionsfähigkeit, Versorgung oder wirtschaftliche Stabilität unverzichtbar sind. Diese Daten gehören klar in vollsouveräne Umgebungen. Gleichzeitig braucht es eine klare Klassifizierung mit abgestuften Schutzmechanismen, um einen gewissen Austausch von Daten zu ermöglichen und Innovationen voranzutreiben.
3. Zusammenarbeit
   Kein Akteur kann digitale Verteidigung allein stemmen. Staat, Industrie und IT-Wirtschaft müssen gemeinsam an resilienten Architekturen arbeiten und sichere Schnittstellen schaffen. Gemeinsame Standards sind entscheidend, um Kooperation zu ermöglichen, ohne Steuerungsfähigkeit aufzugeben. Multi-Cloud-Ansätze und modulare Systeme können helfen, Flexibilität mit Souveränität zu verbinden.

Fazit: Europas Resilienz beginnt im digitalen Dreiklang

Europas Sicherheit und Verteidigungsfähigkeit beginnt im digitalen Dreiklang aus Staat, Industrie und Gesellschaft. Deshalb sollte digitale Souveränität nicht länger als nachgeordneter Aspekt der Sicherheitsstrategie behandelt werden. Sie gehört in ihr Zentrum. Dabei muss Europa nicht alle Technologien selbst neu erfinden, aber das Wesentliche selbst beherrschen: Daten, Betrieb, rechtliche Kontrolle, resiliente Architekturen und die Fähigkeit, globale Technologie in eigene Regeln einzubetten. Genau darin liegt der Unterschied zwischen digitaler Abhängigkeit und digitaler Handlungsfähigkeit. •

IDENTITÄTEN FÜR KI-AGENTEN: Warum Europa vorne liegen könnte

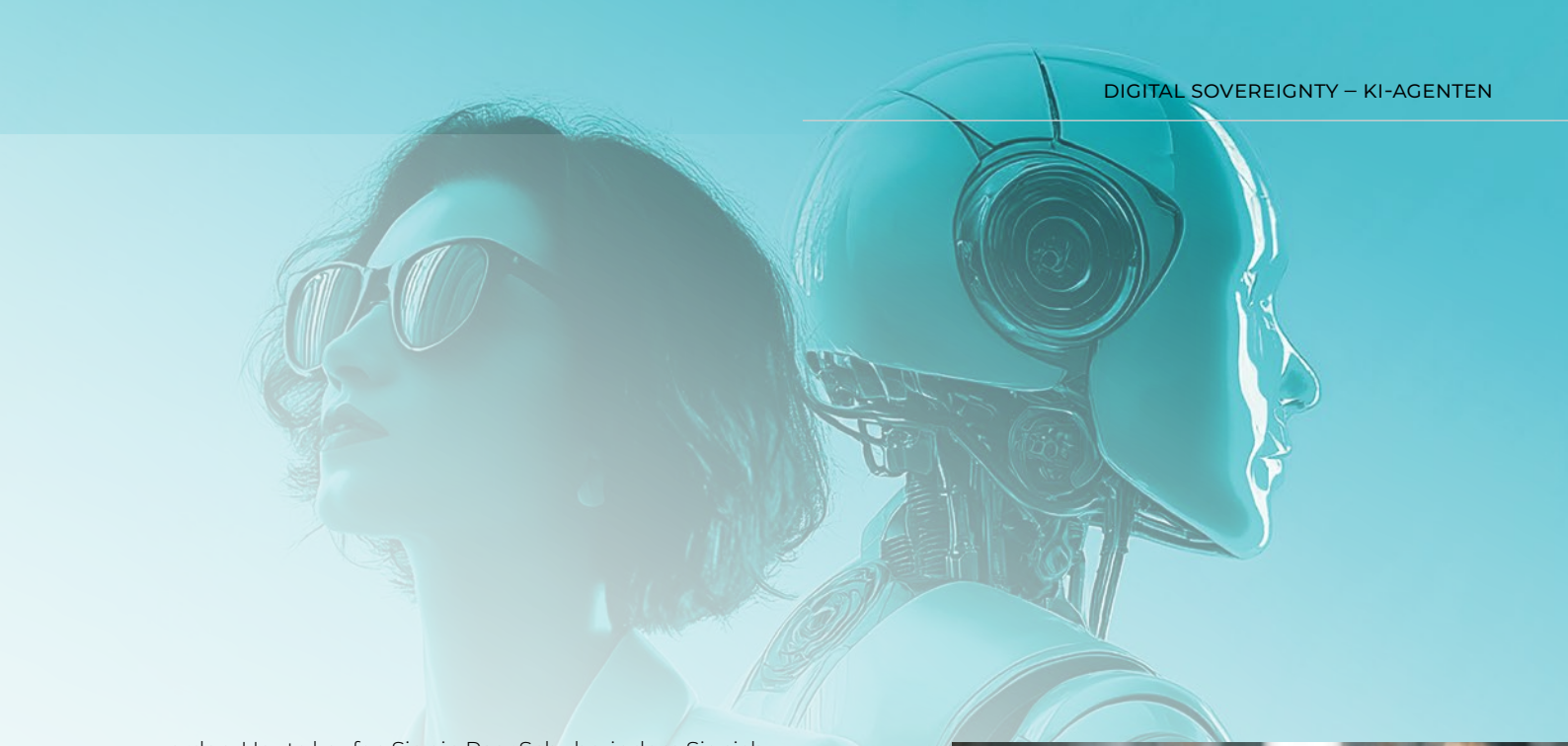
Wenn KI-Agenten künftig Schuhe, Aktien oder Versicherungen kaufen, braucht es belastbare Identitäts- und Intent-Delegation. Dr. Claudio Marforio erklärt, warum gerade Europas Regulierungstradition zum strategischen Vorteil werden kann. /// von Heiner Sieger

Herr Dr. Marforio, beginnen wir mit einer kurzen Einordnung: Wofür steht Futurae und was ist Ihr Auftrag?
Claudio Marforio | Futurae ist ein Unternehmen für Authentifizierung und Transaktionsbestätigung mit Sitz in Zürich. Wir arbeiten seit unserer Gründung an der Schnittstelle von Cybersicherheit und Usability. Ich habe selbst an der ETH Zürich zu Mobile Security promoviert. Wir wissen also, wie sich starke Sicherheitsgarantien umsetzen lassen – aber genauso entscheidend ist die Bedienbarkeit. Die größten Schwachstellen liegen meist nicht im System, sondern beim Menschen. Wer Sicherheit unbedienbar macht, dessen Nutzer finden Wege, sie zu umgehen. Wir begannen mit Authentifizierung für Endkunden, also dem Login in Online-Banking- und Mobile-Banking-Anwendungen. Dazu kamen Transaktionsbestätigung und Anti-Fraud. Geleitet hat uns dabei stets ein europäischer Anspruch an Datenerhebung, Datennutzung und Privatsphäre. Heute setzen Häuser wie Scalable Capital in Deutschland, Qonto in Frankreich, aber auch traditionelle Institute wie Santander, Raiffeisen oder Barclays unsere Software ein.

Wenn wir über digitale Souveränität sprechen: Wie definieren Sie Souveränität im Identity- und Access-Management (IAM) für Europa – und welche Kompromisse sind beim Spagat zwischen Souveränität, Interoperabilität und Nutzererlebnis akzeptabel?
CM | Souveränität hat mehrere Dimensionen. Erstens die Datensouveränität: Wer hat Zugriff auf welche Daten? Zweitens die Frage nach dem Code – Open Source und auditierbar oder proprietär und geschlossen? Drittens: Setzt eine Lösung auf offene Standards oder auf geschlossene Schnittstellen? Europa – und die Welt insgesamt – ist im Bereich Cybersecurity stark abhängig von US- und israelischer Technologie. Solange wir alle Freunde sind, ist das unproblematisch. Sobald die politische Lage kippt, wird es kritisch. Im IAM-Umfeld geht es um sensible Daten: Benutzernamen, Passwörter, Adressen, E-Mail-Adressen, Telefonnummern, Ausweis- oder Passdaten. Parallel dazu setzt Europa auf Standards für Interoperabilität – Stichwort EUDI-Wallet. Diese Standards basieren auf OpenID Connect und werden in den nächsten Jahren verpflichtend. Die spannende Frage ist: Welches Unternehmen baut die Software, die diese Standards spricht – und welches Unternehmen hat anschließend Zugriff auf die Daten? Europäische Entscheider sollten hier genau prüfen, mit welchen Anbietern sie zusammenarbeiten.

Die Lieferkette gilt als eine der kritischen Stellen digitaler Souveränität. Wie kann Europa eine resiliente, souveräne Identitäts-Lieferkette aufbauen, ohne Wettbewerb und Tempo zu ersticken?
CM | Supply Chain ist enorm komplex – es kommt darauf an, wo man die Linie zieht. Die Chips in den Servern werden in Taiwan oder China gefertigt. Die USA bauen ihre Fab-Kapazitäten aus, in Europa wird darüber kaum gesprochen, zumal es zweistellige Milliardeninvestitionen aus staatlichen Mitteln erforderte. Wenn wir die Hardware außen vor lassen und auf die digitalen Dienste schauen, brauchen Unternehmen ein gründliches Review ihrer Anbieter und deren Subprozessoren – im DSGVO-Sinn. Es gibt europäische Anbieter für Customer-IAM, für Authentifizierung, Transaktionsbestätigung und EUDI-Wallet-Provisionierung – Futurae ist einer davon. Mit ihnen zu arbeiten, kann einen Aufpreis bedeuten oder eine etwas kleinere Funktionsbreite. Im Gegenzug ist man aber nicht in seinen Möglichkeiten gegenüber den eigenen Nutzern beschnitten.

Welche strategische Rolle spielt KI im europäischen IAM – und wie lassen sich risikobasierte Entscheidungen mit den EU-Werten Privatsphäre, Transparenz und Fairness vereinbaren?
CM | Europa ist berühmt dafür, große, komplexe Gesetzeswerke zu schaffen, bevor die Produkte am Markt sind. Das war in der Vergangenheit oft schlecht, kann bei KI aber zum Vorteil werden. Beim Rennen um die KI-Modelle hat Europa weitgehend verloren – die Forschung passiert mehrheitlich in den USA, und sie zieht europäisches Talent ab. Der jüngste Fall ist der österreichische Erfinder hinter „Open Claw", den OpenAI binnen Monaten engagiert hat. Aber: Weil wir streng reguliert sind und weil wir digitale Identitäten konsequenter aufbauen, kann Europa zum Innovationsraum für agentische KI-Identitäten



werden. Heute kaufen Sie ein Paar Schuhe, indem Sie sich einloggen, Karte hinterlegen und Kauf bestätigen. Morgen sagen Sie Ihrem Agenten: „Bestell mir blaue Schuhe." Heute gibt es keinen Weg, meine Identität rechtssicher an einen Agenten zu delegieren – und keinen Weg für den Händler, meine Absicht zu verifizieren. Im IAM-Umfeld sehe ich genau hier Raum für europäische Anbieter: erstens die Delegation einer digitalen Identität an einen Agenten, zweitens das Einbetten der ursprünglichen Nutzerabsicht. Bei Schuhen ist eine Fehllieferung kein Drama. Wenn der Agent statt Nvidia-Aktien Qualcomm-Aktien ordert, entsteht ein finanzieller Schaden in einem hochregulierten Markt. Genau hier kann Europa Vorreiter werden.

Letzte Frage: Wenn Sie CEOs, CIOs und CISOs in der EU beraten – welche drei Schritte sollten sie in diesem Jahr für ein souveränes IAM gehen?

CM | Ganz einfach. Erstens: Erstellen Sie eine Inventarliste Ihrer Anbieter. Klären Sie, ob sie europäisch sind – auch auf Ebene der Anteilseigner. Jeder CIO darf diese Information einfordern. Zweitens: Wenn ein Anbieter nicht europäisch ist, prüfen Sie ernsthaft einen Wechsel innerhalb der nächsten zwölf Monate. Es gibt europäische Player, und der Wechsel ist heute leichter als früher. Drittens: Warten Sie nicht länger. Europa hat 20 Jahre gewartet. Vor zwei, drei Jahren sind wir schweißgebadet aufgewacht – und trotz milliardenschwerer staatlicher Förderprogramme hat sich zu wenig bewegt. Gehen Sie Ihre Vendor-Liste durch, identifizieren Sie die kritischen Komponenten und legen Sie los. Ich bin Optimist – aber die Zeit des Wartens ist vorbei. Sonst wird die Zukunft Europas nicht so hell, wie ich sie mir wünsche. •

DER GESPRÄCHSPARTNER

Dr. Claudio Marforio

ist CEO und Mitgründer der Futurae Technologies AG, eines Spin-offs der ETH Zürich mit Sitz in Zürich. Das Unternehmen versorgt mehr als 100 Enterprise-Kunden in über 40 Ländern – darunter Santander, Barclays, Raiffeisen, Scalable Capital und Qonto – mit Authentifizierungs-, Transaktionsbestätigungs- und Anti-Fraud-Lösungen.

> „Unternehmen starten typischerweise mit einem Anbieter – GCP, AWS, Azure oder OVH – und verstricken sich zunehmend in dessen Ökosystem. Wichtig ist deshalb, **von Beginn an Bausteine unterschiedlicher Anbieter nutzbar zu machen**, damit sich Daten verschieben oder gezielt bei nicht US-kontrollierten Anbietern halten lassen.
>
> *Claudio Marforio*

MEHR ERFAHREN ...

Lesen Sie das gesamte Interview mit Claudio Marforio auf der Website des DIGITAL BUSINESS MAGAZINS und erfahren Sie:

- Wie sieht eine souveräne Cloud-Strategie für Identitäten konkret aus?
- Welche Prinzipien sichern Portabilität und verhindern Vendor-Lock-in im IAM – und was sollte in Procurement und Verträgen nicht verhandelbar sein?
- Was sollten Unternehmen und Service-Provider in den nächsten zwölf bis 24 Monaten tun, um wallet-basierte Identitäten zu integrieren und zukunftssicher aufzustellen?

Digitale Souveränität: ANSPRUCH, ILLUSION UND REALITÄT

Digitale Souveränität wird oft gefordert, aber selten zu Ende gedacht. Warum Software und Daten sich nicht einfach europäisieren lassen und wo die eigentlichen Probleme liegen. /// von Michael R. Berthold

DIGITALE SOUVERÄNITÄT IST EIN VIELDISKUTIERTES THEMA IN EUROPA – besonders wenn es um Datenschutz, geopolitische Abhängigkeiten und KI geht. Oft heißt es dann vereinfacht: „Kauft europäische Software" und „Nutzt europäische Daten". Beides ist aber in der Realität gar nicht so trivial, da Software praktisch immer aus einem Konglomerat internationaler Komponenten besteht und insbesondere das Training von KI-Modelle nur durch die Nutzung vieler und möglichst diverser Daten zu hoch performanten Modellen führt. Man kann also nur in wenigen Fällen wirklich komplett autark agieren.

Dieser Beitrag zeigt auf, warum digitale Souveränität komplexer ist als gedacht, wo die größten Probleme liegen und welche Fragen wir dringend klären müssen.

Souveräne Software – (meist) eine Illusion

Der Wunsch nach souveräner Software klingt plausibel, und der Verzicht auf nicht-europäische Lösungen (z.?B. Windows) ist theoretisch möglich - etwa durch den Einsatz von Open-Source-Alternativen wie Linux. Allerdings besteht Linux aus einer Vielzahl international entwickelter Komponenten, die nicht ausschließlich in der EU entste-

DER AUTOR
Prof. Michael Berthold
Michael Berthold ist Informatiker und international anerkannter Experte für Data Science, Künstliche Intelligenz und maschinelles Lernen. Er war Mitgründer und treibende Kraft hinter der Open-Source-Plattform KNIME, die heute weltweit von mehreren Hunderttausenden Menschen sowie internationalen Unternehmen genutzt wird. Als Forscher und Unternehmer prägt er, wie Organisationen Daten analysieren und datenbasierte Entscheidungen treffen.

DIE EIGENTLICHE FRAGE: WAS BEDEUTET SOUVERÄNITÄT ÜBERHAUPT?

Digitale Souveränität scheitert weniger an fehlendem Willen als an der globalen Verwobenheit von Software, Daten und Infrastruktur. Vollständige Kontrolle ist kaum realisierbar, sondern allenfalls eine fallbasierte Teil-Souveränität.

Wir sollten also erst einmal klären, was wir unter Souveränität in einem bestimmten Kontext verstehen.

Geht es darum, dafür zu sorgen, dass meine E-Mail auch noch funktioniert, wenn jemand in den USA meinen Account sperrt? Das ist relativ einfach zu verhindern, indem man seinen E-Mail Provider wechselt.

Geht es darum, meine persönlichen Daten – oder die meiner Firma – vor Regierungszugriffen zu schützen: auch hier ist ein Umzug auf einen europäischen Provider möglich, wird aber schon mühsamer. Microsoft- oder Google-Dienste sind weitverbreitet und erheblich besser integriert als viele Alternativen. Das zeigt sich bereits an einigen Bundesländern, die auf Open Source Software wechseln (wollen): Nicht nur die Migration selbst verursacht Aufwand, auch der Betrieb ist nicht immer ganz so reibungslos, wie man das von Microsoft und Co. gewohnt ist.

Geht es darum, Software einzusetzen, die in der EU entwickelt oder wenigstens hier validiert wurde? Das wird schon erheblich schwieriger und wird sich nur für wenige, wichtigen Anwendungen wirklich durchführen lassen. Für die wirklich kritischen Anwendungen müsste man sich wohl vom World-Wide Web abnabeln und auf eine reine EU-Infrastruktur wechseln. In diesen Fällen schlägt Sicherheit klar Innovationsgeschwindigkeit.

Bei Daten ist allerdings Alarmstufe rot. Die EU sollte zügig beginnen, wichtige Daten (Forschungs- aber auch schlicht historisch relevante Informationen) zu kopieren und innerhalb der EU zu hosten. Programm-Repositories liegen oft ohnehin schon an vielen Stellen als Kopie vor und sind im Notfall meist wieder auffindbar. Forschungsdaten, Publikationen oder historische Archive sind allerdings oftmals wirklich nur innerhalb von bestimmten Landesgrenzen verfügbar und im Ernstfall verloren.

hen oder gewartet werden. Viele Open Source Projekte sind eine Kombination von Code, der von Menschen weltweit geschrieben und gewartet wird – nicht nur in der EU. Die nicht-europäischen Teile neu zu schreiben, ist praktisch immer illusorisch; am Ende würde eine (erheblich schlechtere) EU-Version entstehen. Theoretisch könnte man den Code aus anderen Regionen zumindest durchsehen, um sicherzugehen, dass keine unerwünschten Funktionen oder Sicherheitslücken enthalten sind. Aber auch das ist in der Praxis kaum realistisch: Teile des Codes ändern sich kontinuierlich und eine manuelle Durchsicht ist schlicht nicht praktikabel.

Abhilfe könnten hier neuere KI-Modelle bieten, die spannendes Potenzial für eine automatisierte Analyse von Code-Repositorien versprechen. KI-Systeme wie die von Anthropic sind mittlerweile so gut darin, Sicherheitslücken zu finden, dass das fast schon ein Problem wird – was sich natürlich auch in die andere Richtung ausnutzen lässt.

Übrigens betrifft dieses Problem auch jede relevante Nicht-Open- Source-Software, selbst wenn diese ausschließlich in der EU programmiert wurde. Praktisch alle Programme (auch Windows) bauen an irgendeiner Stelle auf Open-Source-Komponenten auf.

Aber selbst, wenn ich mir nun einbilde, die nicht-europäischen Teile der Software im Griff zu haben, bleibt ein anderes Problem: Der Code liegt auf Servern, die weltweit verstreut sind – oder auf GitHub, das bekanntlich Microsoft gehört. Also müsste ich eigentlich eine EU-basierte Kopie aller nicht-europäischen Aktivitäten aufsetzen und kontinuierlich abgleichen. Aber selbst das reicht nicht: Ich könnte nicht einfach nur kopieren (wer weiß, was andere reinschmuggeln), sondern müsste alles ständig kontrollieren. Auch hier bietet KI möglicherweise einen Weg, diese Kontrollen zu automatisieren. Wobei das die etwas ältere Generation an den Wettlauf zwischen Kopierschützern und Kopierprogrammen erinnert. Wer sagt, dass die KI, die ich verwende, nicht darauf trainiert wurde, bestimmte Manipulationen zu ignorieren?

Man kann natürlich noch eine Ebene tiefer einsteigen und sich überlegen, auf welcher Hardware denn meine ach so souveräne Software eigentlich läuft. Haben wir die vollständig unter Kontrolle? Unwahrscheinlich. Es hat nicht nur politische Gründe, dass Chips aus bestimmten Ländern nicht in sicherheitskritischer Infrastruktur eingesetzt werden dürfen.

Wirklich souverän bin ich nur, wenn ich in der EU entwickelte und gefertigte Hardware verwende, auf der ein Betriebssystem und Programme laufen, die vollständig in der EU entwickelt wurden und ausschließlich Komponenten verwenden, die ebenfalls aus der EU kommen.

Daten Souveränität – das (oft) ignorierte Problem

Neben der Software rückt zwangsläufig ein weiterer Aspekt in den Fokus: die Daten. Denn Programme sind am Ende auch nur Daten. Aus vielen Gründen ist es daher sinnvoll, nicht nur über die Software, sondern auch über die Souveränität anderer Daten nachzudenken: seien es Forschungsergebnisse, auf denen andere aufbauen, kritische Artikel zu undemokratischen Regierungen, oder aktuell: Trainingsdaten für KI-Modelle.

Auch hier haben wir ein ähnliches Problem und das ist zurzeit durchaus konkret. Wenn die US-Regierung etwa beschließt, ein Klimaforschungsinstitut zu schließen, verschwinden nicht nur die Tools, sondern auch die Daten. Doch gerade diese globale Datenvielfalt ist entscheidend – für viele Analysen, aber auch für das Training von LLMs. Müssen wir also anfangen, alle wichtigen (oder einfach nur diversen) Daten auf EU-Server zu kopieren? Bei Forschungspublikationen und einigen Datensätzen passiert das tatsächlich schon, aber für echte Souveränität müsste das viel, viel umfassender geschehen. Und auch hier besteht noch ein zentrales Risiko: Manipulation. Wer kontrolliert, was in diese Datensätze reinfließt oder, was weggelassen wurde? Mit geschickten Änderungen/Auswahl von auch nicht wissenschaftlichen Daten und Informationen lässt sich massiv beeinflussen, was KI-Systeme lernen – und damit, welche Antworten sie später geben.

Fazit

Digitale Souveränität ist deutlich komplexer, als es auf den ersten Blick erscheint. Wirklich ernst genommen, ist es in den meisten Fällen auch gar nicht durchsetzbar. Ein rein europäischer Ansatz könnte zwar Abhängigkeiten eliminieren, ist jedoch aufwändig, schränkt das Innovationspotenzial ein und ist damit nur in Ausnahmefällen überhaupt realisierbar. Realistischer ist ein differenzierter Ansatz: eine fallbasierte Analyse und die sorgfältige Abwägung des Aufwands und der Kosten einer teilweisen Souveränität gegenüber den tatsächlichen Risiken.

Einen kleinen Lichtblick bietet gerade die KI: mit Hilfe geschickt aufgesetzter Agenten lassen sich die regelmäßigen Überprüfungen externer Programm- oder Datenquellen deutlich besser skalieren. •

» Wirklich souverän bin ich nur, wenn ich in der EU entwickelte und gefertigte Hardware verwende, auf der ein Betriebssystem und Programme laufen, die **vollständig in der EU entwickelt** wurden und ausschließlich Komponenten verwenden, die ebenfalls aus der EU kommen. *Prof. M. Berthold*

Vier Mythen rund um die Quantenresilienz

Quantencomputer nähern sich schneller der Praxis als angenommen und damit rückt auch der „Q-Day“ näher. Das ist der Zeitpunkt, bei dem sich die heutige Verschlüsselung knacken lässt. Fehleinschätzungen zur Quantenresilienz führen dazu, dass Unternehmen die erforderlichen Maßnahmen zur Absicherung ihrer Daten nicht rechtzeitig einleiten.

/// von Yaroslav Rosomakho

ANGREIFER HABEN DIE BEDEUTUNG DER QUANTENCOMPUTER LÄNGST ERKANNT UND BEREITEN SICH DARAUF VOR: Sie fangen bereits heute riesige Mengen an verschlüsselten Datenpaketen ab, um sie später mithilfe der neuen Quanten-Technologie zu entschlüsseln. Selbst wenn Finanz- und Gesundheitsakten, geistiges Eigentum oder Regierungskommunikation bereits einige Jahre alt sind, könnten sie durch den Einsatz von Quantencomputern zur Entschlüsselung dennoch finanzielle, reputationsbezogene und rechtliche Schäden verursachen.

Das damit einhergehende Risiko ist also weder theoretisch noch spekulativ. Es kann jedoch bereits heute durch den Einsatz von Post-Quanten-Kryptografie (PQC) gemindert werden. Das Problem ist, dass viele Unternehmen noch keine Vorkehrungen treffen. Dieses abwartende Verhalten wird durch derzeit kursierende Missverständnisse über PQC begünstigt.

MYTHOS 1:
Gesamte Kryptografie muss ersetzt werden

Diese Annahme stimmt nicht ganz. Nur bestimmte zentrale kryptografische Algorithmen sind anfällig und müssen durch PQC-Upgrades ersetzt werden. Moderne kryptografische Hash-Funktionen bleiben robust und müssen nicht ausgetauscht werden, da Quantencomputer gegenüber herkömmlichen Computern keinen Vorteil haben, wenn es um die Erzeugung von Hash-Kollisionen geht. Auch moderne authentifizierte Verschlüsselung mit zugehörigen Datenalgorithmen wie AES-GCM und ChaCha20-Poly1305 weist keine Schwächen gegenüber Quantencomputern auf.

Zwar können Quantencomputer mit enormer Kapazität Brute-Force-Angriffe auf symmetrische Verschlüsselung durch Quanten-Suchalgorithmen beschleunigen, doch lässt sich dies durch eine Vergrößerung des Keys zur Verschlüsselung der Daten abfedern. Die Lösung besteht hier also nicht im Austausch vorhandener Sicherheit, sondern in deren Verstärkung. Was ersetzt werden muss, sind klassische asymmetrische Algorithmen wie RSA und ECC. Diese basieren auf Verfahren, die bekanntermaßen anfällig für Angriffe durch Quantencomputer sind.

MYTHOS 2:
Ausführung von PQC erfordert Quantencomputer

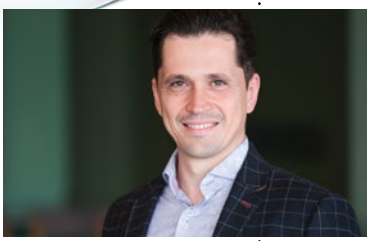
Das ist nicht korrekt. PQC kann bereits auf den Computern, die wir heute verwenden, ausgeführt werden – und das wird auch getan. Diese Computer sind so konzipiert, dass sie Quantenangriffen standhalten und gleichzeitig einen hohen Schutz vor klassischen Bedrohungen bieten. Denn ihre grundlegenden Schutzfunktionen sind für Quantencomputer genauso schwierig zu knacken wie für klassische Computer. PQC-Techniken sind nicht auf Quantengeschwindigkeit oder Quantencomputer angewiesen. Sie wurden vielmehr entwickelt, um die Fähigkeiten von Angreifern zu antizipieren. Dabei kommen Algorithmen zum Einsatz, die sich heute leicht einsetzen lassen. Wichtig ist, zu verstehen, dass das Ziel von PQC nicht darin besteht, Quantentechnologie zu nutzen, sondern sich gegen sie zu verteidigen. PQC läuft effizient auf der Hardware, die derzeit auf klassischen Computern verwendet wird.

MYTHOS 3:
PQC-Standards sind noch nicht fertig

Tatsache ist, dass die Standardisierung von PQC als praktischer, zuverlässiger und realitätsnaher Sicherheitsansatz bereits von nationalen Normungsgremien wie dem NIST in den USA, dem NCSC im Vereinigten Königreich, dem BSI in Deutschland, der ANSSI in Frankreich und anderen vorangetrieben wird. Die Internet Engineering Task Force (IETF) standardisiert die Anwendung von PQC-Kryptografie Primitives in Internetprotokollen wie TLS, SSH und IPSec.

Eine klar definierte Serie quantenresistenter Algorithmen (einschließlich ML-KEM für den Key-Austausch und ML-DSA für digitale Signaturen) gilt weithin als Ersatz für die anfälligen klassischen Algorithmen RSA und ECC. Diese Auswahl ist das Ergebnis jahrelanger globaler Zusammenarbeit und strenger Tests und wird nun in offiziellen

> „ Wichtig ist, zu verstehen, dass das Ziel von PQC nicht darin besteht, Quantentechnologie zu nutzen, sondern sich **gegen sie zu verteidigen**.
>
> *Yaroslav Rosomakho*



DER AUTOR

Yaroslav Rosomakho ist Chief Scientist bei Zscaler.

Bild: Zscaler

Standards formalisiert. Derweil befindet sich die IETF in der Endphase der Ausarbeitung von Updates, um PQC in reale Systeme zu integrieren. Diese Protokolländerungen werden es Browsern, Cloud-Diensten und anderen Infrastrukturen ermöglichen, PQC ohne Beeinträchtigung der Kompatibilität zu übernehmen.

MYTHOS 4:
Quantenbedrohungen sind noch Jahrzehnte entfernt

Dies ist die gefährlichste Fehleinschätzung, da sie das potenzielle Risiko unterschätzt, das von der Quantentechnologie ausgeht. Die Gefahr basiert auf dem Prinzip „jetzt sammeln, später entschlüsseln". Böswillige Akteure konzentrieren sich heute darauf, stark verschlüsselte Datenpakete zu erfassen, um sie später mit einem ausreichend leistungsfähigen Quantencomputer zu entschlüsseln. Das könnte in einem oder in 20 Jahren der Fall sein.

Sobald sensible Daten offengelegt werden – ob heute oder erst in einigen Jahren – ist der Schaden angerichtet. Der Datenschutz wird verletzt, das Vertrauen damit gebrochen und die Folgen sind irreversibel. Die Verantwortung für Maßnahmen liegt sowohl bei den Unternehmen als auch bei ihren Sicherheitsdienstleistern. Anbieter müssen darüber nachdenken, wie sie hybride Verschlüsselungssysteme unterstützen und eine skalierbare sowie nahtlose Integration interoperabler quantenresistenter Protokolle in die Cloud-Infrastruktur ermöglichen können.

Grundlage für Quantenresilienz schaffen

Fehlannahmen über Post Quanten-Kryptografie bremsen viele Unternehmen aus. Tatsache ist, dass Quantenbedrohungen kein zukünftiges Risiko darstellen, sondern bereits Realität sind. Deshalb ist es entscheidend, gezielt die verwundbaren asymmetrischen Verfahren zu ersetzen und PQC-fähige Key-Austauschmechanismen frühzeitig einzuführen. Diese werden bereits in den wichtigsten Sicherheitsprotokollen unterstützt und sind einsatzbereit. Ebenso wichtig ist es, lange Migrationszyklen für digitale Signaturen besonders von großen Unternehmen, die ihre eigene Public-Key-Infrastruktur verwalten, vorausschauend zu planen. Wer diese Schritte jetzt angeht, schafft die Grundlage für echte Quantenresilienz und eine sichere Zukunft für sein Unternehmen. •

Shadow AI:
Die künstliche Intelligenz,
die niemand freigegeben hat

Viele Unternehmen beschäftigen sich derzeit mit dem Einsatz von künstlicher Intelligenz. Idealerweise werden Leitlinien entwickelt, Tools evaluiert und Freigabeprozesse definiert. In der Praxis entsteht ein Teil der Nutzung jedoch parallel dazu – als Shadow AI. /// von Melanie Ludolph

KÜNSTLICHE INTELLIGENZ IST IM UNTERNEHMENSALLTAG ANGEKOMMEN: Texte werden mit generativen Tools erstellt, Präsentationen automatisiert, Daten ausgewertet – schnell und oft ohne Abstimmung. Die Hürde ist niedrig, der Nutzen unmittelbar. Was als pragmatische Lösung beginnt, wird schnell Teil der Arbeit. Für solche Konstellationen hat sich der Begriff „Shadow AI" etabliert. Gemeint ist die Nutzung von KI-Anwendungen durch Mitarbeiter außerhalb der vorgesehenen Prozesse – oft spontan, ohne zentrale Steuerung und ohne formale Freigabe.

Warum Shadow AI entsteht

Die Gründe sind naheliegend. Viele Mitarbeiter nutzen KI-Tools bereits privat und übertragen diese Nutzung in den Arbeitskontext. Gleichzeitig entwickelt sich das Angebot schneller, als interne Freigaben Schritt halten können. Zwischen verfügbaren und freigegebenen Lösungen entsteht so eine Lücke. Hinzu kommt: Freigegebene Tools sind nicht immer so flexibel oder schnell verfügbar wie die Alternativen. Wer effizient arbeiten will, greift dann auf das zurück, was unmittelbar funktioniert.

Zwischen Nutzen und fehlender Steuerung

Für Unternehmen ist das ambivalent. Der Einsatz von künstlicher Intelligenz kann die Produktivität deutlich steigern – entzieht sich aber gleichzeitig den vorgesehenen Steuerungsmechanismen. Deshalb wird die Nutzung nicht freigegebener Anwendungen in der Praxis häufig geduldet: Der Nutzen ist sichtbar, die vollständige Kontrolle schwer durchsetzbar. Gleichzeitig gilt: Unternehmen sollten sich nicht von einzelnen Anforderungen treiben lassen. Auch bei anderen IT-Systemen würde niemand jede gewünschte Lösung ungeprüft zulassen.

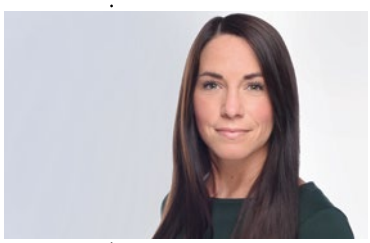
Das eigentliche Risiko von Shadow AI

Das Risiko liegt weniger in den Tools selbst als in ihrer konkreten Nutzung. Wenn Mitarbeiter sensible Informationen in externe Systeme eingeben, Ergebnisse ohne Einordnung weiterverwenden oder Inhalte übernehmen, deren Herkunft unklar ist, entstehen Risiken, die sich im Nachhinein nur schwer kontrollieren lassen. Shadow AI ist damit kein isoliertes IT-Problem, sondern Ausdruck fehlender Klarheit im Umgang mit einer neuen Technologie.

Der Versuch, Ordnung herzustellen

Viele Unternehmen reagieren darauf mit Verboten oder technischen Einschränkungen. In der Praxis bleibt das oft nur begrenzt wirksam. Denn der Bedarf an schnellen, unterstützenden Lösungen verschwindet nicht – er verlagert sich. Statt einzelne Tools zu verbieten, braucht es eine strategische Entscheidung: Welche Rolle soll KI im Unternehmen spielen – und welche nicht? Erst daraus ergibt sich, welche Anwendungen sinnvoll sind und unter welchen Bedingungen sie genutzt werden können. KI ist dabei keine reine IT- oder Datenschutzfrage. Sie betrifft zentrale Geschäftsprozesse und damit auch Verantwortung und Haftung. Entsprechend gehört sie in die Steuerung des Unternehmens.

Die Nutzung nicht freigegebener KI lässt sich technisch begrenzen. Entscheidend ist jedoch, dass Unternehmen festlegen, wie sie genutzt werden darf – und nicht erst reagieren, wenn Probleme entstehen. •



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

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 .

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.

easy software
Jakob-Funke-Platz 1
45127 Essen
+49 201 650 69-166
info@easy-software.com
www.easy-software.com

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

d.velop AG
Schildarpstraße 6-8
48712 Gescher
+49 2542 9307-0
info@d-velop.de
www.d-velop.de

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

MARKETPLACE
03

DIGITAL BUSINESS

04 2026

/// **Cyberrisk & Reslience**
Fünf Warnzeichen
Augen auf bei der Anbieterauswahl für die IT-Infrastruktur für geschäftskritische Kommunikation.

/// **Work & People**
Standardisierte Lösungen
Die Verbindung von Low-Code-Technologie und KI-Agenten schafft neue Spielräume für Personaler bei KMU.

/// **Quantencomputing**
Plattform für Innovation
Die Messe Quantum Effects bietet das gesamte Spektrum quantentechnologischer Innovationen, von sicherer Kommunikation bis zur Sensorik.

/// **Business Strategy & Innovation**
Cloud ERP
KI-Assistenten, Automatisierung und ESG-Integration machen ERP zum strategischen Digital Core für datengetriebene Geschäftsmodelle.

Die nächste Ausgabe erscheint am 30.07.2026

Redaktionell erwähnte Firmen dieser Ausgabe

Adlon, ADN, Asantial, Cancom, Celonis, Dataiku, Dynatrace, Elo, Eset, Esker, Fieldfisher, Flexera, F5, Fortinet, Futurae, German University of Digital Science, Getronics, IntegrityNext, Knime, Kumavision, Noris Network, OutSystems, PwC, Proofpoint, Okta, Rubrik, Sage, SAP, SmapOne, Trend Micro, T-Systems, Workday, Zscaler

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:
Dr. Rafael Arto-Haumacher, Prof. Michael Berthold, Luis Blando, Thomas Chudo, Henning Dittmer, Marius Dunker, Gerald Eid, Tommy Grosche, Dirk Hennig, Katharina Holzapfel, Simon Jaehnig, Markus Kammermeier, Sven Kniest, Rusy Kuhn, Melanie Ludolph, Martin Merz, Thomas Mierschke, Hermann Ramacher, Yaroslav Rosomakho, Oliver Rozic, Simon Russin, Armin Schneider-Lenhof, Michael Schröder, Jörg Schleburg, Stephan Schulz, Frank Schwaak, Sven Selle, Roman Spitzbart, Slatko Sterzenbach, Stefan Tiefel, Richard Werner, Prof. Dr. Feiyu Xu, Sven Zuschlag

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

Einsendungen: Redaktionelle Beiträge werden gerne von der Redaktion entgegen genommen. Die Zustimmung zum Abdruck und zur Vervielfältigung wird vorausgesetzt. Gleichzeitig versichert der Verfasser, dass die Einsendungen frei von Rechten Dritter sind und nicht bereits an anderer Stelle zur Veröffentlichung oder gewerblicher Nutzung angeboten wurden. Honorare nach Vereinbarung. Mit der Erfüllung der Honorarvereinbarung ist die gesamte, technisch mögliche Verwertung der umfassenden Nutzungsrechte durch den Verlag – auch wiederholt und in Zusammenfassungen – abgegolten. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden.

Ausgabe: 03/2026
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

WIN VERLAG

MEDIEN.
MÄRKTE.
MENSCHEN.

EIN PARTNER.
VIELE KANÄLE.
SICHTBARKEIT
AUF ALLEN EBENEN.

AUTOCAD MAGAZIN

BA BAUEN AKTUELL

DIGITAL BUSINESS

DIGITAL ENGINEERING MAGAZIN

DIGITAL MANUFACTURING

e commerce magazin
DER DIGITALE WEG ZUM KUNDEN

KGK RUBBERPOINT
Kautschuk | Gummi | Kunststoffe

r.energy
ERNEUERBARE ENERGIEN UND DIGITALISIERUNG

PLASTVERARBEITER

PLASTX NOW

win-verlag.de

Zahlungsverzug
Ausrede Nr. 210

„Entschuldigung, leider ist die Buchhaltung bis nächste Woche noch im Urlaub!“

Automatisch bereit für die E-Rechnung mit Sage.

Business-Software mit KI

Sage