



it management

Der Motor für Innovation
März/April 2026

INKLUSIVE 48 SEITEN

it
security

Insight⁺

KI: Firmen stecken fest
ab Seite 18

KI-VERANTWORTUNG

Vom Tool zum Akteur

Lumir Boureau, compacer GmbH



SAP JOULE VS.
ANDERE KI-SYSTEME

Was sind wirkliche Unterschiede?

DIGITALE
SOVERÄNITÄT

Mit UEM zur Datenhoheit

SPOT AN FÜR STARKE IT-LÖSUNGEN



Die besten IT-Lösungen | Die innovativsten Anbieter | Alles auf einen Blick!

UNSERE PREMIUMANBIETER



Hier könnte Ihr Logo platziert sein!
Jetzt buchen.

Ihre Ansprechpartner:



Kerstin Fraenzke
Head of Media Consulting
Tel. +49 8104 6494 19
fraenzke@it-verlag.de



Karen Reetz-Resch
Media Consulting
Tel. +49 8121 9775 94
reetz@it-verlag.de



Marion Mann
Media Consulting
Tel. +49 152 363 412 55
mann@it-verlag.de

it-daily.net/it-spotlight



END-TO-END-AUTOMATISIERUNG

”

LIEBE LESERINNEN UND LESER,

Prozessübergreifende Automatisierung ist zur strategischen Nagelprobe im B2B geworden. Viele Unternehmen stecken im „Tool-Wildwuchs“ fest: Marketing nutzt eine eigene Suite, Vertrieb ein eigenes CRM, Service ein Ticketsystem. Überall entstehen Insellösungen und Medienbrüche. Der Preis: doppelte Datenerfassung, fragmentierte Customer Journey, widersprüchliche Reports – und eine IT, die Entscheidungen nur noch nachvollzieht, statt sie zu gestalten.

Der notwendige Schritt ist End-to-End-Automatisierung auf Basis gemeinsamer Datenstrukturen. Kernobjekte wie Leads, Kontakte, Opportunities müssen einmal sauber modelliert und dann entlang der gesamten Wertschöpfungskette orchestriert werden. KI und Analytics entfalten ihren Wert erst, wenn dieser Datenwildwuchs reduziert ist.

IT und Fachbereiche müssen gemeinsam definieren, welche Funktionen zwingend zentralisiert werden (Datenmodelle, Integrations- und Automatisierungslayer) und wo bewusst Vielfalt erlaubt ist (UX-nahe Fachanwendungen, spezialisierte Analytics).

Die Rolle der IT verschiebt sich vom Systembetreiber zum Architekten eines Baukastens. Diese Architekturhoheit ist Voraussetzung für Steuerbarkeit, Compliance und wirtschaftlichen KI-Einsatz. Wer diesen Schritt nicht geht, automatisiert weiter im Kleinen – und verliert im Großen an Handlungsfähigkeit.

Ulrich Parthier
Publisher it management & it security



INHALT

COVERSTORY

- 10 Wie KI Verantwortung neu definiert**
Vom Tool zum Akteur

THOUGHT LEADERSHIP

- 14 Architekturentscheidungen, die Freiheit schaffen**
Wie IT-Systeme unabhängig, kontrollierbar und resilient werden

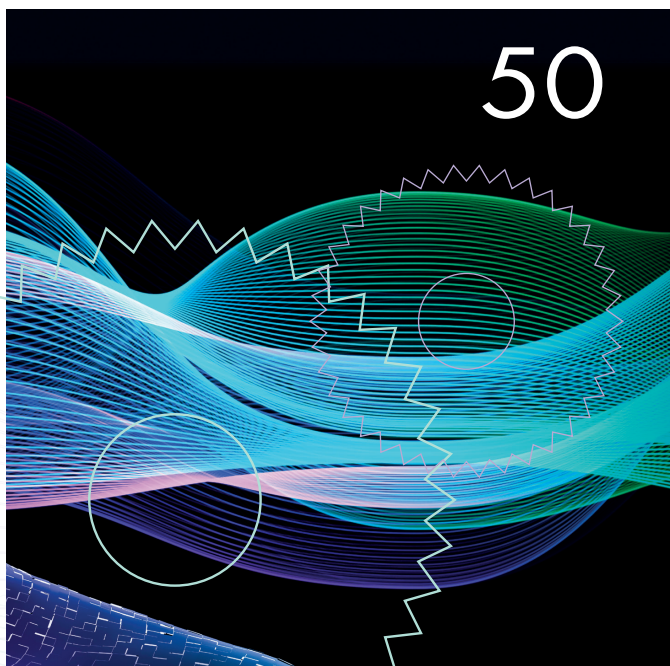
IT MANAGEMENT

- 18 KI: Firmen stecken fest**
Erfolg braucht ganzheitlichen Ansatz
- 20 Steampunk & BPT Summit 2026**
Antworten, Strategien, Roadmaps

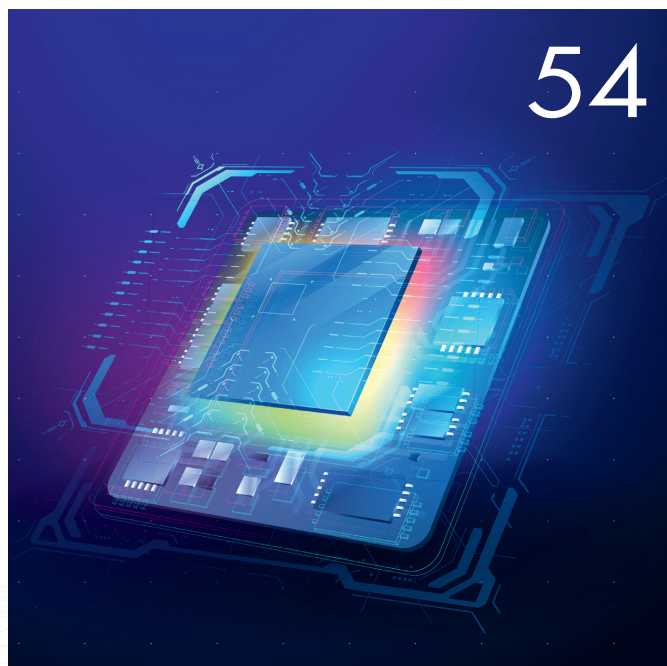
Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

- 22 S/4HANA strategisch nutzen**
Erfolgreiche SAP-Transformation
- 24 SAP Joule vs. andere KI-Systeme**
Was den SAP-Assistenten wirklich unterscheidet
- 28 SAP-Lizenzen: Vom Technikthema zum CFO-Tool**
Die Lizenzstrategie gehört 2026 auf die CFO-Agenda
- 31 Auch 2026: Preissteigerung bei Microsoft**
Wie die Lizenzkosten trotzdem bezahlbar bleiben
- 33 Smart Licensing**
Wenn MRM denkt, ist an alles gedacht
- 34 Unified Endpoint Management**
Mit UEM zu Datenhoheit und digitaler Souveränität
- 36 Souveräne KI statt Schatten-Tools**
Wie Unternehmen ihre KI-Nutzung sicher und wirtschaftlich steuern
- 38 Professionelles Site-Management**
Personallücken im Rechenzentrumsmanagement schließen
- 40 Effizientes Datenmanagement**
Der Trend geht zur KI-Fabrik

50



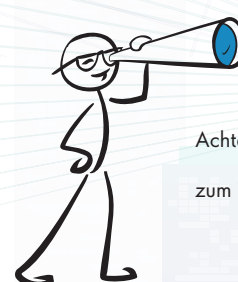
54



- 44 Datenwachstum 2026**
Warum Unternehmen ihre Cloud-Partner neu bewerten müssen
- 46 UCC-Supply-Chain aus seiner Hand**
Vertriebskonsolidierung schafft einheitliche Partnerbetreuung
- 48 Smarte Telefonie unter Kontrolle**
KI in der Telekommunikation kann alles – darf sie das auch?
- 50 Vom KI-Hype zur produktiven Realität**
Warum Unternehmen jetzt auf Open-Source Plattformen setzen sollten
- 54 NextGen CPUs für Multi-Tenant-KI**
Was jetzt anders gedacht werden muss
- 56 Das Digitalisierungs-Paradox**
Warum mehr Tools oft weniger Effizienz bedeuten
- 58 Erfolgreiche ERP-Implementierung**
Bewusste Vorbereitung auf die Veränderung
- 60 ERP-Migration entmystifiziert**
Keine Angst vor dem Wechsel
- 64 Flexible ERP-Systeme**
Der Schlüssel zu digitaler Souveränität



Inklusive 48 Seiten
it security



GUT ZU WISSEN

Achten Sie auf dieses Icon und lesen Sie mehr zum Thema im Internet auf www.it-daily.net

TRENDS IM DIGITALEN MARKETING

UNTERNEHMEN SEHEN KI AN DER SPITZE

LinkedIn-Posts von ChatGPT, Werbegrafiken von Midjourney oder KI-gesteuerte Newsletter-Kampagnen über HubSpot – Künstliche Intelligenz übernimmt bereits heute zahlreiche Aufgaben im digitalen Marketing. Was früher oft manuell erstellt wurde – etwa Social-Media-Posts, Visuals oder der Versand von Newslettern – wird zunehmend durch generative KI-Anwendungen unterstützt oder automatisiert. Dass es sich hierbei nicht nur um einen

kurzfristigen Hype handelt, zeigen Ergebnisse einer Befragung im Auftrag des Digitalverbands Bitkom unter 180 Unternehmen aus dem Netzwerk von Bitkom.

Ohne KI kein erfolgreiches Marketing

Gemäß der Bitkom-Studie sind 67 Prozent überzeugt, dass Marketing ohne den Einsatz von KI künftig nicht mehr erfolgreich sein wird. Mehr als die Hälfte

der Unternehmen (51 Prozent) ist der Ansicht, dass generative KI heute schon einen erheblichen Teil der kreativen Marketingarbeit übernimmt. Allerdings sagen 52 Prozent, dass es in Marketingabteilungen häufig an den nötigen Kompetenzen fehlt, um KI sinnvoll einzusetzen.

Weitere wichtige Trends

Im Trend-Ranking folgt auf KI mit deutlichem Abstand datengetriebenes Marketing, das 6 von 10 der Unternehmen als prägenden Trend bis 2027 einordnen. Knapp 4 von 10 befragten Unternehmen sehen Personalisierung als einen der einflussreichsten Trends bis 2027. Darüber hinaus nennen die Unternehmen weitere relevante Marketingthemen für die kommenden Jahre: 35 Prozent sehen die Customer Experience als einen der zentralen Trends, 31 Prozent verweisen auf Veränderungen im Medien- und Plattformökosystem wie Konsolidierung oder sinkende Reichweiten. Jeweils 25 Prozent nennen Datenschutz und die Cookieless Future, Social-Media-Marketing sowie Influencer- und Creator-Marketing als relevante Entwicklungen. 23 Prozent erwarten wachsende Bedeutung von Events – sowohl physisch als auch digital oder hybrid. 19 Prozent sehen Social Commerce als einen der Marketingtrends, die bis 2027 den größten Einfluss in Deutschland haben werden.

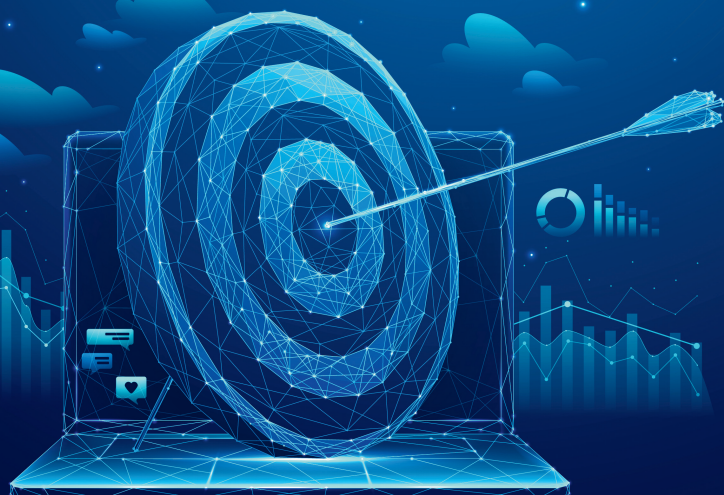
Marketing Automation

Daten und datenbasierte Prozesse sind dabei die Grundlage für Automatisierung im Marketing und Marketing Automation. Künstliche Intelligenz und Personalisierung erweitern diese Automatisierung und machen sie effizienter und zielgerichteter. Für die Mehrheit der befragten Unternehmen ist Marketing Automation relevant.

www.bitkom.org

TRENDS BIS ENDE 2027

Welche Trends werden bis Ende 2027 den größten Einfluss auf Marketing in Deutschland haben?



**MEHR
WERT**

Marketing im digitalen Wandel 2026





Deepfake-Risiken

WARUM FEHLENDES WISSEN ZUR
REALEN GEFahr WIRD

Ob in Social Feeds, Messengern oder KI-gestützten Chatdiensten: Manipulierte Inhalte lassen sich heute in Minuten erzeugen und in Sekunden verbreiten. 96,3 Prozent der Menschen in Deutschland kennen Fake News¹ – also bewusst falsche oder irreführende Informationen. Doch nur 34,3 Prozent wissen, was Deepfakes sind: mit Künstlicher Intelligenz erzeugte, täuschend echte Bild-, Audio- oder Videoinhalte. Das zeigt die repräsentative Studie „Fakt oder Fake? Medienkompetenz in Deutschland“ der IU Internationalen Hochschule, die im September 2025 veröffentlicht wurde.

Diese Wissenslücke ist brisant, wie zum Beispiel die aktuelle Debatte um den KI-Chatbot Grok zeigt: Gegen dessen Plattform X hat die EU-Kommission im Januar 2026 ein Verfahren nach dem Digital

Services Act eingeleitet. Grok ermöglicht es, in Sekunden fotorealistische Bilder zu generieren – auch sexualisierte Deepfakes ohne Einwilligung der abgebildeten Personen.

Wie anfällig die Menschen in Deutschland für Deepfakes sind, belegen weitere Zahlen der IU-Studie: Sie zeigen unter anderem, dass 33,1 Prozent der Befragten bereits Fake News geglaubt haben, die sich für sie nachträglich als falsch herausgestellt haben. Bei Deepfakes sind es 15,0 Prozent.

Weitere Ergebnisse der IU-Studie:

- Jüngere kennen Deepfakes besser: Je jünger die Generation, desto häufiger ist das Wissen über Deepfakes vorhanden. Diese Wissenslücke ist prob-

lematisch, denn die Folgen können gravierend sein: Von den 15,0 Prozent der Befragten, die bereits Deepfakes geglaubt haben, berichten 46,0 Prozent von dadurch ausgelöstem Stress oder Angst, 17,7 Prozent haben sich deswegen mit anderen gestritten.

- KI verstärkt das Problem: 84,8 Prozent stimmen zudem der Aussage zu, dass durch die Nutzung von KI-basierten Suchmaschinen die Verbreitung von Fake News zukünftig weiter zunehmen wird.
- Verantwortung bei Plattformen und Politik: Gleichzeitig verorten 65,1 Prozent der Befragten die Hauptverantwortung für die Bekämpfung von Fake News und Deepfakes bei den Betreibern sozialer Plattformen, 63,1 Prozent bei der Politik.

www.iu.de

Besuchen Sie uns auf der digitalBAU 2026 in Köln

24. – 26. März 2026, Halle 8, Stand 622



DIE SOFTWARE ZUR TRANSFORMATION. KONZIPIERT FÜR LOSGRÖSSE 1+

ams^{ERP}

FEHLENDE PROZESSE UND AUTOMATISIERUNG

VERWALTUNGSaufWAND BREMST BESCHÄFTIGTE AUS

Deutsche Unternehmen kämpfen mit einem Produktivitätsproblem: Mitarbeitende verlieren durchschnittlich 16 Stunden pro Woche – nahezu zwei volle Arbeitstage – für administrative Routineaufgaben. Eine aktuelle Studie von Ricoh Europe zeigt, dass nur 42 Prozent der Beschäftigten angeben, den Großteil ihrer Arbeitszeit mit wertschöpfenden Tätigkeiten zu verbringen.

Obwohl 35 Prozent der Entscheidungsträger erkennen, dass ihre Mitarbeitenden übermäßig viel Zeit mit Verwaltungsaufgaben außerhalb ihrer Kerntätigkeit verbringen, bleibt konkretes Handeln weitgehend aus. Die Kluft zwischen dem Bewusstsein der Führungskräfte für das Problem und der ausbleibenden Umsetzung von Gegenmaßnahmen kostet Unternehmen täglich wertvolle Produktivität.

Die Folgen sind weitreichender als nur der Produktivitätsverlust der Mitarbeiten-

den. Ein ineffizientes Dokumentenmanagement setzt deutsche Unternehmen einem Compliance- und Betriebsrisiko aus. So haben mehr als die Hälfte der Entscheidungsträger (61 %) und 45 Prozent der Büroangestellten in den letzten fünf Jahren erlebt, dass jemand aufgrund veralteter oder falscher Informationen, die durch ineffiziente Systeme oder Prozesse verursacht wurden, einen schwerwiegenden Fehler begangen oder beinahe begangen hätte.

Tägliche Frustrationen verschärfen das Problem

Deutsche Mitarbeitende berichten von alltäglichen, vermeidbaren administrativen Frustrationen, die ihre Produktivität schleichend untergraben. Besonders häufig genannt werden die wiederholte Eingabe identischer Informationen in mehrere Systeme (42 %), die Verwaltung überfüllter Posteingänge (38 %), die Suche nach Dateien in mehreren Systemen oder

auf gemeinsam genutzten Laufwerken (32 %) sowie die manuelle Aktualisierung von Reports (30 %). Diese Probleme können wertvolle Arbeitszeit kosten und die Arbeitsmoral beeinträchtigen.

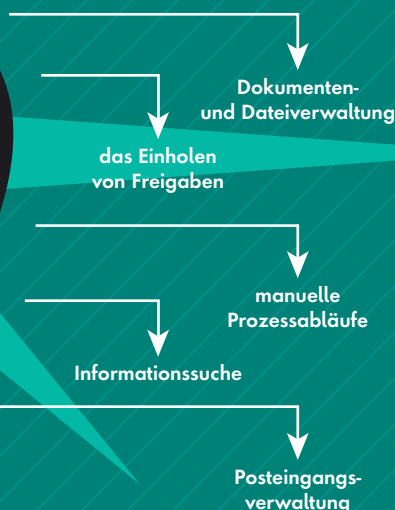
Die Folgen sind eindeutig. So geben 25 Prozent der Befragten an, dass der Verwaltungsaufwand ihre Produktivität einschränkt, und 22 Prozent sagen, dass er ihre Kreativität einschränkt. Die Mitarbeitenden sind sich der positiven Auswirkungen einer Reduzierung des Verwaltungsaufwands bewusst: mehr Freude an der Arbeit durch kreativere Aufgaben (34 %), erhöhte Wertschöpfung (29 %), schnellere Projektdurchführung (26 %), Lösung von mehr Kundenproblemen (25 %) und fundiertere strategische Entscheidungen (21 %).

Anhaltende Kluft und Untätigkeit

Trotz der Auswirkungen haben viele deutsche Arbeitnehmer das Gefühl, dass das Problem nicht erkannt wird. Mehr als ein Viertel (26 %) der Beschäftigten ist der Meinung, dass die Entscheidungsträger unterschätzen, wie viel Zeit durch Verwaltungsaufgaben verloren geht, während derselbe Prozentsatz der Meinung ist, dass die Arbeitsbelastung in der Verwaltung ungerecht verteilt ist. Nur 24 Prozent glauben, dass ihr Arbeitgeber sich aktiv um die Reduzierung ihres Verwaltungsaufwands kümmert. Dennoch stimmen 65 Prozent der Entscheidungsträger der Aussage zu, dass neue Tools und Systeme die Arbeitsabläufe in ihrem Unternehmen vereinfachen und den Verwaltungsaufwand verringern. Fast die Hälfte (44 %) glaubt, dass Automatisierungstools, die sich wiederholende, manuelle Aufgaben beseitigen, den größten Einfluss auf ihr Unternehmen haben würden.

www.ricoh.de

DIE 5 GRÖSSTEN ZEITFRESSER

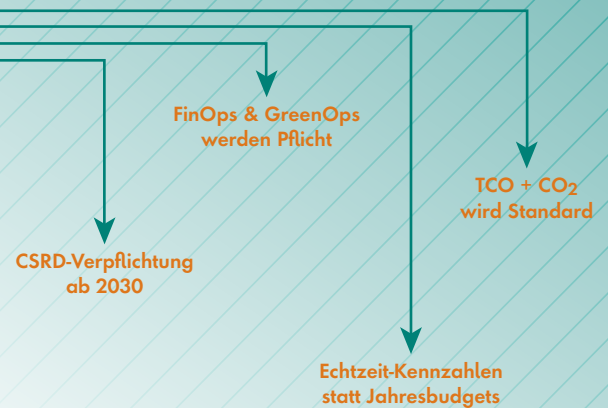




ZENTRALE HANDLUNGSFELDER FÜR CIOs

IT-Budgets 2026

KOSTENSENKUNG DURCH UMDENKEN?



Jahrzehntlang bedeuteten IT-Investitionen vor allem hohe einmalige Ausgaben für Hardware, Rechenzentren und mehrjährige Projekte, so genannte Capital Expenditure (CAPEX). Heute dominiert ein operatives Kostenmodell, so genannte Operational Expenditure (OPEX). Unternehmen zahlen für Cloud-Services, Lizenzen und Plattformen nutzungsbasiert, statt sie selbst zu besitzen. Das bringt Flexibilität, birgt aber auch Risiken.

Bis Ende 2026 werden mehr als 75 Prozent der IT-Ausgaben OPEX-getrieben sein, zeigen Zahlen des Analystenhauses Gartner. Gleichzeitig berichten Unternehmen jedoch von einem so genannten „Bill Shock“ mit durchschnittlich 23 Prozent Kostenüberschreitung. Hinzu kommt ein neuer Kostentreiber: generative KI. Schon heute verursachen KI-Workloads hohe GPU- und Token-Kosten, also Kosten für Rechenleistung und Datenverarbeitung. Prognosen zeigen: Bis 2030 könnte KI bis zu 15 Prozent der gesamten laufenden Kosten für den IT-Betrieb (IT-OPEX) ausmachen. Der Return on AI Investment wird dabei oftmals noch gar nicht firmenintern berechnet. Die Folge: Eine exakte Steuerung der IT-Kosten ist nicht möglich.

Umdenken im

IT-Management rechnet sich

Die Steuerung der IT-Performance in der Post-CAPEX-Ära bringt CFOs, CIOs und IT-Budgetverantwortliche in den Fach-Teams näher zusammen. Das ist eine wichtige Entwicklung, denn neben der Kostenkontrolle rücken ESG-Vorgaben in den Fokus. Ab 2030 wird GreenOps durch die CSRD-Richtlinie verpflichtend, und der Ansatz Total Cost of Ownership (TCO) entwickelt sich in Richtung „Total Cost of Ownership + ökologischer Fußabdruck (TCO + CO₂)“. Für Unternehmen wird damit das Übersetzen ihrer Aktivitäten und deren Auswirkungen in betriebswirtschaftliche Kennzahlen noch wichtiger.

www.soprasteria.com

**MEHR
WERT**

CIO Compass



www.noris.de

noris network

IHR PREMIUM IT-DIENSTLEISTER FÜR

maximale Sicherheit & Verfügbarkeit von Planung bis Betrieb

- Erfüllung aller regulatorischen Vorgaben & Compliance-Anforderungen
- Höchste Sicherheit durch ein mehrstufiges Sicherheitskonzept
- Colocation in zertifizierten Rechenzentren in Deutschland
- Souveräne Cloud „Made in Germany“
- Passgenaue IT-Services nach Ihren Anforderungen

Wie KI Verantwortung neu definiert

VOM TOOL ZUM AKTEUR

Künstliche Intelligenz (KI) verändert derzeit nahezu alle Bereiche der Wirtschaft und Gesellschaft – von der Automatisierung alltäglicher Aufgaben bis hin zu strategischen Entscheidungsprozessen. Unternehmen stehen vor der Herausforderung, Chancen und Risiken dieser Technologie gleichermaßen zu verstehen und verantwortungsvoll zu nutzen. Dabei geht es längst nicht mehr nur um Effizienz, sondern auch um Fragen der Transparenz, Ethik und Zukunftsfähigkeit.

Im Gespräch mit Ulrich Parthier verrät Lumir Boureanu, Geschäftsführer von compacer, was man gegen KI-Halluzinationen tun kann, warum KI nichts mit Wissen zu tun hat und weshalb es in Zukunft trotz aller Herausforderungen nicht mehr ohne KI gehen wird.

Ulrich Parthier: Immer öfter sieht man sich heute mit dem Einsatz von KI konfrontiert – sei es bei der Internetrecherche, der Nutzung von Softwarelösun-

gen oder Analyse-Tools. Wo sehen Sie derzeit den größten Nutzen von KI?

Lumir Boureanu: KI ist dort am wertvollsten, wo die menschlichen Kapazitäten an ihre Grenzen stoßen, beispielsweise bei der Mustererkennung. Hier kann KI Unsichtbares sichtbar machen. Oder bei extrem voluminösen Aufgabenstellungen, etwa wenn große Datenmengen oder Texte – z.B. komplexe Verträge – analysiert werden. Spürbar sind die positiven Effekte von KI aber auch bei repetitiven Tätigkeiten, beispielsweise der Erstellung von Protokollen oder dem Zusammenfassen bzw. Übersetzen von Texten.



KI IST KEINE STRATEGIE, SONDERN EINE FLANKIERENDE MASSNAHME.

Lumir Boureanu, Geschäftsführer, compacer GmbH, www.compacer.com

Kurz gesagt, der größte Nutzen von KI ist nicht, dass sie Dinge kann, die wir nicht können. Vielmehr schafft sie Freiraum für Dinge, die nur wir können: kreativ und empathisch sein, strategisch zu denken. Klar hilft uns KI bei der Erstellung von Prognosen und sie lernt auch dazu, aber KI ist kein Ersatz für das Wissensmanagement der Unternehmen. Das muss man unbedingt unterscheiden.

Ulrich Parthier: Das klingt alles gut. Dennoch gibt es Bedenken, was den Umgang mit KI betrifft.

Lumir Boureanu: Das stimmt. KI ist kein Selbstzweck, sondern ein Werkzeug für nachhaltigen Geschäftserfolg – aber



nur, wenn die Unternehmen jetzt die richtigen Weichen stellen. Man muss abwägen, welche Risiken man im Umgang mit KI eingehen kann und welche nicht. Auch die Datenvalidität spielt dabei eine wichtige Rolle. Für entscheidend halte ich aber, dass die Unternehmen bei Ihren KI-Projekten die Menschen mitnehmen müssen, insbesondere deshalb, weil eine zunehmende Change-Müdigkeit zu beobachten ist. Man muss die Ängste der Menschen ernst nehmen und darf nicht ignorieren, dass sich der ein oder andere von KI durchaus überfordert fühlt.

Ulrich Parthier: Und wenn KI auch noch zu halluzinieren beginnt und man sich nicht sicher ist, ob stimmt, was sie sagt – verstärkt das nicht noch die Ängste der Menschen?

Lumir Boureau: Klar, denn sind wir mal ehrlich: Agentic AI ist ein bisschen wie 'Stille Post'. Man gibt vorne etwas in das System rein und hinten kommt etwas raus. Was dazwischen passiert, ist nicht immer nachvollziehbar und das ist problematisch. Deshalb empfehle ich das 4-Augen-Prinzip: Die KI schlägt etwas vor und der Mensch validiert. Damit dieses Prinzip erfolgreich ist, sollte man KI in der Breite nutzen und sich auf den Menschen verlassen, wenn es in die Tiefe geht. Derartige Guidelines helfen, KI bestmöglich einzusetzen.

Ulrich Parthier: Erklären Sie uns bitte den Unterschied, zwischen einer KI, die arbeitet und entscheidet und dem Agieren eines Menschen.

Lumir Boureau: Ganz wichtig: KI verfügt nicht über 'Wissen' im menschlichen Sinne. Ein Beispiel: Wenn die KI sagt, dass Wasser bei 100 Grad kocht, dann hat KI diese Aussage millionenfach in Texten gesehen. Wenn der Mensch sagt, dass Wasser bei 100 Grad kocht, versteht er den physikalischen Zusammenhang. Also - KI versteht nicht, was sie sagt. Sie erkennt lediglich Muster, kann die statistisch wahrscheinlichste Antwort ermitteln, kann aber nicht beurteilen, ob

diese wahr oder falsch ist. Sehen Sie den Unterschied? Und weil die KI auf Informationen, sprich Daten, zurückgreift ist es so entscheidend, dass diese Daten valide sind, denn die KI ist nicht in der Lage ihre Fehlerhaftigkeit zu erkennen und korrigieren.

Ulrich Parthier: Das klingt ziemlich komplex. Haben wir als Menschen denn überhaupt eine Chance die von KI vorgeschlagenen Ergebnisse richtig einzuschätzen und zu bewerten?

Lumir Boureau: Wir haben nicht nur eine Chance. Wir haben sogar einen Vorteil, wenn wir die richtigen Tools und Methoden nutzen, denn wir besitzen Superkräfte. Wir können Kontexte verstehen. Wir haben ein Bauchgefühl. Wir haben ein ethisches Wertegerüst und wir sind kreativ. All das kann KI nicht, aber sie kann uns unterstützen. Wir müssen keine KI-Experten werden, aber KI-Kompetenz erlangen. Das ist wie beim Autofahren – da muss man auch kein Mechaniker sein, aber die Verkehrsregeln kennen und wissen, wie ein Auto zu steuern ist. Dieses Beispiel zeigt, dass Technologie immer dann am besten ist, wenn man sie nicht mehr wahrnimmt.

Ulrich Parthier: Und dann kommt noch das Thema Cybersicherheit dazu. Dabei sind die Herausforderungen, die KI mit sich bringt, groß genug.

Lumir Boureau: Cybersicherheit ist keine Nebensache, sondern integraler Bestandteil jeder KI-Strategie. Sie funktioniert wie eine Versicherung: Man braucht sie bevor man sie braucht. Gleichzeitig darf Sicherheit niemals der Grund sein, auf den Einsatz von KI zu verzichten. Entscheidend ist, klare Regeln und Leitplanken für den verantwortungsvollen, sicheren und effektiven KI-Einsatz festzulegen. Denn eines können wir schon heute beobachten: In 70 Prozent der Unternehmen existiert bereits heute eine Schatten-KI. Warum? Weil Menschen ChatGPT beruflich nutzen – mit oder ohne Erlaubnis von oben. Schon allein deshalb ist Eile

geboten. Die IT muss sich als Verbündete der Mitarbeiter sehen und KI fördern und nicht verhindern.

Ulrich Parthier: Noch eine letzte Frage: Wenn das Thema KI so komplex und dynamisch ist, worauf sollten Unternehmen denn besonders achten, wenn sie auf KI setzen?

Lumir Boureau: Wir von compacer haben einen breiten Erfahrungsschatz im Umgang und Einsatz von KI und verweisen bei der KI-Adaption auf die 70-10-20-Regel. Demnach hängen 70 Prozent des Erfolgs von der Vorbereitung – also der Datenqualität und den Prozessen – ab, 20 Prozent von der Technologieauswahl und 10 Prozent von der Implementierung. Und obwohl der Erfolgsschlüssel in der Vorbereitung liegt, fokussieren sich die meisten Unternehmen auf die Technologie. Mein Tipp: Bauen Sie KI-Champions auf, veröffentlichen Sie bei der Umsetzung eines KI-Projekts innerhalb der ersten 30 Tage Quick-Wins und investieren Sie dreimal so viel Geld in den Change-Prozess und Trainings wie in die KI-Technologie. Lassen Sie mich abschließend sagen, dass KI keine Strategie ist, sondern eine flankierende Maßnahme, dass KI-Kompetenz die Grundkompetenz der Zukunft ist und sich die Unternehmen auch mal mit einer 80-Prozent-Lösung zufriedengeben sollen, anstatt am Perfektionismus festzuhalten und den Anschluss zu verpassen. Mut ist gefragt und Pragmatismus, aber auch die Fähigkeit, KI als Unterstützung und nicht als Ersatz für den Menschen zu sehen.

Ulrich Parthier: Herr Boureau, vielen Dank für das Gespräch.

”
THANK
YOU

ENTERPRISE ARCHITECTURE MANAGEMENT

EIN PRAKTISCHER LEITFADEN
FÜR DIE EINFÜHRUNG VON EAM



Enterprise Architecture Management (EAM) muss die digitale Transformation enablen und gleichzeitig absichern. Unternehmensarchitekten müssen dafür sorgen, dass Unternehmen in der volatilen Welt auf Basis belastbarer Informationen entscheidungs- und handlungsfähig bleiben.

Enterprise Architecture Management (EAM) in einem Unternehmen einzuführen, ist eine komplexe Aufgabe. Entscheidend für den Erfolg sind ein klares Zielbild und

eine nutzenstiftende, machbare erste Einführungsstufe. Es gilt, zugeschnitten auf die Bedürfnisse der Stakeholder, diese bei ihrer täglichen Arbeit zu entlasten und ihnen zu helfen, die persönlichen Ziele zu erreichen.

Genau dabei unterstützt Sie dieser Praxisleitfaden. Er hat zwei Schwerpunkte: Einerseits vermittelt er eine ganzheitliche Sicht auf das Enterprise Architecture Management, seine Ziele und seinen Nutzen. Aus der Praxis abgeleitete Einsatzszenarien liefern Business- und IT-Verantwortlichen und IT-Strategen nachvollziehbare Argumente, um ihr Unternehmen von der Notwendigkeit von EAM zu überzeugen. Zudem erfahren Sie ganz konkret, wie Sie EAM Schritt für Schritt in Ihrem Unternehmen einführen.

Aus dem Inhalt:

- Einleitung
- Business Architecture 4 Digitalization
- EAM-Leitfaden für den CIO
- EAM Best Practices
- Zoom in die Best-Practice-Unternehmensstruktur
- Einsatzszenarien für EAM im operativen IT-Management, strategischen IT-Management und Business-IT-Alignment sowie zur Unterstützung der Weiterentwicklung des Geschäfts
- Schritt-für-Schritt-Anleitungen
- Glossar



Enterprise Architecture Management – einfach und effektiv: Ein praktischer Leitfaden für die Einführung von EAM;

Inge Hanschke,
Carl Hanser Verlag GmbH &
Co.KG; 02-2026



UNABHÄNGIGE IT-SYSTEME



Cloudbasierte Infrastrukturen, globale Technologieanbieter und komplexe Lieferketten haben den Handlungsspielraum vieler Organisationen in den vergangenen Jahren erheblich eingeschränkt. Wer kritische Prozesse heute digital betreibt, ist zwangsläufig auch abhängig – von Plattformen, Anbietern und Architekturen, die nicht immer unter eigener Kontrolle liegen.

Organisationen müssen ihre IT-Architektur also so gestalten, dass sie unabhängig, kontrollierbar und resilient sind – durch bewusste Architekturentscheidungen wie Modularität, offene Schnittstellen, Plattformunabhängigkeit und Transparenz über Abhängigkeiten. Denn digitale Souveränität entsteht nicht durch einzelne Maßnahmen, sondern als Ergebnis eines langfristigen, konsequent gesteuerten Entwicklungsprozesses.





Architekturentscheidungen, die Freiheit schaffen

WIE IT-SYSTEME UNABHÄNGIG, KONTROLLIERBAR UND RESILIENT WERDEN

Digitale Unabhängigkeit hat sich in den vergangenen Jahren von einer politischen Leitidee zu einem operativen Handlungsfeld für CISOs und IT- und Sicherheitsverantwortliche entwickelt. Spätestens seit der Aussage der heutigen BSI-Präsidentin Claudia Plattner,

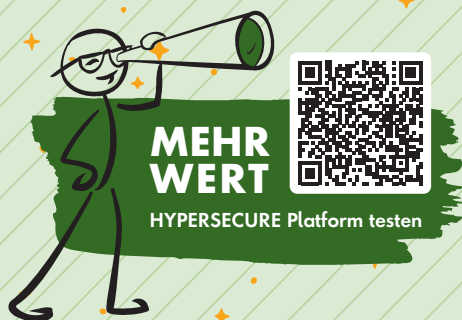
dass ohne digitale Souveränität auch keine europäische Souveränität möglich sei, wird deutlich, wie eng technologische Abhängigkeiten, Cyberresilienz und staatliche Stabilität miteinander verknüpft sind.

Die zunehmende Verlagerung geschäftskritischer Prozesse in cloudbasierte Infrastrukturen, die Abhängigkeit von globalen Technologiekonzernen und die Komplexität moderner Bedrohungslandschaften machen daher eine grundlegende Neuorientierung notwendig: Organisationen müssen technische Entscheidungsfreiheit zurückgewinnen, ohne dabei die Vorteile moderner digitaler Prozesse aufzugeben.

Technische Unabhängigkeit

Der zentrale Begriff, der diese Fähigkeit beschreibt, ist Resilienz. Sie meint die organisatorische, operative und technische Robustheit eines Systems – also die Fähigkeit, Störungen, Angriffe, Lieferkettenprobleme oder regulatorische Veränderungen auszuhalten, ohne in der Funktionsfähigkeit eingeschränkt zu werden. Resilienz beschreibt damit eine Form von Stabilität, die dynamische Entwicklungen nicht ausschließt, sondern bewusst einkalkuliert und darauf vorbereitet ist.

Resilienz entsteht dann, wenn Organisationen ihre Risiken kennen und auf realistischer Grundlage planen. Dazu gehört ein präzises Verständnis





- der technologischen Abhängigkeiten,
- die Fähigkeit, den Ausfall einzelner Komponenten zu kompensieren,
- und das Vorhandensein von Alternativszenarien, die im Ernstfall sofort aktiviert werden können.

Ein Plan B darf nicht nur existieren, er muss getestet, dokumentiert und technisch wie organisatorisch umsetzbar sein. Nur wenn Exit-Pfade geübt werden, lässt sich sicherstellen, dass Plattformwechsel, Notfallmigrationen oder der Austausch kritischer Komponenten nicht erst im Krisenfall improvisiert werden müssen.

In diesem Zusammenhang spielen Daten, Prozesse, Betriebsmodelle und Architekturen eine direkte, wechselseitige Rolle:

- Daten müssen eindeutig klassifiziert, kontrolliert und geschützt sein.
- Prozesse müssen so gestaltet sein, dass sie bei Störungen unkompliziert weitergeführt oder kurzfristig an neue Rahmenbedingungen angepasst werden können.
- Betriebsmodelle benötigen klare Verantwortlichkeiten sowie die Möglichkeit, Arbeitslasten zwischen On-Premises-Umgebungen, souveränen Cloud-Infrastrukturen und globalen Plattformen zu verschieben.
- Architekturen schließlich müssen so strukturiert sein, dass einzelne Komponenten austauschbar bleiben und keine irreversiblen Abhängigkeiten entstehen.

Gleichzeitig spielt die konsequente Kontrolle der eigenen Systeme eine wesentliche Rolle. Dazu gehört nicht nur, jegliche Art von Angriffen abzuwehren, sondern auch sicherzustellen, dass Zugriffswege und Datenflüsse nachvollziehbar bleiben und sich jederzeit an die Begebenheiten anpassen lassen.

Das Zusammenspiel dieser vier Elemente ermöglicht es Organisationen, flexibel zu reagieren, ohne Sicherheit oder Funktionsfähigkeit zu verlieren. Handlungsfähigkeit ergibt sich also aus dem Zusammenspiel von Vorbereitung, Transparenz, erprobten Alternativen und technischer Beherrschbarkeit der eigenen Infrastruktur.

Die Umsetzung unabhängiger IT-Systeme kann nicht mit einer einzelnen Maßnahme erreicht werden. Sie erfordert zwingend eine Reihe aufeinander abgestimmter Prinzipien und Designentscheidungen, die konsequent verfolgt werden müssen.



DIGITALE SOUVERÄNITÄT ENTSTEHT NICHT ÜBER NACHT. SIE IST DAS ERGEBNIS EINES LANGFRISTIGEN, KONSEQUENT GESTEUERTEN ENTWICKLUNGSPROZESSES.

Martin Mangold, Senior Vice President
Platform & Operations, DriveLock SE,
www.drivelock.com

Anders gesagt: Digitale Souveränität entsteht nicht über Nacht. Sie ist das Ergebnis eines langfristigen, konsequent gesteuerten Entwicklungsprozesses.

Im Folgenden geht es um die technischen Erfolgsfaktoren und die Frage, welche Architektur- und Entwicklungsprinzipien notwendig sind, um Unabhängigkeit in modernen IT-Landschaften langfristig zu verankern.

Technische Erfolgsfaktoren für unabhängige IT-Architekturen

Der Weg zu stabilen, kontrollierbaren IT-Infrastrukturen basiert auf einer Reihe technischer Grundprinzipien.

Im ersten Schritt ist vollständige Transparenz über die technologischen Abhängigkeiten erforderlich. Organisationen müssen verstehen, welche technologischen, operativen und architektonischen Abhängigkeiten bestehen und ob diese bewusst oder unbewusst eingegangen wurden.

Zweitens muss Unabhängigkeit als grundlegendes Architekturziel verankert werden. Ein solches Design trennt Daten- und Steuerungsebenen, minimiert proprietäre Abhängigkeiten und setzt auf modulare Komponenten. Containerisierte Anwendungen, standardisierte APIs und Zero-Trust-Prinzipien ermöglichen langfristige Anpassungsfähigkeit. Souveränität wird hier nicht als „add-on“ verstanden, sondern als integraler Teil von Architektur-, Technologie- und Designentscheidungen.

Drittens müssen alle technologischen Komponenten (Frameworks, Libraries, Cloud-Services) systematisch darauf geprüft werden, ob sie die Wechselfreiheit einschränken oder regulatorische Anforderungen gefährden. Komfortable Cloud-Native-Dienste erhöhen oft das Risiko eines Lock-In und müssen daher bewusst abgewogen werden.

Plattformunabhängigkeit ist ein weiterer zentraler Baustein. Software sollte sowohl On-Premises als auch in verschiedenen Cloud-Umgebungen nutzbar sein, ohne Funktionsverluste oder architektonische Brüche. Abstrahierte Infrastrukturebenen, containerisierte Workloads und standardisierte Deployment-Pipelines unterstützen das Ziel. DriveLocks Endpoint Security Lösungen sind beispielsweise sowohl On-Premises wie cloudbasiert verfügbar. Der Software-Stack wurde so weiterentwickelt, dass ein Betrieb in beiden Modellen möglich ist – ohne Funktions- oder Architekturbruch.



Eine Herausforderung ist die technische Dualität zwischen Windows-basierten On-Premises-Systemen und Kubernetes und damit Linux-basierten nativen Cloud-Architekturen. Für moderne Sicherheitslösungen wie DriveLock bedeutet das, dass Funktionen so entwickelt werden, dass sie in beiden Welten laufen, ohne die Codebasis zu verdoppeln. Dafür ist es notwendig Altcode umzuschreiben, bzw. bei Neuentwicklungen direkt zu berücksichtigen, um vollständige Wahlfreiheit zu gewährleisten.

Eine konsequente Entkopplung über APIs bildet die strukturelle Grundlage für flexible Architekturen. Klare Schnittstellen verhindern, dass Funktionen oder Daten in proprietären Systemen eingeschlossen werden und ermöglichen die modulare Weiterentwicklung der Gesamtarchitektur. Sie ermöglichen, dass Komponenten austauschbar bleiben und reduzieren Plattformabhängigkeiten.

Schließlich erfordern unabhängige IT-Systeme langfristige architektonische Entscheidungen. Investitionen in offene Standards, Portabilität und Modularisierung zahlen sich nicht kurzfristig, sondern über Jahre hinweg aus. Organisationen, die diesen Weg gehen, stärken ihre Anpassungsfähigkeit und vermeiden, dass sie in zukünftigen technologischen Umbrüchen feststecken.

Unabhängigkeit am konkreten Beispiel: Die DriveLock HYPERSECURE Platform

Die DriveLock HYPERSECURE Platform zeigt beispielhaft, wie Hersteller grundlegende Prinzipien der Unabhängigkeit in ihre Architektur integrieren können. Die Plattform ist so konzipiert, dass sie sich ohne Funktionsverlust in unterschiedlichen Betriebsmodellen einsetzen lässt. Kunden können entscheiden, ob sie die

Lösung On-Premises, in internationalen Cloud-Umgebungen oder in souveränen europäischen Infrastrukturen wie STACKIT betreiben möchten.

Die technische Architektur basiert auf modularen, containerisierten Komponenten, die unter Linux in der Cloud laufen, während Endpoint-seitige Funktionen nativ für Windows bereitgestellt werden. Diese Dualität ermöglicht einheitliche Sicherheitsmechanismen über alle Betriebspfade hinweg. Klare APIs stellen sicher, dass Richtlinien, Telemetriedaten und Logs unabhängig von der Infrastruktur konsistent verarbeitet werden.

Die Plattform ist damit ein exemplarisches Modell für moderne Security-Lösungen, die Kontrolle, Unabhängigkeit und Resilienz technisch unterstützen, ohne dass Anwenderinnen und Anwender sich auf ein bestimmtes Betriebsmodell festlegen müssen.



Darüber hinaus setzt DriveLock auf konsistente Policy-Modelle. Sicherheitsrichtlinien lassen sich unabhängig vom Infrastrukturtyp identisch anwenden, was sowohl Auditierbarkeit als auch regulatorische Konformität erleichtert. Gleichzeitig ermöglicht die modulare Architektur eine phasenweise Migration zwischen Betriebsmodellen – etwa bei regulatorischen Veränderungen, strategischen Neuausrichtungen oder Kostenüberlegungen.

DriveLocks HYPERSECURE Plattform verdeutlicht, wie technische Gestaltungs-

spielräume geschaffen werden können, ohne die Stabilität oder die Sicherheitsmechanismen zu beeinträchtigen.

Fazit

Technische Unabhängigkeit entsteht dort, wo Architekturprinzipien, Sicherheitsanforderungen und operative Prozesse konsequent zusammengedacht werden. Transparenz über Abhängigkeiten, offene Schnittstellen, plattformunabhängige Architekturen und langfristige Entwicklungsentscheidungen bilden die Grundlage für widerstandsfähige und kontrollierbare

IT-Systeme. Hersteller leisten einen entscheidenden Beitrag, indem sie Lösungen bereitstellen, die nicht durch Architektur oder Infrastruktur eingeschränkt werden.

Organisationen, die diesen Weg einschlagen, erhöhen ihre Widerstandsfähigkeit, verbessern ihre Reaktionsfähigkeit auf regulatorische Veränderungen und gewinnen Spielraum in der Gestaltung ihrer digitalen Zukunft.

Martin Mangold

DIE 4 SÄULEN DER RESILIENZ

Nur wenn alle vier Elemente aufeinander abgestimmt sind, können Organisationen flexibel reagieren, ohne Sicherheit oder Funktionsfähigkeit zu verlieren.



KI: Firmen stecken fest

ERFOLG BRAUCHT
GANZHEITLICHEN ANSATZ



Als der KI-Hype begann, dachten viele, jetzt würde sich schnell alles ändern. KI ist der bedeutendste Beschleuniger der Wirtschaftskraft von Organisationen. Unternehmensführungen drängen daher oft auf Vollgas bei der Einführung und Skalierung der neuen Technologie. Aber in der Praxis zeigt sich, dass eben das deutlich langsamer vorankommt als gedacht. Warum das so ist, welche strukturellen Hürden häufig unterschätzt werden und weshalb ein ganzheitlicher Ansatz für den Erfolg von KI entscheidend ist, erläutert Dr. Jan Schaumburg, Director of Solutions and Delivery DACH bei der Insight Technology Solutions GmbH.

it management: Herr Dr. Schaumburg, der aktuelle KI-Report von Insight zeigt, dass rund 80 Prozent der Unternehmen in Deutschland bei der KI-Einführung noch in den Phasen des Überlegens, des Experimentierens und der Pilotprojekte feststecken. Wie ordnen Sie dieses Ergebnis ein?

Dr. Jan Schaumburg: Die Zahlen bestätigen das Bild, das wir aus der Praxis kennen. Viele Unternehmen haben sich früh und mit großem Enthusiasmus mit KI beschäftigt, sind aber bislang nicht über die Anfangsphasen hinausgekommen. Nur

bei sieben Prozent der befragten Unternehmen ist KI bereits vollständig integriert. Das hängt damit zusammen, dass sich der Weg von der Idee zur produktiven Anwendung als deutlich anspruchsvoller erweist, als zu Beginn vielfach angenommen wurde.

it management: Inwiefern ist es anspruchsvoller?

Dr. Jan Schaumburg: KI ist kein Thema, das sich isoliert oder punktuell angehen lässt. Ihre Einführung wirft eine Vielzahl neuer Fragen auf, die weit über das eigentliche Projekt hinausgehen. Es geht um Themen wie Security und Compliance, um Cloud- und Infrastrukturentscheidungen, um Datenmanagement, Datenklassifizierung und Zugriffsrechte. Hinzu kommen Herausforderungen im Adoption and Change-Management, bei der Hardware, in der Softwareentwicklung sowie die Integration in bestehende, oft historisch gewachsene IT-Landschaften. Viele Unternehmen unterschätzen, auf wie viele unterschiedliche Bereiche der IT die Einführung von KI Einfluss hat und welche Komplexität das nach sich zieht, weil alles miteinander zusammenhängt. Punktuelle Optimierungen greifen hier zu kurz. Genau an diesem Punkt verlangsamt sich die Umsetzung spürbar.

it management: Ist die Frage nach Verantwortlichkeiten ebenfalls ein Hemmnis?

Dr. Jan Schaumburg: Ein entscheidender Punkt. Gerade weil KI die unterschiedlichsten Bereiche des Unternehmens betrifft, fehlt es oft an Klarheit in der Verantwortlichkeit. Wenn nicht eindeutig definiert ist, wer fachlich, technisch und organisatorisch Verantwortung übernimmt, bleibt KI ein Experiment. Erfolgreiche Unternehmen verankern KI klar in ihren Strukturen und verknüpfen sie eng mit den Zielen des Business. Nur so kann KI einen messbaren ROI generieren und tatsächlich als Wachstumsbeschleuniger fungieren.

it management: Komplexität und das Zusammenspiel von unterschiedlichen Verantwortlichkeiten – das klingt nicht nach Höchstgeschwindigkeit. Dabei erwarten doch viele Unternehmensführungen, dass KI schnell eingeführt wird.

Dr. Jan Schaumburg: Schnelligkeit und Nachhaltigkeit schließen sich nicht aus. Entscheidend ist, dass ein Unternehmen eine klare KI-Strategie hat, die sich konsequent an konkreten Business-Zielen ausrichtet. Ansätze wie Insight Rapid AI helfen dabei, in kurzer Zeit funktionierende

Use Cases zu identifizieren und anzugehen sowie Prototypen zu entwickeln, deren Nutzen sich realistisch bewerten lässt. So können Unternehmen schnelle Erfolge mit langfristiger Strategie kombinieren. Wichtig ist aber, dass diese Geschwindigkeit auf einer stabilen Basis aus Governance, Security und Datenqualität aufsetzt.

it management: Welche Defizite be-
gegnet Ihnen in Gesprächen mit Unternehmen besonders häufig bezüglich dieser Basis?

Dr. Jan Schaumburg: Ein zentrales Thema ist der Umgang mit Daten und den über die Zeit gewachsenen Landschaften. In vielen Gesprächen zeigt sich, dass Unternehmen keinen vollständigen Überblick darüber haben, wo ihre Daten liegen, wie sie strukturiert oder gelabelt sind und wer darauf zugreifen darf. Häufig ist zudem unklar, welche Daten sich überhaupt für KI-Anwendungen eignen. Dieses Defizit bleibt lange verborgen. Es wird aber spätestens dann offensichtlich, wenn KI aus der Experimentierphase heraus in den operativen Betrieb überführt und über viele Bereiche hinweg genutzt werden soll.

it management: Viele Unternehmen diskutieren in diesem Zusammenhang intensiv über Cloud- versus On-Premises-Ansätze. Wie bewerten Sie diese Debatte – insbesondere vor dem Hintergrund souveräner Cloud-Lösungen?

Dr. Jan Schaumburg: Die Debatte „Cloud vs. On-Premises“ greift zu kurz – moderne Architekturen sind fast immer hybrid. Unternehmen müssen je nach Workload entscheiden, wo Cloud-Vorteile wie Skalierbarkeit überwiegen und wo On-Premises aus Gründen wie Kontrolle, Compliance oder Latenz besser geeignet ist.

Mit KI steigen die Anforderungen an Datenhoheit und Regulierung weiter. Souveräne Cloud-Lösungen schaffen hier einen wichtigen Mittelweg: Sie ermöglichen Cloud-Innovation und KI-Nutzung, ohne die Kontrolle über sensible Daten

zu verlieren. Eine klare Architekturstrategie ist daher entscheidend, um Komplexität zu vermeiden.

it management: Die steigende Komplexität treibt den Aufwand deutlich nach oben. Können Unternehmen diese Herausforderungen intern bewältigen?

Dr. Jan Schaumburg: Das ist für viele Organisationen eine wichtige Abwägung. KI-Projekte erfordern Budget und Zeit. Interne IT-Teams sind häufig bereits stark ausgelastet. Zudem ist der Fachkräftemangel ein Problem. Unser KI-Report zeigt, dass fehlendes Know-how nach Integrationsfragen das zweitgrößte Hinder-



BEI KI STECKEN
VIELE UNTERNEHMEN
IN PILOTEN FEST.

Dr. Jan Schaumburg,
Director of Solutions and Delivery,
Insight Technology Solutions GmbH,
www.insight.de

nis für die Skalierung von KI ist. Gesucht werden Fachkräfte, die sowohl moderne KI-Technologien beherrschen als auch die bestehenden IT-Infrastruktur verstehen. Diese Kombination ist rar. Ohne externe Unterstützung stoßen viele Unternehmen daher an natürliche Grenzen.

it management: Also ist die Einbindung von Dienstleistern die Lösung?

Dr. Jan Schaumburg: Da KI viele Bereiche der IT tangiert, liegt der Gedanke nahe, dass Unternehmen verschiedene

Dienstleister einbinden müssen. Doch das hat einige Nachteile: Hoher Orchestrierungsaufwand, der Verlust von Synergieeffekten, die Gefahr von Silos, die den Aufbau einer einheitlichen KI-Strategie erheblich erschweren. Wir erkennen bei Unternehmen die Bestrebung, Dienstleister zu konsolidieren, um diese negativen Effekte zu umgehen und Kosten planbar zu halten. Dafür brauchen Unternehmen Dienstleister mit einem breiten Portfolio, die sich sowohl in KI als auch in den verschiedenen Bereichen der Infrastruktur gut auskennen, die das Unternehmen ganzheitlich kompetent beraten und auch ein strategischer Partner sein können. Das ist ein Grund, warum sich Unternehmen an Insight wenden.

it management: Zum Schluss, was raten Sie Unternehmen, die bislang noch in der Pilotphase verharren?

Dr. Jan Schaumburg: Den Blick zu weiten und KI nicht als isoliertes Projekt zu betrachten. KI entfaltet ihren Nutzen nur dann, wenn sie in die Unternehmensstrategie eingebettet und auf die Unternehmensziele ausgerichtet ist. Wer ganzheitlich denkt und die Wechselwirkungen zwischen Daten, Infrastruktur, Sicherheit und Organisation berücksichtigt, erhöht die Chance, aus ersten Experimenten nachhaltige Wertschöpfung zu entwickeln. Erfolgreich sind jene Unternehmen, die KI als integrierte Transformation verstehen und Technik, Prozesse, Governance und Organisation gemeinsam betrachten.

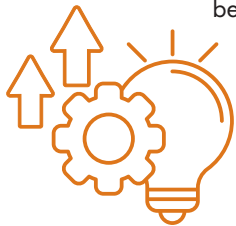
it management: Herr Dr. Schaumburg, vielen Dank für das Gespräch.

”
THANK
YOU

Steampunk & BPT Summit 2026

ANTWORTEN, STRATEGIEN, ROADMAPS

Wer hätte gedacht, dass ausgerechnet ein Begriff aus der Science-Fiction-Literatur die Überlebensstrategie der SAP-Welt definieren würde? Steampunk ist mehr als ein nostalgischer Codename für retro-futuristische Ästhetik; es ist der rettende Anker für die ABAP-Seele in der Cloud-Ära und damit von strategischer Brisanz. Für SAP-Bestandskunden bedeutet Steampunk (das ABAP-Environment) nichts Geringeres als die Lizenz zum Weiterleben ihrer Eigenentwicklungen, jedoch unter neuen, strengen Spielregeln. Es ist der diplomatische Kompromiss im radikalen Clean-Core-Diktat der Walldorfer.



Damit sind wir beim „Elefanten“ im Raum: der Business Technology Platform (SAP BTP). Sie ist nicht bloß eine weitere Middleware, sondern die unvermeidliche „Mautstation“ auf dem Weg zur Innovation. Der Mehrwert für den Bestandskunden liegt in der Entkopplung von Standard und Kür. Während der ERP-Kern zum langweiligen, aber stabilen System-of-Record degradiert wird, findet die Party – also KI, Mobile Apps und fancy Analytics – ausschließlich auf der BTP statt. Wer Innovationen wie den KI-Assistenten Joule will, muss diesen Weg gehen. Kritisch betrachtet entpuppt sich die BTP dabei oft als komplexe Kostenfalle mit undurchsichtigen Credit-Modellen. Doch sie ist das einzige Ticket, um die techni-



STEAMPUNK UND BTP SUMMIT 2026

Am 22. und 23. April findet in Heidelberg der Steampunk und BTP Summit 2026 statt. Dort gibt es alle Antworten, Strategien und Roadmaps zur SAP Business Technology Platform.

schen Schulden der Vergangenheit abzubauen, ohne die eigene Prozess-DNA zu verlieren. BTP ist der Mörtel, der die hybriden Risse zwischen der On-prem-Welt und der Cloud zusammenhält.

www.e3mag.com

SCRUM FÜR DIE NEUE ÄRA

EINE AGILE EVOLUTION

Die Wirtschaftswelt steht an einem Wendepunkt: Hybride Teams, KI-gestützte Entscheidungen, der rasante technologische Wandel und die gesellschaftlichen Herausforderungen brauchen neue Ansätze im agilen Arbeiten, um Unternehmen in die Lage zu versetzen, weiterhin Produkte an ihre Kunden zu liefern, die diese Kunden auch tatsächlich kaufen.

Mit dem vorliegenden Buch führt der Agile-Pionier Boris Gloger Scrum in diese neue Dimension. Er bietet Führungskräften, Agile Coaches und Praktikern eine umfassende Anleitung, wie Teams und Organisationen den Herausforderungen unserer Zeit begegnen können. Dazu verbindet dieses Buch klassische Scrum-Prinzipien mit den Erkenntnissen aus Lean Startup, Design Thinking, OKR und Kanban – die ihrerseits wiederum einer Modernisierung unterliegen. So ist gerade Design Thinking nicht mehr ohne KI-unterstützte Prototypen denkbar. U.a. müssen wir die Rolle der Generativen AI für den Produktentwicklungsprozess zunächst verstehen und ihren Platz als der neue Mitarbeiter in Teams erklären.

Scrum für die neue Ära
– Eine agile Evolution;
Boris Gloger; Carl Hanser
Verlag GmbH & Co. KG;
06-2026





SAP-Transformationen erfolgreich steuern

DER UNTERSCHÄTZTE
HEBEL VON PARTNERSCHAFTEN

Triple-Win für Natuvion, seine Partner und die Kunden: Erst die perfekte Symbiose aus Technologieanbieter, Migrationsexperten und Branchenkennern macht die Datentransformation zum Erfolg für Unternehmen.

SAP-Transformationen sind kein Solo – sie sind ein Team sport. Sie sind komplexe Vorhaben, die nur im Zusammenspiel unterschiedlicher Kompetenzen erfolgreich umgesetzt werden können. Genau hier setzt die Partnerstrategie und Zusammenarbeit von Natuvion mit seinen ausgewählten Partnern an. Als Spezialist mit tiefgehender Expertise in SAP-Datenmigrationen und mit der leistungsfähigen, standardisierten und KI-gestützten Migrationssoftware Natuvion Data Conversion Suite (DCS) schafft Natuvion die Grundlage für eine effiziente und wiederholbare Datentransformation. Die Partnerunternehmen profitieren von dieser Grundlage und komplettieren damit ihre eigene Beratungskompetenz, Branchenkenntnis und Projektsteuerung. Erst diese Symbiose trägt maßgeblich dazu bei, dass Transformationsprojekte bei Unternehmen erfolgreich und im geplanten Zeit- und Budgetrahmen verlaufen können.

Arbeiten auf Augenhöhe

Der ausschlaggebende Faktor der Kooperation von Natuvion und seinen Partnern ist die klare Aufgabenteilung bei gleichzeitigem Arbeiten auf Augenhöhe. Während Natuvion die technologische Basis, bewährte Methoden und beratende Unterstützung bereitstellt, setzen die Partner Projekte eigenständig um und übernehmen Verantwortung. Durch standardisier-

te Prozesse, Automatisierung und integrierte Qualitätsprüfungen ist es möglich, selbst komplexe Migrationen strukturiert, transparent und mit hoher Datenqualität durchzuführen. Das beschleunigt Projekte spürbar und reduziert Risiken für die gemeinsamen Kunden deutlich – völlig unabhängig davon, ob eine Datentransformation mit der Greenfield-, Brownfield- oder der meist sinnvollen Selective-Data-Transition-Methode umgesetzt wird.

Für Kunden entsteht daraus ein klarer Mehrwert: Sie profitieren von gebündelter Technologie- und Beratungsexpertise, klar definierten Vorgehensmodellen und einer hohen Umsetzungsgeschwindigkeit. Projekte werden planbarer, Ergebnisse messbarer und die Akzeptanz bei den Anwendern steigt durch hohe Datenqualität und saubere Systemübergänge. Gleichzeitig sinken Kosten und Aufwände, da wiederholbare Standards und erprobte

Werkzeuge eingesetzt werden – dieser Aspekt ist vor dem Hintergrund, dass Datentransformationen künftig durch schnellere Technologiewechsel viel häufiger oder sogar kontinuierlich stattfinden werden, besonders wichtig.

Partnerschaft und Plattform als Erfolgsfaktor

Auch strategisch bietet die partnerschaftliche Zusammenarbeit Vorteile. Die Migrationsplattform Natuvion DCS kommt nicht nur für einzelne Projekte in dedizierten Branchen zum Einsatz. Sie lässt sich für unterschiedliche Marktsegmente skalieren und weiterentwickeln, was die Plattform jeden Tag wertvoller macht. Die standardisierte Vorgehensweise der DCS-Plattform bietet Natuvion und seinen Partnern die Erschließung neuer Marktsegmente bei hoher oder sogar steigender Qualität und Geschwindigkeit – wie es beispielsweise in den Marktsegmenten Utilities oder Automotive seit vielen Jahren praktisch umgesetzt wird.

Partnerschaften auf Augenhöhe mit dem Fokus auf das bestmögliche Ergebnis sowie die Kombination aus technologischem Fokus und praxisnaher Beratung ermöglichen die Realisierung einer digitalen Datentransformation ohne unnötige Komplexität für die Kunden. Gemeinsame Werte, klare Strukturen und nachweisbare Projekterfolge zeigen, dass sowohl Partnerunternehmen als auch Kunden nachhaltig profitieren.

Philipp von der Brüggen



SAP-TRANSFORMATIONEN
SIND KEIN SOLO –
SIE SIND EIN TEAMSPORT.

Philipp von der Brüggen, CMO, NATUVION,
<https://www.natuvion.com/de/>



Natuvion

S/4HANA strategisch nutzen

DREI HEBEL FÜR EINE ERFOLGREICHE SAP-TRANSFORMATION

Die Transformation zu SAP S/4HANA gehört zu den größten Herausforderungen für Unternehmen, die zukunftsfähig werden wollen. Häufig wird das Projekt jedoch nur als technologische Migration wahrgenommen. Dabei bietet SAP S/4HANA weit mehr: Mit einem klaren Fokus auf Führung, effizienten Prozessen sowie Plattformdenken und KI können Unternehmen echten Mehrwert schaffen und sich strategisch neu positionieren. Wir zeigen Ihnen im Folgenden, wie Sie über drei zentrale Hebel wichtige Innovations Sprünge machen können:

#1 Führung und Change entscheiden – nicht das System

Die erste Voraussetzung für eine erfolgreiche SAP S/4HANA-Transformation liegt in der klaren Projektsteuerung und einem konsequenten Change Management. Technologie allein führt nicht zu bahnbrechenden Innovationen – entscheidend ist stattdessen, dass Führungspersonen im Unternehmen sichtbar Verantwortung übernehmen und Klarheit

schaffen. Alle beteiligten Personen sollten von Anfang an mitgenommen werden.

Klare Projektsteuerung sorgt für Orientierung und vermeidet Endlosschleifen bei einzelnen Prozessen. Sie ermöglicht es, schnelle Entscheidungen zu treffen, Verantwortlichkeiten klar zu definieren und eine transparente Kommunikation im Projektteam zu etablieren. Gerade bei komplexen Transformationsprozessen wie der Migration zu SAP S/4HANA ist Governance kein Bremsklotz, sondern ein Innovationsbeschleuniger, der durch Struktur und Effizienz den Weg für zentrale Neuerungen ebnet.

Ein ebenso wichtiger Erfolgsfaktor ist Change Management. Die Transformation ist nicht nur ein technischer, sondern vor allem ein kultureller Wandel, der das Verhalten und die Arbeitsweise der Mitarbeitenden grundlegend verändert. Ohne deren grundlegende Akzeptanz bleibt Innovation bloße Theorie. Unternehmen müssen Veränderung aktiv gestalten – durch Kommunikation, Befähigung und die Einbindung von Stakeholdern. Nur so lassen sich eventuell vorhandene Widerstände abbauen und ein gemeinsames Verständnis für die Transformation schaffen.

#2 Effizienz entsteht durch Standardisierung – Agilität ist das Ergebnis

Die zweite Voraussetzung für den Erfolg einer Transformation zu SAP S/4HANA ist, ineffiziente Prozesse nicht einfach digital zu übertragen, sondern konsequent End-to-End zu denken und zu standardisieren. Wer alte Prozesse mit neuer Technologie kombiniert, skaliert Ineffizienz. Ein Clean Core bildet die Grundlage für Agilität, Geschwindigkeit und langfristige Innovationsfähigkeit über Upgrades.

Effiziente Prozesse sind die Basis für Skalierung und Wachstum. Unternehmen sollten ihre Geschäftsprozesse daher harmonisieren und optimieren, um Zeitverluste und unnötige Komplexität zu vermeiden. Dabei gilt: Prozessorientierung vor Systemdenken. Tools wie SAP Signavio helfen, Prozesse zu analysieren und Optimierungen gezielt umzusetzen.

Standardisierung und Clean Core sind essenziell, um Unternehmen agil und innovationsfähig zu machen. Individualisierte Lösungen mögen kurzfristig Vorteile bieten, führen aber langfristig zu einem



DIE SAP S/4HANA-TRANSFORMATION IST MEHR ALS EIN TECHNOLOGIEWECHSEL.

Rüdiger Hoffmann, Managing Director,
valantic GmbH, www.valantic.com



hohen Pflegeaufwand und einer eingeschränkten Skalierbarkeit. Der Clean Core-Ansatz reduziert die Komplexität, vereinfacht Updates und schafft Freiraum für die Entwicklung neuer Geschäftsmöglichkeiten. Standardisierung ist in diesem Sinne kein Rückschritt, sondern ein strategischer Hebel für Geschwindigkeit und Flexibilität.

#3 Innovation entsteht durch Plattformdenken und KI

Der dritte zentrale Hebel für eine erfolgreiche SAP S/4HANA-Transformation ist die intelligente Integration von Daten, Systemen und Prozessen sowie der Einsatz von Künstlicher Intelligenz. Unternehmen sollten SAP als ganzheitliche Plattform denken, die Innovationen ermöglicht, statt als monolithisches ERP-System, das nur Prozesse abbildet.

Die zentrale Integration fungiert dabei als Basis für die weitere Skalierung und Flexibilität. Nur wenn Systeme, Daten und Prozesse zusammenarbeiten, entsteht ein Umfeld, das Innovation fördert. Die SAP Business Technology Platform (BTP) bietet hier eine leistungsfähige Grundlage, um branchenspezifische Erweiterungen und neue Anwendungen zu entwickeln. Entkopplung statt Monolith – das sollte die Devise sein, um Innovationen schnell und kosteneffizient umzusetzen.

KI und Generative AI leisten zudem einen entscheidenden Beitrag zur Produktivität und Qualität. Sie übernehmen nicht nur Aufgaben, sondern automatisieren Entscheidungen. Damit schaffen sie einen echten Mehrwert – zum Beispiel, indem sie komplexe Analysen in Echtzeit ermöglichen oder intelligente Empfehlungen für

Geschäftsprozesse liefern. Daten, Prozesse und KI wirken zusammen, um Effizienz zu steigern und Innovation zu fördern. Im Endeffekt entsteht ein messbarer und grundlegender Fortschritt für das Unternehmen.

Fazit: SAP als Innovationsplattform verstehen

Die SAP S/4HANA-Transformation ist weit mehr als ein technischer Systemwechsel. Unternehmen, die klare Führung und Change Management etablieren, ihre Prozesse standardisieren und auf ein Clean Core setzen sowie Plattformdenken und KI nutzen, können ihre Transformation in eine strategische Innovationsplattform verwandeln. Entscheidend ist, die Migration nicht isoliert als IT-Projekt zu betrachten, sondern als Chance für nachhaltige Innovation und echten Mehrwert im gesamten Unternehmen. Im Zentrum steht eine businessgetriebene, zukunftsorientierte, wirkungsvolle Transformation.

Rüdiger Hoffmann

**MEHR
WERT**



Whitepaper: Erfolgsfaktoren für die SAP S/4HANA Transformation

SAP S/4 HANA ALS WERTTREIBER FÜR DAS GESAMTE BUSINESS

PROZESSE

-  Zukunftsfähige Prozesse
-  Einheitliches Steuerungsmodell
-  Einheitliche Data-Governance-Strukturen
-  Integrierte und übergreifende Planungsprozesse

SYSTEM

-  Digitale Innovationsplattform mit modernem User Interface
-  Leistungsfähige Performance in Echtzeit
-  Bessere Wartbarkeit, geringerer Support-Aufwand
-  Flexible Deployment-Optionen und Anbindung von Cloud-Services

ORGANISATION

-  Globales E2E-Prozess-Know-how
-  Motivierte Mitarbeitende
-  Möglichkeit, neue Rollen aufzubauen
-  Attraktivität am Arbeitsmarkt

Einheitliches, zukunftsfähiges System mit effektiven, gruppenweiten Best-Practice-Prozessen als Grundlage, um bisher unerreichbare Effizienzgewinne durch Künstliche Intelligenz, Automatisierung & Data Intelligence zu heben



SAP Joule vs. andere KI-Systeme

WAS DEN SAP-ASSISTENTEN
WIRKLICH UNTERSCHIEDET

Die SAP-Welt steht vor einem fundamentalen Wandel durch Künstliche Intelligenz. Doch was unterscheidet SAP Joule eigentlich von anderen KI-Systemen auf dem Markt? Könnten Unternehmen nicht einfach modifizierte Versionen von ChatGPT, DeepSeek oder Claude.ai verwenden? Die Antwort liegt in der tiefen Integration und spezifischen Ausrichtung von Joule auf Geschäftsprozesse.

Die einzigartige Positionierung von SAP Joule

Im Gegensatz zu generischen KI-Modellen ist Joule speziell für die SAP-Umgebung konzipiert. Während ChatGPT und ähnliche Systeme als allgemeine Sprachmodelle (Large Language Models/LLMs) entwickelt wurden, ist Joule von Grund auf für Unternehmensprozesse und SAP-spezifische Datenstrukturen ausgelegt.

Joule ist bereits seit September 2024 im Einsatz und hat seine Funktionen erheblich erweitert. Das System unterstützt nun Geschäftsprozesse in Customer Experience, Beschaffung und Personalwesen deutlich umfassender als bei der ursprünglichen Einführung.

Der entscheidende Unterschied

Joule versteht nicht nur natürliche Sprache, sondern auch die Semantik von Geschäftsprozessen. Ein Befehl wie „Erkennung von Zahlungsverzug bei unseren Top-10-Kunden“ erfordert ein tiefes Verständnis von Forderungsmanagement, Payment-Terms und Kundensegmentierung.

Joule Agents fungieren als AI-Agenten, die Geschäftsanwender mit Entscheidungsunterstützung und Aufgabenautomatisierung in nicht-deterministischen Workflows unterstützen. Diese Agents wählen aus einem großen Set von Tools und können auf Ergebnisse reflektieren und weiter argumentieren.

Ein wichtiger Aspekt, der die strategische Ausrichtung verdeutlicht, ist die für Q3 2025 geplante SAP AI Foundation. Dieses AI-Betriebssystem soll als zentrale Plattform für alle SAP Business AI-Lösungen dienen und Entwicklern einen einheitlichen Einstiegspunkt für AI-Tools bieten.

Technologische Wurzeln und Entwicklung

SAPs KI-Strategie ist vielschichtig und geht über Joule hinaus. Tatsächlich hat das Unternehmen im Juli 2023 erhebliche Investitionen in KI-Startups getätigt:

- **Aleph Alpha:** Europäischer Anbieter mit Fokus auf unternehmenskritische AI-Lösungen und Datensouveränität
- **Anthropic:** US-basiert mit Schwerpunkt auf sicherer und kontrollierter KI-Entwicklung

- **Cohere:** Spezialisiert auf Unternehmens-KI mit Fokus auf Datenschutz und Compliance

Diese Investitionen ergänzen SAPs über 1 Milliarde US-Dollar Commitment von Sapphire Ventures für AI-gestützte Enterprise-Technologie-Startups. Joule selbst basiert jedoch primär auf SAPs eigener Technologieentwicklung, die durch diese strategischen Investitionen und ein offenes Ökosystem-Konzept ergänzt wird.

Ein praktischer Aspekt, der die tiefe Integration verdeutlicht: Joule wird bereits in SAP Build-Produkte integriert, darunter:

- **SAP Build Process Automation**
- **SAP Build Apps**
- **SAP Build Code**
- **ABAP Cloud**

Diese Integration ermöglicht es Entwicklern aller Kenntnisstufen, effizienter zu arbeiten und AI-gestützte Funktionen direkt in ihre Entwicklungsprozesse zu integrieren.

Der wahre Wettbewerbsvorteil von Joule liegt in der tiefen Integration in das SAP-Ökosystem. Während externe KI-Lösungen über APIs angebunden werden müssen, ist Joule native Bestandteil von:

- **SAP S/4HANA Cloud (Public Edition seit Januar 2025)**
- **SAP SuccessFactors**
- **SAP Ariba**
- **SAP Customer Experience**



Seit Januar 2025 ist Joule auch in SAP S/4HANA Cloud Public Edition und Supply Chain Management-Anwendungen verfügbar, was die Reichweite erheblich erweitert.

Datenschutz und Compliance

Für Unternehmen, besonders in regulierten Branchen oder in Europa, spielen Datenschutz und Compliance eine wichtige Rolle. Während bei US-basierten Lösungen wie ChatGPT datenschutzrechtliche Bedenken bestehen, bietet Joule die Garantie, dass Unternehmensdaten innerhalb des SAP-Ökosystems verbleiben.

Multi-Vendor KI-Agenten im Composable Enterprise

Die Diskussion um SAP Joule und KI-Compliance wird durch einen weiteren strategischen Aspekt komplexer: das aufkommende Composable Enterprise mit Multi-Vendor KI-Agenten. Während das Konzept des modularen, zusammensetzbaren Unternehmens jahrzehntelang theoretisch diskutiert wurde, könnte der massenhafte Einsatz von KI-Agenten nun den praktischen Durchbruch ermöglichen - ähnlich wie Grafikkarten-Power den Durchbruch für neuronale Netze brachte.

In einer Multi-Vendor-KI-Landschaft entstehen kritische Fragen der System-Governance: Darf ein Salesforce-Einstein-Agent ERP-Funktionen übernehmen, oder muss dieser Bereich dem SAP Joule-Agenten vorbehalten bleiben? Diese klassische „System of Record“-Problematik wird durch autonome KI-Agenten exponentiell komplexer.

KI-Agenten-Compliance als neue Disziplin

Während einzelne KI-Systeme wie Joule bereits Enterprise-Compliance erfüllen, wird die Orchestrierung konkurrierender KI-Agenten verschiedener Anbieter zu einer neuen Herausforderung. ERP-Systeme basieren auf Konsistenz und Nachvollziehbarkeit - sich widersprechende KI-Agenten in einem Composable ERP wären ein operativer Super-GAU.



SAP JOULE IST KEIN ISOLIERTES KI-PRODUKT, SONDERN DIE INTELLIGENTE SCHNITTSTELLE ZUM GESAMTEN SAP-ÖKOSYSTEM.

Ulrich Parthier,
Publisher, it management,
www.it-daily.net

Hier positioniert sich SAP Joule strategisch clever: Durch die geplante AI Foundation als orchestrierende Plattform könnte SAP die Rolle des „KI-Dirigenten“ in Multi-Vendor-Umgebungen übernehmen und dabei Compliance und Konsistenz sicherstellen.

Die Lizenzierungs-Revolution

Eine der disruptivsten Auswirkungen von SAP Joule und anderen KI-Agenten betrifft das traditionelle SAP-Lizenzierungsmodell. Bisher basierte die SAP-Lizenzierung primär auf Named Usern - das bedeutet jeder Mitarbeiter, der auf SAP-Systeme zugreift, benötigt eine entsprechende Lizenz.

Wenn jedoch zwei Joule Agents die Arbeit von 20 lizenzierten Mitarbeitern übernehmen - von der Datenerfassung über Workflows bis hin zu Entscheidungsprozessen - bricht die bisherige Lizenzlogik zusammen. Die Frage wird existenziell: Wie lizenziert man KI-Agenten, die autonom agieren und menschliche Tätigkeiten ersetzen?

SAP wird voraussichtlich auf folgende Ansätze setzen:

- #1 Transaktionsbasierte Lizenzierung:** Abrechnung nach verarbeiteten Geschäftsprozessen oder Dokumenten
- #2 Kapazitätsmodelle:** Lizenzierung basierend auf KI-Computing-Power oder gleichzeitigen Agent-Instanzen
- #3 Outcome-basierte Modelle:** Bezahlung nach erreichter Automatisierungsleistung oder Kosteneinsparung
- #4 Hybride Modelle:** Kombination aus traditionellen User-Lizenzen und KI-Agent-Kapazitäten

Für SAP-Kunden bedeutet dies eine fundamentale Neubetrachtung ihrer Lizenzstrategie. Während heute 1.000 Named User 1.000 Lizenzen erfordern, könnte morgen ein Szenario entstehen, in dem 100 KI-Agenten die Arbeit von 2.000 Menschen übernehmen - aber wie wird das abgerechnet?



SAP hat hier die Chance, durch faire und transparente KI-Lizenzmodelle einen Wettbewerbsvorteil zu erzielen. Während andere Anbieter noch experimentieren, könnte SAP mit durchdachten „AI-Workforce“-Lizenzen punkten, die den tatsächlichen Business Value widerspiegeln.

Im Zweifelsfall, so die Erfahrung, wird die SAP das für sie umsatzträchtigste Lizenzierungsmodell wählen. Der nächste Ärger mit den Anwendern ist also quasi per se schon vorprogrammiert.

Offenes Ökosystem statt Isolation
Die Realität wird wahrscheinlich ein offenes Ökosystem verschiedener KI-Systeme sein. SAPs Investitionsstrategie zeigt, dass das Unternehmen auf das „Beste aus verschiedenen Welten“ setzt:

- **Joule für kerngeschäftliche Prozesse**
- **Strategische Partner-AIs für spezialisierte Funktionen**
- **SAP AI Foundation als orchestrierende Plattform**
- **Hybride Architektur für maximale Flexibilität**

Fazit
SAP Joule ist kein isoliertes KI-Produkt, sondern die intelligente Schnittstelle zum gesamten SAP-Ökosystem. Mit der Einführung von Joule Agents, der geplanten AI Foundation und der kontinuierlichen Erweiterung der Integrationen positioniert sich SAP strategisch für die nächste Generation von Business AI.

Die strategischen Investitionen in führende KI-Anbieter und das offene Ökosystem-Konzept zeigen, dass SAP nicht auf eine einzige Technologie setzt, sondern die beste verfügbare AI-Technologie in sein Portfolio einbettet.

Ulrich Parthier



WARUM NICHT EINFACH CHATGPT ODER ANDERE LLMS ODER SMLS?

Aspekt	SAP Joule	Generische LLMs (ChatGPT, etc.)
Datenintegration	Tiefe Integration in SAP-Systemlandschaft	Externe Anbindung erforderlich
Prozessverständnis	Native Understanding von Geschäftsprozessen	Allgemeines Sprachverständnis
Sicherheit & Compliance	Enterprise-grade Security im SAP-Kontext	Zusätzliche Sicherheitsschichten nötig
Customization	Vorkonfiguriert für SAP-Umgebungen	Anpassung für spezifische Use Cases nötig
Datenhoheit	Daten verbleiben im SAP-Ökosystem	Abhängig vom Anbieter
Workflow-Automatisierung	Joule Agents für komplexe Business-Workflows	Manuelle Integration erforderlich
Multi-System-Kontext	Systemübergreifendes Verständnis	Isolierte Betrachtung einzelner Systeme

KI-KOMPETENZEN AUFBAUEN IM UNTERNEHMEN

PRAXISNAHE STRATEGIEN FÜR ENTSCHEIDER

Künstliche Intelligenz ist kein Zukunftsthema mehr. Sie verändert bereits heute Märkte, Arbeitsweisen und Wettbewerbsbedingungen – auch im Mittelstand. Gleichzeitig herrscht große Unsicherheit: Was ist wirklich relevant? Was ist übertrieben? Und wo beginnt man, Fehlentscheidungen zu treffen oder Ressourcen zu binden, ohne Wirkung zu erzielen?

Dieses Buch setzt genau hier an. Es richtet sich an Unternehmen, die sich bislang noch nicht systematisch mit KI beschäftigt haben, aber erkennen, dass Handlungsbedarf besteht. Im Mittelpunkt steht nicht die Technologie, sondern die Frage nach konkreter Wertschöpfung: Wo kann KI sinnvoll entlasten, Prozesse verbessern oder Entscheidungen unterstützen – und wie lässt sich dieser Nutzen realistisch bewerten?

Use Cases und messbare Ergebnisse nutzen

Anhand eines strukturierten Readiness-Checks wird zunächst der eigene Status realistisch eingeordnet. Darauf aufbauend beleuchten die Autoren typische Fehlannahmen, notwendige Voraussetzungen und bewährte Vorgehensweisen aus der Praxis. Konkrete Use Cases, Quick Wins und messbare Ergebnisse machen den KI-Nutzen greifbar. Dabei wird klar aufgezeigt, was heute sinnvoll umsetzbar ist – und wo Erwartungen korrigiert werden sollten. Mit diesem Buch erhalten Sie einen praxisnahen Leitfaden für Unternehmen, die KI fundiert, verantwortungsvoll und wirksam einsetzen wollen.



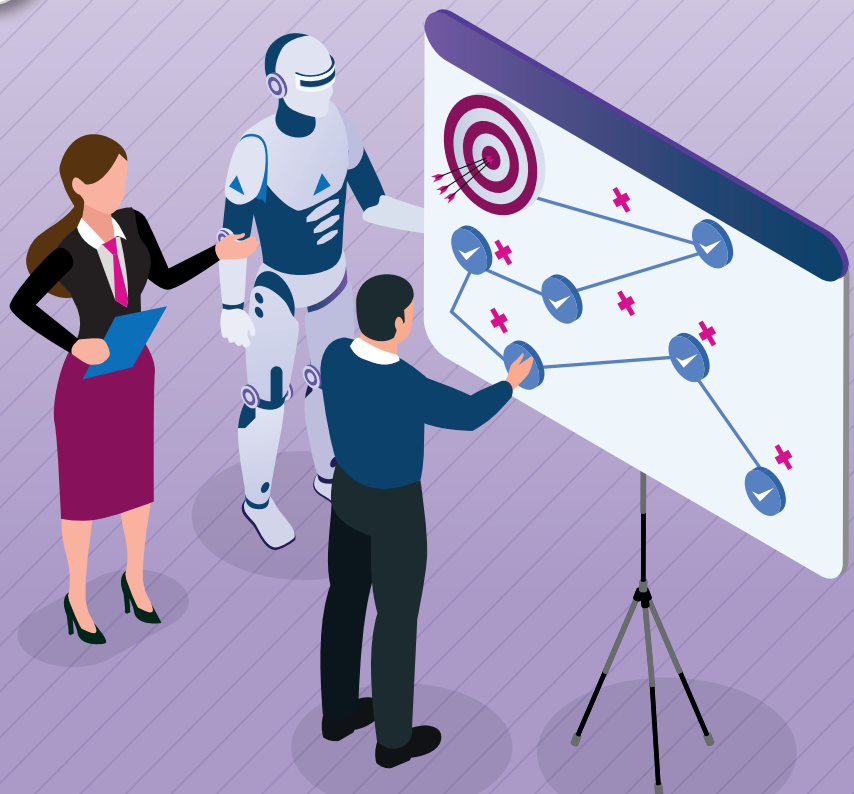
KI-Kompetenzen aufbauen im Unternehmen

– Praxisnahe Strategien für Entscheider; Fabienne Tressin, Omar Langer; mitp Verlags GmbH & Co. KG; 06-2026



Aus dem Inhalt:

- Was Künstliche Intelligenz ist – und warum sie für KMUs relevant ist
- Exponentielles KI-Wachstum und seine Auswirkungen auf den Mittelstand
- Readiness-Check: Reifegrad bestimmen und Handlungsfelder erkennen
- Typische KI-Fehlannahmen im Mittelstand und ihre Folgen
- Technische, organisatorische und kulturelle Voraussetzungen
- Die vier Säulen einer nachhaltigen KI-Transformation
- Kompetenzaufbau für Mitarbeitende und Führungskräfte
- Quick Wins und Pilotprojekte mit realistischem Aufwand
- Messbarkeit, Kennzahlen und Bewertung von KI-Nutzen



SAP-Lizenzen: Vom Technikthema zum CFO-Tool

DIE LIZENZSTRATEGIE
GEHÖRT 2026 AUF DIE CFO-AGENDA

Viele Unternehmen sehen SAP-Lizenzmanagement als operative Pflicht: Berechtigungen prüfen, Audits begleiten, Compliance sichern. Doch dieser Blickwinkel greift zu kurz. Lizenzen sind längst kein technisches Detail mehr, sondern entscheiden über Kosten, Flexibilität und strategische Handlungsfreiheit der IT. Wer hier nicht vorausschauend plant, riskiert Investitions- und Innovationsverluste.

Gerade bei Migrationsprojekten gerät das Lizenzmanagement oft sogar ganz aus dem Blick: „Damit beschäftigen wir uns dann später. Jetzt kümmern wir uns um die Technologie.“ Warum dieser An-

satz gefährlich ist und das strategische Lizenzmanagement trotz der vermeintlichen Transparenz in der Cloud auf die CFO-Agenda gehört, soll Thema dieses Beitrags sein.

Warum „SAP-Lizenzstrategie“ statt klassischem Lizenzmanagement?

Traditionelles Lizenzmanagement konzentriert sich auf operative Aufgaben wie Berechtigungsprüfungen und Audit-Begleitung. Doch in einer Welt, in der SAP-Lizenzen über Jahre hinweg immer höhere Anteile der gesamten IT-Kosten binden und die digitale Transformation maßgeblich beeinflussen, reicht das nicht mehr aus. Unternehmen, die Lizenzen als strategisches Steuerungsinstrument begreifen, vergleichbar mit Investitionen in Technologie oder Personal, gewinnen einen deutlichen Wettbewerbsvorteil. Eine klare Lizenzstrategie bietet Planungssicherheit, verhindert Kostenfallen und schafft Flexibilität für zukünftige Geschäftsmodelle. Genau deshalb gehört das Thema auf die C-Level-Agenda: Wer heute nicht strategisch handelt, riskiert morgen eingeschränkte Handlungsfreiheit und unnötige Mehrkosten. Lizenzentscheidungen und geschickt verhandelte Vertragswerke sind keine IT-Details mehr, sondern ein Hebel für die langfristige Wettbewerbsfähigkeit.

SAP zwischen On-Premises und Cloud

Noch setzen viele Mittelständler auf SAP On-Prem. Doch Nachlizenzierungen im On-Premises-Umfeld werden heute immer

teurer. Rabatte? Kaum noch. Wer unterlizenziert ist oder wachsen möchte, zahlt deutlich mehr als früher. Das macht On-Premises häufig wirtschaftlich unattraktiv. Der Wechsel in die Cloud wirkt wie die Lösung: Mieten statt kaufen und bessere Planbarkeit genießen. Doch Vorsicht: Neue Verträge bringen Mindestlaufzeiten und -abnahmemengen sowie mehrjährige Commitments. Wer hier blind unterschreibt, bindet sich langfristig und oft zu Konditionen, die nicht zur Geschäftsstrategie passen. Man profitiert wenig bis gar nicht von der möglichen Flexibilität in der Cloud. Besonders kritisch kann es dabei werden, wenn während der Migration alte und neue Lizenzkosten parallel laufen.

Ein weiteres Paradoxon der Cloud-Welt: Zwar sind Nutzungsdaten jederzeit abrufbar, sie basieren jedoch stets auf den aktuellen SAP-Nutzungsbedingungen. Für den Kunden relevant ist jedoch die Version, die zum Zeitpunkt des Vertragsabschlusses galt. Da sich Nutzungs-



WER LIZENZEN NUR
VERWALTET, STATT
SIE STRATEGISCH ZU
STEUERN, VERSCHENKT
POTENTIAL FÜR DIE
ZUKUNFT.

Svenja Vorwerk,
Lizenzstrategieberatung,
akquinet GmbH, www.akquinet.com



bedingungen teilweise wöchentlich ändern, können angezeigte Unter- oder Überlizenzierungen trügerisch sein – und müssen immer verifiziert werden.

Eine passgenaue Steuerung der Lizenzen und vorausschauende Verhandlungen mit SAP ermöglichen es, das Maximum aus einer Cloudtransformation rauszuholen. Bevor sich Unternehmen auf drei-, fünf- oder sogar siebenjährige Commitments einlassen, sollten sie sich daher klar darüber sein, wie ihre IT- und Geschäftsstrategie in genau diesem Zeitraum aussehen soll. Spätere Lizenz-Korrekturen sind auch in der Cloud teilweise teuer oder gar nicht mehr möglich.

Die neue SAP Business Suite

Die neue SAP Business Suite bringt mit Produkten wie BTP, Business Data Cloud und KI-Agenten nicht nur technologische Innovation, sondern auch eine völlig neue vertragliche Komplexität ins Unternehmen. Neben der Auswahl des richtigen Betriebsmodells für SAP ERP (von

On-Premises, Private oder Public Cloud bis hin zu hybriden Modellen), müssen Unternehmen die SAP-Welt neu denken und Vertragsmodelle, Lizenzmetriken und sogar Infrastrukturentscheidungen wie die Wahl des Hyperscalers strategisch aufeinander abstimmen.

Die Suite besteht zwar aus technisch optimiert integrierbaren Komponenten, doch die Abstimmung der dazugehörigen Vertragswerke bleibt Aufgabe des Kunden. Wer hier ohne „Big Picture“ agiert, läuft Gefahr, in eine Vielzahl von Problemen zu geraten: hoher operativer Aufwand, unkoordinierte Vertragswerke, unnötige Kosten, Doppellizenzierungen und sogar Innovationshemmnisse.

So gilt es konkret mitgelieferte Package- bzw. Runtime Nutzungsrechte aus der gewählte Cloud ERP Option zu bewerten; die optimierten Pricing-Tiers und Rabattkonditionen der SAP zu nutzen; AI-Unit-Bedarfe anhand von neueren User-Logiken zu planen; BDC-Capacity Units

der nächsten Jahre vorherzusagen und Vieles mehr. Gleichzeitig ist sicherzustellen, dass man compliant ist, jedoch nicht zu viel für ungenutzte Lizenzen zahlt. Eine vielschichtige und gleichzeitig spannende Herausforderung für alle SAP-Kunden.

Fazit: Ein Thema für die Unternehmensspitze

SAP-Lizenzen und -Verträge sind 2026 kein operatives Randthema mehr, sondern ein strategisches Steuerungsinstrument. Sie entscheiden über Wirtschaftlichkeit, Handlungsfreiheit und innovative Optionen. Wer seine SAP-Transformation erfolgreich gestalten will, kommt an einer frühzeitigen und professionellen Auseinandersetzung mit einer eigenen Lizenz- und Vertragsstrategie nicht vorbei. Sie ist der Schlüssel, um tatsächliche technische Transformation zu ermöglichen und schafft die Basis für langfristige Flexibilität sowie Innovationsfähigkeit des Unternehmens, heute und in Zukunft.

Svenja Vorwerk

HERAUSFORDERUNG FÜHRUNGSALLTAG

AKTUELLE STUDIE ZEIGT DISKREPANZEN

2 Prozent der deutschen Führungskräfte sehen sich durch begrenzte Zeit-, Personal- und Budget-Ressourcen vor große Herausforderungen in ihrem Führungsalltag gestellt. Welche weiteren Situationen und Umstände Unternehmen besonders fordern, untersucht der aktuelle Hernstein Management Report in einer repräsentativen Studie. Dafür wurden 1.600 Führungskräfte in Deutschland und Österreich befragt. Laut deren Einschätzung sehen mehr als ein Drittel der Befragten Dokumentations- und Berichtspflichten als problematisch an. Für 19 Prozent der deutschen Unternehmen ist die Budgetplanung aufgrund von Inflation und gestiegenen Kosten schwierig. Je Führungsebene werden Auswirkungen von Remote Work auf das Teamgefüge unterschiedlich bewertet. Während Führungskräfte aus dem oberen Management skeptischer sind, sehen knapp 70 Prozent aus dem unteren Management fast keine negativen Auswirkungen.

Rund 34 Prozent der befragten Führungskräfte berichten von abweichenden Erwartungen zwischen Unternehmensleitung und Team. Etwa ein Fünftel der Befragten betrachtet einen fehlenden Orientierungsrahmen und zu wenig Informationen vonseiten der Unternehmensführung als problematisch.

Eigene Routinen und Erfahrungswerte unterstützen

Für deutsche Führungskräfte sind die Kommunikation und Priorisierung durch die Unternehmensleitung mit 39 Prozent Zustimmung weniger wichtig, dafür werden strukturierte Teamprozesse und Arbeitsabläufe dagegen stärker geschätzt.

Strukturen im Unternehmen als Unterstützung für Führungskräfte

Nur in 44 Prozent der Unternehmen ist ein strukturierter Austausch mit anderen Führungskräften vorgesehen. Knapp 60 Prozent der Befragten geben zudem an, dass es in ihrem Unternehmen keine klar definierten Rollen und Erwartungen gibt, die ihnen in ihrer Führungsrolle Orientierung geben.

Remote Work – Gekommen, um zu bleiben?

Im Jahr 2025 haben etwas mehr als die Hälfte der Befragten die Möglichkeit, im

Homeoffice oder remote zu arbeiten. Das ist ein Rückgang um 8 Prozent im Vergleich zu 2021, dem „Corona“-Jahr. Mitarbeitende haben mit 62 Prozent in höherem Ausmaß die Möglichkeit, remote zu arbeiten, als ihre Führungskräfte (57 Prozent). 54 Prozent der Mitarbeitenden nutzen diese Möglichkeit zumindest teilweise.

60 Prozent der befragten Führungskräfte sind der Ansicht, dass Remote- und Homeoffice-Möglichkeiten kaum negative Auswirkungen auf das Teamgefüge und den Zusammenhalt im Team haben. Positive Effekte von Remote Work werden vor allem beim selbstständigen und kreativen Arbeiten sowie bei Effizienz und Geschwindigkeit in der Aufgabenerledigung gesehen. Am wenigsten positiv wirkt sich Remote Work dagegen auf die Kommunikation der Mitarbeitenden untereinander, die Konfliktlösung im Team und die Kontrolle der Arbeit aus.

www.hernstein.at





Auch 2026: Preissteigerung bei Microsoft

WIE DIE LIZENZKOSTEN TROTZDEM BEZAHLBAR BLEIBEN

Das Jahr beginnt so schön für CIOs: Währungsanpassung bei Microsoft! Minus 7,4 Prozent auf alle Cloud-Dienste im EU-Raum! Allzu lange währt der Glückstaukel leider nicht, denn ab Juni heißt es dann doch „Same procedure as every year!“ Microsoft dreht mit Preiserhöhungen zwischen 5 und 20 Prozent erneut an der Gebührenschaube. Drei Möglichkeiten, Lizenzkosten gegen den Trend herunterzufahren, beschreibt Björn Orth vom Microsoft Cloud Solution Partner VENDOSOFT.

Warum es günstiger ist, passgenau zu lizenzieren

Wenn ab 1. Juni 2026 die neuen Tarife gelten, trifft es Unternehmen, die komplett in der Cloud laufen wieder besonders hart: F3-Pläne kosten dann 20 Prozent mehr, Office-E3 dreizehn, M365 E3 acht Prozent und E5-Pläne werden fünf Prozent teurer. Das lässt grübeln, wie das finanzierbar bleiben soll. Einsparpotenziale liegen laut Björn Orth in der Differenzierung: „Eine Verwaltungsangestellte nutzt Microsoft anders als ein Logistiker. Und jemand in der Produktion oder am Service Point braucht wieder andere Funktionalitäten. M365-Pläne passgenau auf jeden Mitarbeitenden zuzuschneiden, kann zig tausende Euro Lizenzgebühren im Jahr sparen!“ Deshalb rechnet der Anbieter verschiedene Szenarien und

Kostenmodelle durch. Ein Aufwand, der Kunden nichts kostet – und der sich lohnt!

Welche finanziellen Spielräume hybride Lizenzierungen schaffen

Die meisten M365-Pläne sind ab dem dritten Jahr der Nutzung teurer als On-Premises. Office, Visio, Project, Server und CAL zu kaufen, wäre die logische Konsequenz. Doch ganz ohne Cloud-Dienste geht es in vielen Unternehmen nicht. Anders bei hybriden Modellen: Ei-

ne Kombination aus Kauflizenzen und ausgewählten M365-Plänen ist fast immer denkbar. Und sinnvoll. „Office 2024 und Exchange Online erfüllen zusammen denselben Nutzen wie ein Online-Plan – kosten aber 30 bis 40 Prozent weniger“, erklärt Orth. Ein SQL-Server, der Daten im hohen Terrabyte-Bereich speichert, wäre in der Cloud ein vielfaches teurer als lokal gehostet. Einsparungen wie diese gehen je nach Firmengröße in die hunderttausende Euro. Deshalb versichert Björn Orth: „Hybrid ist für die meisten Betriebe die kostenschonendste Lösung!“ Je mehr On-Premises ein Modell enthält, desto weniger preisabhängig und desto mehr Budget entsteht für andere Projekte: KI, Automatisierung, IT-Sicherheit.



ALS MICROSOFT-SPEZIALISTEN FÜR GEBRAUCHT, NEU, HYBRID UND CLOUD BERATEN WIR NEUTRAL – UND DAMIT KOSTENOPTIMIERT.

Björn Orth,
Geschäftsführer, VENDOSOFT GmbH,
www.vendosoftware.de

Die Vorteile von On-Premises-only

Wer volle Kostenkontrolle und Datensouveränität will, bekommt bei VENDOSOFT on-prem-only. Wer noch mehr sparen möchte, bekommt die Programme gebraucht. Einmal gekauft, besteht keine vertragliche Bindung mit Microsoft und IT-Budgets bleiben von Preiserhöhungen unberührt. Vertrauliche Daten liegen sicher auf den eigenen Servern. Und wann immer gewünscht, kann die Software wieder monetarisiert werden, denn das Unternehmen nimmt gebrauchte Microsoft-Lizenzen in Zahlung.

www.vendosoftware.de

Cloud-Nutzung

KOMFORT UND SICHERHEIT ZÄHLEN

**MEHR
WERT**
Cloud-Studie



Cloud-Dienste sind zwar längst im Alltag angekommen, die Akzeptanz ist jedoch an klare Bedingungen geknüpft. Eine aktuelle Studie von Strato zeigt, dass deutsche Nutzer bei Datenschutz und Sicherheit zunehmend anspruchsvoller werden.

Drei Viertel der befragten Cloud-Nutzenden (75 Prozent) wollen, dass keine außereuropäischen Institutionen Zugriff auf ihre Daten haben. Entsprechend legen 73 Prozent Wert auf einen europäischen

Serverstandort und die Einhaltung der DSGVO (und anderer Datenschutzrechte). 67 Prozent geben zudem an, bei Cloud-Diensten von außereuropäischen Anbietern datenschutzrechtliche Bedenken zu haben.

Neben der Sicherheit spielt auch der Komfort eine wichtige Rolle. Laut der forsa-Studie ist das wichtigste Auswahlkriterium bei der Wahl des Anbieters für 83 Prozent der Nutzer der geräteübergrei-

fende Zugriff. Gleichzeitig fordern viele Nutzer klare und verständliche Rahmenbedingungen: Mehr als die Hälfte achtet auf die Vertragskonditionen (58 Prozent) oder die Verschlüsselung (52 Prozent). Für jede zweite Person ist die Speicherung der Daten in Deutschland oder der EU ein entscheidendes Kriterium (50 Prozent).

Wachstumstrend für EU-Cloud-Dienste

65 Prozent der Cloud-Nutzenden geben an, dass ihnen ein europäischer Serverstandort und DSGVO-Konformität wichtiger sind als ein günstiger Preis – selbst wenn europäische Anbieter etwas teurer wären. Nur 39 Prozent bevorzugen ausschließlich EU-Cloud-Dienste, wenn diese nicht mehr kosten als außereuropäische Angebote.

Im Vergleich zu ähnlichen Daten aus der STRATO Studie 2019 lässt sich ein Wachstum interpretieren: Sowohl die Bedeutung des europäischen Serverstandorts (2019: 64 Prozent; 2025: 73 Prozent) als auch die Zahlungsbereitschaft für eine EU-Cloud (2019: 52 Prozent; 2025: 65 Prozent) erzielen im Jahr 2025 deutlich höhere Prozentzahlen.

www.strato.de

PRÄFERENZEN BEIM DATENSCHUTZ

Es stimmen den Aussagen zum Datenschutz bei Cloud-Diensten voll und ganz bzw. eher zu:

	Jahre 18–29	Jahre 30–44	Jahre 45–59	Jahre 60–75
Ich lege Wert auf einen europäischen Serverstandort und die Einhaltung der DSGVO bei der Nutzung von Clouddiensten.	73 %	65 %	77 %	79 %
Es ist mir wichtig, dass keine außereuropäische Institutionen Zugriff auf meine Daten erhalten	73 %	70 %	75 %	86 %
Ich habe bei Cloud-Diensten von außereuropäischen Anbietern datenschutzrechtliche Bedenken.	56 %	64 %	68 %	82 %
Ich lege Wert auf einen europäischen Serverstandort und die Einhaltung der DSGVO bei der Nutzung von Cloud-Diensten, gerade weil ich bei außereuropäischen Anbietern inzwischen datenschutzrechtliche Bedenken habe.	63 %	61 %	71 %	78 %

Basis: 663 Cloudnutzerinnen und -nutzer zwischen 18 und 75 Jahren in Deutschland, Quelle: forsa im Auftrag von STRATO | Sonderauswertung 2025

Smart Licensing

WENN MRM IT DENKT, IST AN ALLES GEDACHT

Wer in Unternehmen IT-Verantwortung trägt, entscheidet heute nicht mehr über Einzelleistungen. Aufgaben und Risiken sind in den vergangenen Jahren komplex geworden, die Abhängigkeiten von Herstellern weittragender. Das belastet nicht zuletzt die Budgets. Der Software Distributor MRM hat sich das Ziel gesetzt, Alternativen zu schaffen: zu kostenintensen

siven Microsoft-Produkten und anderen, scheinbar alternativlosen Anwendungen. Smart Licensing steht für einen Ansatz, der IT-Architekturen ganzheitlich betrachtet und wirtschaftlich optimiert.

Weil die Lizenzierung das ganze Unternehmen betrifft

Melanie Achten ist die Geschäftsführerin der MRM Distribution. Die Lizenzexpertin ist überzeugt, dass viele Unternehmen die Auswirkungen ihrer Lizenzentscheidungen unterschätzen. „Nehmen wir eine Migration in die Microsoft Cloud. Weit über die reine Softwarenutzung hinaus beeinflusst dieser Schritt die Kostenstrukturen, Vertragslaufzeiten und nicht zuletzt die Geschwindigkeit, mit der andere Projekte umgesetzt werden können.“

Bei Smart Licensing geht es darum, Software-Beschaffung als steuerbaren Bestandteil der IT-Gesamtstrategie zu begreifen. „Eine Reduzierung von Kosten und Abhängigkeiten bei der Lizenzbeschaffung kommt anderen wichtigen Investitionen zugute“, erklärt Achten das Konzept. Gebrauchte Microsoft-Lizenzen spielen dabei eine zentrale Rolle: MRM empfiehlt, Office, Server und CAL gebraucht zu kaufen – und um M365-Dienste zu ergänzen, wenn Kollaborati-

on und remotes Arbeiten gewünscht sind. Die Wiederverwendung von Software ist besonders nachhaltig – und bringt erhebliche Kostenvorteile. Die Empfehlungen von MRM legen nicht selten Budgets im hohen fünf- bis sechsstelligen Bereich frei.

Geld fürs Wesentliche

„Bei vielen Kunden fließen diese Gelder direkt in dringend notwendige Investitionen“, sagt die MRM-Frontfrau. Sie versteht sich dabei als Partner von KMU, der nicht nur Software liefert, sondern bedarfsgerechte Lösungen für Automatisierung, Virtualisierung, IT-Sicherheit und KI-Implementierungen. Auch hier zeigt MRM attraktive Alternativen zu altbekannten Lösungen auf:

- ➔ Pragatix Private AI macht Wissen und Daten in Unternehmen durch den Einsatz generativer KI sicher nutzbar.
- ➔ PragatixAI Firewall schützt dabei vor fahrlässigem Umgang mit Schatten-KI. Beide Komponenten sind als SaaS oder on-prem verfügbar.
- ➔ Eine echte Alternative zu VMWare sieht Melanie Achten in der Virtualisierungs-Software Sangfor HCI: fair in der Lizenzierung, leistungsfähig, mittelstandstauglich – und so viel günstiger als VMWare!
- ➔ Quickwork ist die von MRM präferierte Hyperautomation-Lösung für eine durchgängige KI-gestützte Automatisierung von Unternehmensprozessen.
- ➔ Und auch zu den Adobe-Produkten bietet der Distributor eine Alternative, um PDFs zu bearbeiten – ganz ohne Abo-Zwang: FlexiPDF von SoftMaker.

Wenn MRM IT denkt, ist also wirklich an alles gedacht. Statt isolierter Entscheidungen entsteht eine IT-Architektur, die alle Anforderungen abdeckt, finanzielle Spielräume lässt und auch morgen noch trägt.

Angelika Mühleck



„
WIR SIND PARTNER
FÜR KOSTENEFFIZIENTE
IT-LÖSUNGEN AUS
EINER HAND – VON
MICROSOFT ÜBER
KI-TOOLS UND HYPER-
AUTOMATION BIS
VIRTUALISIERUNG.“

Melanie Achten, CEO, MRM Distribution,
www.mrm-distribution.com



Unified Endpoint Management

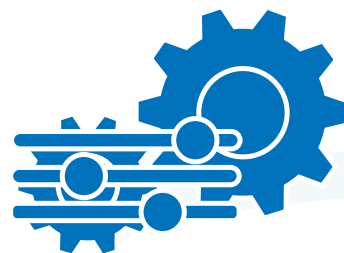
MIT UEM ZU DATENHOHEIT UND DIGITALER SOUVERÄNITÄT

Kurze Wege, direkte Ansprechpartner, geschützt vor US-Rechtsrisiken durch Hosting in Deutschland – Unternehmen sind nur dann digital souverän, wenn sie ihre IT-Infrastruktur nicht in fremde Hände geben.

Linux statt Office 365, StudiVZ statt Facebook, Xing statt LinkedIn? Allein die drei Beispiele zeigen, dass der fromme Wunsch digitaler Souveränität Europas von den US-Tech-Giganten in der Praxis gar nicht so leicht umzusetzen ist. Ein Geschäftsfeld gibt es jedoch, in dem Unternehmen unabhängiger werden können, ohne sich vollkommen vom Rest der Welt abzuschneiden: die Sicherstellung vollständiger Daten-,

Entscheidungs- und Betriebshoheit über IT-Infrastruktur und Endpunkte.

Unternehmen, die mit einer europäischen Unified-Endpoint-Management-Lösung ihre gesamte IT-Infrastruktur managen, von der Softwareverteilung bis zum Sicherheitsmanagement, haben den Schlüssel zu einer selbstbestimmten IT und damit zur digitalen Souveränität in der Hand – ohne Abhängigkeit von außereuropäischen Cloud-Anbietern oder fremden Rechtsräumen, mit maximaler Kontrolle über Daten und Systeme im eigenen Netzwerk. Digitale Souveränität wird 2026 zu einem entscheidenden Auswahlkriterium. Sie verwirklicht sich bei Hoheit über die



IT – ohne dabei auf die sichere Integration von Cloud-Services verzichten zu müssen.

Bedrohungen der Souveränität

US Cloud Act und Patriot Act mögen ureigene amerikanische Interessen nach Kontrolle befriedigen. Wenn US-Softwarefirmen jedoch zur Herausgabe von Daten verpflichtet sind (auch wenn diese auf Servern außerhalb der USA gespeichert sind), gibt es automatisch einen Konflikt mit europäischen Datenschutzbestimmungen, in Deutschland namentlich der DSGVO.

Auf die IT-Infrastruktur bezogen, hat sich dies in den letzten Jahren zunehmend zum Problem entwickelt. Denn immer mehr mobile (iOS/Android) Devices sind im Netzwerk unterwegs. Sie werden oft mit cloud-basierten UEM-Systemen administriert, von denen Microsoft Intune das meist verbreitete ist. Die Unternehmen verlassen sich damit auf einen US-basierten Hyperscaler und stecken so bereits mitten in der Debatte um digitale Souveränität.

Die daraus erwachsende Problemlage ist vielschichtig: Unternehmen werden abhängig von der Verfügbarkeit der Cloud-Plattform, geben die Verwaltung ihrer Gerätedaten in externe Hände, haben keinen Einfluss auf den Zeitpunkt von Software-Updates, und Eingriffe wie das Sperren von Ports sind nur begrenzt möglich. Wenn nicht dies, was sind sonst klare Beschränkungen der Souveränität über das eigene Netzwerkgeschehen?

Hinzu kommen stetig steigende Lizenzkosten ohne Transparenz und grundsätzlich das Problem des Vendor Lock-in. Davon spricht man, wenn ein Unternehmen

so stark an die proprietären Produkte, Technologien oder Dienstleistungen eines bestimmten (US-)Anbieters gebunden ist, dass ein Wechsel auf Alternativen aufgrund hoher Kosten, technischer Hürden oder enormer Aufwände nahezu unmöglich wird.

On-Premises: Hohe Funktionalität und Datenschutz

Mit Unified Endpoint (oder auch Client) Management-Plattformen verwalten heute viele Unternehmen die Endgeräte in ihren Windows/Linux-basierten Netzwerken. Dies sind traditionell On-Premises-Systeme, die auf eigenen Servern betrieben werden (lokal/Private Cloud) und über spezialisierte Agenten für eine umfassende Kontrolle verfügen. Sensible Informationen verlassen damit die eigene Infrastruktur nicht. Microsoft-Dienste (wie Windows Updates, Defender, BitLocker) lassen sich nahtlos integrieren, ohne auf eine Cloud-Anbindung angewiesen zu sein.



Sensible Informationen innerhalb der eigenen Infrastruktur

Die digitale Souveränität steht und fällt mit der Datenhoheit. Solange das Unternehmen eigene Server betreibt, verbleiben sensible Informationen innerhalb der eigenen Infrastruktur und werden nicht für KI-Trainingszwecke verwendet, was in der Cloud immer geschehen kann. Gleichzeitig ist beim lokalen Betrieb der rechtliche Aufwand geringer. Datenverarbeitungsverträge mit Dienstleistern müssen nicht aufwändig verhandelt werden beziehungsweise beschränken sich auf die eigentliche Geschäftsbeziehung und eben nicht auf Firmen- oder Kundendaten.

Eine lokale UEM-Lösung macht das Unternehmen außerdem unabhängig von Internet- oder Serverstörungen des Cloud-Anbieters; die eigene Infrastruktur bleibt steuerbar. Sie ist auch im Hinblick auf Compliance oft die bessere Wahl.

Strenge Vorgaben in sicherheitskritischen Bereichen, die Unabhängigkeit vom Internet vorschreiben – etwa im Umfeld von KRITIS, NIS-2 oder DORA – lassen sich mit On-Premises-Systemen besser umsetzen. Sie sind bei Unternehmen, die in diesem Bereich etwas tun müssen, daher die bevorzugte Betriebsform.

Hybrides Unified Endpoint Management als Lösung

Weil traditionelle UEM-Systeme mobile Endgeräte jedoch nur eingeschränkt unterstützen, sollten moderne Systeme dieser Art heute einem hybriden Ansatz folgen, das heißt Cloud-UEM und On-Premises-Management in einer Plattform vereinigen. Geräte- und Benutzer-Gruppen werden bei diesem Ansatz aus der Cloud-Lösung in das (führende) On-Premises-UEM überführt und sind darin sichtbar.

IT-Abteilungen haben damit eine zukunftsfähige Plattform für die wachsende Device-Vielfalt, in einer rechtsicheren IT-Architektur und sind strategisch unabhängig von Hyperscalern. Datenschutzbeauftragte sichern sensible Informationen, minimieren rechtliche Risiken und können bei Bedarf auf Audit-sichere Nachweise zugreifen. Das Management reduziert Haftungsrisiken, hat Planungssicherheit bei Kosten und Regulierung und erfüllt alle gesetzlichen Pflichten wie etwa NIS-2.

Bei der Unified-Endpoint-Management-Lösung ACMP von Aagon beispielsweise interagieren mehrere Komponenten miteinander und führen damit zu digitaler Souveränität: Inventur und Asset Management bilden das Fundament. Über das Patch Management wird die Souveränität operativ durchgesetzt, über Security- und Compliance Module politisch-regulatorisch sowie über das Lizenzmanagement wirtschaftlich.

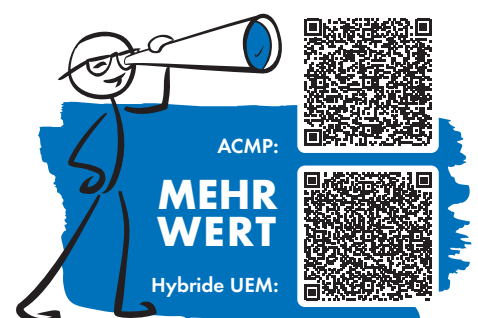
Unabhängigkeit, Kostentransparenz und lokale Unterstützung sind für viele Un-

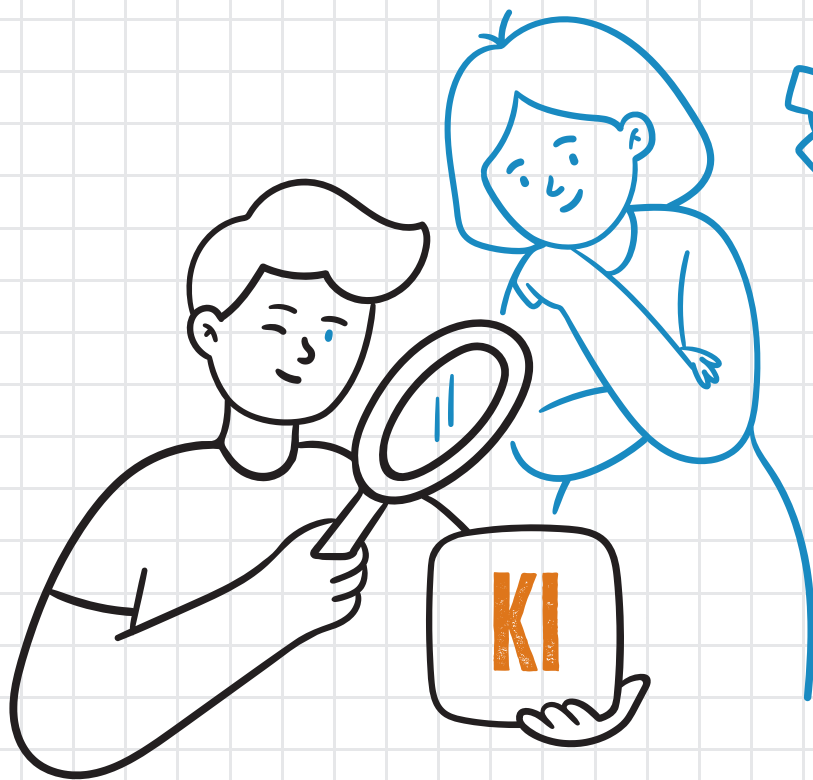
ternehmen des Mittelstands und der Industrie relevante Kriterien bei der Auswahl einer für sie passenden UEM-Lösung. In der öffentlichen Verwaltung ist Datensouveränität heute bereits ein wichtiges Vergabekriterium für neue Softwareprodukte, so die Forderung des IT-Planungsrates aus dem Jahr 2021. Mit einer hybriden UEM-Plattform erfüllen Behörden die notwendigen formalen Anforderungen an Transparenz, Nachvollziehbarkeit und Kontrolle. Im Gesundheitswesen und in Bildungseinrichtungen steht der Schutz hochsensibler Patienten (Kunden-)daten im Vordergrund. Und alle Organisationen, die sich im Bereich kritischer Infrastrukturen bewegen, müssen schon allein deshalb NIS-2- und weitere sektorale Sicherheitsauflagen beachten.

Fazit

Hybrides UEM stärkt die Handlungs- und Steuerungsfähigkeit im öffentlichen Sektor und im Mittelstand. Es versetzt IT-Verantwortliche in die Lage, ihre End-Point-Landschaft souverän gestalten zu können. Mit der Plattform eines lokalen Anbieters verringern sie ihre technologische Abhängigkeit von US-Hyperscalern und haben vollständige betriebliche Transparenz über Endpunkte, Policies, Patch-Status und Security-Maßnahmen. Ein Unternehmen erhöht seine Rechtssicherheit erheblich durch die Einhaltung der DSGVO sowie der Vorgaben aus dem Schrems-II-Urteil, wonach personenbezogene Daten nur dann in Drittländer übermittelt werden dürfen, wenn dort ein im Wesentlichen gleichwertiges Schutzniveau wie in der EU gewährleistet ist.).

Sebastian Weber | www.aagon.com



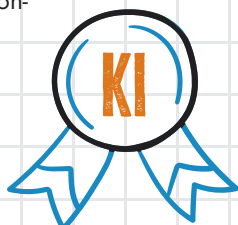


Souveräne KI statt Schatten-Tools

WIE UNTERNEHMEN IHRE KI-NUTZUNG SICHER UND WIRTSCHAFTLICH STEUERN

Immer mehr Mitarbeiter nutzen in ihrer täglichen Arbeit Künstliche Intelligenz – häufig über frei verfügbare Online-Dienste. Was auf den ersten Blick effizient erscheint, führt in der Praxis oft zu einer unkontrollierbaren Schatten-KI. Unternehmen verlieren dabei nicht nur die Übersicht über ihre Kosten, sondern riskieren auch Datenschutz- und Compliance-Verstöße. Um KI sicher, zentral und DSGVO-konform einsetzen zu können, ist eine kontrollierte Plattform unerlässlich. Wie eine solche Lösung aussehen kann, zeigt der Controlware AI Hub.

Der Controlware AI Hub wurde zunächst als ausschließlich interne Lösung entwi-



UM KI SICHER, ZENTRAL UND DSGVO-KONFORM EINSETZEN ZU KÖNNEN, IST EINE KONTROLLIERTE PLATTFORM UNERLÄSSLICH.

Moritz Schürmann, Senior Cloud Solutions Architect, Controlware GmbH, www.controlware.de

ckelt. Wie in praktisch jedem Unternehmen wurde auch bei Controlware von Seiten vieler Kollegen der Wunsch laut, auf innovative KI-Features zuzugreifen –

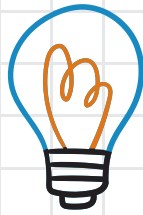
als IT-Dienstleister und MSP wussten wir aber gut um die Risiken, die damit einhergehen. Daher entschieden wir uns, mit einer zentralen KI-Plattform die Voraussetzungen für eine sichere und Compliance-konforme KI-Nutzung zu schaffen, ohne die Kontrolle über Daten und Prozesse aus der Hand zu geben. Das versprach auch wirtschaftliche Vorteile – dezentrale Einzelabonnements hätten erhebliche monatliche Kosten verursacht.

Flexible Open-Source-Plattform, höchste Sicherheitsstandards

Der so entwickelte AI Hub steuert heute als unternehmensweite Plattform alle KI-Zugriffe. Technische Basis ist dabei die Open-Source-Lösung Open WebUI, die als schlüsselfertige und flexible Umgebung bereitgestellt wird. Über eine einheitliche, intuitive Web-Oberfläche lassen sich darauf unterschiedlichste KI-Tools integrieren – neben GPT-5 oder Claude Sonnet 4 auch eigene Open-Source-Lösungen. Sämtliche Zugriffe werden über Microsoft Entra und Single Sign-on geschützt. Berechtigungen können granular nach Abteilungen und Teams vergeben werden, so dass Zugriffsrechte jederzeit transparent und kontrollierbar bleiben. Kurz: Die Lösung vereint ein Höchstmaß an Flexibilität und Sicherheit, bei gleichzeitiger Standardisierung der KI-Nutzung.

Das Modell funktionierte in der Praxis so gut, dass bereits nach kurzer Zeit die Entscheidung fiel, den Controlware AI Hub auch als Service für Kunden bereitzustellen, um eine wirtschaftliche Alternative zur Schatten-KI zu bieten. Der Betrieb des AI Hub kann dabei wahlweise On-Premises oder als Managed Service in einem hochsicheren europäischen Rechenzentrum erfolgen. So können die Verantwortlichen die Plattform nahtlos in

bestehende IT-Umgebungen integrieren und jederzeit die Einhaltung strengster Sicherheitsanforderungen gewährleisten.



Nach einer optionalen und kostenfreien Bedarfsanalyse wird der Controlware AI Hub schlüsselfertig ausgeliefert. Um die Einstiegshürde niedrig zu halten, kann der Hub dabei wahlweise als kostenlose Demo-Umgebung implementiert

oder direkt unternehmensweit ausgerollt werden. Das transparente, nutzungsbasierte Kostenmodell sorgt für Planungssicherheit und ermöglicht erhebliche Einsparungen gegenüber dezentralen Abonnementstrukturen. Auf Wunsch übernehmen wir den vollständigen Betrieb inklusive Updates, Security und Support und entlastet damit die interne IT-Abteilung.

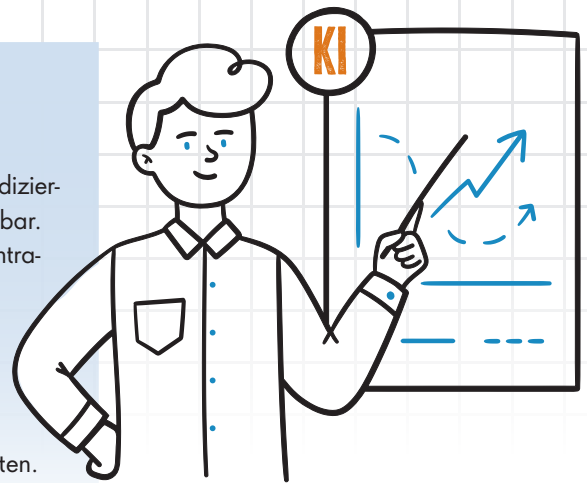
Fazit

Der Controlware AI Hub kann Unternehmen und Behörden in Europa heute als zentraler Baustein bei der Umsetzung einer souveränen KI-Strategie dienen. Die Verantwortlichen profitieren so von einer sicheren und skalierbaren Plattform, die den Innovationsansatz von Open Source mit der Stabilität professioneller Managed Services verbindet.

Moritz Schürmann

FÜR ENTWICKLER: CONTROLWARE AI HUB GATEWAY

Mit dem Controlware AI Hub Gateway ist zusätzlich zum AI Hub eine dedizierte, auf die Anforderungen von Entwicklern zugeschnittene Lösung verfügbar. Das auf LiteLLM basierende Gateway, das auch im AI Hub selbst als zentrale Routing-Schicht zum Einsatz kommt, bietet über eine einzige Schnittstelle Zugriff auf unterschiedlichste KI-Modelle: von Claude Sonnet und Opus über GPT 5 bis hin zu lokalen Open-Source-Modellen. Der große Vorteil dabei: Entwickler können gewohnte Tools wie Cline in VS Code oder OpenCode einfach weiterverwenden und jederzeit flexibel zwischen Modellen wechseln, ohne multiple API-Keys zu verwalten.



CLEAN CODE

REFACTORING, PATTERN, TESTEN UND TECHNIKEN FÜR SAUBEREN CODE

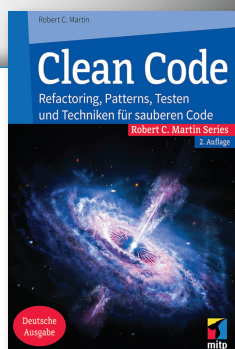


Selbst schlechter Code kann funktionieren. Aber wenn der Code nicht sauber ist, kann er ein Entwicklungsunternehmen in die Knie zwingen. Jedes Jahr gehen unzählige Stunden und beträchtliche Ressourcen verloren, weil Code schlecht geschrieben ist. Aber das muss nicht sein. Mit der zweiten Ausgabe von Clean Code modernisiert Robert C. Martin (»Uncle Bob«) seinen klassischen Leitfaden rund um Techniken für sauberen Code und ergänzt ihn um neue Erkenntnisse, Inhalte und Perspektiven. Diese neue Ausgabe stellt eine umfassende Überarbeitung des Bestsellers dar und vermittelt Programmierern wichtige, praxistaugliche Tipps zum

Schreiben von sauberem, flexiblem und wartbarem Code.

Das Buch befasst sich in vier Teilen mit grundlegenden Programmiertechniken, Designprinzipien und Heuristiken, High-Level-Architektur sowie, zu guter Letzt, der Ethik dieser Kunst. Der Autor fordert dazu auf, die Qualität von Code kritisch zu bewerten und die eigenen beruflichen Werte zu hinterfragen – immer mit dem Ziel, bessere Programme zu schreiben. In dieser Ausgabe erhalten die Themen Testdisziplinen und Design- und Architekturprinzipien sowie verschiedene Programmiersprachen zusätzlichen Raum.

Clean Code – Refactoring, Pattern, Testen und Techniken für sauberen Code; Robert C. Martin; mitp Verlags GmbH & Co.KG; 04-2026





Professionelles Site-Management

PERSONALLÜCKEN IM RECHENZENTRUMSMANAGEMENT SCHLIESSEN

Der anhaltende Fachkräftemangel im IT-Bereich stellt Unternehmen vor Herausforderungen, insbesondere im Bereich der IT-Infrastruktur. Die DeRZ – Deutsche Rechenzentren GmbH begegnet dieser Problematik mit innovativen Dienstleistungen im Rechenzentrumsmanagement, die IT-Abteilungen durch externes Site-Management strategisch entlasten sollen.

„Durch das Outsourcing des TGA-Managements können IT-Verantwortliche ihre ohnehin knappen personellen Ressourcen gezielt für Projekte einsetzen, während der Site-Manager dort agiert, wo er gerade gebraucht wird“, erklärt Sascha

Helmkamp, Bereichsleiter Services. Diese Strategie ermöglicht es Unternehmen, sich vollständig auf ihr Kerngeschäft zu konzentrieren, während Experten das Management der technischen Gebäudeausrüstung übernehmen.

Wirtschaftliche Vorteile und technologische Exzellenz

Das Outsourcing des Site-Managements zielt auf Kostenreduktion durch Prozessoptimierung ab. Durch die Optimierung können Betriebskosten nachhaltig reduziert werden, während gleichzeitig die Effizienz der Rechenzentrumsinfrastruktur gesteigert wird. Kunden erhalten Zugang zu geschulten Fachkräften, die über aktuelle Technologien und Branchenstandards verfügen.

Ein besonderer Vorteil liegt in der Skalierbarkeit und Flexibilität der Dienstleistungen. Das 24/7-verfügbare Service-Angebot kann schnell und unkompliziert an sich verändernde Kundenanforderungen angepasst werden, was eine bessere finanzielle Planbarkeit ermöglichen soll.

„Wir bieten verschiedene Service-Pakete an, die den jeweiligen Bedürfnissen unserer Kunden gerecht werden und eine erhebliche Entlastung für interne IT-Abteilungen schaffen“, erklärt Sascha Helmkamp. So bildet das Servicepaket BASIC die optimale Grundlage für einen sicheren RZ-Betrieb, die ADVANCED-Variante enthält sämtliche Leistungen der BASIC-Version

plus eines ‚Next-Business-Day-Services‘, der die garantierte Bearbeitung betriebsrelevanter Störungen am nächsten Werktag abdeckt. Mit der PREMIUM-Ausführung wird den Kunden schließlich ein Maximum an Sicherheit zur Verfügung gestellt. Sie beinhaltet sämtliche Features der BASIC und ADVANCED-Pakete, geht aber noch einen Schritt weiter: So reagieren die Servicetechniker hierbei innerhalb von nur 4 Stunden nach Eingang einer Störungsmeldung, um Fehler schnellstmöglich zu beheben.

Umfassende Sicherheit und Compliance

„Das Outsourcing des Site-Managements ermöglicht zudem die Implementierung höchster technologischer Sicherheitsstandards unter Einhaltung der Compliance-Richtlinien. Ein kontinuierliches Monitoring und Risikomanagement zur Vermeidung von Sicherheitsvorfällen, das Wartungsmanagement und die allgemeine Risikoüberwachung tun ihr Übriges“, betont Helmkamp.

Die externen Site-Manager sind für die komplette physische Rechenzentrumsinf-



„UNSERE KUNDEN SCHÄTZEN VOR ALLEM, DASS SIE SICH VOLLKOMMEN AUF IHR KERNGESCHÄFT UND STRATEGISCH WICHTIGE AUFGABEN ABSEITS DES TGA-BETRIEBS KONZENTRIEREN KÖNNEN.“

Sascha Helmkamp, Bereichsleiter
Services, Deutsche Rechenzentren GmbH,
www.deutsche-rz.com

rastruktur verantwortlich, einschließlich Zutrittsverwaltung und Überwachung der TGA-Komponenten. Sie fungieren als zentrale Schnittstelle zwischen Herstellern, Dienstleistern und der IT-Abteilung des Kunden.

Individuell angepasste Service-Level-Agreements

Der Umfang des Site-Managements wird über maßgeschneiderte Service-Level-

Agreements (SLAs) definiert und orientiert sich an den spezifischen Anforderungen, dem Budget und den infrastrukturellen Prozessen des jeweiligen Kunden. Das Leistungsspektrum umfasst neben dem Betriebsmanagement auch Störfallmanagement, Energiemanagement sowie Bestands- und Konfigurationsmanagement.

Für eine zukunftsfähige Rechenzentrumsstrategie sind zusätzlich Sicherheits- und Bedarfsanalysen, Redundanzkonzepte sowie energetische Optimierungen im Angebot enthalten. Die Site-Manager leiten proaktiv Vorgänge zur Aufrechterhaltung des Betriebes ein und arbeiten kontinuierlich an der Verbesserung von Performance und Funktionalität der Systeme und Anlagen.

www.deutsche-rz.com



20. – 24. April 2026

THINK TECH FORWARD

Globaler Treffpunkt für industrielle Transformation, wo Innovation und Verantwortung zusammenkommen, um die Zukunft der Produktion zu gestalten.

www.hannovermesse.de/hm26



THINK TECH FORWARD



Effizientes Datenmanagement

DER TREND GEHT ZUR KI-FABRIK

Immer mehr Unternehmen setzen Künstliche Intelligenz großflächig ein. Dabei zeichnen sich einige zentrale Entwicklungen ab: KI-Fabriken bilden die technische Basis, effiziente Datenspeicherung und Datenmanagement werden zum unverzichtbaren Rückgrat, und kleine KI-Modelle sorgen für operative Intelligenz. Gleichzeitig wird deutlich, dass ein stabiler Governance-Rahmen unverzichtbar ist.



ORGANISATIONEN STEHEN HEUTE NICHT MEHR VOR DER FRAGE, OB SIE KI EINSETZEN SOLLEN, SONDERN WIE SIE DIESE ZUVERLÄSSIG, WIRTSCHAFTLICH UND KONTROLLIERBAR BETREIBEN KÖNNEN.

Christian Scharrer, Enterprise Architect und CTO Ambassador, Dell Technologies, www.dell.com

Der Unternehmenseinsatz von Künstlicher Intelligenz tritt in eine neue Phase ein. Was bis dato eine Sammlung einzelner Anwendungsfälle war, wird zunehmend zu einer geschäftskritischen Infrastruktur. Organisationen stehen heute nicht mehr vor der Frage, ob sie KI einsetzen sollen, sondern wie sie diese zuverlässig, wirtschaftlich und kontrollierbar betreiben können. Die entscheidenden Entwicklungen liegen weniger in immer größeren Modellen als vielmehr in der Art und Weise, wie KI technisch, organisatorisch und strategisch im Unternehmen verankert wird, um damit echte Mehrwerte zu schaffen.

IT-Umgebungen werden zu KI-Fabriken

Eine zentrale Rolle spielt dabei der Wandel der IT-Umgebungen hin zu modularen KI-Fabriken. Die Umsetzung von KI-Projekten erfordert eine extrem skalierbare Infrastruktur. Wenn Unternehmen KI immer großflächiger einsetzen und die Zahl der Nutzer steigt, benötigen sie kurzfristig eine Vielzahl an hochperformanten Ressourcen. Damit sind klassische IT-Infrastrukturen schnell überfordert. Darüber hinaus ist es meist nicht praktikabel, KI ausschließlich zentralisiert zu betreiben. Viele Anwendungen müssen aus Latenzgründen lokal ausgeführt werden.

Unternehmen setzen deshalb zunehmend auf hybride Architekturen, bei denen Edge-Systeme latenzkritische Aufgaben übernehmen, während zentrale Rechenzentren für Training, zentrale KI-Dienste und Management zum Einsatz kommen und Public Clouds zur elastischen Skalierung bei weniger sensiblen Informationen genutzt werden. Daten werden dabei nicht pauschal in eine bestimmte Umgebung verschoben, sondern folgen einem regelbasierten Modell: Wo sie verarbeitet werden, hängt davon ab, wo der höchste Nutzen entsteht, wo die Verarbeitung wirtschaftlich sinnvoll ist und wo das geringste Risiko besteht.

Klassische Speicherinfrastrukturen können nicht mithalten

Der Erfolg von KI-Projekten hängt aber nicht nur von der Rechenleistung ab, sondern von der Effizienz des gesamten KI-Stacks. Die Speicherinfrastruktur spielt dabei eine besonders wichtige Rolle. Klassische Ansätze stoßen angesichts der hohen Anforderungen an Datenaggregation und schnellen Zugriff der Workloads an ihre Grenzen.

Aber auch bei einer hyperkonvergenten Infrastruktur kann es zu Engpässen kommen, wenn die Kom-

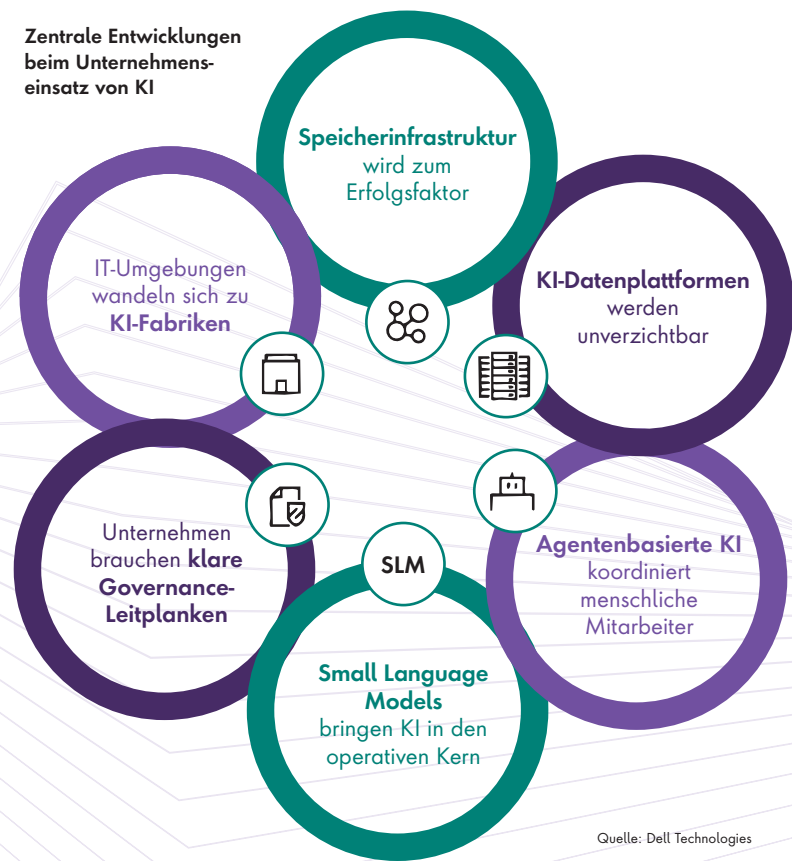
munikation zwischen den verschiedenen Nodes besondere Netzwerkanforderungen stellt. Speicher- und Rechenkomponenten müssen zudem stets gemeinsam erneuert werden, obwohl sie unterschiedliche Modernisierungszyklen haben. KI beschleunigt diesen kostspieligen Kreislauf weiter: GPUs müssen in der Regel bereits nach wenigen Jahren aktualisiert werden, während HDDs deutlich langlebiger sind.

Disaggregierte Architekturen bieten hier eine Lösung: Storage- und Compute-Leistung sind entkoppelt, und speziell für KI entwickelte Netzwerke sorgen für die erforderliche Performance bei der Kommunikation zwischen den KI-Knoten. Über ein weiteres Netzwerk steht zudem eine gemeinsame Speicherebene für KI bereit, die von allen Systemen gleichzeitig genutzt werden kann.

Effizientes Datenmanagement

Zusammen mit der Datenspeicherung wird auch das Datenmanagement zunehmend zum Rückgrat von KI-Innovationen. Weil KI-Systeme immer komplexer werden, wird die Qualität der Daten, die sie verarbeiten, immer wichtiger. Das macht speziell entwickelte KI-Datenplattformen unverzichtbar. Sie sind darauf ausgelegt, unterschiedliche Datenquellen zu integrieren, Datenartefakte zu schützen, Zugriffsberechtigungen unternehmensweit zu regeln und die erforderlichen Informationen über zentrale Zugriffspunkte bereitzustellen.

Zentrale Entwicklungen beim Unternehmens-einsatz von KI



Quelle: Dell Technologies

Die Fähigkeit, KI-Modelle effizient mit sauberen, organisierten und relevanten Daten zu füttern, ist insbesondere für die sich zunehmend verbreitende agentenbasierte KI von großer Bedeutung. Die Qualität der Daten ist bei ihr elementar für die Qualität der Ergebnisse. Agentenbasierte KI macht aus hilfreichen Assistenten integrale Manager für langwierige und komplexe Prozesse. In Bereichen wie Fertigung oder Logistik können KI-Agenten Mitarbeitende unterstützen und dabei helfen, ihre Arbeitsabläufe effizient aufeinander abzustimmen.

Dabei werden Daten nicht nur in erster Linie für das Training der Modelle genutzt, sondern auch beim Einsatz der Modelle aktiv eingebunden und laufend verarbeitet. Sie ermöglichen die Generierung von Wissen und Intelligenz, die sich in Echtzeit weiterentwickeln. Es sind umfangreiche und dynamische Datenströme, die KI-Agenten in die Lage versetzen, über Schichtdienste hinweg für Kontinuität zu sorgen oder Arbeitsabläufe in Echtzeit zu optimieren – und damit ein neues Maß betrieblicher Effizienz zu schaffen.

Kleine KI-Modelle setzen direkt an der Wertschöpfung an

Eine weitere zentrale Entwicklung ist der zunehmende Einsatz kleiner KI-Modelle tief im operativen Kern von Unternehmen. Ein gutes Beispiel dafür ist die Fertigung. Im Gegensatz zu großen KI-Modellen lassen sich Small Language Models (SLMs) in wenigen GPU-Stunden für spezifische Aufgaben wie das Erkennen von Abweichungen oder das Auswerten von Wartungsberichten weiterentwickeln. Techniken wie Low-Rank Adaptation (LoRA) ermöglichen es zudem, bereits vortrainierte Modelle gezielt anzupassen, indem nur kleine zusätzliche Komponenten trainiert werden, statt das gesamte Modell neu zu berechnen. Dadurch können Small Language Models schnell in die Produktionsprozesse integriert werden.

Ein entscheidender Vorteil ist zudem der lokale Einsatz: SLMs lassen sich direkt auf Edge-Geräten oder in abgeschotteten OT-Umgebungen betreiben, wodurch Reaktionszeiten und Sicherheitsrisiken mi-

nimiert werden. Gerade für Anwendungen im Bereich der Physical AI sind solche kompakten Modelle unverzichtbar. Selbstlernende, autonome Roboter funktionieren nur mit eingebetteter Intelligenz. Durch SLMs verschiebt sich KI von einer zentralen Servicefunktion hin zu einer dezentralen Fähigkeit, die direkt an der Wertschöpfung ansetzt.

Governance-Frameworks

KI entwickelt sich rasant weiter. Damit geht aber auch ein gewisses Maß an Volatilität einher. Der Bedarf an robusten Governance-Frameworks für den Unternehmenseinsatz wird dadurch größer denn je. Ohne tragfähige Governance werden Unternehmen mit Unsicherheiten konfrontiert, die die Einführung praktischer und nutzbringender KI-Anwendungen verlangsamen. Die öffentliche Hand, Unternehmen und Technologie-Anbieter sollten deshalb gemeinsam an der Entwicklung einer Governance für den Enterprise-Markt arbeiten.

Die Regulierung öffentlicher Chatbots oder einer öffentlichen Allgemeinen Künstlichen Intelligenz (Artificial General Intelligence, AGI) ist etwas völlig anderes, als Unternehmen dabei zu unterstützen, reale KI-Anwendungen für ihre Betriebe und Prozesse zu gestalten. Hier braucht es einen Governance-Rahmen, der Unternehmen klare Leitplanken bietet und es ihnen ermöglicht, sicher und nachhaltig voranzukommen.

Christian Scharrer



SECURE REMOTE ACCESS-RATGEBER

SICHERHEIT TRIFFT FLEXIBILITÄT

Remote Work, Mobile Office, agiles Arbeiten – das traditionelle Büro hat in den vergangenen Jahren Konkurrenz bekommen. Doch wie lässt sich diese Flexibilität mit der Sicherheit sensibler Daten vereinbaren? Herkömmliche Sicherheitskonzepte stoßen hier schnell an ihre Grenzen, da klassische „VPN-only-Lösungen“ nicht mehr ausreichend Schutz bieten. Gefragt sind maßgeschneiderte Regeln und intelligente Technologien, die den Fernzugriff auf interne Netzwerke und Cloud-Dienste absichern.

In diesem Ratgeber zeigen wir, wie SASE, Zero Trust und KI-gestützte Sicherheitsmechanismen zusammenspielen, um Remote-Zugriffe effektiv abzusichern – und weshalb nachhaltige Security-Architekturen neben Technologie auch klare Prozesse und organisatorische Verankerung erfordern.

NCP
Secure Remote Access-Ratgeber
Remote Access-Architekturen

**WHITEPAPER
DOWNLOAD**

Das Whitepaper umfasst 12 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/Download

**Inklusive
KI-Erlebnisworkshop**

Steampunk und BTP Summit 2026

**22. und 23.
April 2026
Heidelberg**

SAP Business Technology Platform, BTP, wird nach Meinung der SAP-Community die bestimmende ERP-Strategie. Der Summit 2026 präsentiert Abap, CAP, RAP und Steampunk sowie SAP BTP als Basisplattform und S/4-Hana-Nachfolger.

e3mag.com/de/steampunk-summit



Eine Veranstaltung des E3-Magazins:



e3mag.com

Datenwachstum 2026

WARUM UNTERNEHMEN IHRE CLOUD-PARTNER NEU BEWERTEN MÜSSEN

Datenwachstum galt lange als technisches Skalierungsproblem. Mit jeder neuen Anwendung, jedem zusätzlichen digitalen Prozess und jeder regulatorischen Anforderung stieg das Volumen der gespeicherten Informationen und damit der Bedarf an Infrastruktur. Cloud-Strategien wurden entsprechend vor allem unter Gesichtspunkten wie Performance, Verfügbarkeit und Time-to-Market entwickelt. Wer schnell skalieren konnte, galt als gut aufgestellt, weil mehr Daten nahezu automatisch mehr Wertschöpfung versprochen.

Mit dem Übergang in eine KI-getriebene Datenökonomie verändert sich diese Logik jedoch grundlegend. Das Wachstum betrifft nicht mehr nur die Menge der gespeicherten Daten, sondern vor allem deren Nutzungsintensität. Generative KI, automatisierte Sicherheitsprozesse, kontinuierliche Compliance-Analysen und datenbasierte Entscheidungsmodelle greifen permanent auf Datenbestände zu, replizieren sie, verschieben sie zwischen Plattformen und werten sie in hoher Frequenz aus. Damit steigt nicht nur der Speicherbedarf, sondern auch die Anzahl der

Interaktionen und genau hier entsteht die strategische Herausforderung.

Kostenmodelle unter Druck

In vielen Organisationen sind Cloud-Architekturen über Jahre hinweg organisch gewachsen. Hyperscaler betreiben produktive Systeme, spezialisierte Storage-Anbieter übernehmen Backup- und Archivierungsfunktionen, während Managed Service Provider die Integration und den Betrieb orchestrieren. Dieses Modell hat Effizienz geschaffen und Komplexität reduziert. Gleichzeitig hat es jedoch ein



Geflecht unterschiedlicher Kosten- und Governance-Logiken entstehen lassen.

Während Budgets häufig kapazitätsorientiert geplant werden, basieren viele Cloud- und Storage-Modelle zunehmend auf transaktionsabhängigen Mechanismen. API-Aufrufe, Datenbewegungen, Replikationen oder Egress-Gebühren gewinnen an Gewicht, sobald KI-Workloads dominieren und hybride Architekturen zur Regel werden. Die wirtschaftliche Dynamik verschiebt sich damit vom linearen Speicherwachstum hin zu einer komplexeren Kostenstruktur, deren Entwicklung nur eingeschränkt prognostizierbar ist. Für IT-Entscheider bedeutet das: Nicht das Volumen allein bestimmt die Budgetstabilität, sondern die Intensität der Nutzung.

Die verdeckte Risikoverschiebung entlang der Partnerkette

Diese Entwicklung wird besonders deutlich im Zusammenspiel mit Managed Service Providern. Unternehmen schließen Service-Level-Verträge oder pauschalisierte Betriebsmodelle ab, um Planungssicherheit zu gewinnen. MSPs wiederum bauen ihre Leistungen auf den Strukturen ihrer Cloud- und Storage-Partner auf. Wenn dort transaktionsabhängige Gebühren dominieren, verschiebt sich das wirtschaftliche Risiko entlang der Wertschöpfungskette.

Kostensteigerungen wirken dann nicht unmittelbar, sondern indirekt und zeitverzögert. Sie werden häufig erst bei Vertragsverlängerungen oder Budgetanpassungen sichtbar. Für Unternehmen entsteht dadurch eine strukturelle Intransparenz: Die eigene Kalkulation basiert auf stabilen Servicepreisen, während sich im Hintergrund die Kostendynamik verändert. Die Bewertung von Cloud-Partnern muss daher auch die ökonomische Architektur hinter dem Serviceversprechen berücksichtigen.

Storage als strategischer Hebel

Im Storage-Bereich tritt diese Problematik besonders klar zutage. Backup-, Archiv-

und Recovery-Prozesse sind längst keine passiven Speicherfunktionen mehr, sondern integraler Bestandteil von Sicherheits-, Compliance- und Business-Continuity-Strategien. Mit wachsender Datenmenge und steigender KI-Intensität erhöht sich die Interaktionsdichte erheblich.



**DATENWACHSTUM
ALLEIN SCHAFFT KEINEN
WETTBEWERBSVORTEIL.**

Dr. Lennart Gaida, Director Strategy & Innovation, Impossible Cloud GmbH,
www.impossiblecloud.com

Wenn solche Prozesse vollständig in einem einzigen Plattform-Ökosystem verankert sind, entstehen implizite Abhängigkeiten – technisch, wirtschaftlich und organisatorisch. Datenportabilität mag formal gegeben sein, kann jedoch durch Gebührenmodelle oder strukturelle Bindungen faktisch eingeschränkt werden. Für IT-Entscheider bedeutet das, Storage nicht mehr als rein operative Infrastrukturkomponente zu betrachten, sondern als strategisches Element zur Sicherung von Kostenkontrolle und Handlungsfähigkeit. Eine zusätzliche, unabhängige Storage-Säule kann dabei nicht nur technische Redundanz schaffen, sondern auch ökonomische Diversifikation ermöglichen.

Resilienz und Souveränität als Governance-Prinzipien

Mit steigenden Datenmengen verlängern sich potenzielle Wiederherstellungszeiten, während regulatorische Anforderungen an Nachvollziehbarkeit und Auditierbarkeit wachsen. Resilienz wird damit zu

einer betriebswirtschaftlich relevanten Kennzahl. Verzögerungen oder eingeschränkte Steuerbarkeit im Krisenfall können unmittelbare finanzielle und reputative Auswirkungen haben.

Parallel dazu gewinnt digitale Souveränität an Bedeutung. Der Bitkom Cloud Report 2025 zeigt, dass viele deutsche Unternehmen ihre Abhängigkeit von außereuropäischen Anbietern kritisch bewerten. Souveränität bedeutet in diesem Kontext nicht Isolation, sondern Steuerungsfähigkeit. Sie entsteht durch transparente Kostenmodelle, klare Schlüsselverwaltung, realistische Datenportabilität und die Möglichkeit, alternative Anbieter in die Architektur zu integrieren. Gerade im Storage-Bereich können spezialisierte europäische Anbieter eine ergänzende Rolle spielen, indem sie Diversifikation ermöglichen und Lock-in-Strukturen reduzieren.

2026 als Prüfstein für die Cloud-Partnerstrategie

Vor diesem Hintergrund wird 2026 zu einem geeigneten Zeitpunkt, die eigene Cloud-Partnerstrategie systematisch zu überprüfen. Entscheidend ist nicht, wie stark das Datenvolumen wächst, sondern ob Architektur, Partnerstruktur und Kostenmechanismen aktiv gesteuert werden. IT-Entscheider sollten die gesamte Wertschöpfungskette analysieren: Welche Kostenmodelle werden bei steigender KI-Intensität dominant? Wo entstehen implizite Abhängigkeiten? Und bleibt die Datenarchitektur auch unter wachsender Last wirtschaftlich und organisatorisch tragfähig?

Datenwachstum allein schafft keinen Wettbewerbsvorteil. Erst wenn Unternehmen ihre Cloud- und Storage-Partner strategisch auswählen und strukturell diversifizieren, entsteht nachhaltige Wertschöpfung. 2026 wird zwar erneut ein Jahr rasant wachsender Datenmengen, entscheidend wird jedoch sein, wer die Steuerung über Kosten, Abhängigkeiten und Datenökonomie behält.

Dr. Lennart Gaida

UCC-Supply-Chain aus seiner Hand

VERTRIEBSKONSOLIDIERUNG SCHAFFT EINHEITLICHE PARTNERBETREUUNG

Die Gamma-Gruppe hat zum Jahresbeginn 2026 die Vertriebsstrukturen ihrer deutschen Tochtergesellschaften STARFACE, estos und Gamma Deutschland in der neugegründeten Organisation Gamma Sales zusammengeführt. Dr. Alexander Seyferth, Geschäftsführer von Gamma Sales, erläutert die Neuausrichtung und deren Auswirkungen auf Kunden und Channelpartner.

it management: Herr Dr. Seyferth, zum 1. Januar 2026 wurden im Zuge der Neustrukturierung des Vertriebs die ersten Änderungen für Ihre Partner ersichtlich. Warum starteten Sie mit der Zusammenführung just bei den Sales-Teams?

Dr. Alexander Seyferth: Sowohl STARFACE als auch estos und Gamma leben vom engen und vertrauensvollen Austausch mit ihren jeweiligen Partner-Communities. Die Übernahme hat bei den Partnern natürlich die Erwartung geschürt, von nun aus einer Hand über die Gesamtproduktpalette unterstützt zu werden. Dieser Bitte wollten wir so schnell wie möglich nachkommen. Es war uns daher ein Bedürfnis, die Partner als erstes ins Boot zu holen, damit diese möglichst früh von den Synergiepotenzialen profitieren können.

Gleichzeitig ist der Vertrieb auch der Bereich, wo die Effekte der Zusammenführung am deutlichsten spürbar sind. Lassen Sie uns kurz einen Blick auf die bisherigen Strukturen werfen: Der STARFACE-Vertrieb war in zehn Gebiete untergeteilt, Gamma in vier und estos in fünf. Das heißt: Die Partner kommunizierten mitunter mit drei verschiedenen Ansprechpartnern, und im Fall von Gamma und estos

mussten die Vertriebsmitarbeiter riesige Gebiete managen. Das war schlichtweg ineffizient, sowohl für unsere Partner als auch für uns.

it management: Und wie ist die neugegründete Vertriebsorganisation Gamma Sales strukturiert?

Dr. Alexander Seyferth: Wir haben die neue Situation zur weiteren Optimierung genutzt und versucht, für unsere Partner passgenaue Gebiete zu definieren, die wir hinsichtlich ihrer geografischen Ausdehnung und der Anzahl an Partnern möglichst vergleichbar gehalten haben. Das funktioniert natürlich nicht hundertprozentig – aber wir haben es am Ende geschafft, Deutschland in 16 relativ gleiche Gebiete aufzuteilen, um die sich jeweils ein Tandem aus einem Außen- und einem Innendienstler kümmert. Allein aus STARFACE-Sicht haben sich die Gebiete

dadurch bereits um 35 Prozent verkleinert. Der Außendienst verbringt also wesentlich weniger Zeit auf der Straße und kann die neuen Freiräume nutzen, um die Partner gezielt beim Endkunden zu unterstützen.

Neben dem Vertrieb koordiniert Gamma Sales auch die Bereiche Presales und Customer Care, wobei wir speziell im Support-Bereich noch auf die technische Grundlage in Form eines einheitlichen Ticketsystems warten. Ab Sommer werden wir dann daran arbeiten, auch den Service aus einer Hand anbieten zu können.

it management: „Aus einer Hand“ ist ein gutes Stichwort: Ihre Vertriebs-Tandems dienen nun als One-Stop-Shop für drei vormals unabhängige Lösungsportfolios und müssen sich dementsprechend auch mit den jeweiligen Produkten auskennen. Wie gelingt das?





Dr. Alexander Seyferth: Das war tatsächlich eine unserer größten Herausforderungen. Daher haben wir bereits im Juli damit begonnen, eine wöchentliche Schulungsreihe aufzusetzen – lange bevor die Tandems feststanden. Dabei werden unsere Vertriebsmitarbeiter jeden Freitag in kompakten „Wissenssnack“-Formaten in allen Produkten geschult. Natürlich können wir nicht garantieren, dass sie bereits auf jede Frage die perfekte Antwort haben. Hier bitten wir unsere Partner um Verständnis und etwas Geduld – und verweisen im Zweifelsfall auf die Presales- und Customer Care-Abteilungen. Wir sind aber optimistisch, dass der Knowhow-Transfer bis zum zweiten Quartal abgeschlossen sein wird.

Damit schaffen wir auch die Grundlage, unseren Partnern künftig die gesamte UCC-Supply-Chain aus einer Hand anzubieten. Jeder Partner, der unser gesamtes Portfolio vertreiben möchte, kann seine Kunden damit also ganzheitlich unterstützen – und dank umfangreicher Up- und Cross-Selling-Potenziale sein eigenes Business nachhaltig stärken.

it management: Auf dem Gamma-verse in Hof haben Sie von einem neuen ‚More Business Team‘ berichtet, das Partner gezielt unterstützen soll. Was hat es damit auf sich?

Dr. Alexander Seyferth: Das Team existiert bereits und ist das Resultat aus vielen Gesprächen mit unserer Community. Hier ein Beispiel: Wir weisen regelmäßig darauf hin, dass viele STARFACE-Anwender noch mit veralteten Plattform-Versionen telefonieren und dementsprechend nicht auf die neuesten Features zugreifen können. Wir haben uns lange gefragt, warum das so ist. Bis wir von einigen technisch orientierten Partnern erfahren haben, dass diese schlichtweg nicht die Kapazitäten haben, systematisch an ihrem Bestand zu arbeiten.

An dieser Stelle setzen wir jetzt gezielt mit dem More Business Team an. Gemeinsam mit unseren Partnern analysieren wir

MIT DER UMSTRUKTURIERUNG SCHAFFEN WIR DIE GRUNDLAGE, UNSEREN PARTNERN KÜNFTIG DIE GESAMTE UCC-SUPPLY-CHAIN AUS EINER HAND ANZUBIETEN.

Dr. Alexander Seyferth,
Geschäftsführer, Gamma Sales GmbH,
www.gammacommunications.de/

den Kundenbestand und erörtern interdisziplinär, wo ungenutzte Geschäftspotenziale gehoben werden können. Dafür können Partner entweder aktiv auf uns zugehen, oder wir laden sie ein. Das bisherige Feedback war übrigens durchweg positiv. Viele Partner haben uns mit eigenen Ideen überrascht, die sie mithilfe des More Business Teams umsetzen wollen!

it management: Eine weitere Änderung betrifft die bisherigen Partnerprogramme der drei Schwesterunternehmen, die nun zusammengeführt werden. Wie sieht dies in der praktischen Umsetzung aus?

Dr. Alexander Seyferth: Dazu möchte ich zunächst erst einmal festhalten, dass wir nach dem Motto „alles kann, nichts muss“ vorgehen. Sprich: Wir zwingen niemanden, 2026 am neuen, gemeinsamen Partnerprogramm teilzunehmen. Aber natürlich laden wir dazu ein, indem wir übergreifende Umsätze belohnen.

Konkret bedeutet dies, dass alle bestehenden Verträge ihre Gültigkeit behalten. Zusätzlich gibt es neuerdings den Gamma Sales Mantelvertrag, der bestehende Verträge integriert. Im Rahmen des neuen Partnerprogramms werden die

übergreifenden Umsätze schließlich aufaddiert und entsprechend gewürdigt – etwa über das diesjährige, gemeinsame Incentive. Um am neuen Programm teilzunehmen, können sich die Partner ganz einfach in ihrem jeweiligen Partnerportal anmelden und digital beitreten.

it management: Wie steht es um die unmittelbare Zukunft von Gamma Sales – welche nächsten Meilensteine planen Sie an?

Dr. Alexander Seyferth: Wie vorhin schon angeschnitten, arbeiten wir derzeit an der Zusammenlegung der Customer Care-Abteilungen. Dafür bauen wir ein einheitliches Ticketsystem und eine zentrale Telefonhotline auf, um für einen geringeren Koordinationsaufwand bei unseren Partnern und einer schnelleren Problemlösung zu sorgen. Um die Support-Prozesse zusätzlich zu beschleunigen, werden wir sie mittelfristig KI-gestützt weiter optimieren.

Ein weiterer Meilenstein, der unmittelbar bevorsteht, ist unsere ‚Grow Together Tour 2026‘ die die bisherigen Roadshow-Formate von STARFACE, estos und Gamma ablöst. Mit diesem Event, das im ersten und zweiten Quartal 2026 in neun Städten im DACH-Raum stattfindet, erhalten Partner einen Überblick über unser gesamtes Produkt- und Lösungsportfolio. Darüber hinaus ist die Grow Together Tour natürlich auch die ideale Möglichkeit, offene Fragen zu Gamma Sales, zur Neuaufteilung der Partnergebiete oder zum neuen Partnerprogramm zu stellen.

it management: Herr Dr. Seyferth, wir danken Ihnen für das Gespräch.





Smarte Telefonie unter Kontrolle

KI IN DER TELEKOMMUNIKATION KANN ALLES –
ABER DARF SIE DAS AUCH?

KI hält zunehmend in der Business-Kommunikation nicht mehr nur „als Feature“ Einzug, sondern als neue Schicht über Sprach- und Kollaborationsprozessen: automatische Transkription und Zusammenfassung, intelligente Rufverteilung, kontextbasierte Assistenz, Qualitäts- und Compliance-Checks, Betrugs- und Deepfake-Erkennung. Was auf den ersten Blick nach mehr Komfort klingt, entspricht in der Praxis einer

Entscheidung über Vertrauen, Risiko und Differenzierung – und damit über Wettbewerbsfähigkeit. Denn sobald KI Gespräche analysiert, Inhalte ableitet oder Entscheidungen vorschlägt (z. B. Eskalationsstufen, Priorisierungen, Routing), verschieben sich die entscheidenden Fragen weg von „Kann das Tool das?“ hin zu „Dürfen wir das?“, „Können wir es nachweisen?“ und „Wer kontrolliert die KI?“.

Genau an dieser Stelle werden Governance, Transparenz und Datensouveränität zu echten Differenzierungsmerkmalen – insbesondere für europäische Unter-

nehmen, die sich gegenüber Compliance-Anforderungen, geopolitischen Abhängigkeiten und Kundenanforderungen absichern müssen.

Der neue Wert von Vertrauen

Telefonie war lange ein Transportsystem: Sprachpakete rein, Sprachpakete raus. Mit KI wird Telefonie entscheidungsrelevant. Aus Gesprächen werden Daten, aus Daten werden Handlungsempfehlungen – und in manchen Fällen automatisierte Routinen. Governance bedeutet hier nicht Bürokratie, sondern Betriebssicherheit: klare Regeln, Rollen, Kontroll-



punkte und Nachweise. In einer KI-gestützten Kommunikation ist Governance die Voraussetzung, um Innovation skalierbar und auditierbar zu machen – in jeder Branche, in jeder Abteilung einer Organisation. Somit rücken die IP-Telefone wieder ins Zentrum der Debatte.

KI-Kommunikationsfunktionen laufen nämlich nicht im luftleeren Raum. Sie hängen an Signalketten: vom Endgerät über Netz und PBX/UC-Plattform bis hin zu KI-Services, CRM und Archivsystemen. Wenn ein Glied dieser Kette unsicher, intransparent oder schlecht steuerbar ist, wird das gesamte Setup fragil. So agieren IP-Telefone als „authentischer“ Kommunikationsendpunkt: Gerade in Contact-Centern, Empfangsbereichen, der Produktion, der Logistik, dem Healthcare oder der Hospitality sind IP-Telefone oft zuverlässiger und kontrollierbarer als BYOD-Smartphones oder gemischte Softphone-Landschaften. Durch zentrale Provisionierung, Zertifikate, Rollenprofile sowie nachvollziehbare Standort- und Nutzerwechsel („Hot Desking“)

sind sie Governance-fähig und lassen sich mit entsprechenden Sicherheitsrichtlinien in Security- und Device-

Management-Prozesse integrieren: Ob der Sprachverkehr verschlüsselt ist (SIP-TLS/SRTP), ob das Logging sauber erfolgt, ob Firmware-Integrität gesichert ist, ob ein Gerät „mitlauschen“ könnte: All das ist Teil der Datensouveränität.

Wer also „KI in der Kommunikation“ einführt, aber die Telefonie-Endgeräte als Nebensache behandelt, baut eine Governance auf Sand.

Front Desk:

Vertrauen beginnt am Empfang

Am Empfang laufen sensible Informationen zusammen: Besucher, Termine, Lieferungen, Notfälle. KI kann hier Gespräche



transkribieren, Anfragen kategorisieren oder automatisch Tickets erstellen. Ohne klare Governance bleibt das jedoch riskant. Mit professionellen IP-Telefonen wie der Snom-D8xx-Serie

lässt sich der Front Desk sauber absichern: eine verschlüsselte Sprachübertragung (SIP-TLS/SRTP), eine zentrale Provisionierung und eine rollenbasierte Nutzung verhindern Fehlbedienungen sowie unkontrollierte Datenabflüsse. Gleichzeitig bleibt transparent nachvollziehbar, wann welche KI-Funktion aktiviert wurde – ein entscheidender Pluspunkt für Compliance und Vertrauen.

Logistik & Produktion: Robuste

Kommunikation statt Schatten-IT

In Lager- und Produktionsumgebungen setzen Teams häufig auf DECT-fähige Snom-Telefone, weil sie stabil, mobil und einfach zu bedienen sind. Wird hier KI eingesetzt – etwa zur automatischen Dokumentation von Lieferungen oder zur Priorisierung von Störmeldungen –, braucht es eine klare Datensouveränitätsstrategie. Eine Edge-nahe Verarbeitung, definierte Speicherfristen und eine transparente Protokollierung stellen sicher, dass betriebliche Daten nicht unkontrolliert in externe Clouds wandern. Das IP-Telefon bleibt dabei der verlässliche, souveräne Endpunkt in einer zunehmend intelligenten Prozesskette.

Contact-Center: KI braucht klare Leitplanken

Im Contact-Center entfaltet KI den größten Mehrwert – von Live-Zusammenfassungen über Coaching bis hin zur Betrugserkennung. Zum Beispiel wenn sie erkennt, dass ein Anrufer wiederholt verschiedene Agenten kontaktiert, um durch Dringlichkeit und Verwirrung an Zahlungs- oder Kontodaten zu gelangen. Hier ist das Risiko am höchsten. Standardisierte Snom-Endgeräte helfen, klare Sicherheits- und Governance-Grenzen zu ziehen: eindeutige Nutzeridentitäten, sichere Firmware-Updates und nachvollziehbare Call-Flows reduzieren Fehler-

quellen und erleichtern Audits. Entscheidend ist nicht nur, was die KI kann, sondern dass Unternehmen jederzeit erklären können, auf welcher Datenbasis sie arbeitet und wer Zugriff hat.

Smart Working: Souveränität auch außerhalb des Büros

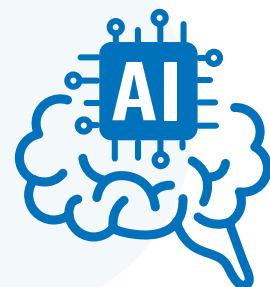
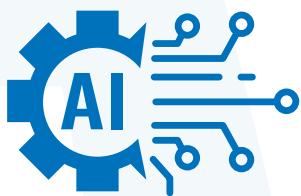
Hybrides Arbeiten verlagert Kommunikation ins Homeoffice – ohne Governance drohen Insellösungen. Professionelle IP-Telefone mit zentralem Management ermöglichen konsistente Sicherheitsstandards unabhängig vom Standort. KI-gestützte Funktionen wie Meeting-Zusammenfassungen oder automatische CRM-Updates bleiben dabei kontrollierbar: Unternehmen bestimmen Region, Speicherort und Nutzungszweck der Daten. So wird Flexibilität mit echter Datensouveränität verbunden.

Fazit

KI-gestützte Kommunikation wird 2026 nicht primär über Funktionslisten gewonnen, sondern über Vertrauen und Nachweisbarkeit. Governance, Transparenz und Datensouveränität werden zu Verkaufsargumenten, weil Kunden, Regulatorik und interne Stakeholder genau dort hinschauen.

Für Anbieter und Hersteller im Umfeld von IP-Telefonie bedeutet das: IP-Telefone sind nicht nur „das Device am Tisch“, sondern ein Teil der Sicherheits- und Governance-Kette. Wer KI-Kommunikation anbietet und gleichzeitig eine robuste, standardbasierte und souverän betreibbare IP-Telefonie-Basis liefert, kann sich klar differenzieren: weniger Risiko, bessere Compliance-Story – und am Ende eine überzeugendere Customer-Experience.

www.snom.com



Vom KI-Hype zur produktiven Realität

WARUM UNTERNEHMEN JETZT AUF OPEN-SOURCE KI-PLATTFORMEN SETZEN SOLLTEN

Der Einsatz von KI nimmt in deutschen Unternehmen spürbar Fahrt auf, doch zwischen Experimenten und sinnvoller Anwendung besteht weiterhin eine deutliche Lücke. Wie der EPAM AI Report verdeutlicht, ist Deutschland international führend bei Proofs of Concepts sowie bei teaminternen und prozessbezogenen KI-Einsätzen, während der Einsatz in kundenbezogenen Anwendungen deutlich zurückhaltender erfolgt. Dieses Vorge-

hen spricht für eine innovationsfreudige, zugleich aber vorsichtige Herangehensweise.

Gerade diese Zurückhaltung macht sichtbar, wo viele Unternehmen aktuell stehen. Trotz zahlreicher Initiativen und erster messbarer Effekte bleibt der Schritt von internen Experimenten hin zu skalierter, produktiver Nutzung oft aus. Die Studienergebnisse zeigen, dass sich viele Organisationen als fortgeschritten im Umgang mit KI einschätzen, nur ein kleiner Teil die Technologie jedoch bereits als strategischen Hebel nutzt oder in größerem Umfang operationalisiert hat. Damit rückt eine zentrale Frage in den Fokus, die über einzelne Technologien hinausgeht: Wie gelingt der Übergang vom KI-Hype zur produktiven Realität in Unternehmen?

Doch die technischen Hürden sind nur die halbe Wahrheit. Organisatorisch fehlen oft Governance-Strukturen, klare Verantwortlichkeiten und qualifizierte Mitarbeitende. Laut der internationalen Ergebnisse der EPAM Studie sehen 22 Prozent der Befragten fehlende Kompetenz als größte Herausforderung. Das führt zu unsicheren Entscheidungen, Verzögerungen und Projekten, die in Abstimmungsschleifen stecken bleiben.

Hinzu kommt eine strategische Fehlannahme: KI wird häufig als Tool für punktuelle Probleme betrachtet. Das Ergebnis sind isolierte Projekte ohne gemeinsame Basis. Erst wenn KI als Bestandteil einer übergreifenden Systemarchitektur verstanden wird – statt als lose Sammlung einzelner Initiativen – entsteht eine Basis für Skalierung und nachhaltigen Wert.



”

DAS WICHTIGSTE FÜR DEN ERFOLGREICHEN EINSATZ VON KI IM UNTERNEHMEN IST EIN GRUNDLEGENDER PERSPEKTIVWECHSEL.

Matthew Gorelik, Manager
Business Consulting, EPAM Systems Inc.,
www.epam.de

Die unterschätzten Hürden auf dem Weg zur skalierten KI

Ambitionierte KI-Pläne scheitern in der Praxis häufig an grundlegenden Voraussetzungen: Veraltete Tech-Stacks, fragmentierte Daten und unzureichende Cloud-Infrastrukturen verhindern, dass Pilotprojekte skalieren. In regulierten Branchen kommt der Schutz sensibler Daten hinzu – ohne robuste Sicherheitsmechanismen dürfen viele Anwendungen nicht in den operativen Betrieb.

Vom Pilotprojekt zur produktiven Plattform

Entscheidend ist deshalb nicht die Anzahl der Anwendungen, sondern eine klare Reihenfolge strategischer Schritte. Am Anfang steht eine verlässliche Governance. Verantwortlichkeiten, Datenrichtlinien sowie Anforderungen an Sicherheit und Qualität müssen eindeutig definiert sein – ohne diesen Rahmen bleibt jede KI-



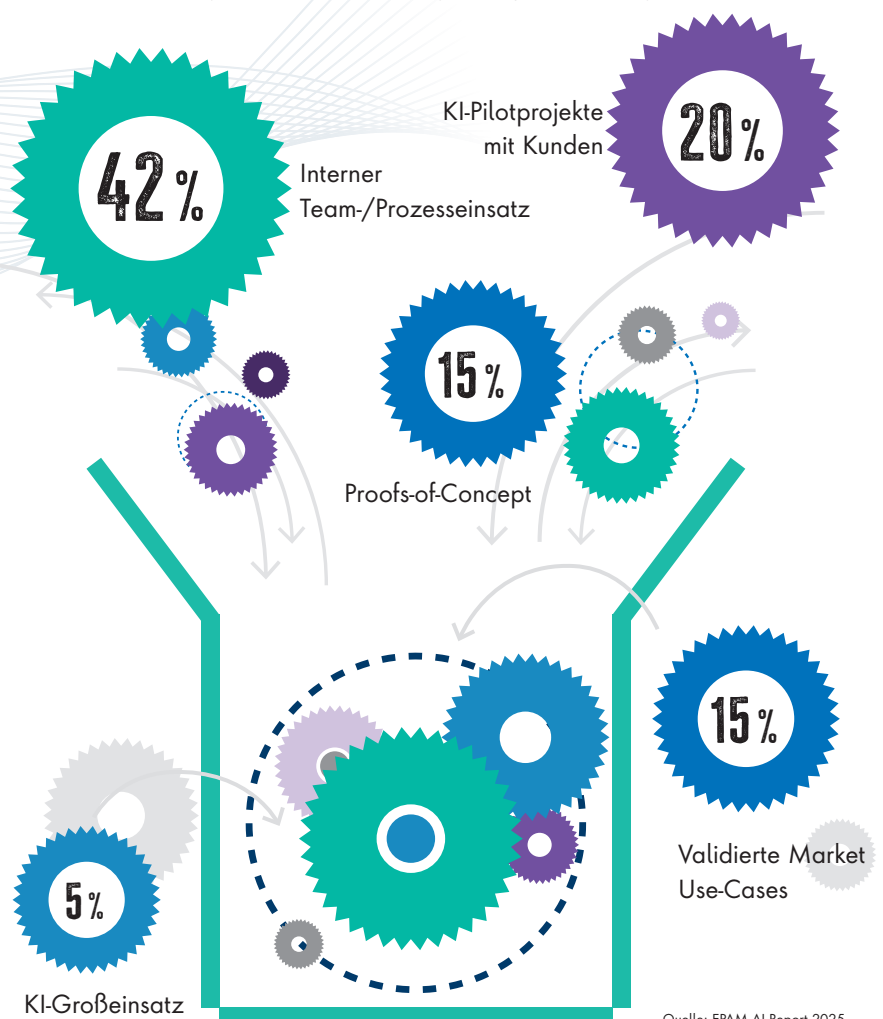
Lösung fragil. Darauf aufbauend braucht es eine technologische Architektur, die unterschiedliche Modelle unterstützt, ohne in Abhängigkeiten zu führen. Modellagnostische Plattformen schaffen die nötige Flexibilität und ermöglichen es, neue Entwicklungen schnell zu integrieren.

Ebenso zentral ist der Zugang zu Daten: Erst wenn strukturierte und unstrukturierte Informationen konsistent zusammengeführt werden, lassen sich verlässliche Workflows und nachvollziehbare Entscheidungen aufsetzen. Transparenz, Datenqualität und klare Schnittstellen sind dafür unverzichtbar.

Sind diese Grundlagen geschaffen, können agentenbasierte Workflows sinnvoll eingeführt werden. Moderne KI soll Prozesse nicht nur unterstützen, sondern aktiv steuern. Agenten verbinden Schritte, schaffen Reproduzierbarkeit und erhöhen die Steuerbarkeit komplexer Abläufe.

Damit KI nicht ausschließlich in der IT verankert bleibt, müssen Fachbereiche aktiv einbezogen werden. Niedrigschwellige Werkzeuge für schnelles Prototyping ermöglichen es Mitarbeitenden, eigene Ideen zu testen und praktikable Automatisierungen selbst zu identifizieren. So entsteht aus vielen Einzelinitiativen eine produktive, skalierbare Plattformlandschaft.

AKTUELL KI-IMPLEMENTIERUNG NACH ANWENDUNGSBEREICH



Quelle: EPAM AI Report 2025

Open-Source-Plattformen als Schlüssel zur Skalierung

Leicht zugängliche Open-Source KI-Plattformen können einen strukturellen Ansatz für den Weg vom Pilotprojekt zum Unternehmen mit KI-zentrierter Architektur bieten. Sie verknüpfen Daten, Modelle und Prozesse in einem einheitlichen Rahmen, unterstützen verschiedene LLMs flexibel und ermöglichen transparente, reproduzierbare sowie sichere Workflows. Aus vielen Einzellösungen entsteht so ein belastbares Gesamtsystem, das den Übergang von der Experimentierphase in die produktive Nutzung erheblich erleichtert.

Ein Beispiel für einen solchen Plattformansatz ist DIAL, eine von EPAM entwickelte Open-Source KI-Plattform, die ohne Lizenzkosten verfügbar ist. Sie unterstützt die Orchestrierung unterschiedlicher Sprachmodelle, agentenbasierter Abläufe und nachvollziehbarer Entscheidungslogiken innerhalb einer gemeinsamen Architektur. Die modellagnostische Ausrichtung reduziert Abhängigkeiten und erlaubt hybride Architekturen, die sich flexibel an technische Entwicklun-

gen anpassen lassen. Ergänzend bietet die Plattform Mechanismen, um heterogene Daten strukturiert aufzubereiten und einfache Anwendungen prototypisch umzusetzen.

DIAL wurde so konzipiert, dass Unternehmen die volle Kontrolle und Eigentümerschaft über ihr KI-Ökosystem behalten. Die modulare Architektur ermöglicht die Integration externer Tools und Anwendungen und stellt Werkzeuge bereit, um KI-Agenten zu entwerfen, bereitzustellen, zu überwachen und Kosten zu kontrollieren. Telemetriefunktionen unterstützen dabei, Nutzerverhalten zu analysieren, Akzeptanz zu messen und Weiterentwicklungen gezielt auf reale Bedarfe auszurichten.

Beispielsweise ist DIAL eXpressive Logic (XL) ein Tool, das DIAL und agentenbasierte KI nutzt, um die Interaktion nicht-technischer Anwender mit Daten zu vereinfachen und die Datenanalyse für alle zugänglich, transparent und kollaborativ zu gestalten. Kleine und mittlere Unternehmen können Daten aus strukturierten CSV-

Datensätzen in Alltagssprache abfragen und gleichzeitig die Ergebnisse ihrer Analysen systematisch validieren. Dies macht datengestützte Entscheidungen einfacher, zuverlässiger und transparenter.

Auch Altera Digital Health konnte von dem Plattformansatz in der Praxis profitieren. Das Unternehmen stand vor der Herausforderung, stark fragmentierte Legacy-Systeme zusammenzuführen, in denen relevante, aber schwer zugängliche Daten vorlagen. Als Teil der Zusammenarbeit nutzte EPAM die DIAL-Plattform als technische Basis, um spezifische KI-Agenten für definierte Anwendungsfälle zu entwickeln.

Diese kamen unter anderem in der Weiterentwicklung des Produkts Note+ zum Einsatz, das an das bestehende EHR-/EMR-System gekoppelt ist. Parallel dazu wurden Mitarbeitende befähigt, eigenständig weitere Agenten zu entwickeln. Ergänzend etablierte EPAM ein Rahmenwerk zur Bewertung des wirtschaftlichen Nutzens, um den Beitrag bestehender und zukünftiger KI-Initiativen transparent zu erfassen und Investitionsentscheidungen zu unterstützen.

Warum KI als System Wirkung entfaltet

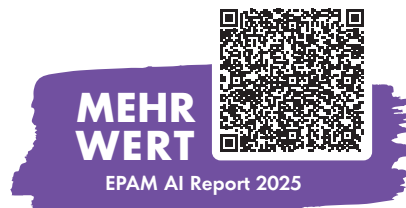
Das Wichtigste für den erfolgreichen Einsatz von KI im Unternehmen ist ein grundlegender Perspektivwechsel: KI sollte nicht als Sammlung einzelner Projekte verstanden werden, sondern als zusammenhängendes System. Erst wenn Unternehmen den Schritt weg von isolierten Lösungen hin zu einer offenen, integrierten Plattformarchitektur gehen, entsteht die Grundlage für nachhaltigen, skalierbaren und sicheren KI-Einsatz. Dies kann sich dann in echtem geschäftlichem Nutzen widerspiegeln.

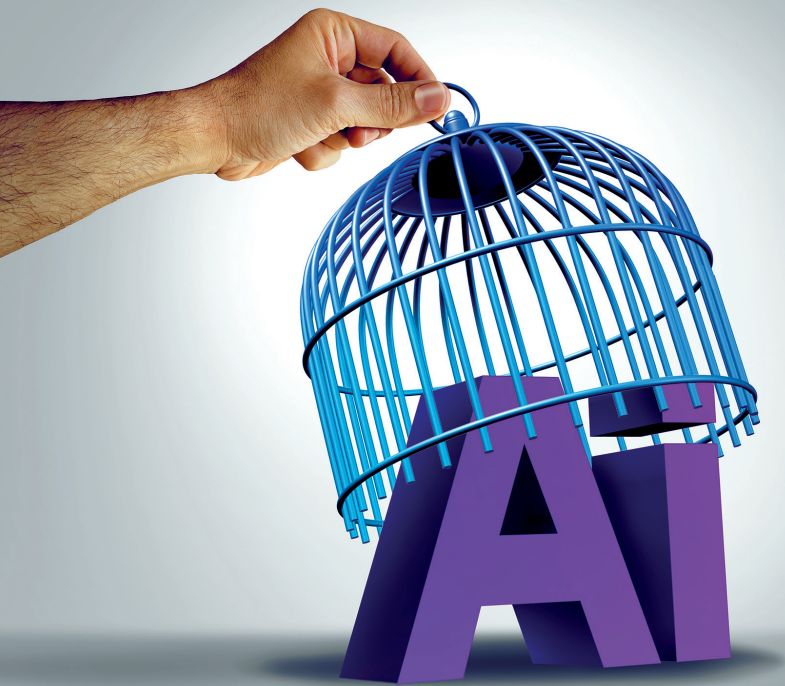
Matthew Gorelik

TOP 3 ZIELE FÜR DIE KI-EINFÜHRUNG



Quelle: EPAM AI Report 2025





OpenClaw

EIN ENTERPRISE-ALBTRAUM?

Bei OpenClaw handelt sich um einen kostenlosen KI-Agenten ohne jegliche Einschränkungen. Sicherheit war kein Teil des ursprünglichen Designs, also kein Sandboxing, voller Zugriff auf Computer, Dateien, E-Mail, Kalender, Messaging-Anwendungen und vieles mehr.

Erstaunlicherweise scheint das die meisten Leute nicht zu stören. OpenClaw zeigt die Leistungsfähigkeit eines uneingeschränkten Agenten.

Das wachsende Ökosystem

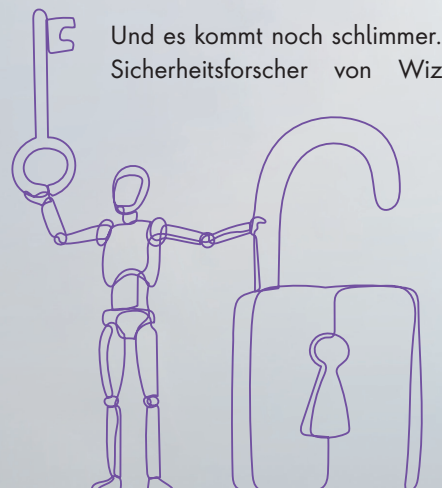
Nach und nach sind weitere Fähigkeiten („Skills“) hinzugekommen und auf ClawHub, der öffentlichen Skills Registry des Agenten geteilt. Das Cybersicherheitsunternehmen Snyk hat in einer umfassenden Untersuchung von 3.984 Skills festgestellt, dass die Agent Skills 13,4 Prozent kritische Sicherheitsprobleme aufwiesen, darunter Möglichkeiten zur Verbreitung von Malware, Diebstahl von Zugangsdaten und für Prompt Injection-Angriffe. Die Sicherheitsforscher identifizierten 76 bestätigte bössartige Payloads, von denen acht zum Zeitpunkt der Veröffentlichung noch auf ClawHub verfügbar waren. Trend Micro stellte in der oben erwähnten Untersuchung klar, dass diese

Risiken mit dem Paradigma der KI-Agenten zusammenhängen. Token Security aber stellte fest, dass bereits 22 Prozent seiner Unternehmenskunden Mitarbeitende haben, die OpenClaw ohne IT-Genehmigung verwenden.

Moltbook:

Ein soziales Netzwerk für Bots

Seit Kurzem gibt es nun Moltbook, ein soziales Netzwerk für OpenClaw-Bots, in dem diese chatten, ihre Fähigkeiten teilen und auch austauschen können. Aus technischer Sicht ist der unbegrenzte Austausch beeindruckend, doch darum, dass viele Skills bössartige Fähigkeiten enthalten, kümmert sich niemand..



Und es kommt noch schlimmer. Sicherheitsforscher von Wiz

entdeckten eine schlecht konfigurierte Supabase-Datenbank, die 1,5 Millionen API-Schlüssel, 35.000 E-Mail-Adressen und private Nachrichten zwischen Agenten offenlegte, von denen einige OpenAI-API-Schlüssel im Klartext enthielten. Die „1,5 Millionen Agenten“ der Plattform wurden in Wirklichkeit von etwa 17.000 Personen betrieben, ein Verhältnis von 88:1. Das Ganze wurde ohne angemessene Sicherheitskontrollen „vibe-coded“.

Größte Sorge:

Die Nachfrage aus Unternehmen

Die größte Sorge ist die Nachfrage von Unternehmen, OpenClaw in größerem Umfang einzusetzen. Berichte über seine Fähigkeiten erscheinen in den Mainstream-Medien wie New York Times, NBC und Forbes. Führungskräfte sehen darin einen Wettbewerbsvorteil und ignorieren die Sicherheitsrisiken, die den meisten nicht bewusst sind oder bewusst ausgeblendet werden.

Wenn ähnliche KI ohne Einschränkungen in Unternehmen mit vollem Zugriff auf Unternehmenssysteme eingesetzt wird, könnte es katastrophal werden.

Genau das hat Token Security demonstriert: Ein Mitarbeiter verbindet OpenClaw mit dem Slack des Unternehmens und plötzlich fließen vertrauliche Umsatzzahlen über einen nicht verwalteten KI-Agenten auf einem privaten Gerät zu WhatsApp, komplett an DLP-Kontrollen und Audit-Trails vorbei.

Fazit

Unternehmen, die Enterprise-Versionen einsetzen, priorisieren offenbar Wettbewerbsvorteile gegenüber Sicherheitsaspekten. Gehostete OpenClaw-Dienste für Unternehmen sind bereits verfügbar. Die Geschwindigkeit, mit der sich die Technologie verbreitet, steht im starken Kontrast zu bestehenden Sicherheitsbedenken. Das Ausmaß der Adoption erfolgt deutlich schneller als bei vergleichbaren Technologien in der Vergangenheit.

www.trendmicro.com

NextGen CPUs für Multi-Tenant-KI

WAS JETZT ANDERS GEDACHT WERDEN MUSS

Multi-Tenant-KI verspricht Skalierung und Wirtschaftlichkeit – doch die Realität sieht oft anders aus. Schwankende Latenzen, unvorhersehbarer Durchsatz und überdimensionierte Kapazitäten kosten Unternehmen Geld und untergraben das Versprechen der Cloud-Ökonomie. Wir sprachen mit Jeff Wittich, Chief Product Officer von Ampere, darüber, dass Software-Isolation allein nicht ausreicht und wie Next-Gen-Prozessoren geteilte KI-Umgebungen planbar machen.

it management: Der Begriff Multi-Tenant-Cloud ist mittlerweile geläufig. Doch auch Multi-Tenant-KI findet immer öfter Gehör. Was steckt hinter diesem Wandel?

Jeff Wittich: Die Antwort ist einfach: Skalierung und Wirtschaftlichkeit. KI ist nicht mehr ein einzelner Workload, der für einen einzelnen Nutzer isoliert läuft. In Produktionsumgebungen spielen sich mehrere unabhängige Inferenzaufgaben parallel zu API-basierten Webservern, Datenbanken, nutzerorientierten Services und anderen KI-Modellen ab. Diese Prozesse geschehen meist in geteilten Infrastrukturen. Um allerdings für eine skalierbare, nachhaltige KI zu sorgen, müssen Plattformen viele Tenants gleichzeitig sicher und effizient bedienen können – mit vorhersehbarer Performance und Kosten.

Die Herausforderung ist jedoch, dass die meisten Legacy-Server-CPU's nie für diese Realität entwickelt wurden. Sie wurden für Spitzenleistungen in Einzelanwendungen optimiert, nicht für Konsistenz unter geteilten Workloads.



DIE BRANCHE ERKENNT AN, DASS MULTI-TENANT-KI KEINE VORÜBERGEHENDE PHASE IST – SIE IST DAS DOMINIERENDE ZUKUNFTS-MODELL.

Jeff Wittich, Chief Product Officer,
Ampere Computing LLC,
www.amperecomputing.com

it management: Was passiert, wenn KI-Inferenzen auf Alt-CPU's in Multi-Tenant-Umgebungen laufen?

Jeff Wittich: Sie bringen Variabilität mit. Wenn mehrere Workloads ihre Ressourcen im Prozessor teilen, entstehen Interferenzen. Die Latenz schwankt. Der Durchsatz wird unvorhersehbar. Betreiber kompensieren das, indem sie die Kapazität überdimensionieren, nur um SLAs zu erreichen.

Dieses Vorgehen ist teuer und untergräbt das Versprechen der Cloud-Ökonomie. Das System mag auf dem Papier effizient

wirken, aber in der Realität zahlen Unternehmen für den Headroom statt für die Rechenleistung.

it management: Einige Plattformen versuchen, dies auf Softwareebene zu lösen. Warum reicht das nicht?

Jeff Wittich: Software-Isolation kann helfen, ist aber grundsätzlich reaktiv. Wenn die Hardware selbst Variabilität wie dynamische Frequenzänderungen, geteilte Ausführungspfade und Konkurrenz um interne Ressourcen einführt, kann Software nur begrenzt helfen.

An einem gewissen Punkt muss Vorhersehbarkeit in der Architektur durchgesetzt werden. Andernfalls werden ständig Symptome gemanagt, anstatt die eigentliche Ursache anzugehen.

it management: Wie sieht gutes Hardware-Design für Multi-Tenant-KI dann aus?

Jeff Wittich: Es beginnt mit strikter Isolation. Das bedeutet, pro physischen Kern ein Thread. Dadurch kommt es nicht zum simultanen Multithreading oder internen Konflikten. Denn jede Anfrage wird nach und nach kontinuierlich ausgeführt. Auch die Taktfrequenz ändert sich nicht während des laufenden Vorgangs und keine Ressourcen werden im falschen Moment „gestohlen“.

Zusätzlich muss eine ausreichende Speicherbandbreite diese Vorhersehbarkeit sichern, damit Workloads voll ausgelastet stabil bleiben. Trifft dies alles zu, verhält sich die Inferenz gleich, egal ob

das System nur gering oder vollständig ausgelastet ist.

it management: Wie sollten Chips entwickelt werden, um diesem Bedarf gerecht zu werden?

Jeff Wittich: Neue CPU-Generationen sollten so entwickelt werden, dass sie eine reproduzierbare, vertrauenswürdige Leistung auf realen, geteilten KI-Plattformen bieten. Unser neuer AmpereOne M-Prozessor beispielsweise wurde genau für diese Art von Multi-Tenant-Umgebung entwickelt. Jeder Kern betreibt ohne Ausnahme einen einzelnen Thread. Zwischen den Workloads gibt es keinen gemeinsamen Execution State, was auf Prozessorbene den Noisy-Neighbor-Effekt eliminiert.

Die neue Generation kombiniert diese Isolation mit ausreichender Speicherbandbreite – 12 DDR5-Kanälen. Dadurch können Inferenz-Workloads auch dann kontinuierlich eingespeist werden, wenn viele Tenants gleichzeitig laufen. Das Ergebnis ist eine konstant vorhersehbare Latenz und ein gleichbleibender Durchsatz.

it management: Welche Möglichkeiten eröffnet diese Vorhersehbarkeit den Nutzern?

Jeff Wittich: Zunächst ändert sich die Arbeitsweise in Teams. Kapazitätsplanung wird messbar statt wahrscheinlichkeitsbasiert.

Infrastrukturbudgets brauchen keine versteckten Puffer „für alle Fälle“. Preismodelle werden klarer, da die Leistung unter Last nicht schwankt.

Des Weiteren wirkt sich die Vorhersehbarkeit auf Sicherheit und Compliance aus. Sind Workloads wirklich isoliert, verringert sich das Risiko von Side-Channel-Verhalten zwischen Tenants. Auch Ingenieure profitieren, da sie nun weniger Zeit für Störungen aufwenden müssen, und mehr Zeit haben, Modelle und Nutzererfahrungen zu verbessern.

it management: Wird sich der Ansatz in der gesamten Branche durchsetzen?

Jeff Wittich: Ja, und das ist ein wichtiger Punkt. Die Branche erkennt an, dass Multi-Tenant-KI keine vorübergehende Phase ist – sie ist das dominierende Zukunftsmodell. Mit dieser Erkenntnis rücken bei Prozessoren nicht mehr Spitzenwerte, son-

dern stabile und berechenbare Leistung in den Fokus.

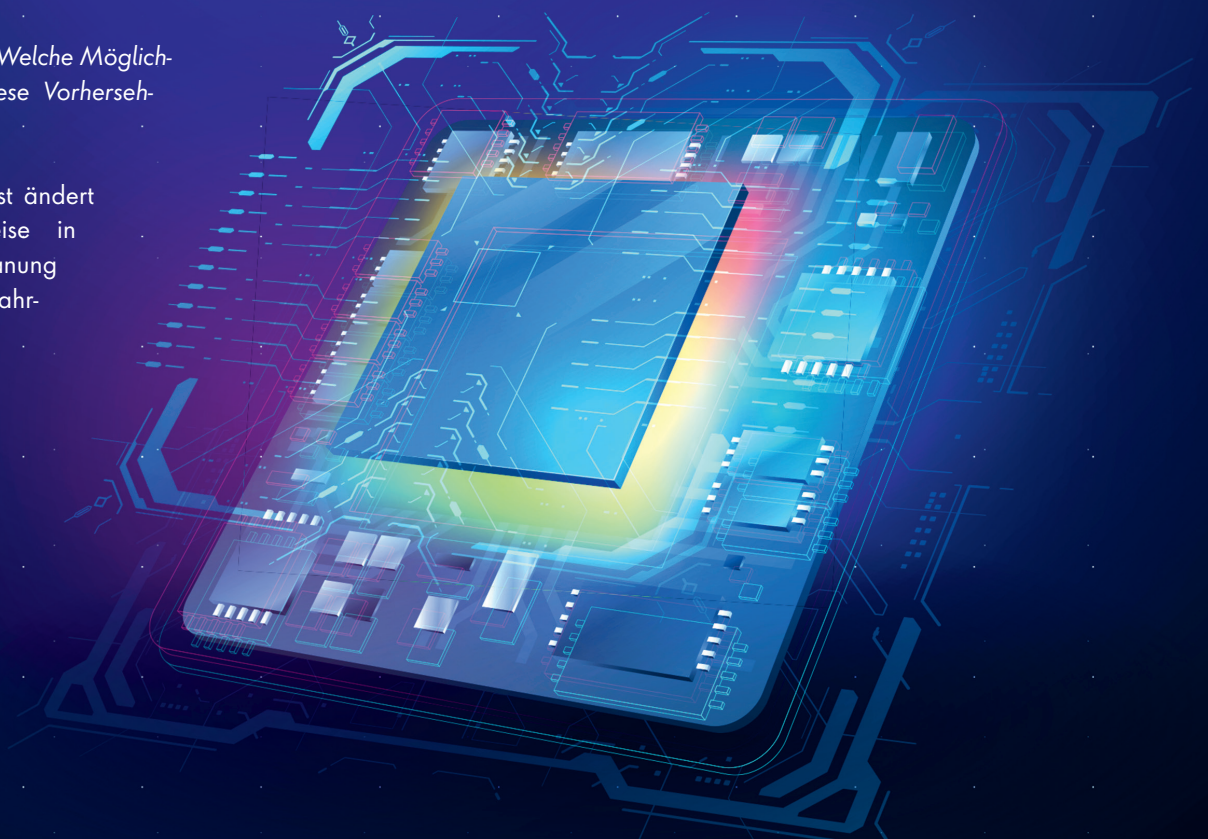
it management: Kurz gesagt: Was ist der zentrale Vorteil der Next-Gen CPUs für Multi-Tenant-KI?

Jeff Wittich: Vorhersehbarkeit durch Design. Wenn man die Variabilität auf Hardware-Ebene entfernt, wird alles darüber hinaus einfacher, einschließlich Betrieb, Wirtschaftlichkeit, Sicherheit und Engineering.

Genau das braucht Multi-Tenant-KI, um verantwortungsvoll skalieren zu können.

it management: Herr Wittich, wir danken für dieses Gespräch

”
THANK
YOU



Das Digitalisierungs-Paradox

WARUM MEHR TOOLS OFT WENIGER EFFIZIENZ BEDEUTEN

In vielen Unternehmen wächst die IT-Landschaft schneller als die Produktivität. Der Grund liegt häufig in fragmentierten Daten- und Prozessketten: Datensilos, Medienbrüche und ein hoher Anteil manueller Übergaben verhindern Skalierung. Aktuelle Befunde untermauern das Problem. So berichten im Schnitt 90 Prozent der IT-Verantwortlichen, dass Datensilos spürbare geschäftliche Herausforderungen verursachen. Gleichzeitig liegt die durchschnittliche Zahl eingesetzter Anwendungen laut Connectivity-Benchmark bei mehreren Hundert (Salesforce nennt 897 Apps im Mittel).

Das Problem:

Die Falle der Informationsinseln

Historisch gewachsene IT-Architekturen entstehen häufig abteilungsweise. Der Vertrieb nutzt ein CRM, Finance ein ERP oder eine Buchhaltungslösung, der Service ein Ticket-System, daneben existieren Branchenlösungen, Excel-Listen und lokale Datenbanken. Fachbereiche haben ihre Tools oft pragmatisch und isoliert gewählt. Das Ergebnis gleicht einem Puzzle, bei dem alle Teile vorhanden sind, aber kein zusammenhängendes Bild ergeben. Abteilungen optimieren ihren „vertikalen“ Ausschnitt – während Wertschöpfung typischerweise „horizontal“ durch das Unternehmen läuft (Lead-to-Cash, Procure-to-Pay). Häufig fehlen dabei Prozessverantwortliche für horizontale end-to-end Prozesse. In der Praxis entstehen drei wiederkehrende Effekte:

- **Widersprüchliche Datenstände:** Kunden-, Vertrags- oder Lieferstatus sind je System unterschiedlich. Das führt zu Nachfragen, Doppelpflege und Fehlerkorrekturen.
- **Manuelle Brücken:** Informationen wandern per E-Mail, Datei-Export oder



**WETTBEWERBSFÄHIGKEIT
ENTSTEHT DURCH VER-
NETZUNG, NICHT
DURCH DIE APP-ANZAHL.**

Bernd Goger, Director ITS,
Konica Minolta Business Solutions
Deutschland GmbH,
www.konicaminolta.de

Copy-&-Paste zwischen Anwendungen. Das kostet Zeit und erhöht das Risiko von Übertragungsfehlern.

- **Verlust von Kontext:** Selbst wenn Daten vorhanden sind, fehlt die durchgängige Historie entlang eines Vorgangs (z. B. Angebot – Auftrag – Lieferung – Reklamation – Gutschrift).

Die unbequeme Wahrheit: Je mehr isolierte Tools eingeführt werden, desto sichtbarer werden die Brüche. Die Digitalisierung wirkt hier nicht als Beschleuniger, sondern deckt gnadenlos organisatorische Schwächen auf. Oft versuchen Unternehmen, organisatorische Schwächen mit neuer Software zu „überdecken“. Doch wer einen ineffizienten analogen Prozess 1:1 digitalisiert, erhält lediglich einen ineffizienten digitalen Prozess.

Warum KI keine kaputten Datenflüsse repariert

Die in allen Unternehmen überlebensnotwendige Vorbereitung auf KI darf jedoch

nicht zu der Annahme verleiten, dass künstliche Intelligenz Prozessfehler einfach ausbügeln könne. Das Gegenteil ist der Fall. Der KI-Einsatz verstärkt sie häufig – weil KI nur so gut ist wie die Daten, die sie konsumiert. Unvollständige, widersprüchliche oder unverbundene Daten führen dazu, dass Assistenzsysteme falsche Schlüsse ziehen, Prioritäten verfehlen oder Ergebnisse nicht nachvollziehbar sind. KI wirkt in diesem Fall wie ein Brandbeschleuniger für schlechte Datenqualität.

Ein KI-Algorithmus oder Copilot, der auf fragmentierte Datensilos zugreift, wird genau diese Brüche reproduzieren:

- **Fehlender Kontext:** Eine KI kann keine verlässliche Umsatzprognose erstellen, wenn ihr die Daten aus laufenden Service-Fällen fehlen.
- **Falsche Priorisierung:** Automatisierte Workflows scheitern, wenn Vertragsdaten nicht mit Projektdaten verknüpft sind.

Das Potenzial von KI entfaltet sich durch saubere Prozesse, Strukturen und vollständige Daten in einem integrierten System. Für IT-Verantwortliche bedeutet das: Ohne einheitliche Begriffe, saubere Stammdaten und klare Datenverantwortlichkeiten bleibt KI eher Verstärker von Inkonsistenzen als Hebel für Automatisierung.

Ganzheitlichkeit als Grundlage

Um eine KI-gerechte Daten- und Digitalisierungskompetenz zu schaffen, benötigen Unternehmen ein organisatorisches „gemeinsames Gedächtnis“. Ein Geschäftsvorgang darf seine Bedeutung nicht verlieren, nur weil er die Abteilung wechselt.

Um Unternehmen aus der Falle der Insel-lösungen zu befreien, verfolgt Konica Minolta in seinen Kundenprojekten den Ansatz des intelligent vernetzten Arbeitsplatzes. Im Mittelpunkt steht das Ziel, vertikale Strukturen aufzubrechen und eine Balance aus moderner IT, schlanken Prozessen und eingebundenen Mitarbeitenden zu erreichen.

In der Umsetzung bewährt sich dabei eine enge Verzahnung aus einem ERP/CRM-Kern mit Dokumenten- und Informationsmanagement – ergänzt um ein Fundament aus Datenservices und -governance.

ERP/CRM auf einer konsistenten Datenbasis

Für viele mittelständische Organisationen ist ein integrierter ERP-Kern der Hebel, um Finance, Sales, Service, Projekte und Supply Chain zu synchronisieren. Über Microsoft Dynamics 365 Business Central als Cloud-ERP stellt Konica Minolta sicher, dass alle Abteilungen auf derselben Datenbasis arbeiten. Der Vorteil: Ein Vorgang bleibt vom Erstkontakt bis zur Verbuchung konsistent. Ein Status – statt Parallelwelten mit nachgelagerter „Synchronisation“.

ECM/DMS zur Kontextsicherung

Datensilos entstehen nicht nur in Fachanwendungen, sondern auch „in Dokumenten“: Wissen darf nicht in E-Mail-Postfächern, Dateiablagen und lokalen Share-Strukturen sterben. Durch die Integration mit einem modernen ECM digitalisiert und lenkt Konica Minolta dokumentenbasierte Prozesse: Ziel ist, Informationen ohne Prozessbezug zu vermeiden. Rechnungen, Verträge, Lieferscheine, Spezifikationen oder Serviceberichte sind direkt mit dem jeweiligen Geschäftsvorgang im ERP verknüpft und liefern Kontext.

Mehrwert durch Daten

Wer die entscheidenden Daten erkennt, trifft bessere Entscheidungen im Geschäftsalltag. Vielen KMUs mangelt es jedoch an Zeit, Ressourcen und Know-how, um Daten kontinuierlich zu analysieren und gewinnbringend einzusetzen. Der Einsatz von Business Intelligence Services ist letztlich die zentrale Säule für den Mittelständler, um Datenkompetenz in gute Geschäftsentscheidungen zu übersetzen.

Neben der Integration aus Prozess und Information gilt es allerdings auch Erfolgsfaktoren zu beachten, die über die Technik hinausgehen:

- **Stammdaten-Governance:** Klare Rollen (Data Owner, Data Steward), Definitionen, Qualitätsregeln, Pflegeprozesse.
- **API- und Integrationsstrategie:** Standardisierte Schnittstellen, Wiederverwendbarkeit, Monitoring; Vermeidung punktueller „Spaghetti-Integrationen“.
- **Messgrößen für Integrationserfolg:** Durchlaufzeiten, First-Time-Right-Quoten, Anteil manueller Übergaben, Datenqualitätsindikatoren, Automatisierungsgrad.
- **Change-Management:** Silos sind auch kulturell. Ohne abgestimmte Verantwortlichkeiten werden neue Systeme schnell wieder „lokal“ betrieben.

Fazit

Der Nutzen moderner Plattformen hängt direkt von der Vollständigkeit, Konsistenz und Verfügbarkeit der Daten ab. Datensilos sind deshalb nicht nur ein IT-Thema, sondern ein Hemmschuh für Automatisierung, Compliance und schnelle Entscheidungen. Erst die harmonische Balance aus medienbruchfreien Schnittstellen, prozessualer Klarheit und befähigten Mitarbeitenden führt zum Erfolg.

Bernd Goger





Erfolgreiche ERP-Implementierung

BEWUSSTE VORBEREITUNG AUF DIE VERÄNDERUNG

verfahren entwickelt, die mittlerweile Alleinstellungscharakter im Markt für Geschäftssoftware besitzen.

Wie fast alle größeren IT-Projekte sind auch ERP-Einführungen, die ohne Zwischenfälle abgeschlossen werden, eher die Ausnahme. Die Gründe hierfür sind vielschichtig. Verzögerungen können technischer oder organisatorischer Natur sein, wenn sich beispielsweise die Erstellung von Schnittstellen aufwendiger gestaltet als erwartet oder wenn Personalkapazitäten zu gering ausgelegt wurden. Während die Projektpartner für solche Störfaktoren meist angemessen schnell passende Lösungen finden, weil sie über das entsprechende Fachwissen und die Entscheidungskompetenzen verfügen, wird es ungleich komplexer, wenn psychologische Aspekte ins Spiel kommen. Denn an diesem Punkt fehlen bei vielen Mittelständlern die notwendigen Kenntnisse.

Die Vorbereitung der internen Führungskräfte auf die zu erwartende Projektdynamik ist nicht die einzige Zielsetzung der Kooperation zwischen dem Coaching-Unternehmen und dem ERP-Anbieter. Eingebunden werden auch die Key User und – sofern gewünscht – ausgewählte Endanwender. Beide Gruppen profitieren vor allem dadurch, dass sie wissen, was an Veränderungen und eventuellem Mehreinsatz auf sie zukommt. Nicht zuletzt erfährt der ERP-Anbieter, wie das implementierende Unternehmen organisiert ist, um im Bedarfsfall individuell reagieren zu können.

ERP-Implementierungen sind für Unternehmen aller Größenordnungen mehr als „nur“ IT-Projekte. Dies gilt auch für hochspezialisierte Mittelständler aus der Einzel-, Auftrags- und Variantenfertigung. Wenn deren Geschäftsprozesse durchgängig modernisiert, digitalisiert und automatisiert werden, ändern sich zwangsläufig gewohnte Arbeitsabläufe und -routinen. Bei den betroffenen Mitarbeitenden ruft dies nicht selten eine psychologisch bedingte Abwehrhaltung hervor, mit der viele Führungskräfte überfordert sind. Denn die allerwenigsten haben Erfahrung in professioneller Konfliktmoderation oder kennen situativ geeignete Motivationsstrategien. Daher ist es ratsam, alle Projektbeteiligten gemeinsam auf den bevorstehenden Change-Prozess und ihre jeweilige Rolle darin vorzubereiten.

Mit diesem Ziel hat das in Hamburg sitzende Coaching-Unternehmen Lux & Lux in enger Kooperation mit dem ERP-Anbieter ams.Solution eine Reihe spezifischer Workshops, Schulungsformate und Test-

Workshop, in dem grundsätzliche Methoden der Projektsteuerung und -begleitung vermittelt werden. Es geht um die Einbindung, Motivation und Schulung der Belegschaftsmitglieder sowie um Techniken zur Überwindung von Widerständen und um Methoden zur Deeskalation von Konflikten. Die Teilnehmer sind danach keine ausgebildeten Change-Manager oder Mediatoren, gehen aber mit einem ganz anderen Verständnis an ihre jeweilige Aufgabe heran. „Reine ERP- und IT-Aspekte lassen wir bewusst außen vor“, sagt Geschäftsführer Thomas Lux. „Vielmehr vermitteln wir in den Workshops eine Menge Grundlagenwissen zum Thema Change und lernen im Gegenzug selbst viel über die interne Führungsstruktur und



WIR VERMITTELN IN WORKSHOPS EINE MENGE GRUNDLAGENWISSEN ZUM THEMA CHANGE UND LERNEN IM GEGENZUG SELBST VIEL ÜBER BEI DEN JEWEILIGEN ERP-KUNDEN.

Thomas Lux,
Geschäftsführer, Lux & Lux
www.lux-seminare.de

Change als zentralen Projektfaktor einkalkulieren

Ein wichtiger Baustein der von Lux & Lux angebotenen Projektvorbereitung ist ein

Teamkultur bei den jeweiligen ERP-Kunden. Dieses Wissen teilen wir mit ams, um eine möglichst reibungslose Projektabwicklung zu gewährleisten.“

Bei der Auswahl der Key User, die in ERP-Projekten als wichtige Multiplikatoren fungieren, kommt es neben ihrem Fachwissen auf entsprechende Lösungskompetenz an. Zudem sollten sie Verständnis für Prozesse sowie Organisationsstrukturen mitbringen und möglichst IT-affin sein. Während sich die genannten Attribute relativ objektiv bewerten lassen, wird es ungleich schwerer, wenn es an weiche Faktoren und Soft Skills geht: Dazu zählt beispielsweise, inwieweit die Key-User-Kandidaten im Vorgesetzten- und Kollegenkreis akzeptiert sind. Wichtig ist zudem, ob sie kommunizieren und moderieren können, wie durchsetzungsfähig und entscheidungsstark sie sind, wie sie mit Widerständen und Kritik umgehen können und welche didaktischen und methodischen Fähigkeiten sie mitbringen. Um an dieser Stelle möglichst viel Sicherheit zu geben, bietet Lux & Lux Unterstützung bei der Auswahl an.

Das strukturierte Vorgehen der Hamburger hat bereits vielen Mittelständlern aus der Unikatfertigung die Implementierung von ams.erp erleichtert. Bei dem emsländischen Maschinenbauer Herrmann Paus waren Lux & Lux im Rahmen ihres Coaching-Programms „Fit fürs Projekt“ maßgeblich daran beteiligt, die Key User und die zuständigen Abteilungsleiter auf das bevorstehende Projekt einzustellen. „In einer ersten großen Runde waren 60 Personen anwesend. Diese alle inhaltlich mitzunehmen und zu motivieren, war für den Referenten eine enorme Aufgabe“, erinnert sich die Organisationsleiterin Marlies Pöppe, die in dieser Funktion auch für das ERP-Projekt zuständig war.

Sie fügt hinzu, dass es kurz vor dem Echtstart einen weiteren Workshop gab, in dem speziell die Key User darauf eingeschworen wurden, wie wichtig sie als Multiplikatoren sein werden. „Viele der damals behandelten Themen sind den Teilnehmenden bis heute sehr präsent.



**MIT VORBEREITENDEM
WORKSHOP WÄREN
DIE PROJEKTEINFÜHRUN-
GEN SCHNELLER UND
MIT VIEL WENIGER
STRESS VERLAUFEN ALS
IM ALLEINGANG.**

Manuel Krass,
Prokurist, Post Gruppe
<https://post-gruppe.de/>

Vor allem das Wissen um die eigene Rolle im Projekt und darum, wie man die unvermeidlichen Durststrecken überwindet, um letztlich zu einem positiven Gesamtergebnis zu gelangen, haben die Coaches sehr anschaulich und realitätsnah transportiert.“ Das Ergebnis sei gewesen, dass sowohl die Key User und Endanwender als auch die Führungskräfte in allen Phasen das Vertrauen hatten, auch schwierige Situationen meistern zu können. Dies habe vieles erleichtert.

Mehrere ERP-Implementierungen erfolgreich begleitet

Bei der Partzsch Elektromotoren GmbH aus Döbeln waren einige Mitarbeitende anfangs skeptisch. Sie hatten keine Vorstellung davon, was sie in dem geplanten Workshop erwarten würde. Aber genauso wie bei Hermann Paus zogen auch die 40 Teilnehmenden der Partzsch Elektromotoren GmbH laut der ERP-Verantwortlichen Mandy Schütze im Nachhinein ein durchgehend positives Fazit. Einerseits, weil sie sehr konkret auf die Herausforderungen während der ERP-Implementierung hingewiesen wurden und dadurch im Projekt entsprechend sensibilisiert waren. Andererseits, weil ihnen die Stärken und Schwächen der firmeninternen Strukturen ungeschönt vor Augen geführt worden waren. Im Vergleich zu einem größeren

IT-Projekt einige Jahre zuvor habe sich zudem ein starkes Wir-Gefühl entwickelt, für das der Workshop der Grundstein war.

Die Verantwortlichen der Post Gruppe aus dem westfälischen Altenberge griffen ebenfalls auf die Unterstützung durch Lux & Lux zurück. Manuel Krass, Prokurist in der Geschäftsleitung, berichtet, dass die Workshop-Teilnehmer umfassend darauf eingestellt wurden, was die Software-Implementierung an Mehrarbeit und eventuellen Überstunden für sie bedeuten würde. Wichtiger war seiner Einschätzung nach jedoch die Auflistung der Vorteile des ERP-Wechsels. In diesem Zuge wurden die Sorgen, Ängste und Vorurteile der Mitarbeiter gehört, beleuchtet und beantwortet. Dadurch entstand ein Team an Key Usern, die ihm als Projektleiter einen gehörigen Teil der Implementierungsverantwortung abnahmen.

Manuel Krass hat den direkten Vergleich zu einem Projekt, in dem diese Unterstützung fehlte: „Ich selbst war in einer anderen Unternehmung als Hauptansprechpartner für die Einführung eines ERP-Systems zuständig“, schildert er die Ausgangslage. Unter anderem musste er die richtigen Kollegen für Vorarbeiten gewinnen, was ihm selten gelang, weil die Notwendigkeit für die Nutzung einer neuen Software nicht gesehen wurde. Folglich musste er sämtliche Vorbereitungen selbst erledigen und sich die relevanten Informationen aus den einzelnen Abteilungen beschaffen. Außerdem organisierte er Workshops und verfasste ein Handbuch zum Nutzen der Software. „Als Einzelkämpfer habe ich die Einführung für drei Mandanten zwar in unter einem Jahr realisieren können. Hätte es jedoch einen Workshop wie ‚Fit fürs Projekt‘ gegeben, wäre es noch schneller und mit viel weniger Stress für mich verlaufen. Denn ich hätte das damalige Projekt nicht alleine schultern müssen, sondern hätte ein Team gehabt, um Arbeiten zu delegieren. Zudem hätte ich Befürworter gehabt, die mitgearbeitet und Daten sowie Infos bereitgestellt hätten“, bekräftigt er.

Guide Piech | www.ams-erp.com

ERP-Migration entmystifiziert

KEINE ANGST VOR DEM WECHSEL

ERP-Migrationen gelten als Mammutprojekte und werden gerne auf die lange Bank geschoben. Kein Wunder: Immer noch machen Geschichten über gescheiterte Implementierungen die Runde und schrecken Verantwortliche vor dem eigentlich dringend notwendigen Schritt ab. Doch die Angst vor dem Wechsel ist ein schlechter Ratgeber. Wer aus Sorge vor Risiken am Altsystem festhält, gefährdet die eigene Wettbewerbsfähigkeit. Ein Blick in die Praxis zeigt: Die richtige Strategie und Herangehensweise kann viele Sorgen zerstreuen.

Technischer Stillstand kostet. Was auf den ersten Blick wie eine Binsenweisheit klingt, ist in vielen Unternehmen bittere Realität, denn immer noch bremsen ver-

altete ERP-Systeme Mitarbeitende aus, erschweren Datenauswertungen und verhindern, dass Unternehmen von neuen Technologien profitieren. Moderne ERP-Plattformen schaffen hingegen die Grundlage für ein Maximum an Transparenz, steigern die Effizienz und ebnen den Weg für Automatisierung, Künstliche Intelligenz und datengetriebene Entscheidungen. Ein Wechsel ist also nicht nur ein IT-Projekt, sondern eine Investition in die eigene Zukunftsfähigkeit. Und dennoch zögern viele Entscheider eine oftmals dringend notwendige Migration ihrer Systeme weiter hinaus, auch weil sich Berichte und Horrorgeschichten über gescheiterte Projekte hartnäckig halten. Und ja, wer seine angestaubte, aber funktionierende ERP-Lösung durch ein modernes System ersetzt, geht eine Aufgabe von Tragweite an – sowohl technologisch als auch kulturell. Nichtstun ist allerdings weitaus gefährlicher.



EINE MIGRATION BEDEUTET DABEI MEHR, ALS ALTE DATEN IN EIN NEUES SYSTEM ZU ÜBERTRAGEN: SIE IST EIN UMFASSENDES TRANSFORMATIONS-PROJEKT.

Sebastian Spicker,
Managing Director DACH, IFS,
www.ifs.com/de

Eine strategische Notwendigkeit

Viele Unternehmen sind sich zunehmend bewusst, dass sie ohne ein modernes ERP-System weder Komplexität beherrschen noch agil auf Marktveränderungen reagieren können. Eine Migration bedeutet dabei allerdings mehr, als alte Daten in ein neues System zu übertragen. Es ist ein umfassendes Transformationsprojekt, das Technologie, Organisation und Kultur gleichermaßen betrifft.

Ein zentrales Missverständnis besteht dabei darin, die Migration als eine rein technische Aufgabe zu betrachten. Tatsächlich geht es um weit mehr – um das Neu-denken und Neuordnen von Prozessen, Verantwortlichkeiten und Informationsflüssen. Wer das versteht und strukturiert

vorgeht, kann Risiken kontrollieren und Mehrwerte schnell realisieren.

Was macht eine erfolgreiche Migration aus?

ERP-Migrationen sind kein Projekt, das Unternehmen einfach nebenbei abwickeln können. Vielmehr kommt es auf eine passende Strategie und solide Planung an – und die beginnt lange vor dem ersten Datenexport. Eine Prämisse ist dabei die Gewissheit darüber, was das neue System eigentlich leisten soll. Um diese ganz zentrale Frage zu beantworten, müssen bestehende Prozesse analysiert, Schwachstellen identifiziert und die Anforderungen aller Abteilungen dokumentiert werden. Schritte, die



durchaus mit Aufwand verbunden sein können, aber dennoch die Grundlage für das restliche Projekt legen, inklusive der Konfiguration und der Auswahl des passenden Systems. Nicht eindeutig definierte Ziele führen hingegen fast immer zu Verzögerungen, Kompromissen und Fehlentscheidungen.

Daneben ist das Datenmanagement ein weiterer Schlüsselfaktor. Zwischen Alt- und Neusystem bestehen oft gravierende Unterschiede in Datenformaten, Feldern oder Strukturen. Wer hier unvorbereitet agiert, importiert alte Fehler in die neue Umgebung. Die Migration ist daher auch eine wunderbare Gelegenheit, die eigenen Daten zu bereinigen und zu konsoli-

dieren, bevor sie übertragen werden. Denn: Nur eine solide Datenlandschaft kann verlässliche Analysen, stabile Prozesse und Vertrauen in das neue System gewährleisten.

Ein klar definierter Migrationsplan – inklusive Datenmapping und Testmigrationen – reduziert das Risiko von Inkonsistenzen dabei erheblich. Damit einher geht auch eine intensive Testphase, in der das neue ERP-System unter realen Bedingungen vor dem Go-Live auf Herz und Nieren geprüft wird. Dazu gehören Unit Tests für einzelne Funktionseinheiten, Schnittstellentests zu anderen Systemen sowie umfassende Integrationstests. Testmigrationen helfen nicht nur dabei,

Schwachstellen frühzeitig zu erkennen, sondern vermitteln auch ein Gefühl für die Nutzerakzeptanz.

Dieser letzte Aspekt ist mehr als nur eine Fußnote, denn nur wenn sich die Mitarbeitenden auf ein neues System einlassen und damit fundamentale Änderungen in ihrem Arbeitsalltag zulassen, können ERP-System und Belegschaft ihre volle Wirkung entfalten. Der Faktor Mensch wird auf diese Weise zu einem zentralen Erfolgsfaktor. ERP-Migrationen verändern Abläufe, Terminologien und Verantwortlichkeiten – und verlangen ein aktives Change-Management. Ein Tipp aus der Praxis: Unternehmen, die offen über die Vorteile von System-

wechseln und neuen Lösungen kommunizieren, erreichen ihre Mitarbeitenden schneller, können Zweifel entkräften und Vertrauen aufbauen. Ein bewährter Ansatz ist das sogenannte Key-User-Konzept: Frühzeitig eingebundene Mitarbeitende aus den Fachbereichen werden intensiv geschult und geben ihr Wissen an Kolleginnen und Kollegen weiter. Das schafft zusätzliche Akzeptanz und reduziert Reibungsverluste nach dem Go-Live.

Schließlich ist auch die Planung des Go-Live ein kritischer Punkt. Ob ein ERP-System in einem „Big Bang“ komplett oder schrittweise eingeführt wird, hängt von der Komplexität und Risikobereitschaft des Unternehmens ab. In jedem Fall sollte der Start gut vorbereitet und auf einen ruhigen Geschäftszeitraum gelegt werden. Notfallpläne und eine stabile Supportstruktur sind Pflicht. Sie stellen sicher, dass Kernprozesse selbst bei unerwarte-

ten Problemen weiterlaufen. Wer parallel alte Systeme vorübergehend absichert, gewinnt zusätzlichen Handlungsspielraum.

Erfolgsfaktor Kultur

Technologie allein entscheidet nicht über den Erfolg einer ERP-Migration. Genauso wichtig sind Führung und Unternehmenskultur. Migration ist immer auch ein Lernprozess – sie verlangt Offenheit, Vertrauen und die Bereitschaft, Gewohntes zu hinterfragen.

Führungskräfte müssen Orientierung bieten und Veränderung als Chance vermitteln. Wer dagegen die Migration als rein technisches Projekt delegiert, riskiert Akzeptanzprobleme und teure Nachjustierungen. Die Risiken liegen weniger in der Technik als in unklaren Zielen, mangelhafter Kommunikation und fehlender Vorbereitung. Wer die Migration als strategische Aufgabe versteht und me-

CHECKLISTE ERP-MIGRATION:

- Ziele und Anforderungen klar definieren
- Prozesse analysieren und dokumentieren
- Alt-Daten bereinigen und konsolidieren
- Datenmapping erstellen
- Testmigrationen durchführen
- Schnittstellen prüfen
- Nutzerakzeptanz testen
- Key-User schulen
- Kommunikationsplan aufsetzen
- Go-Live-Strategie wählen (Big Bang oder schrittweise)

thodisch angeht, kann den Wandel nicht nur meistern, sondern als Wettbewerbsvorteil nutzen.

Sebastian Spicker

8 TOP-TIPPS FÜR IT-SECURITY-LÖSUNGEN

NACH DIESEN KRITERIEN WÄHLEN IT-PROFIS IHRE PERFEKTE LÖSUNG AUS

Der nahtlose und sichere Wechsel zwischen Büro und Homeoffice oder einem anderen RemoteArbeitsplatz ist im Jahr 2025 eine Selbstverständlichkeit. Damit Remote Work auch in der Praxis umsetzbar ist, sollten IT-Verantwortliche bei der Auswahl der richtigen VPN-Lösung auf einige Punkte achten.

Die Lösung sollte:

- alle Gerätetypen unterstützen,
- keine Abstriche bei Sicherheit und Benutzerfreundlichkeit machen,
- den Einsatz von MFA mit berücksichtigen,
- Passwortmanagement smart abbilden,
- von den Vorteilen des Split Tunneling Gebrauch machen,
- Cloud-Kompatibilität sicherstellen (sowohl jetzt als auch in Zukunft),
- Endpoint Security zu einer Priorität machen
- und einen „Single Point of Administration“ bieten.

Sind alle diese Punkte erfüllt, steht einer benutzerfreundlichen, hochsicheren und vernünftig administrierbaren IT-Security-Lösung nichts mehr im Wege! Weitere Hintergründe und Details liefert unser Techpaper.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 15 Seiten und steht zum kostenlosen Download bereit.

www.it-daily.net/Download



KI-HALLUZINATIONEN IM CODE

RISIKEN FÜR ENTWICKLUNG UND SICHERHEIT

KI-Assistenten im Software-Entwicklungsprozess liefern nicht immer das, was sie versprechen. Sogenannte Halluzinationen erfinden Pakete, die nicht existieren, schlagen API-Methoden vor, die nie implementiert wurden und generieren Dokumentationen, die nicht zur tatsächlichen Implementierung passen. Was auf den ersten Blick wie ein kleines Qualitätsproblem wirkt, kann weitreichende Konsequenzen für Softwaresicherheit und -stabilität haben.

Die gefährlichsten Halluzinationstypen

#1 Nicht existierende Bibliotheken und Pakete

Sie zählen zu den häufigsten Problemen. Die KI schlägt Paketnamen vor, die logisch klingen und zum Kontext passen, aber nie existiert haben oder falsch geschrieben sind. Ein Entwickler, der „data-validator-pro“ als Dependency hinzufügen möchte, stellt erst beim Build-Prozess fest, dass dieses Paket nicht existiert.

#2 Slopsquatting: Wenn Angreifer Halluzinationen ausnutzen

Besonders gefährlich wird es beim sogenannten Slopsquatting: Angreifer beobachten, welche nicht existierenden Paketnamen KI-Tools häufig halluzinieren, und veröffentlichen dann schädliche Pakete unter genau diesen Namen. Ahnungslose Entwickler installieren diese Pakete und öffnen damit Tür und Tor für Malware. Dieser Angriffsvektor im letzten Jahr dramatisch zugenommen und stellt eine ernsthafte Bedrohung für die Software-Supply-Chain dar.

#3 Erfundene API-Methoden täuschen Entwickler

Erfundene API-Methoden sehen aus wie legitime Funktionsaufrufe, existieren aber in der referenzierten Bibliothek nicht. Die KI schlägt beispielsweise `database.connect().autoMigrate()` vor, obwohl die verwendete Datenbank-Bibliothek keine `autoMigrate`-Methode kennt. Der Code kompiliert nicht oder schlägt zur Laufzeit mit kryptischen Fehlermeldungen fehl.

#4 Veraltete Syntax aus alten Trainingsbeständen

Veraltete oder falsche Syntax tritt auf, wenn die KI auf Trainingsmaterial zurückgreift, das nicht mehr dem aktuellen Stand entspricht. JavaScript-Frameworks wie React, Vue oder Angular entwickeln sich schnell weiter. Code-Patterns, die vor zwei Jahren üblich waren, gelten heute als deprecated. Die KI kann nicht zuverlässig zwischen verschiedenen Versionen unterscheiden und mischt manchmal Syntax aus unterschiedlichen Framework-Generationen.

#5 Fehlerhafte Konfigurationen mit Sicherheitsfolgen

Fehlerhafte Konfigurationen entstehen, wenn die KI-Einstellungen für Build-Tools, Container oder Cloud-Services vorschlägt, die in der verwendeten Version nicht funktionieren oder schlimmstenfalls Sicherheitslücken öffnen. Eine Docker-Konfiguration, die veraltete Basis-Images nutzt, oder Kubernetes-Manifeste mit falsch gesetzten Security-Policies können gravierende Folgen haben.

#6 Falsche Dokumentation führt zu Missverständnissen

Falsche Dokumentation ist besonders tückisch. Die KI generiert Kommentare und Docstrings, die beschreiben, was der Code angeblich tut – aber die Beschreibung stimmt nicht mit der tatsächlichen Implementierung überein. Ein nachfolgender Entwickler verlässt sich auf die Dokumentation und trifft auf dieser Basis falsche Annahmen.

Ulrich Parthier





Flexible ERP-Systeme

DER SCHLÜSSEL ZU DIGITALER SOUVERÄNITÄT IM MITTELSTAND

Kein Unternehmen kommt heute noch ohne ERP-System aus. Dies gilt insbesondere für den Mittelstand. Herkömmliche ERP-Lösungen sind jedoch durch standardisierte Prozesse und eine starre Architektur gekennzeichnet. Demgegenüber überzeugt das Konzept eines offenen Open Source ERP-Baukastens durch maximale Flexibilität. Das System wächst mit den Anforderungen und Prozessen im Unternehmen mit und fungiert daher als wichtiger Treiber für nachhaltige Expansion und Internationalisierung.

Die Wirtschaft in Deutschland und Europa sieht sich angesichts der aktuellen geopolitischen Lage mit steigenden Herausforderungen konfrontiert. Dies betrifft auch den Mittelstand, der als tragende Säule der Wirtschaft gilt. Wie alle Unternehmen sind auch kleine und mittlere Unternehmen (KMU) gefordert, die Effizienz ihrer Prozesse zu optimieren und Kosten zu sparen. Unabdingbar hierfür ist eine solide IT-Basis, die ein leistungsfähiges ERP-System einschließt. Dieses steuert und bildet alle betriebswirtschaftlichen Workflows ganzheitlich ab. Es gilt daher als Garant für stabile und verlässliche Geschäftsprozesse und damit auch für maximalen Unternehmenserfolg.

hängig von ausländischen Cloud-Anbietern und Hyperscalern auf sicheren Servern in Deutschland hosten lassen. Dies gewährleistet ein Maximum an Transparenz, Unabhängigkeit und Integrität im Hinblick auf sensible Geschäftsdaten. Eine weitere zentrale Anforderung an ein ERP-System besteht darin, dass es sich flexibel an veränderte Bedingungen anpasst und mit der Entwicklung des Unternehmens laufend Schritt hält. Nur so kann das System das Wachstum bestmöglich unterstützen und seine Vorteile zur Verbesserung der Prozesseffizienz optimal ausspielen.

Klassische ERP-Lösungen sind hierfür jedoch häufig zu starr und rein auf standardisierte Workflows fixiert. Sie sind meist nicht in der Lage, die Geschäftsprozesse im Unternehmen individuell und kundenspezifisch abzubilden. Einen anderen Weg geht hier das Konzept eines Open Source ERP-Baukastens wie etwa Nuc-

Digitale Souveränität durch ERP aus Deutschland

Wichtig dabei ist, dass ein entsprechendes System den Gedanken der digitalen Souveränität optimal unterstützt. Dies bedeutet: Die ERP-Lösung sollte sich unab-



los. Dieser wächst dank seiner offenen Architektur flexibel mit den steigenden Anforderungen und sich stetig verändernden Prozessen mit. Daher gilt dieser Ansatz nicht nur als wichtiger Treiber für nachhaltige Firmen-Expansion. Auch bildet er ein solides Fundament für die Internationalisierung des Geschäfts und bereitet den Weg für neue Business-Modelle. Hinzu kommt: Da Nuclos komplett auf Servern in Deutschland gehostet wird, sind Anwender bezüglich Datenschutz und digitaler Souveränität auf der sicheren Seite.

BusinessBike automatisiert Fahrrad-Leasing mit Nuclos

Wie insbesondere mittelständische Unternehmen von den vielfältigen Vorteilen des Open Source ERP-Baukastens profitieren können, zeigen verschiedene Anwendungsfälle aus der Praxis: Dienstrad-Leasing-Anbieter BusinessBike beispielsweise nutzt Nuclos, um sämtliche Prozesse rund um das Fahrrad-Leasing durchgängig zu automatisieren. Dabei fungiert die ERP-Software als zentrale Daten-Drehzscheibe und vernetzt alle Beteiligten wie Arbeitgeber, Arbeitnehmer, Fachhändler und Selbständige nahtlos. So bildet das System sämtliche Prozesse in dem komplexen Beziehungsgeflecht transparent ab.

Zudem spielte der ERP-Baukasten seine Vorteile in diesem Anwendungsszenario optimal aus: Flexibel ließ sich ein Web-Interface in die Software integrieren, über das alle Beteiligten wie Leasing-Nehmer, Arbeitnehmer und Fachhändler schnell und komfortabel auf die Anwendung und die relevanten Daten zugreifen können. Dabei lassen sich auch Leasing-Geber und Versicherungsgesellschaft mittels Schnittstellen durchgängig anbinden. Darüber hinaus überprüft Nuclos kontinuierlich den aktuellen Status der Vertragsgestaltung und benachrichtigt die Beteiligten automatisiert über Veränderungen. Sind beispielsweise alle erforderlichen Unterlagen eingereicht, kann der Händler zeitnah reagieren und das Fahrrad an den Nutzer ausliefern.

Der entscheidende Vorteil: Durch die komplette Digitalisierung der Workflows lässt sich die Vertragsabwicklung erheblich beschleunigen. So dauert dieser Vorgang heute nur noch wenige Sekunden, während der Versand papierbasierter Dokumente früher mehrere Tage in Anspruch nahm. Von diesem Effizienzgewinn profitieren auch die Kunden von BusinessBike, die ihre Leasing-Fahrräder nun wesentlich schneller erhalten.

Klassische Geschäftsprozesse mit Nuclos steuern

Auch die Dr. Höhn GmbH, Hersteller von Hardtops und Aufbauten der Marke „Road Ranger“ für Pickups und Pritschenwagen, profitiert vom Open Source ERP-Baukasten: Das mittelständische Unternehmen steuert damit seine kompletten Prozesse rund um Vertrieb, Logistik und Einkauf – sowie in naher Zukunft auch die Produktion am Standort in Polen. Dabei lassen sich mit dem ERP-Baukasten umfangreiche Stücklisten mit weit mehr als 1.000 Varianten pro Artikel transparent verwalten. Ein besonderer Vorteil: Durch das gewählte System entstehen keinerlei Lizenzkosten, sodass die Gesamtbetriebskosten (TCO) der ERP-Landschaft bei Dr. Höhn überschaubar bleiben.

Mit Nuclos verfügt der Mittelständler nun über eine übersichtliche, prozessübergreifende Informationsdrehzscheibe, mit der sich die große Variantenvielfalt optimal abbilden lässt. Alle berechtigten Akteure wie interne Mitarbeiter, Händler und Produktionspartner können auf einen zentral verwalteten, einheitlichen und konsistenten Datenbestand zugreifen. Das System bildet zudem die Datenbasis für den angebundenen Webshop, den das gesamte Händler-Netzwerk nutzt. Von der Angebotserstellung über die Bestellabwicklung bis hin zur Erzeugung und Versendung von Rechnungen – das



**ERP-LÖSUNGEN SOLLTEN
SICH UNABHÄNGIG
VON AUSLÄNDISCHEN
CLOUD-ANBIETERN
UND HYPERSCALERN
AUF SICHEREN SERVERN
IN DEUTSCHLAND
HOSTEN LASSEN.**

**Klaus Röder, Geschäftsführer,
Novabit Informationssysteme GmbH,
www.nuclos.de**

ERP-System sorgt für eine transparente Verwaltung und Steuerung des gesamten Auftragsdurchlaufs.

Ein weiterer Vorteil: Nuclos unterstützt auch die Expansion des Kfz-Spezialisten. Dank der hohen Skalierbarkeit lässt sich das System flexibel erweitern und auf neue Betriebsstätten ausrollen. So soll das System in naher Zukunft auch das Kontaktmanagement (CRM) und die Veranstaltungsplanung mit Partnern wie Großhändlern, Importeuren und Fahrzeugherstellern sowie die Produktionsplanung und -Steuerung (PPS) abbilden.

ERP als Wachstumstreiber für den Mittelstand

Wie beide Anwendungsszenarien belegen, kann ein Open Source ERP-Baukasten zur lohnenden Investition avancieren. So unterstützt das System nicht nur neue Business-Modelle wie das Fahrrad-Leasing, sondern bildet auch klassische Geschäftsprozesse in traditionellen produzierenden Unternehmen eins zu eins ab. In beiden Fällen fungiert das flexible ERP-System dabei als entscheidender Wachstumstreiber für den Mittelstand.

Klaus Röder

it management **UNSERE THEMEN**

Spezialthema: Health Special

Fokusthema: Cloud & Edge Computing

Schwerpunktt Themen: ITSM, Unified Communications, Data Center & Data Management, DNA Data Storage, Holographische Speicher

Die Ausgabe
05/06 2026
erscheint am

**4. Mai
2026**



it security **UNSERE THEMEN**

Spezialthema: Health Special

Cybersecurity: Die Cybersecurity-Landschaft wandelt sich permanent – und wir wandeln uns mit. Statt starrer Themenplanung folgen wir dem Puls der Security-Welt und bleiben so immer aktuell.



WIR WOLLEN FEEDBACK VON IHR

Mit Ihrer Hilfe wollen wir dieses Magazin weiter entwickeln. Was fehlt, was ist überflüssig? Schreiben sie an u.parthier@it-verlag.de

INSERENTENVERZEICHNIS

it management

Insight GmbH (Teaser)	U1, 18
it verlag GmbH	U2, U3, U4
ams.Solution AG	7
noris network	9
Natuvion GmbH (Advertorial)	21
HannoverMesse	39
E3 / B4B Media	43

it security

Beazley Solutions International Limited	U2
it verlag GmbH	7, U3
Vodafone D2 GmbH (Advertorial)	8
WatchGuard Technologies GmbH (Advertorial)	13
HannoverMesse	15
INFODAS GmbH	23
Aagon GmbH	U4

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Lars Becker, Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistent und Sonderdrucke: Eva Neff (-15)

Autoren: Lars Becker, Philipp von der Brüggen, Dr. Lennart Gaida, Bernd Goger, Matthew Gorelik, Sascha Helmkamp, Rüdiger Hoffmann, Martin Mangold, Carina Mitzschke, Angelika Mühleck, Ulrich Parthier, Guido Piech, Klaus Röder, Christian Scharer, Dr. Jan Schaumburg, Moritz Schürmann, Sebastian Spicker, Svenja Vorwerk, Sebastian Weber, Jeff Wittich

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbrief: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion. Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Ge-

währleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 33. Preisliste gültig ab 1. Oktober 2025.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:

Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94, reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Head of Marketing:
Vicky Miridakis, 08104-6494-15, miridakis@it-verlag.de

Objektleitung: Ulrich Parthier (-14), ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben, PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung: VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC
Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abbonementsservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.





Haben Sie etwa eine Ausgabe der
itmanagement und **itsecurity**

verpasst?

...mit einem Abo wäre das nicht passiert.

Trends von heute und morgen sowie Fachartikel und Analysen renommierter Branchenexperten: Die Fachmagazine IT Management und IT Security bieten einen fundierten Einblick in verschiedene Bereiche der Enterprise IT.

ZUM ABO



it-daily.net/leser-service

it-daily.net
 Das Online-Portal von **itmanagement** & **itsecurity**

IT-EXPERTENWISSEN AUF KNOPFDRUCK

UNSERE

 **it-daily.net**

ONLINE-EVENTS

FÜR DIE DIGITALE ZUKUNFT



**JETZT
ENTDECKEN!**

IMMER AM PULS DER IT



Detect. Protect. Respond.

März/April 2026

DIGITALE SOUVERÄNITÄT
DANK SWISS MADE SOFTWARE

Vertrauen ist unsere tägliche Arbeit

Dennis Monner, Open Systems

CYBER- VERSICHERUNG

Wie Unternehmen
Versicherungsprämien senken

KI-GESTÜTZTES PENTESTING

Die neue Ära der
Cybersicherheit?

DREI HEBEL GEGEN SPEAR-PHISHING

Tools, Tempo und
Training

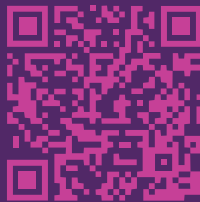
www.it-daily.net

CYBERATTACKEN IM KEIM ERSTICKT

In einer Welt voller Cyber-Risiken existieren keine Regeln.
Mit Full Spectrum Cyber von Beazley bleiben
Versicherungsnehmer im Kampf gegen Cyberkriminalität
immer einen Schritt voraus - denn eines der besten Teams
der Branche hält ihnen den Rücken frei.

#GameOnCyber

Erleben Sie unser
Cyber-Ökosystem auf beazley.de



beazley
Insurance. Just different.



Inhalt

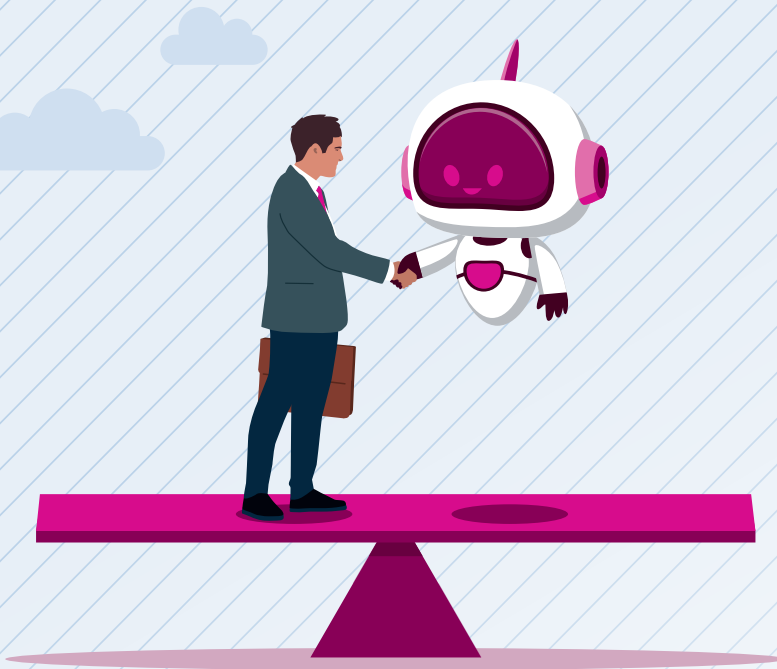
COVERSTORY

- 4 Vertrauen ist unsere tägliche Arbeit**
Digitale Souveränität dank Swiss Made Software

IT SECURITY

- 10 Von PoC zu produktiv**
Wie Datensouveränität die KI-Nutzung sicher macht
- 14 Tools, Tempo, Training**
Drei Hebel gegen Spear-Phishing
- 16 NIS2: Digitale Resilienz durch klare Verantwortung**
Governance-Anforderungen 2026
- 18 Security by Governance**
So gelingt Compliance im Alltag
- 20 Compliance für Cyberversicherungen**
Wie Unternehmen Versicherungsprämien senken

- 25 Cyberresilienz gemeinsam stärken**
Aktive Versicherungslösungen
- 26 Besseres Scoring in der Cyberversicherung**
Ein Leitfaden zur Prämienoptimierung
- 32 Cyberattacken: Die neue Realität**
Warum viele Firmen ein leichtes Ziel sind
- 36 DevSecOps**
Drei praxisnahe Wege, um Security und Operations zu verbinden
- 38 Von Erkennung zu autonomer Abwehr**
Warum KI ein neues Sicherheitsparadigma erfordert
- 40 Netzwerke für die KI-Ära**
Warum der Channel heute den Unterschied macht
- 42 KI-gestütztes Pentesting**
Die Zukunft von Sicherheitstests gestalten



„Vertrauen ist unsere tägliche Arbeit“

DIGITALE SOUVERÄNITÄT DANK
SWISS MADE SOFTWARE

Dennis Monner ist seit Oktober 2025 CEO von Open Systems. In seinen ersten 100 Tagen hat er den Fokus ganz deutlich auf Umsetzung, Kundennähe und Positionierung gelegt. Ein sichtbarer Meilenstein dieser Phase ist das Label „Swiss Made Software“ – ein Nachweis überprüfbarer Wertschöpfung in der Schweiz. Im Gespräch mit Carina Mitzschke, Redakteurin *it security*, erläutert Monner, warum Transparenz, Datenhoheit und operativer Betrieb für IT-Entscheider in Zeiten zunehmend entscheidender werden.

Carina Mitzschke: Herr Monner, Sie sind nun seit 100 Tagen CEO von Open Systems. Welche erste Bi-

lanz ziehen Sie, und was waren die wichtigsten Meilensteine in dieser Anfangsphase?

Dennis Monner: Die ersten 100 Tage waren eine Umsetzungsphase. Open Systems ist ein rund 100-Millionen-US-Dollar-Unternehmen, das nicht neu erfunden werden muss, sondern eines, dessen Profil und Positionierung wir schärfen müssen. Ganz praktisch bedeutet das, Entscheidungswege verkürzen, Verantwortlichkeiten klarstellen und die Nähe zu unseren Kunden intensivieren. Meine Aufgabe ist es, unsere Stärken noch sichtbarer zu machen und konsequent in nachhaltiges Wachstum zu übersetzen.

Carina Mitzschke: Sie kamen mit dem Ziel ins Unternehmen, nachhaltiges Wachstum und Marktnähe zu stärken. Welche Marktsegmente und Partnerschaften stehen dabei im Fokus?

Dennis Monner: Wir konzentrieren uns vor allem auf: regulierte Branchen, kritische Infrastrukturen und globale Organisationen mit hohen Anforderungen an Verfügbarkeit, Compliance und Betriebssicherheit. Unsere größten Kunden betreiben Umgebungen mit bis zu 60.000 Mitarbeitenden weltweit. In dieser Größenordnung geht es weniger um einzelne Features. Entscheidend sind vielmehr Zuverlässigkeit, Transparenz und ob sich Sicherheit langfristig stabil betreiben lässt.

Carina Mitzschke: Das Label „Swiss Made Software“ ist eine der ersten großen Auszeichnungen unter Ihrer Führung. Was bedeutet das Label konkret für Open Systems und seine Kunden?

Dennis Monner: Das Label ist kein Marketing-Preis, sondern ein überprüfbarer Nachweis realer Wertschöpfung. Es bestätigt, dass der wesentliche Teil unserer Entwicklungs- und Produktionsleistung in der Schweiz stattfindet und dass Open Systems hier rechtlich und operativ verankert ist. Für unsere Kunden bedeutet das ganz konkret: Volle Schweizer Datenhoheit und keine verdeckten Abhängigkeiten von fremden Rechtsräumen. In Zeiten geopolitischer Unsicherheit ist diese Klarheit ein echtes Entscheidungskriterium bei der Suche nach zuverlässigen Partnern.

Carina Mitzschke: Welche konkreten Kriterien musste Open Systems erfüllen, um das Label zu erhalten, und wie aufwendig war der Zertifizierungsprozess?

Dennis Monner: Die Anforderungen sind klar messbar. Mindestens 60 Pro-

zent der relevanten Entwicklungs- und Herstellungskosten müssen in der Schweiz anfallen, und der zentrale Teil der Wertschöpfung, insbesondere Entwicklung und Qualitätssicherung, muss ebenfalls hier stattfinden. Zudem muss das Unternehmen seinen Sitz in der Schweiz haben.

Der Zertifizierungsprozess ist anspruchsvoll, keine Frage. Für uns war er aber dennoch keine große Herausforderung, weil er exakt das abbildet, was wir ohnehin schon seit Jahren umsetzen.

Carina Mitzschke: Inwiefern unterscheidet sich das Swiss Made Software Label von anderen Qualitätssiegeln oder Zertifizierungen in der Cybersecurity-Branche?

Dennis Monner: Viele Labels oder Zertifizierungen bewerten einzelne Aspekte wie Prozesse oder technische Controls. Swiss Made Software geht einen

sungen im Vergleich zu Anbietern aus anderen Regionen?

Dennis Monner: Der Standort Schweiz steht für Präzision, Verlässlichkeit und langfristiges Denken. Dafür setzen wir bei unseren Produkten und Services auch nicht auf maximale Feature-Dichte, sondern auf klare Architekturen, stabile Plattformen und sauberen Betrieb. Sicherheit entsteht nicht durch Komplexität, sondern durch Kontrolle. Genau das prägt unsere SASE- und Secure-Connectivity-Lösungen.

Carina Mitzschke: Welche konkreten Vorteile bietet das Label IT-Ent-

scheidern, die vor der Wahl eines SASE-Anbieters stehen? Sehen Sie bereits erste Reaktionen von Kunden auf die Label-Vergabe?

Dennis Monner: Für IT-Entscheider und insbesondere auf C-Level bietet das Label vor allem Orientierung. Es ersetzt keine Risikoanalyse, schafft aber eine belastbare Entscheidungsgrundlage in Bezug auf Compliance, Datensouveränität und geopolitische Abhängigkeiten. Wir erhalten daher auch eindeutige Reaktionen, weil unsere Kunden in der Vergabe des Labels eine Bestätigung ihrer bisherigen Entscheidung für Open Systems sehen. Damit haben Sie

VERTRAUEN IN CYBERSECURITY
ENTSTEHT NICHT DURCH
VERSPRECHEN, SONDERN DURCH
VERANTWORTUNG. GENAU DAFÜR
STEHT OPEN SYSTEMS.

Dennis Monner, CEO, Open Systems, www.open-systems.com

anderen Weg. Es geht um überprüfbare Wertschöpfung in der Schweiz, klare Verantwortung und volle Transparenz. In der Cybersecurity ist das entscheidend. Kunden wollen nicht nur wissen, ob eine Lösung zertifiziert ist, sondern wo sie entwickelt wird, wem sie gehört und unter welchen rechtlichen Rahmenbedingungen sie betrieben wird. Genau diese Fragen beantwortet das Label sehr klar.

Carina Mitzschke: Welche Rolle spielt der Schweizer Standort für Ihre SASE- und Secure-Connectivity-Lö-



auch ein starkes Argument bei internen Diskussionen rund um die Anbieterwahl und langfristige Sicherheit zur Hand.

Carina Mitzschke: Wie passt das Label „Swiss Made Software“ in Ihre langfristige Vision?

Dennis Monner: Unsere Vision ist klar, wir wollen Open Systems als führenden europäischen Anbieter für gemanagte, souveräne Cybersecurity etablieren. Das Label ist dabei kein Ziel, sondern das Fundament. Es unterstreicht unseren Anspruch, Sicherheit nicht nur bereitzustellen, sondern Verantwortung über den gesamten Lebenszyklus zu übernehmen.

Carina Mitzschke: Welche Schritte planen Sie, um das Vertrauen in Ihre Lösungen weiter zu stärken?

Dennis Monner: Vertrauen entsteht nicht durch Auszeichnungen allein, sondern durch die konsequente Umsetzung. Deshalb investieren wir weiter in

operative Exzellenz, Automatisierung und Transparenz. Klare SLAs, nachvollziehbare Architekturen und ein enger, ehrlicher Dialog mit unseren Kunden sind für uns keine Extras, sondern der Standard. Vertrauen bedeutet bei Open Systems keine Momentaufnahme, es ist unsere tägliche Arbeit.

Carina Mitzschke: Wie verändert sich die Rolle des CISOs, und was bedeutet das für Security-Anbieter?

Dennis Monner: CISOs tragen heute die operative Verantwortung auf Vorstandsniveau, oft mit begrenzten Ressourcen aber steigenden regulatorischen Anforderungen. Gleichzeitig müssen sie Security-Architekturen für globale Organisationen mit 10.000, 30.000 oder 60.000 Mitarbeitenden absichern. Das verändert die Erwartungen an Anbieter fundamental. Gefragt sind Partner, die Security nicht nur liefern, sondern auch zuverlässig und skalierbar betreiben können. Genau hier positionieren sich Open Systems.

Carina Mitzschke: Wie vermeiden Sie, dass steigende Compliance-Anforderungen Innovation ausbremsen?

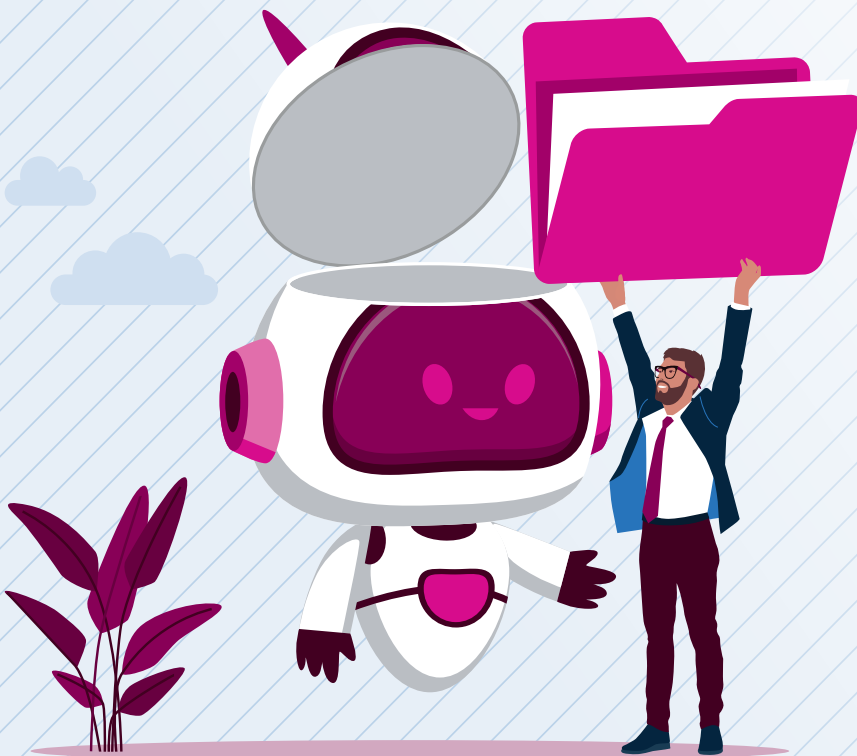
Dennis Monner: Compliance wird nur dann zum Bremsklotz, wenn sie nachträglich adressiert wird. Wir integrieren regulatorische Anforderungen von Anfang an in Architektur und Betrieb.

Das schafft Planungssicherheit für unsere Kunden und gibt ihnen die Freiheit, Innovation voranzutreiben. Auf diese Weise müssen sie nicht jedes Mal Grundsatzdiskussionen über Datenstandorte, Zuständigkeiten oder rechtliche Risiken führen.

Carina Mitzschke: Was unterscheidet Open Systems kulturell von großen internationalen Security-Anbietern?

Dennis Monner: Wir kombinieren die Stabilität eines etablierten, profitablen Unternehmens mit der Geschwindigkeit eines fokussierten Spezialisten. Entscheidungen werden dort getroffen, wo die Kompetenz sitzt, nicht in anonymen Gremien. Diese Kultur erlaubt es uns, als global aufgestelltes Multi-Millionen-Dollar-Unternehmen schnell zu handeln und gleichzeitig Verantwortung zu übernehmen. Für Kunden mit kritischen Umgebungen ist genau diese Kombination entscheidend.

Carina Mitzschke: Herr Monner, wir danken für dieses Gespräch.



A leader is one who knows the way, goes the way, and shows the way.

John C. Maxwell



Wenn Vertrauen zur Schwachstelle wird

WIE HELDELE MIT VODAFONE BUSINESS UND ZSCALER CLOUD SECURITY NEUE MASSSTÄBE IN SACHEN CYBERSICHERHEIT SETZT



CYBERANGRIFFE SIND MITTLERWEILE AN DER TAGESORDNUNG.

Daniel Baron,
IT-Leiter der HELDELE GmbH
www.heldele.de

Laut Bitkom entsteht der deutschen Wirtschaft jährlich ein Schaden von über 200 Milliarden Euro durch digitale Angriffe. Jeder zweite Angriff trifft KMUs – oft dort, wo das Vertrauen am größten ist: im eigenen Netzwerk.

Die HELDELE GmbH, ein Mittelständler aus Baden-Württemberg, hat diesen Realitätscheck früh gemacht. Als IT-Dienstleister mit über 1.500 Mitarbeitenden, verteilt auf Mutter-, Tochter- und Schwesterfirmen, weiß das Unternehmen: Sicherheit beginnt nicht am Firewall-Router – sondern bei der Haltung.

„Zero Trust“: Misstrauen als Prinzip

Die Zeiten, in denen Unternehmen intern auf blindes Vertrauen setzen konnten, sind vorbei. Heute gilt: Kein Zugriff wird automatisch für sicher gehalten. Stattdessen wird jede Verbindung und jeder Datenfluss kontinuierlich überprüft – unabhängig vom Ursprungsort des Zugriffs.

Das „Zero Trust“-Prinzip ist ein Paradigmenwechsel. Und genau dieser Ansatz überzeugte HELDELE, als es um die Modernisierung der eigenen Cybersicherheitsstrategie ging.

Vom Flickenteppich zur integrierten Lösung

IT-Sicherheit ist für HELDELE von zentraler Bedeutung, um Unternehmens- und Kundendaten zu schützen, die eigene Arbeitsfähigkeit zu gewährleisten sowie gesetzliche Vorgaben zu erfüllen. Gleichzeitig möchte die Gruppe als attraktiver Arbeitgeber wahrgenommen werden: Der Einsatz moderner, cloud-basierter Lösungen und die Möglichkeit, aus dem Homeoffice zu arbeiten, sind daher „state of the art“.

ZERO-TRUST: DER NEUE STANDARD

Drei Fragen für IT-Experte Daniel Baron

Vodafone Business: Welchen Stellenwert hat IT-Sicherheit für Ihr Unternehmen?

Daniel Baron: Die Bedeutung des Themas Sicherheit kann gar nicht zu hoch bemessen werden. Als IT-Dienstleister sind wir in vielen Branchen aktiv und sehen dort, was außerhalb unseres eigenen Unternehmens passiert. Gegenmaßnahmen schützen nicht nur unsere Unternehmens- und Kundendaten, sondern sind auch vom Gesetzgeber klar vorgeschrieben.

Vodafone Business: Wie sind Sie auf Zscaler Cloud Security aufmerksam geworden?

Daniel Baron: Im Rahmen eines Jahres-Meetings haben uns unsere Vodafone-Ansprechpartner Eduard Kaiser und

Mehmet Ediz diese Lösung vorgestellt. Der cloudbasierte Zero-Trust-Ansatz hat uns sofort überzeugt. Vodafone Business hat uns dann bei der Implementation eines ersten Pilotprojekts umfangreich unterstützt.

Vodafone Business: Welche Vorteile bringt Ihnen Zscaler konkret?

Daniel Baron: Zunächst minimiert Zscaler das Geschäftsrisiko erheblich, da die Zero-Trust-Architektur das Risiko einer Cyberattacke massiv reduziert. Unsere Mitarbeitenden werden direkt mit Applikationen und nicht mit dem Netzwerk verbunden. Alle Zugriffe werden identitätsbasiert gesteuert, protokolliert sowie auf Risiken überprüft. Zudem reduziert Zscaler die Komplexität und erhöht die Visibilität im Datenverkehr, etwa durch SSL Inspection. Das hilft uns, Bedrohungen zu erkennen sowie den Abfluss sensibler Daten zu verhindern.

MEHR WERT

Weitere spannende Erfolgsgeschichten



Für die IT-Abteilung der HELDELE GmbH war es äußerst aufwändig, diese Anforderungen mit einer VPN-Struktur und Firewalls an den verschiedenen Standorten umzusetzen. Deshalb suchte HELDELE eine moderne, übergreifende Sicherheitslösung. Das Unternehmen entschied sich für Zscaler Cloud Security von Vodafone Business.

Sicherheit aus der Cloud

Zscaler Cloud Security kombiniert cloudbasierte Sicherheitsfunktionen mit den sicheren Netzwerkdiensten von Vodafone Business. So lassen sich herkömmliche Inbound- und Outbound-Gateways durch moderne, cloudbasierte Services ersetzen. Zscaler fungiert als Web Security Gateway und sichert den Internetzugang über jede Verbindung. Die Komponente Zscaler Private Access ermöglicht als Remote-Access-Lösung den Zugriff auf interne Applikationen – sowohl „on premises“ als auch in der Cloud.

Daniel Baron, IT-Leiter der HELDELE GmbH, erklärt: „Häufige und zunehmend professionell ausgeführte Cyberangriffe sind mittlerweile an der Tagesordnung. Die von Vodafone Business angebotene Lösung passt zudem hervorragend zu unserer Unternehmensstruktur mit mehreren Tochter- und Schwesterfirmen.“

Cyberangriffe live beobachten

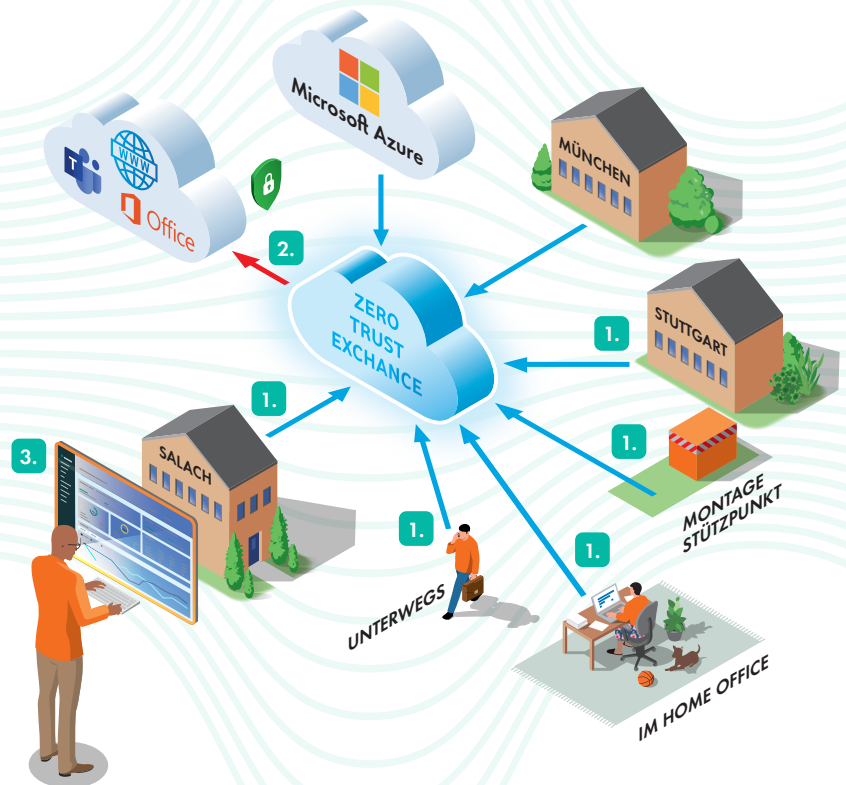
Die Migration zu Zscaler Cloud Security startete bei der HELDELE GmbH im Mai 2024 als Pilotprojekt mit rund 50 Anwendenden. Vodafone unterstützt dabei umfassend – vom Consulting bis hin zum Projektmanagement.

„Wir erhalten jetzt ein hohes Maß an Transparenz über alle Datenflüsse im Firmennetz. Als sehr hilfreiches Element hat sich auch das Modul ‚Deception‘ erwiesen – ein Honeypot, mit dessen Hilfe wir Angriffe auf unser Firmennetz beobachten können“, berichtet Daniel Baron. „Die gemeinsam implementierte Lösung überzeugt auf ganzer Linie.“

„Zero Trust“ verbindet höchste IT-Sicherheitsstandards mit einer effizienten, transparenten Vernetzung – und bleibt dabei skalierbar und flexibel. In Zusammenarbeit mit einem Partner wie Vodafone Business hebt die Lösung den Schutz von Unternehmensnetzwerken auf ein neues Niveau und schafft eine zukunftsfähige Sicherheitsarchitektur.

www.vodafone.de

CYBERSECURITY FÜR DEN MITTELSTAND



1. Geschäftsrisiko minimieren

Zscaler ermöglicht, von jedem Ort und jedem HELDELE-Gerät aus zu arbeiten. Autorisierte Nutzer werden über einen Zero Trust Exchange mit Anwendungen verbunden – niemals mit dem Netzwerk.

2. IT-Sicherheit steigern

Den Internetzugang sichert ein „Web Security Gateway“. Die Mitarbeitenden von HELDELE können somit sicher auf Cloud-Dienste wie Office 365 zugreifen.

3. Transparenz erhöhen

Das Monitoring gewährleistet eine hohe Transparenz aller Datenströme im Firmennetzwerk. Bedrohungen werden in Echtzeit erkannt und abgewehrt, bevor sie die Geräte oder das Firmennetzwerk beeinträchtigen können.



Von PoC zu produktiv

WIE DATENSOUVERÄNITÄT DIE KI-NUTZUNG SICHER UND SKALIERBAR MACHT

Zwischen Aufbruchsstimmung und Sicherheitsbedenken suchen Organisationen nach einem Weg, KI im Alltag zu nutzen. In einigen Abteilungen entstehen Pilotprojekte, andere warten ab. Nicht aus Desinteresse, sondern aus Unsicherheit, was mit ihren Daten geschieht.

Ob KI Spielwiese bleibt oder zu einem echten Wettbewerbsvorteil wird, entscheidet sich nicht allein durch die Wahl des Modells, sondern auch dadurch, ob Unternehmen die Kontrolle über ihre Daten behalten. Datensouveränität wird zum Schlüssel, um KI vom Proof of Concept in den Alltag zu überführen. Sie muss sich jedoch in Architektur und Prozessen widerspiegeln: Nur wenn der Weg der Daten sauber geregelt ist, lassen sich sensible Informationen verantwortungsvoll mit KI verarbeiten.

Wenn Daten lebendig werden

Eine Ende-zu-Ende-Verschlüsselung, Verschlüsselung mittels TLS oder sichere Storage-Systeme gelten als Standard. Sie schützen Daten, wenn sie übertragen (Data in Transit) oder gespeichert werden (Data at Rest). Für KI reicht das nicht: Modelle arbeiten mit Informationen, die während der Verarbeitung (Data in Use) im Klartext vorliegen. In dieser Phase greifen klassische Verschlüsselungsmechanismen nicht mehr. Entweder bleiben Daten verschlüsselt und sind nur extrem eingeschränkt nutzbar, oder sie liegen ungeschützt vor. Hier entsteht die Sicherheitslücke.

Es besteht die Gefahr, dass Inhalte eingesehen, kopiert oder unkontrolliert zum Training von Modellen genutzt werden – besonders bei öffentlich zu-

gänglichen Large Language Models. Heikel sind auch KI-Funktionen, die direkt in bestehende Collaboration-Tools integriert sind. Ein vermeintlich hilfreicher AI-Bot in der Seitenleiste kann im Zweifel auf weit mehr Daten zugreifen, als ein Nutzer jemals sehen dürfte – etwa auf Dokumente aus gemeinsamen Dateispeichern oder fremden Share-Point-Bereichen, wenn Rollen und Datenpfade nicht sauber getrennt sind.



KI ENTFALDET IHR POTENZIAL NUR DORT, WO UNTERNEHMEN DIE HOHEIT ÜBER IHRE DATEN BEHALTEN.

Dr. Sebastian Eder, CTO, idgard GmbH,
www.idgard.com

Souveränität als Architekturprinzip

Die Grundlage sicherer KI ist Datensouveränität: Ein Unternehmen weiß jederzeit, wo seine Informationen liegen, wer sie verarbeitet, und kann dies auch steuern. Diese Kontrolle darf nicht bei Richtlinien auf Papier enden, sondern muss technisch verankert sein. Gefragt ist eine souveräne Infrastruktur, in der Daten auch während der Verarbeitung

im eigenen Kontrollbereich bleiben. Im Kern basiert sie auf drei Bausteinen.

BAUSTEIN A:

Souveräne Cloud als Fundament

Im Zentrum dieser Infrastruktur steht eine Cloud-Umgebung, die Datenschutz zur Systemlogik macht. idgard setzt dabei auf das Sealed-Cloud-Prinzip: vollständig verschlüsselte Datenübertragung, Schlüsselverwaltung durch Nutzer sowie eine hochgesicherte Verarbeitungszone, in der Daten nur für die Dauer der Verarbeitung unverschlüsselt vorliegen – ohne Zugriff für Betreiber oder Administratoren.

BAUSTEIN B:

Sicherer Datenraum für sensible Informationen

Auf dieser Basis lässt sich ein Unternehmensdatenraum einrichten, etwa in Form des Company Drive von idgard. Er bündelt vertrauliche Informationen an einem geschützten Ort. Rollen, Rechte und Klassifizierungen sind klar geregelt, jede Freigabe oder Änderung wird automatisch protokolliert. Über einen nativen Client, der sich wie ein Laufwerk in das Betriebssystem integriert, lassen sich Daten bearbeiten und synchronisieren, ohne den geschützten Bereich zu verlassen. Für KI-Szenarien ist das entscheidend: Nur wenn bekannt ist, wo relevante Inhalte liegen und wie sie klassifiziert sind, lässt sich steuern, welche Daten in ein KI-Modell fließen dürfen.

BAUSTEIN C:

Dediziertes KI-Cluster im souveränen Perimeter

Ein weiterer Baustein ist ein dediziertes KI-Cluster, das ausschließlich innerhalb dieser abgeschirmten Zone betrieben wird. KI-Modelle laufen in einer Umgebung, die auf den Schutz von Data in Use ausgelegt ist. Prompts, Berechnun-

gen und Ergebnisse verbleiben im souveränen Perimeter und nur ausdrücklich freigegebene Resultate verlassen den geschützten Bereich. idgard entwickelt derzeit erste Prototypen einer solchen Umgebung.

Gerade für KRITIS-Unternehmen und hochregulierte Branchen ist das ein Gamechanger. So können etwa Energieversorger Netzpläne oder Lastdaten analysieren, ohne sensible Informationen in unkontrollierte Umgebungen auszulagern.

7-Punkte-Checkliste:

Sicher zur produktiven KI

Die Architektur schafft den technischen Rahmen. Ob KI im Alltag sicher funktioniert, entscheidet sich jedoch im Prozess. Die folgenden Schritte helfen Unternehmen, vom PoC zur produktiven Nutzung zu gelangen:

#1 Daten klassifizieren und Freigaberahmen definieren

Welche Daten gelten als vertraulich, welche dürfen durch KI verarbeitet werden, und was ist tabu? Eine klare Klassifizierung ist die Basis für Schutzmechanismen und Freigabeprozesse.

#2 Architektur festlegen und Datenpfade modellieren

Die Architektur definiert, wo welche Daten verarbeitet, gespeichert und wohin sie übertragen werden. Unternehmen sollten dokumentieren, wo Eingaben entstehen, wo der Output gespeichert wird und welche Systeme Daten verarbeiten. Diese Datenpfade müssen audittierbar sein.

#3 Compliance-Nachweise bündeln

Auftragsverarbeitungsverträge, ISO-Standards, Datenlokation und Prüfberichte gehören in ein zentrales Repository. Das erleichtert Prüfungen und beschleunigt Freigaben für neue KI-Use-Cases.

#4 Governance verankern und Verantwortlichkeiten zuordnen

Neben CISO und Datenschutzbeauftragtem sollten Unternehmen Verantwortliche für KI benennen. Klare Freigabeprozesse und Eskalationswege verhindern, dass KI zum ungeregelten Experimentierfeld wird.

#5 Technische Leitplanken konsequent umsetzen

Schutz von Data in Use, Netzsegmentierung und sicheres Secrets-Handling sind Pflicht. Modellaufufe sollten nur aus klar definierten Zonen erfolgen, Schlüsselmaterial strikt getrennt verwaltet werden. Vom Datenraum über das KI-Cluster bis zu Schnittstellen muss alles einem einheitlich hohen Sicherheitsstandard genügen.

#6 Schulung und Sensibilisierung der Mitarbeitenden

Nur wer Informationen richtig klassifiziert, teilt und schützt, kann im Alltag sicher handeln. Schulungen sollten daher nicht nur grundlegende Sicherheitsregeln adressieren, sondern auch konkret auf KI eingehen.

#7 Mit einem Pilotprojekt starten und skalieren

Zum Start empfiehlt es sich, klar umrissene Use Cases in einem begrenzten Anwenderkreis zu testen. Was sich im Kleinen bewährt, lässt sich auf weitere Bereiche übertragen, ohne die Organisation zu überfordern.

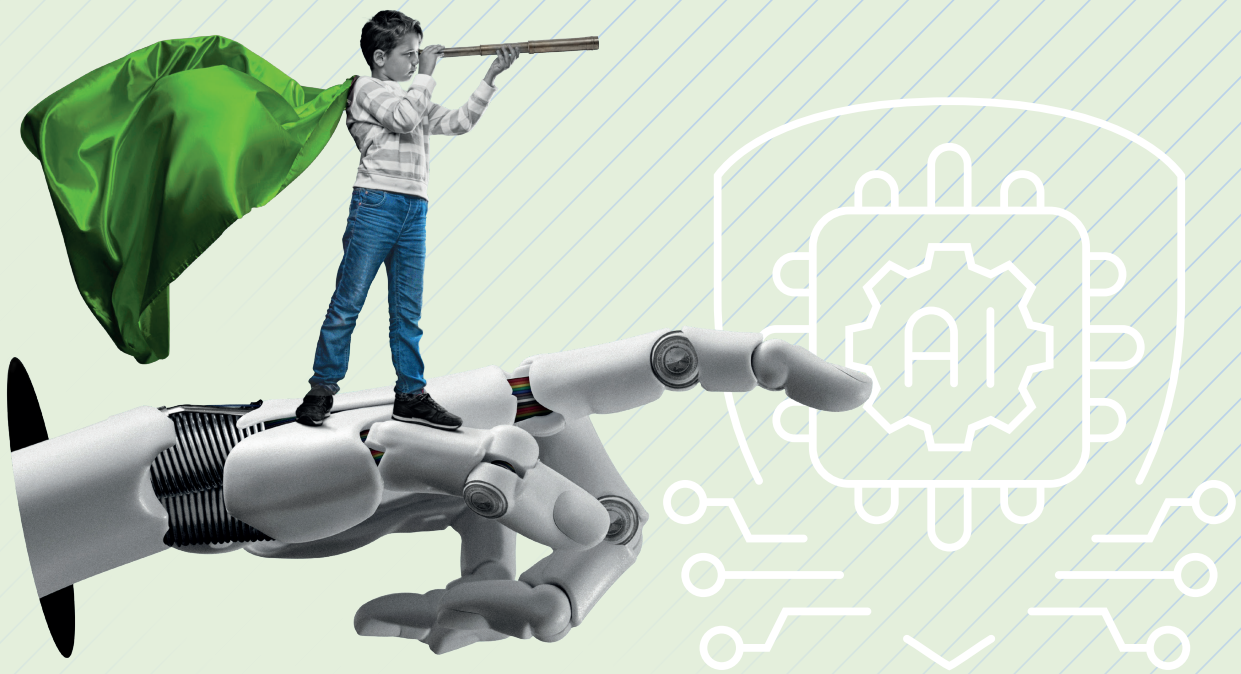
Souveränität ist die Basis für KI-Erfolg

KI entfaltet ihr Potenzial nur dort, wo Unternehmen die Hoheit über ihre Daten behalten. Souveräne Infrastrukturen sind dafür die technische Voraussetzung. Doch erst das Zusammenspiel von Management, CISO, Fachbereichen und IT-Betrieb entscheidet, ob Datensouveränität zur gelebten Praxis wird.

Gerade sicherheitskritische Branchen müssen Innovation und Regulierung in Einklang bringen, um nicht den Anschluss zu verlieren. Wer auf souveräne Architekturen setzt, schafft sich die Freiheit, KI verantwortungsvoll und skalierbar einzusetzen. Datensouveränität wird so vom Bremser zum Motor für produktive, sichere KI-Nutzung.

Dr. Sebastian Eder





DER HOHE STELLENWERT SICHERER KI

LEITFADEN FÜR SECURITY LEADER

Unternehmen setzen verstärkt auf KI. Anfang 2024 nutzten 65 Prozent der Unternehmen, die von McKinsey befragt wurden, regelmäßig generative KI, doppelt so viele wie noch 10 Monate zuvor. Es steht viel auf dem Spiel. KI-Modelle können Aufgaben ausführen, mit Systemen interagieren und sogar Anmelde-daten erstellen und verwalten. Das Aufkommen agentenbasierter KI – KI-Systeme, die in der Lage sind, eigenständige Entscheidungen zu treffen – führt zu einem verstärkten Einsatz von Maschinenidentitäten und vergrößert die Angriffsfläche in vielen Unternehmen. Wenn ein Angreifer erfolgreich eine Maschinenidentität attackieren kann, kann er auch erfolgreich die KI angreifen.

Dieser Leitfaden behandelt die Sicherheitsrisiken und Schutzmaßnahmen im Umgang mit KI-Systemen, insbesondere mit KI-Agenten und Maschinenidentitäten.

Der Leitfaden zeigt Ihnen:

- Warum KI-Sicherheit heute geschäftskritisch ist
- Wie Angreifer KI-Systeme manipulieren („KI-Ver-giftung“)
- Welche Risiken durch ungesicherte Maschinen-identitäten entstehen
- Und welche konkreten Schritte Sie ergreifen können, um Ihre KI sicher zu machen

Erfahren Sie, wie Sie Ihre KI sicher in bestehende Sicherheitsstrukturen integrieren und Risiken proaktiv managen.



**WHITEPAPER
DOWNLOAD**

Das Whitepaper umfasst 10 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/Download

VPN war gestern, jetzt zählt Zero Trust



SICHERER REMOTE-ZUGRIFF OHNE VERTRAUENSVORSCHUSS

Anstelle von VPN tritt heute Zero Trust – als sicherer, identitätsbasierter Ansatz für den Fernzugriff, mit dem sich Risiken, Komplexität und Frustration auf Anwenderseite reduzieren lassen.

Über zwei Jahrzehnte lang galt VPN (Virtual Private Network) als De-facto-Standard für einen sicheren Fernzugriff auf Unternehmensressourcen. Zu seiner Zeit war es ein Durchbruch – über verschlüsselte Tunnel zurück zum Unternehmensnetzwerk waren auch mobile Mitarbeitende in direkter Verbindung mit der „unternehmensinternen“ Sphäre.

Doch mittlerweile sehen die Rahmenbedingungen im Tagesgeschäft ganz anders aus: Teams arbeiten verteilt, Mitarbeitende greifen direkt über das Internet auf Cloud-Dienste zu und wechseln ständig zwischen Geräten und Standorten. Vertrauliche Daten liegen in privaten Rechenzentren, öffentlichen Cloud-Umgebungen und hybriden Systemen. Der „Alles-oder-nichts“-Ansatz des VPN hat damit ausgedient.

Zumal VPN-Strukturen besonders häufig im Visier von Angreifern stehen. Schwachstellen in der Software, per Phishing erbeutete Zugangsdaten und Fehlkonfigurationen ebnen den Weg. Sobald eine Verbindung erst einmal gekapert ist, liegen in der Regel oft große Teile des Firmennetzes offen – die horizontale Ausbreitung fällt leicht. Für Unternehmen, die bei der Absicherung von

hybriden, dezentralen Arbeitsszenarien weiterhin auf VPN setzen, steigen die Risiken – und die Folgen einer Kompromittierung können verheerend sein.

Zero Trust:

Zugriff, der zur Realität passt

Zero Trust ersetzt den pauschalen Netzwerkzugriff durch präzise, identitätsbasierte Entscheidungen. Statt eines Tunnels ins gesamte Unternehmensnetzwerk erhalten Nutzer nur Zugriff auf die Anwendungen, die sie tatsächlich benötigen. Jede Verbindung wird geprüft – basierend auf Identität, Gerätezustand und Kontext. Vertrauen wird nicht vorausgesetzt, sondern bei jeder Sitzung neu bewertet. So sinkt die Gefahr, dass gestohlene Passwörter, infizierte Geräte oder unerkannte Malware zum Einfallstor werden.

Schrittweise zu Zero Trust

Die gute Nachricht: VPN zu ersetzen heißt nicht, dass über Nacht alles umgekrempelt werden muss. Moderne Lösungen wie das neue Zero Trust Bundle von WatchGuard bieten Unternehmen einen praktikablen Übergang zu Zero Trust. Zunächst werden Remote-Nutzer vor internetbasierten Angriffen geschützt, dann folgt Schritt für Schritt die Einführung von identitätsbasiertem Zugriff auf eigene und SaaS-Anwendungen.

Alles in einer Plattform

WatchGuard bündelt alle Bausteine für

Zero Trust in einer einzigen cloudbasierten Architektur und liefert ein vollständiges Zero-Trust-Framework, das sich ohne Umbauten oder lange Migrationsphasen einführen lässt.

- **Identitätsschutz mit AuthPoint:** Adaptive MFA, Single Sign-On und Risikobewertung stellen sicher, dass nur verifizierte Nutzer Zugriff erhalten.
- **Sichere Geräte mit Endpoint Protection, Detection & Response (EPDR):** Jedes Gerät wird vor der Verbindung geprüft. Malware, Ransomware und unbekannte Prozesse werden automatisch blockiert.
- **Moderner Zugriff mit FireCloud Total Access:** Kontextbasierter Zugriff ersetzt klassische VPN-Tunnel. Nutzer sehen nur die Anwendungen, die sie wirklich brauchen.
- **Intelligente Korrelation mit Threat-Sync:** Identitäts-, Endpoint- und Netzwerkdaten fließen zusammen und ermöglichen schnelle, automatisierte Reaktionen.

Zero Trust für die reale Welt

Das Zero Trust Bundle fügt sich nahtlos in bestehende Umgebungen ein, adaptiert vorhandene Identitäten sowie Richtlinien und lässt sich sukzessive erweitern. Unternehmen profitieren von präzisen Zugriffsentscheidungen, gehärteten Geräten und einem Fernzugriff ohne VPN-Engpässe. Wer jetzt modernisiert, schafft mehr Sicherheit – und mehr Freiheit für Mitarbeitende, IT-Teams und das gesamte Unternehmen.

www.watchguard.de



Tools, Tempo, Training

DREI HEBEL GEGEN SPEAR-PHISHING

Spear-Phishing zählt heute zu den gefährlichsten Cyberbedrohungen für Unternehmen. Anders als bei klassischem Massen-Phishing zielen Angreifer auf einzelne Personen, häufig Führungskräfte oder Mitarbeitende der Finanzabteilung, und nutzen interne Informationen, um Vertrauen aufzubauen.

Sind sie erfolgreich, verursachen solche Attacken erhebliche finanzielle Verluste und reputative Schäden. Um das abzuwenden, braucht es ein Zusammenspiel aus integrierten Tools, schneller Reaktion und geschulten Mitarbeitenden.

Tools: Integration statt Tool-Wildwuchs

Ein wirksamer Schutz beginnt bei der technischen Basis im E-

Mail-Verkehr. Schon die Markierung externer Absender reduziert das Risiko, dass Mitarbeitende manipulierte Nachrichten für interne Kommunikation halten. Ergänzend sichern Authentifizierungsstandards wie SPF, DKIM und DMARC die Maildomäne gegen Spoofing ab.

Das allein reicht jedoch nicht. Spear-Phishing eskaliert häufig, weil Warnsignale in isolierten Tools versanden und Gegenmaßnahmen deshalb erst verzögert eingeleitet werden. Eine internationale Umfrage der OTRS AG und EasyVista zeigt:



Fast die Hälfte der knapp 300 befragten IT-Security-Spezialisten stimmt zu, dass die Vielzahl an Tools die Reaktionsfähigkeit bei Vorfällen verlangsamt.

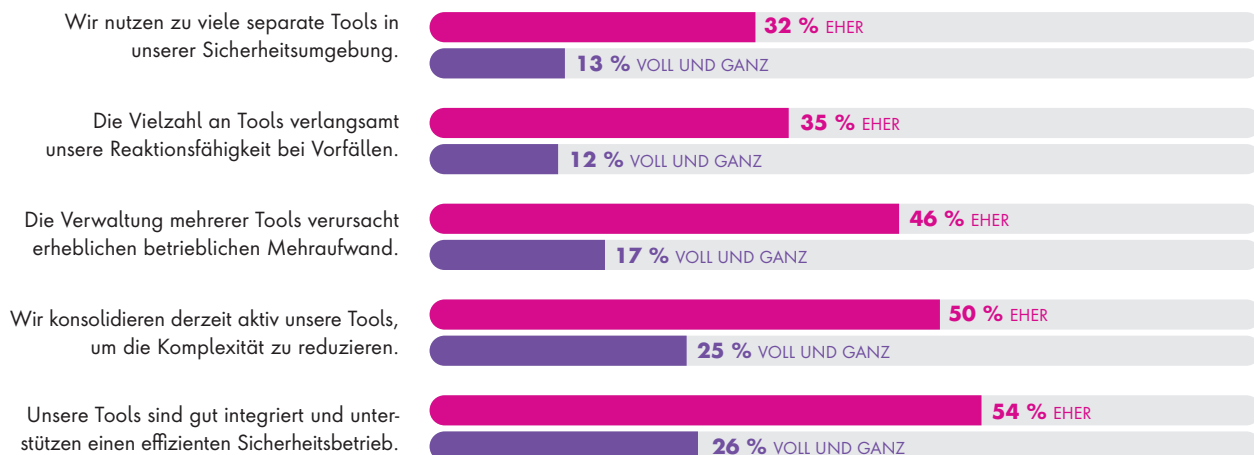
Tempo: Meldewege und Reaktion beschleunigen

Dringt eine Attacke durch, können solche Verzögerungen Millionen kosten. Mitarbeitende brauchen deshalb niedrigschwellige Wege, um verdächtige Mails oder einen erfolgreichen Angriff sofort zu melden, etwa über einen „Report-Button“ im Mailclient. Diese Meldungen müssen direkt und standardisiert ins Security Operations Center (SOC) gelangen.



WIE SECURITY-TOOLS DEN TÄGLICHEN BETRIEB BEEINFLUSSEN

Anteil der Zustimmung zur Frage: „Wie würden Sie Ihre aktuellen Sicherheitstools und deren Auswirkungen auf den täglichen Betrieb bewerten?“



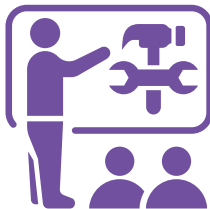
Die Security-Tool-Landschaft wirkt sich entscheidend auf Reaktionsgeschwindigkeit und operative Effizienz aus.

©2026 EasyVista & OTRS Research

Jeder Hinweis muss einen koordinierten Abwehrprozess auslösen. Das SOC braucht dafür eine gebündelte Sicht auf Meldungen, klare Priorisierung und automatisierte Workflows: etwa durch Korrelation mit SIEM-Daten, schnelle Quarantäne verdächtiger Inhalte und definierte Eskalationswege. KI kann dabei unterstützen, Muster schneller zu erkennen, Vorfälle automatisiert zu priorisieren und Abwehrmaßnahmen zu triggern. Zudem kann sie helfen, Stakeholder-Informationen und Reporting zu beschleunigen und so Ausbreitung sowie Compliance-Risiken zu begrenzen.

Training: Awareness, Kultur und Führung als Schutzschild

Im Kern greift Spear-Phishing nicht Systeme an, sondern Menschen. Angreifer arbeiten mit Zeitdruck, Hierarchiesignalen und Vertrauen, zum Beispiel durch dringende Zahlungsanweisungen „vom CEO“ oder subtil manipulierte Projektkommunikation. Generative KI macht solche Angriffe noch glaubwürdiger. Angreifer nutzen sie, um Nach-



richten noch besser zu personalisieren und sprachlich anzupassen.

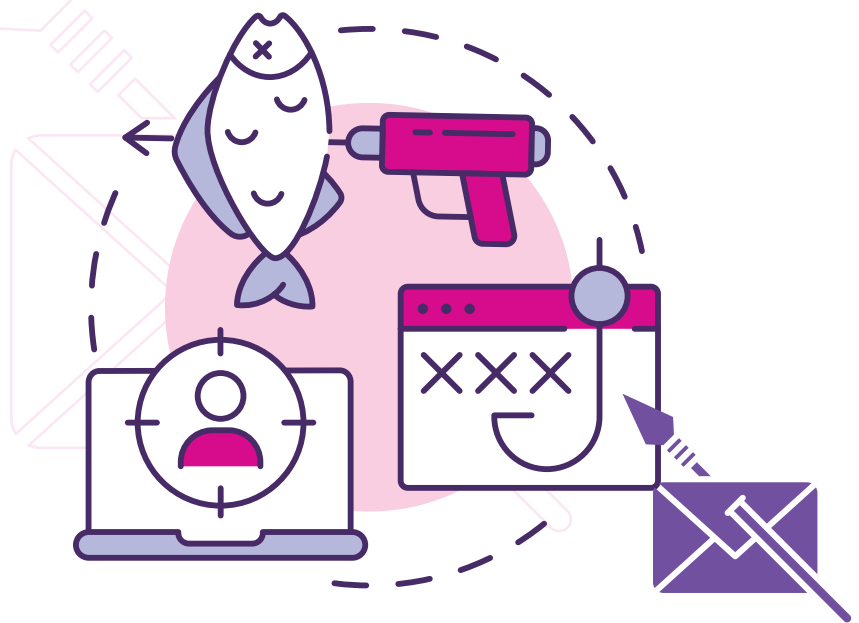
Deshalb braucht es Awareness als dauerhafte Führungsaufgabe. Schulungen sollten rollenspezifisch ansetzen, besonders bei Führungskräften, Assistenzfunktionen oder Finance-Teams. Realistische Beispiele aus der eigenen Organisation wirken dabei stärker als generische Lernmodule.

Zusätzlich liefern Phishing-Simulationen Kennzahlen

wie Click- und Report-Raten und zeigen, wo Teams noch Unterstützung brauchen. Wichtig bleibt ein konstruktiver Ansatz: Mitarbeitende müssen Sicherheit als Verantwortung erleben, nicht als Fehlerfalle.

Im Dreiklang gegen Spear-Phishing
Spear-Phishing lässt sich nicht allein mit Technik stoppen. Unternehmen, die den Dreiklang aus Tools, Tempo und Training schaffen, verhindern, dass aus einer einzelnen Mail ein Geschäftsrisiko wird.

Jens Bothe | <https://otrs.com/de/>



20.–24. April 2026

THINK TECH FORWARD

Globaler Treffpunkt für industrielle Transformation, wo Innovation und Verantwortung zusammenkommen, um die Zukunft der Produktion zu gestalten.
www.hannovermesse.de/hm26



THINK TECH FORWARD



www.it-daily.net

NIS2: Digitale Resilienz durch klare Verantwortung

GOVERNANCE-ANFORDERUNGEN 2026

Deutschland bereitet sich auf die Umsetzung der EU-Richtlinie NIS2 ab 2026 vor. Mit ihr rücken Cybersicherheit und digitale Resilienz direkt in den Kern der Corporate Governance. Der erweiterte Anwendungsbereich der NIS2-Richtlinie führt dazu, dass künftig deutlich mehr Organisationen – darunter auch mittelständische Unternehmen – erhöhten Anforderungen an Verantwortlichkeit und Transparenz unterliegen. Für Vorstände und Geschäftsleitungen bringt diese Ausweitung neue Berichtspflichten sowie eine erweiterte persönliche Haftung mit sich. Welche Prioritäten sollten Unternehmen jetzt setzen und wie kann ihre Governance-Struktur entsprechend ausgerichtet werden?

NIS2 geht über klassische Sektoren hinaus

NIS2 erweitert den Kreis der künftig regulierten Organisationen ab 2026 erheblich. Über klassische Sektoren wie Energie, Verkehr, Gesundheitswesen und Finanzdienstleistungen hinaus erfasst die Richtlinie nun auch Dienstleister sowie Akteure entlang der Lieferkette.

Für Unternehmen erfordert diese Ausweitung einen ganzheitlichen Ansatz im Risikomanagement. Während Organisationen bislang vor allem auf technische Sicherheitsmaßnahmen setzen konnten, verlangt NIS2 zusätzlich

den Aufbau organisatorischer Prozesse, klar definierter Berichtsstrukturen sowie eine unmittelbare Einbindung des Managements. In der Praxis bedeutet dies, Wertschöpfungsketten zu analysieren, Cyberrisiken systematisch zu identifizieren und bestehende Governance-Prozesse zu überprüfen. Ohne diesen strukturierten Ansatz wird es Unternehmen schwerfallen, ihre regulatorischen Verpflichtungen zu erfüllen.

Haftung von Führungskräften unter NIS2

Eine zentrale Veränderung durch NIS2 ist die Einführung der persönlichen Haftung für Führungskräfte. Vorstandsmitglieder und C-Level-Executives sind individuell dafür verantwortlich, dass die Anforderungen an Cybersicherheit und digitale Resilienz erfüllt werden. Das Versäumnis, angemessene Sicherheitsmaßnahmen umzusetzen oder Verzögerungen bei der Meldung von Sicher-

heitsvorfällen können direkte rechtliche und reputationsbezogene Konsequenzen nach sich ziehen.

Sicherheits- und Resilienzthemen sind damit keine reine IT-Aufgabe mehr. Entscheidungen über Investitionen in IT-Sicherheit, Risikoüberwachung oder Mitarbeiterschulungen müssen auf Vorstandsebene getroffen und nachvollziehbar dokumentiert werden. Unternehmen sollten Verantwortlichkeiten klar definieren und sicherstellen, dass Sicherheitsinformationen regelmäßig an die Geschäftsleitung fließen.

Konforme Governance-Strukturen aufstellen – aber wie?

NIS2 verlangt eine enge Abstimmung zwischen Vorstand, Prüfungsausschüssen und Sicherheitsbeauftragten, um Cyberrisiken proaktiv zu identifizieren und zu steuern.



Wichtige Maßnahmen hierbei sind:

- Regelmäßige Risiko- und Compliance-Überprüfung auf Vorstandsebene
- Einbindung von IT- und Sicherheitsabteilungen in strategische Entscheidungen
- Klare Berichts- und Eskalationswege, die Sicherheitsinformationen direkt an die Führungsebene liefern

In der Praxis bieten integrierte Governance-, Risiko- und Compliance-Strukturen den Unternehmen die notwendige Grundlage, um diese Anforderungen zu erfüllen. GRC-Programme schaffen Transparenz bezüglich der Sicherheitsverpflichtungen, ermöglichen prüfungsbereite Berichterstattungen und klären Verantwortlichkeiten innerhalb der Organisation. Richtig umgesetzt befähigen diese Strukturen Vorstände und Prüfungsausschüsse, effektiv zu handeln, ohne die operativen Prozesse zu verlangsamen.

Frühe Compliance verschafft Wettbewerbsvorteile

Frühzeitige Umsetzung bedeutet nicht nur Compliance, sondern legt die Basis für Vertrauen bei Kunden, Partnern und Behörden. Organisationen, die Risiken systematisch identifizieren und steuern,



FRÜHZEITIGE UMSETZUNG BEDEUTET NICHT NUR COMPLIANCE, SONDERN LEGT DIE BASIS FÜR VERTRAUEN BEI KUNDEN, PARTNERN UND BEHÖRDEN.

Peter Herr, Senior Director, Diligent,
www.diligent.com

sind weniger anfällig für Sicherheitsvorfälle und können im Falle eines Angriffes schneller reagieren.

Proaktive Governance stärkt sowohl die Reputation als auch den Wettbewerbsvorteil – ein entscheidender Faktor in zunehmend digitalen Märkten, in denen Sicherheitsvorfälle Millionen kosten und den Marktwert dauerhaft schädigen können. Unternehmen, die ihre Strukturen und Prozesse bereits heute auf NIS2 ausrichten, erfüllen nicht nur regulatorische Anforderungen, sondern

sichern langfristig auch ihre Geschäftskontinuität und Marktposition.

Schritte zur Umsetzung:

Compliance gestalten

Unternehmen müssen jetzt einen strategischen und systematischen Ansatz zur NIS2-Compliance verfolgen, beginnend mit diesen fünf Schritten:

#1 Risikomanagement: Relevante Bedrohungen für Geschäftsprozesse und Lieferketten identifizieren und bewerten.

#2 Governance-Check: Bestehende Management- und Kontrollstrukturen prüfen, Verantwortlichkeiten der Führungskräfte klären und an die Anforderungen der persönlichen Haftung anpassen.

#3 Richtlinienaktualisierung: IT-Sicherheits-, Vorfallmanagement- und Melde-Richtlinie überarbeiten, um den NIS2-Standards zu entsprechen.

#4 Berichtsprozesse für den Vorstand: Strukturierte Kanäle einrichten, damit Vorstand und Prüfungsausschuss zeitnah Sicherheitsinformationen erhalten.

#5 Kontinuierliches Monitoring: GRC-Tools implementieren, um fortlaufend Compliance, Berichterstattung und Risikomanagement sicherzustellen – Prozesse bleiben somit transparent und prüfungsbereit.

Organisationen, die jetzt handeln, legen das Fundament für digitale Resilienz, stärken das Vertrauen der Stakeholder und sichern sich einen Wettbewerbsvorteil gegenüber Wettbewerbern, die erst 2026 mit der Umsetzung beginnen.

Peter Herr



Security by Governance

SO GELINGT COMPLIANCE IM ALLTAG

Neue EU-Regulierungen wie DSGVO, NIS2 und der Cyber Resilience Act erhöhen den Compliance-Druck auf Unternehmen spürbar. Datenschutz, Cybersicherheit und Governance lassen sich nicht mehr getrennt betrachten, sondern müssen im Alltag integriert und risikoorientiert umgesetzt werden.

Viele Unternehmen stehen vor der Aufgabe, eine wachsende Zahl europäischer Regulierungen in bestehende Strukturen einzubetten. Das zentrale Problem liegt dabei weniger in der Anzahl der Vorgaben als darin, abstrakte rechtliche Anforderungen in konkrete Abläufe in IT, Security und Fachbereichen zu überführen.



UM RISIKEN BELASTBAR BEWERTEN ZU KÖNNEN, MÜSSEN UNTERNEHMEN IHRE DATEN SYSTEMATISCH EINORDNEN.

Thomas Vini Pires,
Product Specialist für Data Privacy und
AI, EQS Group GmbH, www.eqs.com

In der Praxis betrachten Unternehmen Datenschutz, Cybersicherheit und Governance häufig getrennt voneinander. Genau an dieser Stelle setzt Data Governance an. Sie übersetzt rechtliche Prinzipien in praktikable Steuerungsmechanismen und sorgt für Konsistenz. Wer Data Governance ausschließlich als juristische Pflicht versteht, erreicht zwar formale Compliance, gewinnt jedoch keine echte Kontrolle über Daten, Risiken und Systeme.

Warum Data Governance und Cybersicherheit zusammengehören

Data Governance und Cybersicherheit verfolgen ein gemeinsames Ziel: Sie sollen einen kontrollierten und verantwortungsvollen Umgang mit Daten über deren gesamten Lebenszyklus hinweg gewährleisten – von der Erhebung bis zur Löschung.

Während sich der Datenschutz lange Zeit auf Prinzipien wie Zweckbindung konzentrierte, rücken aktuelle Regelwerke wie NIS2, der Cyber Resilience Act oder DORA technische und operative Sicherheitsanforderungen in den Fokus. Sie alle zielen auf den Schutz von Systemen und die Kontinuität kritischer Dienste ab. Eine strikte Trennung dieser Bereiche ist im Alltag unpraktisch, da ein einzelner Sicherheitsvorfall meist alle Ebenen gleichzeitig betrifft.

Data Governance als verbindendes Steuerungsmodell

Auf europäischer Ebene verschiebt sich der Fokus von isolierten Einzelpflichten hin zu Resilienz- und Risikologiken. Data Governance entwickelt sich damit zum verbindenden Element zwischen Recht, IT, Security und Business.

Dabei dient sie als Steuerungsmodell, das Prioritäten festlegt und Zielkonflikte sichtbar macht. In der Praxis unterstützen hierbei spezialisierte Lösungen wie beispielsweise das EQS Privacy Cockpit. Solche Lösungen helfen Unternehmen dabei, die Anforderungen der DSGVO und des neuen AI Acts synergetisch zu verwalten, indem sie unterschiedliche regulatorische Ebenen in einer gemeinsamen Oberfläche zusammenführt. Unternehmen, die diesen integrierten Ansatz früh umsetzen, schaffen eine belastbare Grundlage für den Umgang mit operativen Risiken.

Transparenz und klare Zuständigkeiten als Grundlage

Eine wirksame Data Governance setzt Transparenz voraus. Unternehmen müssen wissen, welche Daten sie wo speichern und welche Dienstleister in-

volviert sind. Gleichzeitig braucht es klare Zuständigkeiten: Datenschutz, IT-Sicherheit und Fachbereiche müssen koordiniert zusammenarbeiten, statt isoliert Pflichten abzuarbeiten. Eine risikoorientierte Sichtweise ersetzt dabei die Vorstellung vollständiger Absicherung. EU-Regulierungen verlangen keine maximale Sicherheit, sondern angemessene Maßnahmen auf Basis konkreter Risiken.

Datenklassifizierung als Basis wirksamer Sicherheitsprozesse

Um Risiken belastbar bewerten zu können, müssen Unternehmen ihre Daten systematisch einordnen. Die Datenklassifizierung und -inventarisierung bildet

dabei das Fundament jeder Sicherheitsstrategie, da Schutzmaßnahmen nur dann sinnvoll gestaltet werden können, wenn die Sensibilität der Daten und deren Abhängigkeiten bekannt sind. In der Praxis scheitert dies jedoch häufig an dezentralen Informationen, die oft nur anlassbezogen für Audits aufbereitet werden, statt als fester Bestandteil im operativen Alltag verankert zu sein.

Um den Sprung von der Theorie in die Praxis zu schaffen, müssen diese Klassifizierungen in dauerhafte, integrierte Governance-Prozesse überführt werden. Aufsichtsbehörden legen dabei zunehmend Wert auf nachvollziehbare Entscheidungslogiken statt auf rein for-

male Vollständigkeit, während Initiativen wie der „Digitale Omnibus“ darauf abzielen, redundante Meldepflichten zu reduzieren. Unternehmen sollten sich daher weniger an starren Checklisten orientieren und stattdessen belastbare Strukturen etablieren, die Sicherheit und Compliance als kontinuierliche Aufgabe verstehen.

Fazit

Pragmatische Compliance erfordert einen Wechsel in der Herangehensweise: Weg von Silo-Projekten, hin zu funktionsübergreifenden Prozessen. Viele Vorfälle entstehen nicht durch technische Schwächen, sondern durch organisatorische Unklarheiten.

Data Governance umfasst daher auch das Organisationsdesign. Klare Zuständigkeiten und transparente Entscheidungsmechanismen helfen, Risiken frühzeitig zu erkennen. So wird Compliance zur Voraussetzung für Resilienz, Innovationsfähigkeit und digitales Vertrauen.

Thomas Vini Pires



Compliance für Cyberversicherungen

WIE UNTERNEHMEN VERSICHERUNGSPRÄMIEN SENKEN

Obwohl Unternehmen Cybersicherheitsbedrohungen als ihr Hauptanliegen einstufen, hat etwa ein Fünftel der mittleren und großen Unternehmen noch keine Cyberversicherung abgeschlossen. Warum? Der Preis der Versicherung ist das am häufigsten genannte Hindernis, da Marktforschungen darauf hindeuten, dass Unternehmen mit 30-prozentigen Prämienerrhöhungen konfrontiert sind.

Da Cyberversicherungen zu einem zentralen Bestandteil der Risikovorsorge-strategie werden, müssen Sicherheitsverantwortliche in Zeiten verschärfter Prüfung durch die Versicherer einen Weg finden, die Prämien zu minimieren.

Anforderungen für eine Cyberversicherung

Um sich für eine Cybersicherheitsversicherung zu qualifizieren, müssen Unter-

nehmen eine Reihe von technischen Sicherheitskontrollen und operativen Best Practices nachweisen. Die spezifischen Anforderungen variieren je nach Versicherer, Police und Sicherheitslage des einzelnen Unternehmens, umfassen jedoch in der Regel Strategien wie Multi-Faktor-Authentifizierung (MFA), Netzwerksegmentierung, identitätsbasierte Zugriffskontrollen und Pläne für die Reaktion auf Vorfälle.

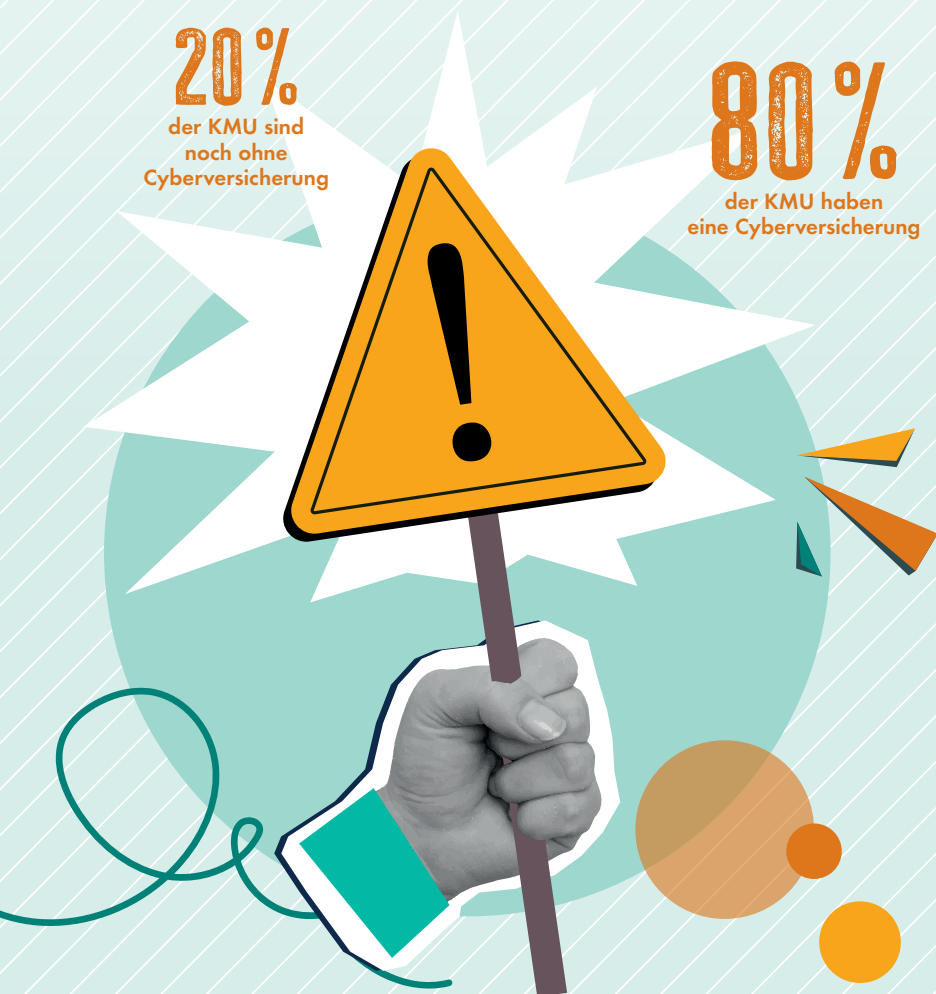
Während solche Kernanforderungen nach wie vor relevant sind, legen Versicherer angesichts der sich wandelnden Bedrohungslage zunehmend Wert auf Cyberhygiene und proaktiven Schutz. So wird beispielsweise erwartet, dass Versicherer im Jahr 2026 strengere KI-Risikomanagementprogramme sowie strengere identitätsbasierte Kontrollen verlangen werden, um die Eskalation von Privilegien angesichts einer Welle von Schadensfällen durch kompromittierte Geschäfts-E-Mails zu minimieren.

Best Practices zur Senkung der Prämien

Sich überhaupt für eine Cybersicherheitsversicherung zu qualifizieren, kann sich als schwierig erweisen – die Minimierung der Prämien ist eine noch größere Herausforderung. Sicherheitsverantwortliche, die mit der Verbesserung des Schutzes bei gleichzeitiger Kostensenkung beauftragt sind, können eine mehrdimensionale Verteidigung aufbauen, die das Vertrauen der Versicherer stärkt, indem sie wichtige Best Practices priorisieren.

20%
der KMU sind
noch ohne
Cyberversicherung

80%
der KMU haben
eine Cyberversicherung



#1 Laterale Bewegungen verhindern mittels Mikrosegmentierung:

Laterale Bewegungen sind ein wichtiger Bestandteil des Erfolgsrezepts von Cyberangreifern. Unternehmen können durch die Unterbindung lateraler Bewegungen Bedrohungen eindämmen und gleichzeitig die Kosten für Cyberversicherungen senken.

Mikrosegmentierung ist der Goldstandard bei der Verhinderung lateraler Bewegungen, da sie Bedrohungen sofort isoliert und neutralisiert. Aus diesem Grund geben fast 70 Prozent der Unternehmen an, dass ihr Cyberversicherungsanbieter eine Netzwerksegmentierung verlangt – aber nicht alle Netzwerksegmentierungsstrategien sind gleich.

Beispielsweise verwenden viele Unternehmen VLANs als grundlegende Netzwerksegmentierungsstrategie, aber dieser Ansatz ist weit weniger umfassend als die automatisierte Mikrosegmentierung. Aus diesem Grund bewerten 75 Prozent der Versicherer mittlerweile die Segmentierungslage bei der Risikoprüfung; Unternehmen mit einer höheren Segmentierungsreife geben an, dass sie niedrigere Versicherungsprämien erhalten haben.

#2 Durchsetzung von Zugriff mit geringsten Rechten überall mit granularen identitätsbasierten Kontrollen:

Der Missbrauch von Anmeldedaten ist nach wie vor der häufigste Erstzugriffsvektor für Datenverletzungen weltweit. In dieser Zeit zunehmender identitätsbasierter Angriffe verändert sich die Sichtweise von Cyber-Versicherern auf Risiken.

Inzwischen haben viele Unternehmen detektororientierte Sicherheitsstrategien eingeführt und setzen auf Lösungen wie EDR und SIEM, wodurch identi-

tätsbasierte Taktiken für Angreifer zu einem praktikablen Weg werden, um unter dem Radar zu bleiben. Beispielsweise zielen Angreifer auf Maschinenidentitäten wie Dienstkonten ab, die mittlerweile über 70 Prozent der vernetzten Identitäten ausmachen, um sich unbemerkt im Netzwerk zu bewegen.

Anbieter von Cyberversicherungen benötigen den Nachweis, dass ein gestohlener Zugangsdatensatz keine Katastrophe bedeutet. Durch die Anwendung granularer Kontrollen auf der Grundlage der Identität von Benutzern, Geräten oder Anwendungen zur Skalierung von Richtlinien für minimalen Zugriff im gesamten Netzwerk können Sicherheitsteams einen hervorragenden Schutz vor Identitätsbedrohungen nachweisen.

TREIBER DES MARKTWACHSTUMS

Der weltweite Markt für Cybersicherheitsversicherungen ist bis 2026 auf rund 20 Milliarden US-Dollar angewachsen – ein Trend, der sich voraussichtlich fortsetzen wird.

• RANSOMWARE-KAMPAGNEN

• REGULATORISCHER DRUCK



• WACHSENDE SCHUTZLÜCKEN

• KI-GESTÜTZTE ANGRIFFE

#3 Sicherer privilegierter Zugriff mit Just-in-Time-MFA:

Selbst wenn ein Netzwerk keine Fehlkonfigurationen oder übermäßigen Berechtigungen aufweisen würde, blieben bestimmte Konten, Ports und Ressourcen für Hacker ein Ticket zur Eskalation von Berechtigungen. Durch die Anwendung von Just-in-Time-MFA auf alle Administratorkonten und privilegierten Protokolle wie RDP, SSH und WinRM fügen Unternehmen eine wichtige Schutzebene hinzu, um wichtige Wege abzuschneiden, ohne den Betrieb zu stören.

Die Kombination aus Netzwerksegmentierung und Identitätssegmentierung, verstärkt durch Just-in-Time-MFA, schafft eine mehrdimensionale Verteidigung,

die Cyberversicherern zeigt, dass ein Unternehmen darauf vorbereitet ist, Sicherheitsverletzungen in Echtzeit einzudämmen.

Geschäftsresilienz priorisieren – Incident Response transformieren

Die Planung der Reaktion auf Vorfälle (Incident Response, IR) reduziert die durchschnittlichen Kosten einer Datenverletzung um fast 250.000 US-Dollar. Daher ist es nicht verwunderlich, dass Versicherungsanbieter häufig IR-Pläne als Voraussetzung für den Versicherungsschutz verlangen. Im Kontext der heutigen dynamischen digitalen Landschaften sind Vorlagen für die Reaktion auf Vorfälle jedoch schnell veraltet.

Letztendlich wollen Cyberversicherer den Nachweis, dass ein Unternehmen darauf vorbereitet ist, unvermeidliche Cybervorfälle mit minimalen Auswirkungen zu bewältigen. Anstatt sich ausschließlich auf starre und von Natur aus reaktive IR-Pläne zu konzentrieren, sollten Unternehmen proaktiven Kontrollen Vorrang einräumen, um die Widerstandsfähigkeit ihres Unternehmens zu verbessern.

Über die Demonstration von Erkennungs- und Reaktionsfähigkeiten hinaus können Sicherheitsteams nachweisen, dass eine automatisierte Eindämmung von Bedrohungen die Anforderungen der Versicherer an die Resilienz besser erfüllt.

Zukunftssichere Compliance

Die Cyberversicherung des Erstversicherers deckt häufig Gebühren, Bußgelder oder Strafen ab, die sich aus einer Verletzung ergeben. Der erhöhte regulatorische Druck bedeutet daher, dass Versicherer zunehmend nach Möglichkeiten suchen, Zahlungen aufgrund von Verstößen zu vermeiden. Angesichts einer Vielzahl von regulatorischen Anforderungen und bewährten Verfahren der Branche müssen Unternehmen die zentralen Cybersicherheitsstandards imple-



SICH ÜBERHAUPT FÜR EINE CYBERSICHERHEITS-VERSICHERUNG ZU QUALIFIZIEREN, KANN SICH ALS SCHWIERIG ERWEISEN.

Kay Ernst,
Manager DACH, Zero Networks,
www.zeronetworks.com

mentieren, die für alle Rahmenwerke gelten, um sowohl Auditoren als auch Versicherer zufrieden zu stellen.

Diese Kontrollen und Verfahren sollten kontinuierlich an Netzwerkänderungen

angepasst werden, um zu signalisieren, dass die Compliance-Strategie eines Unternehmens flexibel ist, und gleichzeitig sicherzustellen, dass Cyberbedrohungen nicht durch versteckte Sicherheitslücken schlüpfen können.

Sicherheit stärken, Cyberversicherungsprämien senken

Cyberversicherer müssen wissen, dass die Sicherheitslage eines Unternehmens auf der Grundlage einer Zero-Trust-Architektur für die Geschäftskontinuität ausgelegt ist. Eine entsprechende Plattform kombiniert fortschrittliche Lösungen für Netzwerksegmentierung, Identitätssegmentierung und Zero-Trust-Netzwerkzugang, die durch MFA auf Netzwerkebene verstärkt werden, um einen mehrdimensionalen Schutz zu bieten, der sich dynamisch an veränderte Netzwerke und sich entwickelnde Risiken anpasst. Dies gelingt mit einer sich selbst schützenden Netzwerkarchitektur, die das Vertrauen der Versicherer und die Sicherheit der Sicherheitsteams stärkt und gleichzeitig die Prämien senkt.

Kay Ernst



infodas Cybersecurity.

Nicht nur compliant, sondern wirklich sicher!

Vertrauensvolles Cybersecurity Consulting auf militärischem Sicherheitsniveau.
Spezialisiert auf Behörden, KRITIS und hochregulierte Bereiche.

+++ VS-NfD Fitness +++ ISMS +++ Sicherheitskonzepte +++



Let's get in touch!

www.infodas.de

+49 221 70912-0





VERSICHERT HEISST NICHT ABGESICHERT!

EINE CYBERVERSICHERUNG STOPPT KEINE CYBERANGRIFFE

Wer glaubt, eine Cyberversicherung hilft, sich gegen Hacker zu schützen, täuscht sich leider. Sie ist kein Abwehrschild gegen Angriffe, sondern ein Weckruf. Sie zeigt klar, wo die IT-Sicherheitslücken im eigenen Unternehmen liegen – vom schwachen Passwort über ungesicherte Backups bis hin zu fehlenden Erkennungsmechanismen für Angriffe.

IT Security-Spezialisten haben verstärkt alle Hände voll zu tun. Unabhängig von Größe und Branche werden Unternehmen und Organisationen immer häufiger Ziel von Cyberangriffen. Vor diesem Hintergrund denken Entscheider an eine Cyberversicherung. Sie glauben, im Falle eines Angriffs würden sie die finanziellen Kosten für Betriebsausfall, die Wiederherstellung ihrer Daten, Schadensersatzansprüche von Kunden oder Partnern und ggf. Lösegeldzahlungen ausgleichen. Viele haben die (falsche) Vorstellung, dass sie eine Art „Rundumschutz“ ist, der automatisch alle Risiken abdeckt.

Im Whitepaper erfahren Sie, warum eine Police kein Ersatz für echte Cybersecurity ist – inklusive praktischer Checkliste am Ende, mit der Sie den Sicherheitsstatus Ihres Unternehmens direkt überprüfen können.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/Download



Cyberresilienz gemeinsam stärken

AKTIVE VERSICHERUNGSLÖSUNGEN

Aufgrund der fortschreitenden Digitalisierung wachsen die Angriffsflächen, und damit auch die Zahl der Cyberangriffe. Während gezielte Hackerangriffe nur etwa ein Drittel aller Angriffe ausmachen, nutzen die meisten Angreifer bewusst bekannte Schwachstellen aus. Dadurch wird grundsätzlich jedes Unternehmen, unabhängig von seiner Größe, potenzielles Ziel eines Hackerangriffes. Es trifft in der Regel das „schwächste Glied“.

Als einer der größten Cyberversicherer am deutschen Markt begleitet die ERGO Versicherung AG mehrere hundert Cybervorfälle pro Jahr über alle Branchen hinweg: vom Kleinstunternehmen bis hin zur Aktiengesellschaft mit Milliardenumsätzen. Dadurch gewinnt der Versicherer einen guten Überblick über die verschiedenen Angriffsflächen eines Unternehmens. Die zentrale Erkenntnis: Es ist unerlässlich, sich laufend im Rahmen eines proaktiven Risikomanagements mit den bestehenden Sicherheitslücken im eigenen Unternehmen auseinanderzusetzen. Es kommt jedoch nicht darauf an, alle denkbaren Szenarien auszuschließen, sondern priorisiert die einfachsten Einfallstore abzusichern.

Outside-In Scans

Outside-In Scans spielen dabei eine entscheidende Rolle. Aus der Perspektive eines Angreifers wird die IT-Infrastruktur eines Unternehmens online und von au-

ßen auf Schwachstellen überprüft. Ausgehend von der Webdomain wird zunächst die IT-Infrastruktur identifiziert, z.B. Server, Webanwendungen, Datenbanken, VPN-Zugänge oder andere kritische Systeme. Basierend auf der identifizierten Infrastruktur wird nach potenziellen Schwachstellen gesucht, sei es veraltete Software, unsichere Konfigurationen oder veröffentlichte Daten im Darknet. Outside-In Scans bieten eine gute Möglichkeit zur regelmäßigen Überwachung der nach außen sichtbaren Angriffsflächen. Durch den hohen Automatisierungsgrad lassen sie sich im erweiterten Risikomanagement sinnvoll einsetzen. Sie unterstützen beim effizienten Management von Lieferketten und helfen Unternehmen bei der Erfüllung regulatorischer Anforderungen, wie z.B. NIS2.

Auch die ERGO Versicherung hat die Vorteile von Outside-In Scans erkannt. Gemeinsam mit dem Partner cysmo werden diese im Rahmen einer aktiven Versicherungslösung genutzt und unterstützen damit Kunden aktiv beim Thema IT-Sicherheit. Viele Cybervorfälle hätten verhindert werden können oder wären weniger schwerwiegend ausgefallen, wenn die Betroffenen rechtzeitig über bestehende, bereits erfolgreich ausgenutzte, Schwachstellen informiert und ent-



PRÄVENTION UND PROAKTIVES RISIKO-MANAGEMENT SIND DAS GEBOT DER STUNDE.

Maren Schweier, Teamleiterin
Produktmanagement Cyber,
ERGO Versicherung AG, www.ergo.de

sprechend sensibilisiert worden wären. Daher zeigt ERGO auf, welche potenziellen Gefährdungen sich aus den von außen sichtbaren Sicherheitslücken ergeben und geben Handlungsempfehlungen, wie die Schwachstellen behoben werden können. Aus der Betreuung von mehreren Tausend Gewerbekunden hat ERGO einen guten Einblick darüber, wie erfolgreiche Angriffe auf vergleichbare Systeme aussehen, wie andere Unternehmen das Beheben der Schwachstellen im laufenden Betrieb bewerkstelligt haben, ob der aktuelle Patch ausreichend ist oder ob dies zu Folgeproblemen führte. IT-Verantwortliche bringen dadurch ihre Expertise zur Schließung der Sicherheitslücken direkt ein und können ihre Ressourcen effizienter einsetzen.

Fazit

Wer heute IT-Sicherheit verantwortet, weiß: Reaktive Schadensbegrenzung reicht längst nicht mehr aus. Prävention und proaktives Risikomanagement sind das Gebot der Stunde. Denn wenn sich IT-Verantwortliche und Cyberversicherer ergänzen, wird der Versicherer vom reinen Risikoträger und Schadenregulierer zum Partner für das Thema IT-Sicherheit. Gelingt dies, ist die Cyberresilienz im Unternehmen gestärkt und man ist den Angreifern einen Schritt voraus.

Maren Schweier





Besseres Scoring in der Cyberversicherung

EIN LEITFADEN ZUR PRÄMIENOPTIMIERUNG

In einer Welt, in der digitale Bedrohungen allgegenwärtig sind, haben Cyberversicherungen für Unternehmen jeder Größe an essentieller Bedeutung gewonnen. Doch ähnlich wie bei anderen Versicherungsarten beeinflusst das individuelle Risikoprofil maßgeblich die Höhe der Prämie. Das sogenannte Scoring – eine risikobasierte Bewertung Ihres Unternehmens – entscheidet darüber, ob Sie günstige Konditionen erhalten oder einen Aufschlag zahlen müssen. Die Prämienunterschiede können dabei erheblich sein: Zwischen einem Unternehmen mit schwachem und einem mit starkem Sicherheitsprofil liegen oft 40 bis 60 Prozent Preisdifferenz. Dieser Leitfaden zeigt, wie Sie Ihr Cyberrisiko-

Profil verbessern und damit Ihre Versicherungsprämien senken können.

Warum Scoring so wichtig ist

Versicherer bewerten bei der Cyberversicherung nicht nur Branche und Unternehmensgröße, sondern vor allem Ihre konkreten IT-Sicherheitsmaßnahmen. Je besser diese sind, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs – und desto attraktiver sind Sie für den Versicherer. Ein gutes Scoring signalisiert dem Versicherer, dass Sie ein verantwortungsvoller Risikoträger sind, der proaktiv mit Gefahren umgeht. Dabei gilt: Versicherer nutzen heute häufig automatisierte Bewertungstools, die Ihre Angaben im Antragsfra-

gebogen systematisch auswerten. Widersprüche oder Lücken fallen sofort auf und führen zu Rückfragen oder Ablehnungen.

Der Weg zu einem besseren Scoring

Die Optimierung Ihres Cyber-Scorings ist kein punktuelles Projekt, sondern ein kontinuierlicher Prozess, der in Ihre IT-Sicherheitsstrategie integriert sein sollte.

#1 Grundlagen schaffen: Dokumentation und Struktur

Versicherer schätzen Transparenz. Eine klare Dokumentation Ihrer IT-Infrastruktur, Sicherheitsrichtlinien und Verantwortlichkeiten bildet die Basis. Dazu

CHECKLISTE

für ein besseres Cyberversicherungs-Scoring

Nutzen Sie diese Punkte als Selbstbewertung und Aktionsplan:

Organisation & Dokumentation

- Aktuelle Inventarliste aller IT-Systeme, Software und kritischen Daten
- Schriftliche Sicherheitsrichtlinien (Passwort, Datenschutz, Nutzung)
- Klare Zuordnung von Sicherheitsverantwortlichkeiten
- Verträge mit IT-Dienstleistern enthalten Sicherheitsklauseln (AVV)

Technische Schutzmaßnahmen

- Next-Generation-Firewall (NGFW) mit aktivierten Security-Funktionen
- EDR/XDR-Lösung auf allen Endgeräten und Servern
- Zentrale Patch-Management-Strategie mit regelmäßigen Updates
- Multi-Faktor-Authentifizierung (MFA) für alle externen Zugänge und Admin-Accounts
- Verschlüsselung sensibler Daten (im Transit und at Rest)
- Segmentierung des Netzwerks (etwa Gäste-WLAN, Produktionsnetz)
- Sicherheitskonfiguration (Hardening) für Server und kritische Systeme

Mitarbeiter & Zugriff

- Regelmäßige Security-Awareness-Schulungen (mind. jährlich, mit Dokumentation)
- Simulierte Phishing-Tests zur Sensibilisierung
- Prinzip der geringsten Berechtigungen umgesetzt
- Formales On- und Offboarding-Prozedere für Zugänge
- Admin-Accounts werden nur für administrative Tätigkeiten genutzt
- PAM/PIM-Lösung für Verwaltung privilegierter Accounts
- Zentrale IAM-Lösung für Identity & Access Management
- Session-Recording für administrative Zugriffe
- Just-in-Time (JIT) Zugriffsvergabe für sensible Systeme
- Zero-Trust-Prinzipien in kritischen Bereichen umgesetzt

Notfallvorsorge & Kontinuität

- Vorhandener und getesteter Incident-Response-Plan
- Regelmäßige, isolierte Backups der kritischen Daten und Systeme
- Dokumentiertes und geübtes Disaster-Recovery-Konzept
- Definierte Kommunikationswege im Schadensfall (inkl. PR/Recht)

Verifikation & Verbesserung

- Regelmäßige Sicherheits-Scans (etwa Vulnerability Assessments)
- Externe Penetrationstests (mind. jährlich)
- Umsetzung von Maßnahmen aus Audits/Tests
- Angestrebte oder vorhandene Zertifizierungen (ISO 27001, BSI-Grundschutz, etc.)
- Regelmäßige Risikoanalysen und Review der Sicherheitsmaßnahmen

gehören ein aktuelles Asset-Management (welche Systeme und Daten existieren wo?) und definierte Prozesse für den Ernstfall. Unstrukturierte IT-Landschaften werden als hohes Risiko eingestuft. Häufiger Fehler: Viele Unternehmen haben Richtlinien, können diese aber nicht nachweisen oder zeigen, dass sie gelebt werden.

#2 Technische Sicherheitsmaßnahmen systematisch umsetzen

Hier geht es um die konkreten Schutzvorkehrungen. Eine mehrstufige Verteidigungsstrategie (Defense-in-Depth) ist überzeugend. Dazu zählen nicht nur Basisvorkehrungen wie Firewalls und Virenschutz, sondern auch moderne Maßnahmen wie Endpoint Detection and Response (EDR), regelmäßige Sicherheitsupdates (Patch-Management) und eine starke Absicherung des Remote-Zugriffs. Besonders kritisch bewerten Versicherer fehlende Multi-Faktor-Authentifizierung (MFA) – mittlerweile ein K.O.-Kriterium bei vielen Anbietern.

#3 PAM und Zero Trust als neue Standards

Besonders im Fokus stehen heute Identity & Access Management (IAM) und das Management privilegierter Zugänge (PAM/PIM). Versicherer bewerten kritisch, wie Sie administrative Accounts schützen: Werden privilegierte Zugänge überwacht? Gibt es eine zeitlich begrenzte Rechtevergabe (Just-in-Time Access)? Sind alle Admin-Aktivitäten protokolliert? PAM-Lösungen, die privilegierte Accounts isolieren und jede Nutzung dokumentieren, gelten als Goldstandard. Ergänzend gewinnt die Zero-Trust-Architektur an Bedeutung – ein Sicherheitsmodell, das grundsätzlich keinem Zugriff vertraut und jeden kontinuierlich verifiziert. Statt auf Perimeter-Schutz zu setzen, wird jeder Zugriff einzeln authentifiziert und autorisiert. Unternehmen mit Zero-Trust-Ansätzen signalisieren Versicherern höchste Sicherheitsreife.

#4 Der Mensch als kritischer Faktor

Da die meisten Cybervorfälle auf menschliches Versagen zurückgehen (Studien nennen 80-90 Prozent), legen

Versicherer großen Wert auf Sicherheitsschulungen. Regelmäßige, dokumentierte Awareness-Trainings für alle Mitarbeiter sind ein starkes Signal. Ebenso wichtig sind klar geregelte Zugriffsberechtigungen (Prinzip des geringsten Privilegs) und spezielle Schulungen für Administratoren. Praxistipp: Simulierte Phishing-Tests mit anschließender Schulung der „Klicker“ zeigen messbare Lernfortschritte.

#5 Vorbereitung auf den Ernstfall

Ein Unternehmen, das einen Incident-Response-Plan hat und diesen regelmäßig testet, zeigt, dass es auch im Schadensfall handlungsfähig bleibt. Dies reduziert die potenzielle Schadenshöhe und wirkt sich positiv auf das Scoring aus. Dazu gehört auch ein aktuelles, gesichertes Backup-Konzept nach der 3-2-1-Regel (3 Kopien, 2 verschiedene Medien, 1 offline), das regelmäßig auf Wiederherstellbarkeit überprüft wird. Wichtig: Ein ungetestetes Backup ist im Ernstfall oft wertlos.



#6 Externe Bestätigungen einholen

Zertifizierungen wie ISO 27001 oder branchenspezifische Standards sind der sichtbare Beweis für ein etabliertes Informationssicherheits-Managementsystem (ISMS). Auch regelmäßige Penetrationstests oder Sicherheitsaudits durch externe Dienstleister liefern objektive Nachweise für Ihre Sicherheitsbemühungen. Diese externen Validierungen können Prämienzuschläge von 10 bis 20 Prozent vermeiden.

Häufige Fehler vermeiden

Aus der Praxis zeigen sich immer wieder die gleichen Stolpersteine: Unternehmen überschätzen ihr Sicherheitsniveau, weil grundlegende Maßnahmen vorhanden sind, während kritische Lücken bestehen. Typisch ist etwa eine Firewall ohne aktuelle Regelwerke, Backups ohne Restore-Tests oder Schulungen ohne Erfolgskontrolle. Auch widersprüchliche Angaben im Antrag fallen negativ auf: Wer angibt, MFA zu nutzen, aber nur für einen Teil der Zugänge, schadet seiner Glaubwürdigkeit. Transparenz zahlt sich aus – auch bei bestehenden Schwachstellen.

Ein weiterer kritischer Punkt: privilegierte Accounts ohne besondere Überwachung. Admin-Zugänge ohne PAM-Lösung, fehlende Protokollierung oder dauerhaft vergebene Vollzugriffe sind für Versicherer ein Alarmsignal – diese Accounts sind das bevorzugte Angriffsziel bei Cyberattacken.

Der nächste Schritt

Sammeln Sie zunächst die Dokumente und Nachweise für bereits umgesetzte Maßnahmen. Führen Sie dann eine Lückenanalyse anhand der Checkliste durch und priorisieren Sie die wichtigsten Maßnahmen mithilfe der Tabelle. Bei der nächsten Versicherungsanfrage oder Vertragsverlängerung können Sie so ein umfassendes Sicherheitspaket vorlegen.

PRIORISIERUNG: WAS BRINGT AM MEISTEN?

„Scoring-Impact“ bezieht sich auf die Auswirkung der Maßnahme auf die Versicherungsprämie. „Sehr hoch“ bedeutet potenziell 15-25% Prämienreduktion.

Sehr hoher Scoring-Impact

Sehr hohe Priorität – sofort starten

- Multi-Faktor-Authentifizierung (MFA)
- PAM-Lösungen für privilegierte Accounts
- Isolierte, getestete Backups (3-2-1 Regel)

Hoher Scoring-Impact

Hohe Priorität – zeitnah umsetzen

- EDR/XDR-Lösung auf allen Endgeräten
- IAM/IAG-System implementieren
- Security-Awareness-Training (dokumentiert)
- Patch-Management-Prozess etablieren

Mittlerer Scoring-Impact

Mittlere Priorität – strategisch planen

- Zero-Trust-Architektur (schrittweise)
- Netzwerksegmentierung
- Incident-Response-Plan entwickeln und testen
- Externe Penetrationstests

Hoher Scoring-Impact

Langfristig – für maximale Exzellenz

- ISO 27001 Zertifizierung

Denken Sie daran: Die Investition in IT-Sicherheit verbessert nicht nur Ihr Scoring, sondern schützt vor allem Ihr Unternehmen vor existenziellen Bedrohungen. Ein geringerer Versicherungsbeitrag ist dabei ein willkommener Nebeneffekt einer grundlegend resilienteren Organisation. Als Faustregel gilt: Jeder in IT-Sicherheit investierte Euro spart durchschnittlich drei bis fünf Euro an potenziellen Schadenskosten.

Weitere Hilfestellungen

Für die praktische Umsetzung bieten sich mehrere Ressourcen an: Muster-Fragebögen und Risiko-Checks von Versicherern geben Ihnen einen Eindruck, worauf es ankommt. Vergleichs- und Vermittlungsportale ermöglichen Tarifvergleiche, sollten aber immer durch persönliche Beratung ergänzt werden. Checklisten der Allianz für Cyber-Sicherheit (ACS) und des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) bieten branchenspezifische Orientierung. Ein Testlauf mit den Fragebögen verschiedener Versicherer hilft, Wissenslücken zu identifizieren, bevor Sie den offiziellen Antrag stellen.

DIE CYBER-SCORING-PYRAMIDE

Ihr Weg zu optimalen Versicherungskonditionen



Noch ein Tipp zum Thema Tarifrechner: Ein reiner Online-Tarifrechner wird der Komplexität einer Cyberversicherung

selten gerecht. Der Wert liegt in der professionellen Beratung und der individuellen Anpassung des Deckungsschutzes an Ihre spezifischen Risiken.

Ulrich Parthier | www.it-daily.net



WAS SIND LOTL-ANGRIFFE?

DIE 10 AM HÄUFIGSTEN MISSBRAUCHTEN TOOLS

LOTL (Living Off the Land) steht für Angriffe, bei denen Angreifer legitime Systemverwaltungstools, die in einer kompromittierten Umgebung standardmäßig installiert sind, für ihre kriminellen Machenschaften missbrauchen. Auf diese Weise nehmen sie am normalen Systembetrieb teil, sodass es auch für die leistungsfähigsten Erkennungs- und Reaktionstools sowie SOC-Teams schwierig ist zu erkennen, was im System vor sich geht. Die Angreifer schleusen keine externe Schadsoftware ein, sondern nutzen die eigentlich vertrauenswürdigen, systeminternen Dienstprogramme für ihre Zwecke. Die Begriffe LOTL und Living-Off-the-Land-Binaries (LOLBins) werden häufig synonym zur Beschreibung dieser Art von Angriffen verwendet.

Das Grundprinzip von LOTL-Angriffen besteht darin, dass das natürlicherweise vorhandene Vertrauen in legitime, digital signierte Tools missbraucht und zur Umgehung von Sicherheitsmechanismen genutzt wird, deren Ziel unbekannte oder unsignierte Dateien sind.

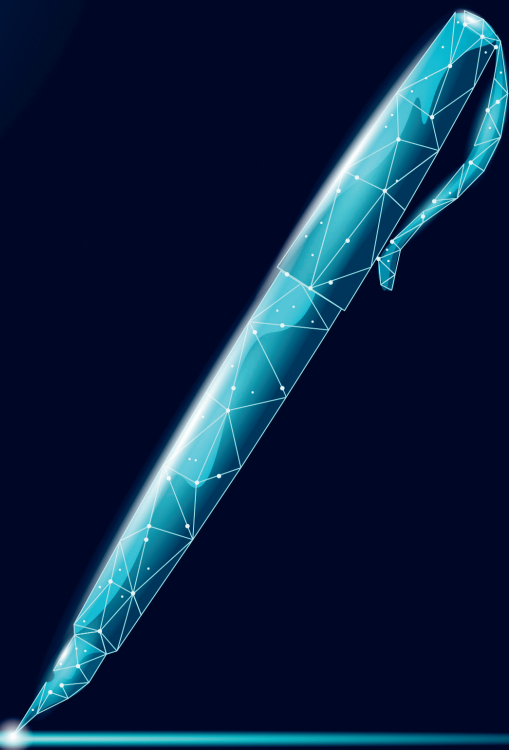
Im folgenden Whitepaper erfahren Sie kompakt und praxisnah, wie Living-Off-the-Land-Techniken funktionieren, warum sie so schwer zu stoppen sind und worauf Unternehmen jetzt achten müssen. Jetzt herunterladen!



WHITEPAPER DOWNLOAD



Das Whitepaper umfasst 25 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download



Cyberattacken: Die neue Realität

WARUM VIELE FIRMEN
EIN LEICHTES ZIEL SIND

Jaguar, die European Space Agency und Vorwerk: Drei Unternehmen aus unterschiedlichen Branchen mit einer Gemeinsamkeit: Sie waren bereits Opfer einer Cyberattacke mit zum Teil gravierenden Folgen. Im Interview erklärt Tim Berghoff, Security Evangelist bei G DATA CyberDefense, warum Unternehmen Cyberattacken oft erst zu spät erkennen und wie Verantwortliche trotz Fachkräftemangel ihre IT wirksam schützen können.

it security: Warum erkennen viele IT-Verantwortliche Cyberangriffe zu spät oder gar nicht?

Tim Berghoff: Es fehlt bei vielen Firmen, die einer Cyberattacke zum Opfer fallen, an grundlegenden Sicherheitsmaßnahmen: klare Prozesse, Notfallpläne oder Security Awareness unter Mitarbeitenden. Wenn dann eine Phishing-Mail eintrifft oder ein veralteter Dienst offen zum Internet exponiert ist, haben Angreifergruppen leichtes Spiel. Viele Unternehmen haben zudem kein durchgängiges Logging- und Monitoring-Konzept. Ereignisse werden nur punktuell geloggt und wichtige Event-IDs fehlen. Damit sind frühe Warnzeichen deutlich schwerer zu erkennen. Dazu kommen schlechte Meldewege. Die Mitarbeitenden wissen im Zweifel nicht, was zu tun ist, wenn sie etwa auf eine Phishing-Mail hereingefallen sind. Viele IT-Teams sind oft

dünn besetzt. Da reicht es nur für das Nötigste im Tagesgeschäft. Wichtige Themen wie Prävention, Awareness Trainings und saubere Prozesse fallen oft unter den Tisch.

it security: Was sind typische Angriffsmuster?

Tim Berghoff: Klassische Einfallstore sind schwache Passwörter, nicht gepatchte Systeme sowie fehlende Zwei-Faktor-Authentifizierung bei VPN-Zugängen. Ein weiteres Sicherheitsrisiko, das sehr verbreitet ist: Nutzt ein IT-Admin ein und dasselbe Passwort für sein persönliches Profil und den Admin-Zugang, die dann auch nicht zusätzlich mit einer Zwei-Faktor-Authentifizierung abgesichert sind, können sich die Täter ungehindert im Netz bewegen, Daten ausleiten und Systeme verschlüsseln. Viele Firmen haben sehr lasche Passwort-Richtlinien. Beispielsweise erfolgt die automatische Entsperrung nach Zeit X, wenn mehrfach versucht wurde, sich mit einem fehlerhaften Passwort anzumelden. Das ist faktisch eine Einladung für Angreifergruppen.

it security: Welche Fallstricke können bei der Aufarbeitung eines erfolgreichen Angriffs aufkommen?

Tim Berghoff: Ohne Notfallkonzepte dauert schon die Aufklärung über die aktuelle Lage lange. Zusätzlich bricht die Kommunikation zwischen Außenstellen weg und die IT kämpft parallel mit Krisenkommunikation, Forensik und

Wiederaufbau. Viele unterschätzen einfach die bestehenden Abhängigkeiten. Erst der Vorfall zeigt, welche Dienste miteinander verknüpft sind – vom Identitäts- und Zugriffsmanagement bis zu Fachverfahren. Wer seine Kritikalitäten nicht vorher bewertet hat, priorisiert unter Stress und verliert dabei wertvolle Zeit.

it security: Was passiert, wenn ein Angriff erfolgreich ist?

Tim Berghoff: Wenn Cyberkriminelle Daten und Systeme verschlüsselt ha-

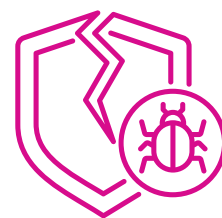




Erst dann ist eine geregelte Kommunikation wieder möglich und wichtige Services sind abrufbar. Idealerweise sind Identitätsmanagement und Netzwerkbasis dann gehärtet, kritische Verfahren eingeschränkt nutzbar. Der Fokus unserer Arbeit liegt im schnellen Wiederanlauf und dem Verhindern von Reinfektionen.

it security: Wann ist der Normalbetrieb wiederhergestellt?

Tim Berghoff: Mit externer Unterstützung stellen Unternehmen den Normalbetrieb nach sechs bis neun Monaten wieder her.



Dann sind zentrale Projekte umgesetzt und der Notbetrieb abgelöst. Das ist aus unserer Sicht aber noch lange kein Endzustand, sondern eine spürbar gehärtete Basis, auf die weiter aufgebaut werden muss.

Denn „Normalbetrieb“ heißt nicht: Alles ist jetzt sicher. Es bedeutet, dass die ausgenutzten Schwachstellen geschlossen wurden – meist mit überschaubaren Ressourcen. Eine langfristige Steigerung des IT-Sicherheitsniveaus erfordert mehr Budget, mehr Zeit und vor allem mehr Personal. Und genau daran hapert es leider bei vielen.

ben, kommt der Geschäftsbetrieb zum Erliegen. Die Produktion steht still, Bestellungen können nicht ausgeliefert werden. Kurz gesagt: Mit jeder Minute steigt der wirtschaftliche Schaden.

Wer keine Notfallpläne und keinen Überblick über die Systemlandschaft hat, ist hilflos und verliert wertvolle Zeit. Dabei sind die ersten Stunden besonders wichtig, um etwa einen Notbetrieb vorzubereiten. Dafür muss aber definiert sein, welche Systeme dafür priorisiert benötigt werden. Besonders kritisch ist es, wenn keine klare Kommuni-

kationsstrategie existiert. Ohne einen Notfallplan geraten viele Unternehmen in einen Panikmodus, den wir den „Headless Chicken Mode“ nennen.

it security: Wie lange dauert es, bis ein betroffenes Unternehmen wieder arbeitsfähig ist?

Tim Berghoff: In den ersten Tagen befinden sich IT und Krisenstab im Ausnahmezustand – 12-Stunden-Tage, auch am Wochenende. Bis sukzessive ein stabiler Notbetrieb steht, vergehen in der Regel vier bis sechs Wochen.

it security: Was können Unternehmen sofort tun, um ihre IT-Sicherheit zu verbessern – auch mit knappen Mitteln?

Tim Berghoff: **Erstens:** Sichtbarkeit schaffen. Ohne Monitoring bleiben verdächtige Aktivitäten unsichtbar. Wer weiß schon, was im eigenen Netzwerk passiert? Tools wie XDR (Extended Detection and Response) oder ein Security Operations Center (SOC) können eine große Hilfe sein – vor allem, wenn externe Dienstleister mit an Bord sind.



Zweitens: Die Reaktionsfähigkeit erhöhen. Ein Notfallplan, also eine Handlungsanleitung für den Ernst-

fall, hilft enorm. Er muss nicht perfekt sein, aber realistisch: Wer macht was, wenn jemand auf einen Phishing-Link klickt? Welche Accounts müssen sofort gesperrt werden? Wer informiert wen? Und das Wichtigste: Wer darf welche Entscheidungen treffen?

Drittens: Passwörter und Perimeter prüfen. Exponierte Dienste sollten zwingend mit einer Zwei-Faktor-Authentifizierung abgesichert sein. Schwache Passwörter gehören abgeschafft – auch wenn das unbequem ist. Es geht hier nicht um „gängeln“, sondern um das digitale Überleben.

Und ergänzend: Passwort-Richtlinien mit Vorgaben zur Länge und Komplexität verbindlich einführen und privilegierte Konten besonders schützen. Dazu noch den automatischen „Self-Unlock“ abschalten. Das sind günstige, sofort wirksame Stellschrauben.

it security: Was raten Sie Firmen, die wenig Personal haben und trotzdem etwas bewegen wollen?

Tim Berghoff: Priorisieren und Auslagern ist mein Rat. Mit einem verlässlichen Dienstleister und dem passenden Angebot wie etwa Managed Extended Detection and Response (MXDR), ein gemanagtes SOC oder Incident-Response-Retainern gewinnen Organisationen 24/7-Detektion, Forensik-Know-how und Entlastung beim Wiederanlauf. Parallel muss intern Klarheit geschaffen werden: Was ist kritisch? Welche Services müssen zuerst laufen? Im Anschluss müssen diese Maßnahmen in eine realistische Roadmap gegossen werden. Dabei empfehle ich lieber drei robuste Schritte als zehn halbfertige.

Es geht darum, den ersten Schritt zu gehen. Wer seine größten Schwachstellen kennt und einen Plan hat, bewegt sich vom reaktiven Krisenmodus hin zur souveränen Sicherheitskultur. Starten sollten die Verantwortlichen mit einem Infrastruktur-Assessment: Inventarisieren, Abhängigkeiten verstehen und Quick-Wins heben. Das bringt Ordnung in „gewachsene“ Umgebungen und liefert die Grundlage für Segmentierung, Patch-Priorisierung und saubere Prozesse.



ES FEHLT BEI VIELEN FIRMEN, DIE EINER CYBERATTACK ZUM OPFER FALLEN, AN GRUNDLEGENDEN SICHERHEITSMASSNAHMEN.

Tim Berghoff, Security Evangelist,
G DATA CyberDefense,
www.gdata.de

it security: Wie sinnvoll bzw. hilfreich sind Cyberversicherungen?

Tim Berghoff: Versicherungen können die finanziellen Auswirkungen eines Sicherheitsvorfalles deutlich mildern. Sie gewähren auch Zugang zu einem Netzwerk aus Fachleuten, die einem Betrieb schnell wieder auf die Beine helfen können. Auch garantierte Service Level sind Bestandteil vieler Versicherungen. Aber eine Versicherung entbindet nicht von der Verpflichtung,

Sicherheitsmaßnahmen zu entwickeln und umzusetzen.

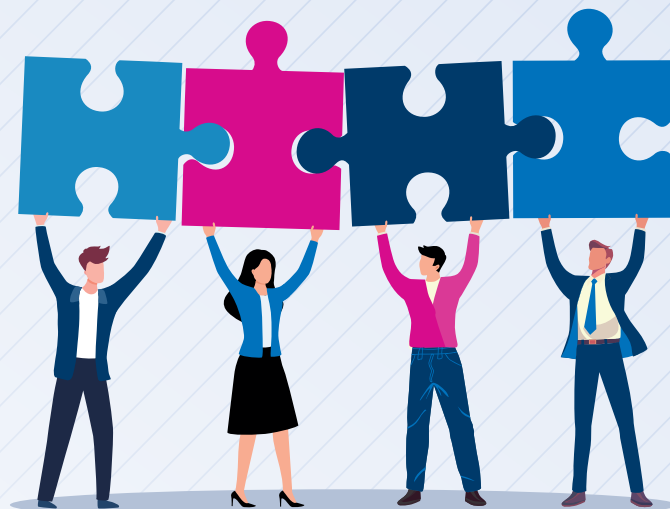
it security: Worauf müssen Verantwortliche achten, wenn sie eine Versicherung abschließen wollen?

Tim Berghoff: Das Wichtigste, auf das Unternehmen achten sollten, ist der genaue Leistungsumfang, die Deckungssummen und auch Ausschlussklauseln. Sind die Deckungssummen nicht ausreichend, um etwa bestimmte Kosten wirkungsvoll auffangen zu können, droht schnell eine Unterversicherung, die im Ernstfall entweder nicht greift oder nur einen Bruchteil der Deckung auszahlt. Kommt es zu einem Sicherheitsvorfall, schreiben manche Versicherungen die Beauftragung eines speziellen Unternehmens vor, während dieser „Werkstattzwang“ bei anderen nicht existiert und Unternehmen einen externen Incident-Response-Dienstleister frei wählen können.

Auch die Art eines Vorfalls kann darüber entscheiden, ob die Versicherung zahlt. Die Folgen „kriegerischer Handlungen“ sind meist ausgeschlossen. Gerade Angriffe aus bestimmten Ländern werden gerne als solche deklariert und somit von der Deckung ausgeschlossen. Hier drohen gegebenenfalls langwierige Gerichtsverfahren, an dessen Ende aber nicht unbedingt eine Zahlung stehen muss.

it security: Herr Berghoff, wir danken für das Gespräch.

THANK YOU



BAUANLEITUNG FÜRS cIAM

DIE PUZZLETEILE MODERNER AUTHENTIFIZIERUNG

Digitale Identitäten stehen im Zentrum nahezu aller modernen Geschäftsmodelle. Ihre sichere und effiziente Verwaltung entwickelt sich zunehmend zur Herausforderung für Unternehmen und öffentliche Einrichtungen. Wer Nutzer zuverlässig authentifizieren will, muss sensible Informationen schützen und gleichzeitig eine reibungslose Nutzererfahrung ermöglichen. Im Customer Identity and Access Management (cIAM) spielen moderne Authentifizierungsverfahren deshalb eine Schlüsselrolle: Sie helfen, Sicherheitsrisiken zu minimieren und das Nutzererlebnis spürbar zu verbessern.

Letztlich verhält es sich beim Identitätsmanagement nicht anders als bei einem Puzzle. Es gilt zunächst, eine klare Vorstellung vom Gesamtbild der Herausforderungen (Kapitel 1) zu gewinnen

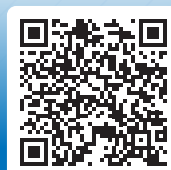
und zu verstehen, was die Aufgabe jedes einzelnen Puzzleteils ist (Kapitel 2). Mit der richtigen Herangehensweise (Kapitel 3) lässt sich jedes noch so komplexe Puzzle erfolgreich zusammensetzen. Die umfassende Funktionsvielfalt von Airlock, das Fundament offener Schnittstellen sowie das Commitment zu künftigen Standards (Kapitel 4) können massgeblich dazu beitragen, Unternehmen schnell und erfolgreich ans Ziel zu bringen.

Dieses Whitepaper richtet sich an Verantwortliche für Identitäts- und Zugriffsmanagement in mittleren bis grossen Unternehmen. Die folgenden Seiten liefern praxisnahe Einblicke, technische Lösungsansätze und konkrete Handlungsempfehlungen, die helfen, die aktuellen Herausforderungen moderner Authentifizierung erfolgreich zu bewältigen.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 31 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download



DIE LÜCKE BEI DER KI-AUFSICHT

(Quelle: IBM Cost of DATA Breach Report 2025)

63 % Anteil der Unternehmen, die über KI-Governance-Richtlinien verfügten, um KI zu verwalten

1,9 Mio. Kosteneinsparungen in USD durch den umfassenden Einsatz von KI im Sicherheitsbereich



97 % Anteil der Unternehmen, die einen KI-bezogenen Sicherheitsvorfall gemeldet haben und über keine ordnungsgemäße KI-Zugriffskontrolle verfügten

Die durchschnittlichen Kosten eines Datenlecks lagen 2025 bei **4,4 Mio. USD**

DevSecOps

DREI PRAXISNAHE WEGE, UM SECURITY UND OPERATIONS ZU VERBINDEN

Die Trennung zwischen Security Operations und IT Operations birgt erhebliche Risiken. DevOps-Verantwortliche, IT-Manager und Unternehmensteams stehen vor großen Herausforderungen, wenn sie die zunehmende Komplexität von Bedrohungen, endlose Patches und Compliance-Anforderungen bewältigen müssen, obwohl sie in Silos arbeiten. Um solche Risiken gut managen und die betriebliche Effizienz steigern zu können, sollte diese Trennung unbedingt aufgehoben werden.

Doch warum sind Security und Operations eigentlich so gegensätzlich? Weil sie oft mit sehr unterschiedlichen Prioritäten, Tools und Zeitplänen arbeiten. Während sich Sicherheitsteams darauf konzentrieren, Risiken zu mindern und die Compliance zu gewährleisten, liegt der Fokus der Operations-Teams auf der Performance, den Betriebszeiten und der Bereitstellung von Services. Obwohl sich diese Ziele nicht gegenseitig

ausschließen, werden sie in der Regel getrennt verwaltet – was zu Reibungen und Unstimmigkeiten führt.

Besonders problematisch wird es, wenn Sicherheitslücken entstehen. Ohne integrierte Arbeitsabläufe und gemeinsame Zuständigkeiten kommt es schnell zu einer Situation, in der „zu viele Köche den Brei verderben“: Wichtige Korrekturen bleiben in Warteschlangen stecken, und Genehmigungen werden verzögert. Und auch die Kosten sind enorm: Im Jahr 2024 kostete eine Datenpanne durchschnittlich 4,88 Millionen US-Dollar und damit mehr als je zuvor.

Einige Unternehmen haben bereits manuelle Ansätze für Sicherheitsmaßnahmen installiert, dennoch sind diese nicht besonders effizient. Auch haben viele von ihnen traditionelle Security Operations Center (SOCs) im Einsatz, aber auch diese sind schnell überlastet. Da

sie sich auf manuelle Meldungen und volle Warteschlangen für Warnmeldungen stützen, haben sie Mühe, mit der heutigen Angriffsszene Schritt zu halten. Es lohnt sich deshalb umso mehr, Security bereits von Anfang an in den DevOps-Lifecycle zu integrieren, gemeinsame Verantwortungsbereiche zu schaffen und Arbeitsabläufe auf einer einheitlichen Plattform zu optimieren.

#1 Frühzeitige Fehlerbehebung: „Security-Shift-Left“ in DevOps

Um sämtliche Sicherheitsprozesse zu verbessern, ist es ratsam, die Sicherheit möglichst früh in den DevOps-Lebenszyklus zu integrieren – nicht erst ganz am Ende, denn allzu oft wird Sicherheit als letzte Hürde angesehen, die noch zu meistern ist. Durch die „Verschiebung nach links“ werden Sicherheitspraktiken von Anfang an in die Entwicklung eingebunden. Damit werden sie direkt von Beginn eines jeden Entwicklungsprozesses

ses zur Routine und sind nicht länger eine reaktive Maßnahme.

Automatisierung spielt dabei eine wichtige Rolle. Sicherheits-Checks können und sollten in Build- und Release-Pipelines integriert werden. So ist es möglich, Probleme zu erkennen, bevor sie eskalieren. Wenn Schwachstellen frühzeitig entdeckt werden, lassen sie sich einfacher und kostengünstiger beheben. Unternehmen, die einen Shift-Left-Sicherheitsansatz verfolgen, können die durchschnittliche Zeit zur Behebung von Schwachstellen um 72 Tage verkürzen. Die Einführung einer „Security-by-Default-Mentalität“ in allen Teams verstärkt diesen Ansatz und fördert einheitliche Standards, ohne die Bereitstellung zu verlangsamen.

Sicherheitsscanner, die mit Plattform-Automatisierungstools integriert werden und Echtzeitdaten liefern, helfen Teams, sofort zu handeln. Mit dem Wechsel von reaktivem zu proaktivem Handeln können Teams Probleme sofort angehen, sobald sie auftreten, anstatt auf regelmäßige Audits zu warten. Das Ergebnis ist eine Kultur, in der das Vorbeugen und Erkennen von Störungen Hand in Hand gehen.

#2 Zusammenarbeit: Gemeinsame Ziele und integrierte Richtlinien

Schnellere Fehlerbehebung beginnt mit gemeinsamen Zielen. Die Zusammenarbeit wird leichter, wenn sowohl das Sicherheits- als auch das Betriebsteam den Erfolg anhand derselben Kennzahlen messen – beispielsweise anhand der mittleren Fehlerbehebungszeit (MTTR). Durch die Vereinbarung klarer Service Level Agreements (SLAs) werden Zuständigkeiten geschaffen und die Prioritäten aufeinander abgestimmt.

Einer der effektivsten Faktoren hierbei ist die Umsetzung von Sicherheitsrichtlinien in Code. Anstatt sich auf manuel-

le Überprüfungen oder Genehmigungsprozesse zu verlassen, können Teams Schutzmaßnahmen direkt in ihre Arbeitsabläufe integrieren. So wird Sicherheit nicht nachträglich berücksichtigt, sondern ist von Anfang an Teil des Prozesses.

Durch die Kodierung von Sicherheits- und Compliance-Richtlinien können Betriebsteams von automatisierten Überprüfungen und Durchsetzungsmaßnah-



DAS ZUSAMMENFÜHREN VON SECURITY- UND OPERATIONS-TEAMS IST DER SCHLÜSSEL ZUM ERFOLG EINES UNTERNEHMENS.

Volker Rippegather, Regional Director DACH & CEE, Perforce Puppet, www.puppet.com

men profitieren, die Abweichungen, Fehlkonfigurationen oder Richtlinienverstöße sofort erkennen. Gleichzeitig sehen Sicherheitsteams, dass Standards konsequent eingehalten werden. Alle Anpassungen der Regeln oder Richtlinien sind vollständig nachvollziehbar, was Audits vereinfacht und die Verantwortung regelt, ohne die Entwicklung zu verlangsamen.

Durch diese Umstellung kommen beide Teams schneller voran, ohne Kompromisse bei der Sicherheit oder Compliance eingehen zu müssen.

#3 Silos aufbrechen: Eine einzige Plattform für Maßnahmen

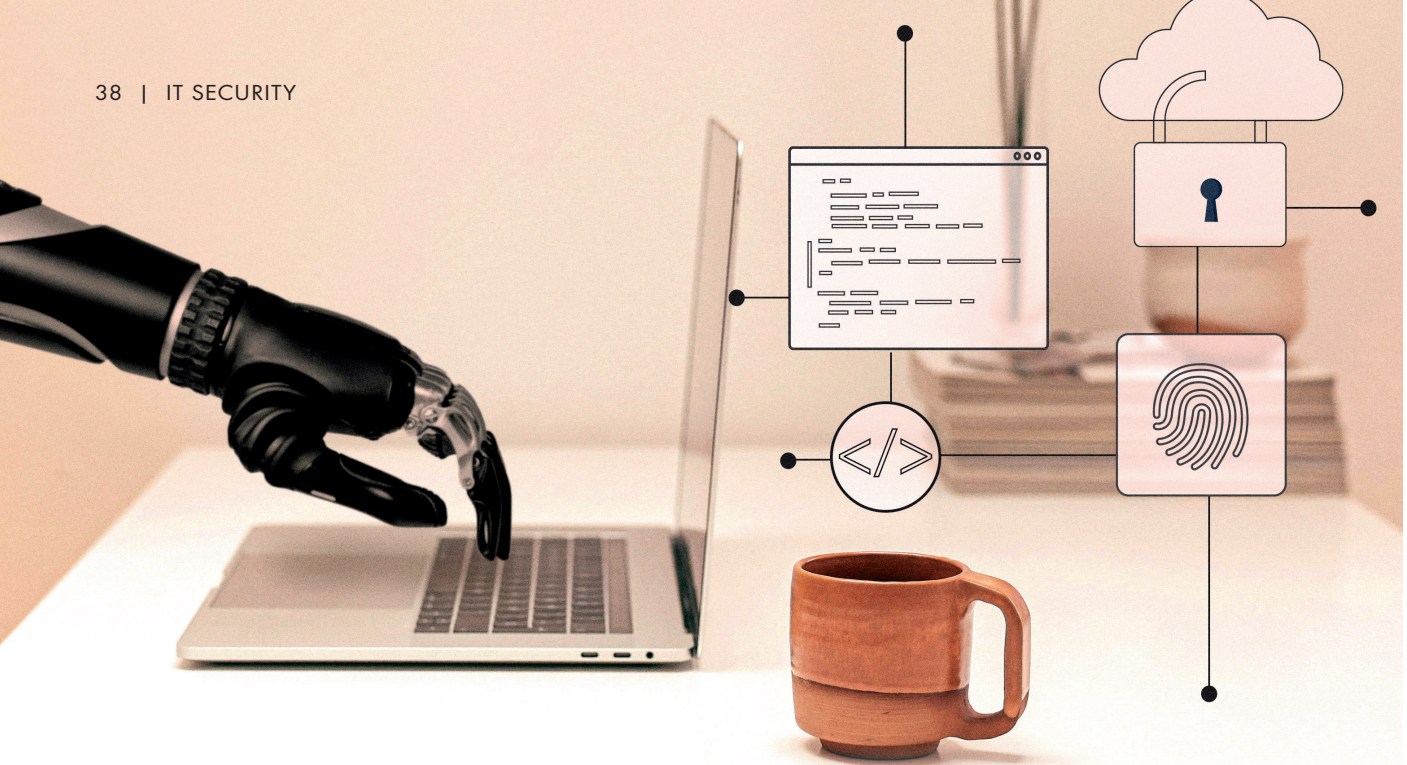
Arbeiten Security- und Operations-Teams in getrennten Silos, sind Verzögerungen vorprogrammiert. Schwachstellen werden an der einen Stelle entdeckt und an der anderen behoben – dabei gehen oft entscheidende Infos verloren. Und da ganze 70 Prozent der Unternehmen mehr als sechs Stunden pro Woche allein für das Patchen aufwenden – sind die Auswirkungen dieser Trennung dramatisch.

Helfen kann hier eine gemeinsame Plattform, auf der alle Teams sämtliche Informationen in Echtzeit einsehen, Maßnahmen ergreifen und Ergebnisse gemeinsam messen können. Anstatt Tickets einfach weiterzureichen, arbeiten sie über dieselbe Plattform zusammen, mit denselben Daten und einheitlichen Prioritäten. Dank klarerer Einblicke in den Problembehebungsprozess wissen Sicherheitsteams, was wann behoben wird – ohne Statusaktualisierungen nachverfolgen zu müssen. Die operativen Teams profitieren von klareren, besser verwertbaren Schwachstellendaten, die mit den ihnen bereits bekannten Systemen verknüpft sind. Zudem wird das Erstellen von Berichten zur Überprüfung der Compliance um ein Vielfaches leichter, die Teams können präzise und umfassende Dokumentationen erstellen.

Warum die Verknüpfung von Sicherheit und Betrieb wichtig ist

Das Zusammenführen von Security- und Operations-Teams ist der Schlüssel zum Erfolg eines Unternehmens. Aufeinander abgestimmte Teams können Schwachstellen schneller beheben, Angriffsflächen reduzieren und gesetzliche Anforderungen effektiver erfüllen. Dies sorgt für weniger Störfälle, weniger Ausfallzeiten und mehr Vertrauen bei den Kunden.

Volker Rippegather



Von Erkennung zu autonomer Abwehr

WARUM KI EIN NEUES SICHERHEITSPARADIGMA ERFORDERT

Die dominierenden Cybersicherheitsarchitekturen, die Unternehmen jahrzehntelang geschützt haben, könnten das KI-Zeitalter möglicherweise nicht überstehen. Dies liegt vor allem an einer sich verändernden Bedrohungslandschaft. KI-getriebene Bedrohungen weisen Eigenschaften auf, mit der traditionellen Sicherheitsarchitekturen überfordert sind.

Der Trend führt zu professionellen KI-gestützten Baukästen, mit denen sich vielschichtige Kampagnen erstellen lassen, und zwar ohne Fachkenntnisse. Stabile, wiederverwendbare Muster wie Signa-

turen verschwinden. Schlussendlich wird jeder Angriff individuell, maßgeschneidert und damit einzigartig. Bedrohungsakteure nutzen Workflows, missbrauchen Vertrauensbeziehungen und gekaperte digitale Identitäten, so dass die Grenze zwischen legitimem und böartigem Verhalten verschwimmt. Die missbrauchten KI-Systeme lernen über Versuche und Umgebungen hinweg und werden mit jeder Interaktion effektiver.

In der Folge entsteht ein strukturelles Problem für Systeme, die auf Alerts, Analysten und nachgelagerte Reaktion setzen – oft gesteuert durch starre Playbooks. Wenn Angriffskosten beinahe gegen null sinken und mehr Automation stattfindet, führen Alarmierung, Detektierung und menschliches Urteilsvermögen zu Flaschenhälsen. Besonders häufig tritt dieses Phänomen in den SOC's auf.

Traditionelle Designs sind anfällig

Fügt man nun hinzu, wie sich die Designprämissen vieler etablierter Anbieter aus dem Security-Bereich in Schwachstellen verwandeln, wird das deutlich: Netzwerkgrenzen als primäre Kontrollpunkte versagen, wenn KI-getriebene Bedrohungen innerhalb vertrauenswürdiger Workflows agieren und Netzwerkänderungen ignorieren. Massive Sichtbarkeit und Erkennungsfähigkeiten auf Geräten werden angreifbar, wenn Reaktionslatenz und menschliche Entscheidung selbst zur Angriffsfläche werden. Zentrale Transparenz und Korrelation schränken Echtzeit-Lernsysteme nicht ein. Identität als Vertrauensprämisse verliert an Zugkraft, wenn KI-gestützte Angreifer hervorragend darin sind, wie legitime Nutzer zu agieren. Richtlinienbasierter Zugriff, der vorhersehbares Verhalten und stabile Absichten voraussetzt, bricht gegenüber Gegnern zusammen, die sich kontinuierlich anpassen.

Zeit für Neues

Die traditionellen Security-Systeme wurden gebaut, um Angriffe zu beobachten und zu erklären. Die Fehlerbehebung in den heutigen Cloud-nativen, agilen Umgebungen besteht jedoch nicht aus einer Reihe manueller Tickets oder „Patch-and-Pray“-Maßnahmen.

**MEHR
WERT**



State of Vulnerability
Remediation Reports 2025

Sie erfordert eine Automatisierungs-orientierte Denkweise, die Tools und Plattformen benötigt, die in das Entwicklungs- und Betriebsökosystem integriert sind. Infrastrukturänderungen müssen als Code in großem Umfang und mit hoher Geschwindigkeit automatisch generiert, getestet und bereitgestellt werden.

KI-native Bedrohungen erfordern Systeme, die auffälliges Verhalten in Echtzeit begrenzen und eindämmen. Der Verteidigungsansatz muss deshalb kontinuierlich anstatt Incident-basiert aufgestellt sein. Erkennung und Reaktion werden zu einem einzigen Kontrollkreislauf zusammengeführt und nicht nacheinander ausgeführt. Sicherheitslösungen handeln autonom innerhalb enger Netzwerkgrenzen. Das Warten auf menschliche Freigaben ist nicht effektiv, sondern fehleranfällig. Eindämmung ist wichtiger als Attribution; Schaden zu stoppen hat Vorrang vor der Frage, wer ihn verursacht hat. Kontrolle rückt näher an die Ausführung statt an die Beobachtung. Der Erfolg dieses Ansatzes wird in der Geschwindigkeit der Eindämmung gemessen.

Moderne Sicherheitslösungen adressieren diese Herausforderungen und haben die erforderliche Geschwindigkeit, um als integraler Bestandteil eines modernen, automatisierten Remediation-Loops zu funktionieren. Sie schließen die Lücke zwischen Erkennung und Behebung. Sie sprechen die Sprache der Infrastruktur. Hierfür nutzen sie die Möglichkeiten der Agentic AI, denn sie stellt eine grundlegende Veränderung in der Funktionsweise von Sicherheitssystemen dar. Im Gegensatz zu traditioneller KI, die Eingaben verarbeitet und Ergebnisse ausgibt, agieren agentische Systeme autonom, planen Aufgaben, treffen Entscheidungen und ergreifen Maßnahmen, ohne dass eine ständige Überwachung durch den Menschen erforderlich ist.

Moderne Sicherheitslösungen sollten deshalb die folgenden vier Anforderungen erfüllen:

#1 Kontinuierliche Erkennung:

Agentische Systeme überwachen Umgebungen in Echtzeit und erkennen Schwachstellen, sobald sie auftreten, statt auf den nächsten geplanten Scan zu warten. Wenn eine neue CVE veröffentlicht wird, wissen Sicherheitsteams sofort, welche Systeme betroffen sind.

#2 Intelligente Priorisierung:

Anstatt Teams mit CVSS-geordneten Listen zu überhäufen, filtern KI-Agenten Störsignale heraus und zeigen nur kritische Probleme an. Ein anfälliger Entwicklungsserver erhält nicht die gleiche Priorität wie eine exponierte Produktionsdatenbank.

#3 Autonome Behebung:

Hier findet ein echter Paradigmenwechsel statt. Agentic AI teilt Sicherheitsteams nicht nur mit, dass ein Server einen Patch benötigt, sondern generiert auch die Korrektur, testet sie sicher und kann sie automatisch oder

mit einer Ein-Klick-Genehmigung bereitstellen. Der gesamte Workflow von der Erkennung bis zur Lösung erfolgt mit Maschinengeschwindigkeit.

#4 Geschlossene Verifizierung:

Nach der Behebung überprüft das System automatisch, ob die Korrektur funktioniert hat, und aktualisiert die Sicherheitslage entsprechend. Sicherheitsteams müssen nicht mehr auf den nächsten Scan warten, um zu bestätigen, dass sie das Problem tatsächlich gelöst haben.

Fazit

Der Sicherheitsansatz verschiebt sich von der reinen Sichtbarkeit zur schnellen und automatisierten Behebung von Schwachstellen und Sicherheitslücken. Die Cybersicherheitsbranche hat ca. zwei Jahrzehnte damit verbracht, Lücken in der Verteidigung zu finden. Aber das Auffinden kommt nicht einer Behebung gleich. Heute sind nach Angaben des 2025 State of Vulnerability Remediation Reports von Mondoo 60 Prozent der Warnmeldungen im SOC wie ein lautes Rauschen ohne Business-Kontext. 62 Prozent der Remediation-Workflows bleiben manuell oder werden Spreadsheet-basiert gemanagt. Die „Mean Time to Remediate“ liegt bei über 30 Tagen, was eine Ewigkeit in der heutigen KI-Welt entspricht. Dies alles führt zu der Erkenntnis, dass Sicherheitsteams Risiken katalogisieren, aber Schwierigkeiten haben, diese zu eliminieren.

Diese Lücke muss eine neue Generation Sicherheitslösungen schließen. Dieser Wechsel von Tickets zu Code steht stellvertretend genau für die Art architektonischer Veränderung, die eine reine Erfassung und Kontrolle näher an die wirkliche Behebung bringen wird. Mit diesem Paradigmenwechsel wird es Unternehmen gelingen, die Herausforderungen der KI-generierte Bedrohungswelt zu meistern.

Patrick Münch



**SICHERHEITSTEAMS
KÖNNEN ZWAR RISIKEN
KATALOGISIEREN,
HABEN ABER SCHWIE-
RIGKEITEN, DIESE ZU
ELIMINIEREN.**

Patrick Münch,
Mitgründer und CISO, Mondoo,
www.mondoo.com

Netzwerke für die KI-Ära

WARUM DER CHANNEL HEUTE DEN UNTERSCHIED MACHT

Der Einsatz von KI erfordert eine grundlegende Neuausrichtung der Netzwerkinfrastruktur in Unternehmen. Damit steigt die Nachfrage nach schnelleren, intelligenteren und anpassungsfähigeren Networking-Komponenten und begleitenden Services – für den IT-Channel eine attraktive Wachstumschance. Der folgende Beitrag erläutert, wie Partner ihre Kunden bei der Migration auf KI-optimierte Infrastrukturen unterstützen können.

Die inzwischen allgegenwärtigen KI-Workloads – von generativer KI bis hin zu Inferenzdiensten – stellen enorme Anforderungen an die Performance, Skalierbarkeit und Sicherheit moderner Enterprise-Netzwerke. Unternehmen kommen daher nicht umhin, ihre Kommunikation auf eine zeitgemäße, smarte Infrastruktur zu migrieren. Dabei sprechen wir aber nicht von einem einfachen technischen Update – sondern von einem tiefgreifenden Paradigmenwechsel, der für die Zukunft der betroffenen Unternehmen von entscheidender Bedeutung ist.

Unternehmen mit KI-optimierten Netzwerken können Services schneller bereitstellen, die Customer Experience nachhaltig verbessern und ihre Abläufe resilient konzipieren. Die Nachfrage nach den entsprechenden Lösungen nimmt daher über alle Branchen hinweg rasant zu – von IT und Finanzwesen über Gesundheitswesen und Fertigung bis hin zum Handel und zum öffentlichen Sektor.

Eine aktuelle Studie von Westcon Comstor belegt jetzt aber, dass derzeit nur 33 Prozent der befragten Systemintegratoren ihre Kunden als „vollständig KI-ready“ einschätzen. Oder umgekehrt: 67 Prozent sehen die Kunden erst am Anfang eines langen Weges – und genau hier liegt eine große Chance für den Channel.



ANGESICHTS DER HOHEN GESCHWINDIGKEIT DES TECHNOLOGISCHEN WANDELS SIND UNTERNEHMEN VOR ALLEM AUF EINES ANGEWIESEN: AUF VERTRAUENSVOLLE PARTNER.

Evelyn Vogt, Director Business Development, Westcon Group Germany, www.westconcomstor.com

Zentrale Herausforderungen der Anwender

KI-Workloads sind heute überall: in der Cloud, auf Edge-Systemen und in On-Premises-Umgebungen. Damit all diese Komponenten reibungslos zusammenspielen, sind intelligente, nahtlos integrierte Architekturen erforderlich. Doch

derzeit tun sich viele Unternehmen noch schwer, eine tragfähige Brücke zwischen KI, Infrastruktur, Sicherheit und Cloud zu schlagen.

Mit einzelnen Produkten und Insellösungen ist diesen Kunden nicht geholfen. Sie brauchen umfassende KI-Lifecycle-Services – von der Beratung über Design und Implementierung bis hin zu kontinuierlicher Betreuung und Optimierung, die auch wichtige Themen wie Datenschutz, Compliance und Governance berücksichtigt.

Die Challenge: Aktuell sind drei von vier befragten Channelpartnern nicht in der Lage, ganzheitliche KI-Netzwerklösungen anzubieten. Wer diese Lücke zu schließen weiß, kann sich also klar vom Wettbewerb differenzieren – mit modularen, anpassungsfähigen und zukunftsicheren Architekturen, die Endkunden agil und innovationsfähig halten.

Im Rahmen der Umfrage wurden vor allem zwei große Hemmnisse erkennbar: die hochkomplexe Integration bestehender Systeme und das in vielen Betrieben fehlende Fachwissen.

Alt trifft auf Neu – die Integrationsherausforderung

46 Prozent der Befragten sehen die Integration als größte Hürde für ihre Kunden. Immerhin sind die Netzwerke oft über Jahre unkontrolliert gewachsen, setzen auf veraltete Technologie und sind nicht für die Performance-Anforderungen von heute ausgelegt. Werden in



einer solchen Umgebung modernste KI-Lösungen aufgesetzt, sind Engpässe und Performance-Einbrüche vorprogrammiert.

Hier kann der Channel greifbaren Mehrwert bieten – etwa durch:

- AI Readiness Assessments, um den Modernisierungsbedarf zu ermitteln
- Migrationsfahrpläne, die den Weg in Richtung KI-Readiness ganz klar aufzeigen
- Hybridstrategien, die bestehende und neue Systeme intelligent miteinander verbinden
- Laufende Unterstützung und Schulungen, um einen reibungslosen Übergang sicherzustellen

Auf diese Weise schlägt der Channel die Brücke von der Vision zur Umsetzung – und ermöglicht es Unternehmen, ihre Netzwerke für die Zukunft fit zu machen und so das volle Potenzial der KI-Technologie auszuschöpfen.

Der Fachkräftemangel als Chance

Ein weiteres Hindernis: der Mangel an internem Know-how. 39 Prozent der Befragten beklagen die fehlende KI-Expertise auf Seiten der Kunden als große Herausforderung. Immerhin erfordert der Betrieb von KI-Infrastrukturen ein breites Kompetenzspektrum – von Cloud-nativen Technologien über Datenmanagement bis zu modernen Sicherheitsarchitekturen.

Auch hier kann der Channel mit folgenden Services punkten:

- Trainings und Enablement, um IT-Teams beim internen Wissensaufbau zu unterstützen
- Managed Services, bei denen der operative Betrieb von KI-Infrastrukturen auf externe Dienstleister ausgelagert wird
- Strategische Beratung, um Kunden bei der stetigen Optimierung ihrer KI-Strategie zu begleiten

Channelpartner, die sich für diesen Weg entscheiden, können sich langfristig als strategischer Partner ihrer Kunden etablieren und deren Geschäftserfolg aktiv mitgestalten.

Ein starkes Partnernetzwerk für die KI-Ära

Angesichts der hohen Geschwindigkeit des technologischen Wandels sind Unternehmen vor allem auf eines angewiesen: auf vertrauenswürdige Partner. Als Endkunden suchen sie nicht nach Produkten, sondern nach einem Trusted Advisor, der ihnen während der gesamten KI-Journey zur Seite steht. Channelpartner, die sich im Zentrum dieser Transformation positionieren, schaffen langfristige Beziehungen, die beiderseitiges Wachstum sichern.

Ein erfahrener Distributor wirkt dabei als wertvoller Multiplikator: er wirkt nicht nur als Supply-Chain-Partner, sondern auch als kompetenter Enabler, der für jede Aufgabe sofort die richtigen Tools, Daten, Insights und Services bereithält. So können die Channelpartner die KI-Transformation ihrer Kunden erfolgreich mitgestalten – und selbst mit ihr wachsen.

Evelyn Vogt

KI-gestütztes Pentesting – Die neue Ära der Cybersicherheit?

WIE AUTOMATISIERUNG UND EXPERTISE DIE ZUKUNFT VON SICHERHEITSTESTS GESTALTEN

Während traditionelle Penetrationstests an Grenzen stoßen, eröffnen KI-gestützte Systeme völlig neue Möglichkeiten für Unternehmen. Die Transformation betrifft nicht nur die Geschwindigkeit und Skalierung der Tests, sondern auch die Art und Weise, wie Sicherheitsexperten arbeiten und welche Fähigkeiten sie benötigen.

Laut Gartner-Prognosen werden KI-Agenten bis 2027 die Zeit zur Ausnutzung von Konto-Schwachstellen um 50 Prozent reduzieren. Solche Prognosen basieren auf modellhaften Annahmen und beschreiben Trendszenarien, keine garantierten Eintrittswahrscheinlichkeiten. Sie verdeutlichen jedoch die zunehmende operative Dynamik KI-gestützter Angriffs- und Testmethoden.

Die wahre Innovation liegt in der intelligenten Kombination von maschineller Effizienz und menschlicher Expertise. Während automatisierte Systeme datenintensive, repetitive Aufgaben übernehmen und riesige Datenmengen analysieren, konzentrieren sich Sicherheitsexperten auf komplexe Bedrohungsszenarien, strategische Entscheidungen und kontextuelle Bewertungen.

Sieben Zukunftsszenarien des KI-gestützten Pentesting

#1 Ethische Automatisierung mit menschlicher Aufsicht

Die Implementierung KI-gestützter Penetrationstests erfordert robuste Governance-Strukturen. Unternehmen müssen

Eskalationspfade definieren, Transparenzanforderungen festlegen und sicherstellen, dass kritische Entscheidungen von menschlichen Experten getroffen werden. Die größte Herausforderung besteht darin, False Positives zu minimieren und gleichzeitig Datenschutzverletzungen durch autonome Scans zu verhindern. Erfolgreiche Organisationen entwickeln klare Richtlinien, die den ethischen Einsatz von KI-Agenten regeln und gleichzeitig Innovation ermöglichen.

#2 Transformation der Berufsbilder und Kompetenzen

Das Berufsbild des Penetrationstesters durchläuft einen fundamentalen Wandel. Während repetitive Einstiegspositionen seltener werden, entstehen spezialisierte Rollen: KI-Sicherheitsforscher analysieren maschinell generierte Angriffsmuster, Prompt-Engineers entwickeln präzise Testszenarien für KI-Systeme, und hybride Fachkräfte verbinden tiefes Cybersecurity-Wissen mit Data-Science-Expertise. Remote-Teams, die KI-Agenten orchestrieren und deren Ergebnisse interpretieren, etablieren sich als neuer Standard in der Branche. Viele dieser Rollen befinden sich derzeit noch in einer frühen Entwicklungsphase und sind bislang eher funktions- als titelbasiert in bestehenden Security-Teams verankert.

#3 Neuausrichtung der Aus- und Weiterbildung

Moderne Pentester benötigen ein erweitertes Kompetenzprofil, das weit

über traditionelle Sicherheitskenntnisse hinausgeht. Praktische Erfahrung mit KI-Tools, Datenvorverarbeitung und Prompt-Optimierung werden zu Kernkompetenzen. Ausbildungsprogramme integrieren zunehmend interaktive Labore, in denen klassisches Pentesting mit Data-Science-Methoden verschmolzen wird. MLOps-Grundlagen wie Datenversionierung, Modelltraining und kontinuierliche Integration werden für Sicherheitsexperten ebenso wichtig wie das Verständnis von Exploit-Techniken.

#4 Regulatorische Anpassung und Haftungsfragen

Automatisierte Sicherheitstests stellen etablierte Compliance-Frameworks vor neue Herausforderungen. Die DSGVO und PCI-DSS wurden für eine Ära entwickelt, in der Menschen Tests durchführten – autonome KI-Systeme benötigen spezifische Regelungen. Organisationen entwickeln dedizierte Richtlinien für KI-Testbereiche, implementieren strenge Datenhandhabungsprozesse und verankern klare Haftungsregelungen in Service-Level-Agreements. Das EU-KI-Gesetz könnte bestimmte Pentesting-Modelle als Hochrisiko-Systeme klassifizieren, was zusätzliche Compliance-Anforderungen nach sich zieht. Ob KI-gestützte Pentesting-Systeme tatsächlich als Hochrisiko-Anwendungen eingestuft werden, hängt stark vom Automatisierungsgrad, dem Einsatzkontext und dem Zugriff auf produktive Daten ab.

#5 Wirtschaftlichkeitsanalyse und ROI-Betrachtung

Die Investition in KI-gestützte Pentesting-Plattformen erfordert eine ganzheitliche Kostenanalyse. Unternehmen müssen die Effizienzgewinne durch Automatisierung gegen die Aufwände für Lizenzen, kontinuierliches Re-Training und Datenlabeling abwägen. Entscheidend sind jedoch nicht nur die direkten Kosten, sondern auch indirekte Einsparungen: verkürzte Time-to-Remediation, einheitliche Reporting-Strukturen für das Management und die Möglichkeit, Sicherheitsexperten auf strategisch wichtigere Aufgaben zu fokussieren. Eine differenzierte ROI-Betrachtung berücksichtigt sowohl quantifizierbare Metriken als auch qualitative Verbesserungen in der Sicherheitspostur.

#6 Differenzierte Tool-Landschaft und Auswahlkriterien

Der Markt für KI-gestützte Sicherheitslösungen hat sich stark diversifiziert. Spezialisierte Tools adressieren unterschiedliche Anforderungen: Web Application Fuzzing mit integrierten Threat-Intelligence-Feeds identifiziert Zero-Day-ähnliche Schwachstellen in Echtzeit. Dabei handelt es sich in der Regel nicht um echte Zero-Day-Exploits, sondern um heuristisch erkannte Anomalien und Angriffspfade, die von klassischen Signatur-basierten Scannern nicht erfasst werden. API-Sicherheitstests mit adaptiven Angriffsmustern passen sich dynamisch an moderne Microservices-Architekturen an. Maßgeschneiderte Module ermöglichen die Integration in individuelle Testumgebungen. Die Auswahl sollte sich an bestehenden Infrastrukturen, verfügbaren Budgets und der Fähigkeit zur nahtlosen Integration in bestehende Security-Workflows orientieren.



#7 Innovative Forschungsrichtungen

Die Zukunft des KI-gestützten Pentesting wird von mehreren Innovationslinien geprägt: Selbstlernende Angriffsgagenten entwickeln Echtzeit-Anpassungsfähigkeit und können sich an veränderte Verteidigungsmaßnahmen anpassen. Multi-Modell-Frameworks kombinieren verschiedene KI-Architekturen für kontextuelle Angriffsanalysen. Digitale Zwillinge ermöglichen die Simulation kompletter Netzwerkumgebungen ohne Risiko für Produktsysteme. Kausale Sicherheitsmodelle modellieren komplexe If-Then-Angriffketten und helfen, mehrstufige Angriffe vorherzusagen, bevor sie auftreten.

Die Zukunft:

Symbiose statt Substitution

Die erfolgversprechendste Vision für die Zukunft der Cybersicherheit ist kein vollautomatisiertes System, sondern

ein ausgewogenes Zusammenspiel von Mensch und Maschine. KI-Systeme ermöglichen eine Skalierung, die mit rein menschlichen Ressourcen unmöglich wäre. Gleichzeitig bleiben menschliche Experten unverzichtbar für die Bewertung komplexer Geschäftslogik und die Identifikation innovativer Angriffspfade, die über standardisierte Muster hinausgehen.

Marcus White, Cybersecurity Specialist bei Outpost24, fasst diese Vision prägnant zusammen: „Es ist die Verschmelzung von maschineller Geschwindigkeit und menschlicher Findigkeit, die die tiefsten Einblicke und kreativsten Angriffspfade bietet.“ Diese Symbiose ermöglicht es Organisationen, sowohl die Breite als auch die Tiefe ihrer Sicherheitstests zu maximieren – ein Ziel, das weder mit rein manuellen noch mit vollautomatisierten Ansätzen erreichbar wäre.

PTaaS-Anbieter 2026: Marktübersicht und Auswahlkriterien

Penetration Testing as a Service (PTaaS) unterscheidet sich von klassischen Pentests durch einen plattformbasierten Ansatz, der kontinuierliche Tests, Echtzeit-Ergebnisse und nahtlose Integration in Software-Entwicklungsprozesse ermöglicht. Die DevSecOps-Integration macht PTaaS besonders attraktiv für agile Entwicklungsteams, die Sicherheit nicht als nachgelagerten Prüfschritt, sondern als integralen Bestandteil des Entwicklungszyklus verstehen.

Globale Marktführer mit Plattform-Fokus

Cobalt gehört zu den Pionieren im PTaaS-Bereich und nutzt eine globale Community zertifizierter Hacker. Die Stärke liegt in der außergewöhnlich schnellen Projektplanung – Tests starten oft innerhalb von 24 bis 48 Stunden. Dies macht Cobalt ideal für agile Teams, die schnelle Feedback-Zyklen benötigen. BreachLock kombiniert KI-

gestützte Scans mit manuellen Tests und bietet eine hochskalierbare Plattform, die auch Compliance-Reporting für Standards wie SOC 2 und ISO 27001 automatisiert. NetSPI positioniert sich als Schwergewicht für Großunternehmen und bietet tiefe Einblicke in Schwachstellen-Behebung sowie starkes Programm-Management für komplexe IT-Landschaften. Synack nutzt ein exklusives, kuratiertes Netzwerk von Sicherheitsforschern und ist besonders stark in der kontinuierlichen Überprüfung von Assets.

Outpost24 hingegen verfolgt einen hybriden Ansatz, der besonders auf kontinuierliche Überprüfung von Webanwendungen und APIs spezialisiert ist. Das Kernprodukt „SWAT“ kombiniert automatisierte Schwachstellenerkennung mit manueller Verifizierung durch hauseigene Experten. Im Gegensatz zu punktuellen Pentests überwacht SWAT Anwendungen das ganze Jahr über.

Die wichtigsten Merkmale umfassen kontinuierliches Monitoring bei Code-Änderungen, das „Zero False Positives“-Versprechen durch manuelle Validierung aller automatisierten Funde, nahtlose Integration in Tools wie Jira, Azure DevOps oder ServiceNow sowie unbegrenzte Re-Tests ohne Zusatzkosten.

Während Anbieter wie Cobalt häufig auf Crowdsourced-Hacker setzen, arbeitet Outpost24 primär mit festangestellten Experten in eigenen Security Operations Centers. Dies bietet höhere Vorhersehbarkeit und erfüllt strenge DSGVO-Anforderungen – besonders attraktiv für europäische Kunden.

Spezialisierte und innovative Lösungen

Astra Security ist besonders beliebt bei SaaS-Unternehmen und bietet ein intuitives Dashboard mit direkter Integration in CI/CD-Pipelines wie GitHub



TRADITIONELLES VS. KI-GESTÜTZTES PENTESTING

Traditionelles Pentesting	KI-gestütztes Pentesting
manuelle Prozesse	automatisierte Workflows
begrenzte Skalierbarkeit	hohe Skalierbarkeit
erfahrungsbasierter Ansatz	datengetriebener Ansatz
reaktive Identifikation	proaktive Prädiktion
menschliche Kreativität	algorithmische Effizienz

und Jira. HackerOne und Bugcrowd, ursprünglich Bug-Bounty-Plattformen, bieten mittlerweile strukturierte PTaaS-Engagements, die auf ihre riesigen Netzwerke ethischer Hacker zurückgreifen. Edgescan konzentriert sich auf Full-Stack-Abdeckung und hohe Genauigkeit durch intelligente Kombination von Automatisierung und menschlicher Validierung.

Auswahlkriterien für PTaaS-Lösungen

Bei der Auswahl einer PTaaS-Lösung sollten Unternehmen mehrere strategische Faktoren berücksichtigen. Die Integrationsfähigkeit in bestehende Entwicklungs- und Ticketing-Tools ist entscheidend für effiziente Workflows. Die Qualität der Tester – ob festangestellte Experten oder anonyme Crowd-Tester – beeinflusst die Konsistenz und Tiefe der Ergebnisse erheblich. Das Retesting-Modell sollte klären, ob Nachprüfungen behobener Schwachstellen im Grundpreis enthalten sind,

was bei PTaaS-Anbietern meist der Fall ist. Ein Echtzeit-Dashboard bietet sofortigen Zugriff auf Findings, während traditionelle PDF-Berichte zu Verzögerungen führen können. Nicht zuletzt spielt die Compliance-Konformität eine zentrale Rolle, insbesondere in regulierten Branchen.

Strategische Implementierung als Erfolgsfaktor

Organisationen, die KI im Pentesting erfolgreich einsetzen möchten, benötigen einen strukturierten, differenzierten Implementierungsansatz. Dieser basiert auf vier zentralen Säulen, die synergistisch zusammenwirken müssen.

#1 Erstens erfordern **klare Governance-Richtlinien** für den ethischen KI-Einsatz eindeutige Regelungen darüber, welche Systeme automatisiert getestet werden dürfen, wie mit sensiblen Daten umgegangen wird und wann menschliche Expertise eskaliert werden muss.

#2 Zweitens muss **kontinuierliche Kompetenzentwicklung** des Security-Personals sicherstellen, dass Teams nicht nur KI-Tools bedienen, sondern deren Ergebnisse kritisch bewerten und strategisch einordnen können.

#3 Drittens ermöglichen **hybride Testansätze** die optimale Verbindung von KI-Effizienz mit menschlicher Expertise – automatisierte Systeme übernehmen Breadth-Testing, während Experten Depth-Testing in kritischen Bereichen durchführen.

#4 Viertens gewährleistet die **regelmäßige Evaluierung** von Testqualität und messbaren Sicherheitsverbesserungen, dass Investitionen in KI-Technologie tatsächlich den gewünschten Effekt erzielen.

Handlungsempfehlungen für Unternehmen

Beginnen Sie mit einer Pilotphase in nicht-kritischen Umgebungen, um Erfahrungen mit KI-gestützten Tools zu sammeln. Entwickeln Sie klare Metriken für Erfolg – nicht nur technische KPIs wie Scan-Geschwindigkeit, sondern auch qualitative Indikatoren wie Reduktion der Mean-Time-to-Remediation. Investieren Sie parallel in die Weiterbildung Ihres Teams und etablieren Sie einen kontinuierlichen Feedback-Loop zwischen automatisierten Scans und manueller Validierung. Die erfolgreichsten Organisationen behandeln KI-Integration nicht als einmaliges Projekt, sondern als kontinuierlichen Transformationsprozess.

Ulrich Parthier | www.it-daily.net

Quellenverzeichnis

- ▶ White, Marcus: „Wie sich KI auf die Zukunft von Pentests auswirkt: 7 Szenarien“, Outpost24 Blog (November 2025)
- ▶ Gartner: „Predictive Analysis of AI in Cybersecurity“ (2024)
- ▶ Europäische Union: „AI Act – Regulatory Framework for Artificial Intelligence“ (2024)
- ▶ ISC²: „Cybersecurity Workforce Study: AI Skills Gap Analysis“ (2024)

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26),
Stellvertretender Chefredakteur: Lars Becker

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistent und Sanderdrucke: Eva Neff (-15)

Objektleitung:
Ulrich Parthier (-14),
ISSN-Nummer: 0945-9650

Autoren:
Lars Becker, Jens Bothe, Dr. Sebastian Eder, Kay Ernst,
Peter Herr, Carina Mitzschke, Patrick Münch, Ulrich Parthier,
Volker Rippegather, Maren Schweier, Thomas Vini Pires,
Evelyn Vogt

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0,
Fax: 08104-6494-22

E-Mail für Leserbrief: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.
Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen:

Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:

Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise:

Es gilt die Anzeigenpreisliste Nr. 33.
Preisliste gültig ab 1. Oktober 2025.

Mediaberatung & Content Marketing-Lösungen

it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Head of Marketing:

Vicky Miridakis, 08104-6494-15,
miridakis@it-verlag.de

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung:

VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52,
BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.



IDENTITY & ACCESS MANAGEMENT

EIN ENTSCHEIDENDER ASPEKT DER NIS2-KONFORMITÄT

Die Nutzung und Abhängigkeit von IT-Systemen in allen Bereichen der Gesellschaft, der Wirtschaft und des Privatlebens hat in den letzten zehn Jahren rapide zugenommen. Die EU und viele nationale Regierungen haben die zunehmende Abhängigkeit von diesen Netzwerken und Informationssystemen erkannt, die oft über organisatorische und nationale Grenzen hinausgehen.

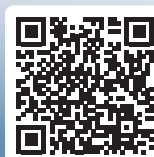
Um den zunehmenden und sich weiterentwickelnden Cybersicherheitsproblemen zu begegnen, hat die EU im Januar 2023 die Richtlinie über Netz- und Informationssicherheit (NIS) aktualisiert. Viele Mitgliedstaaten haben nun ihre bestehenden Vorschriften aktualisiert, um die erweiterten Anforderungen von NIS2 zu berücksichtigen. Betreiber von wesentlichen Diensten in EU-Staaten, die Dienstleistungen in kritischen Sektoren wie Gesundheitswesen, Energie, Verkehr, Bankwesen und digitale Infrastruktur erbringen, müssen die verschärften Anforderungen an die Cybersicherheit und die Meldung von Vorfällen erfüllen.

IAM ist ein wichtiger Bestandteil einer umfassenderen Cybersicherheitsstrategie, und viele Unternehmen und Führungskräfte müssen mit Geldstrafen, Sanktionen und Reputationsschäden rechnen, wenn sie von NIS2 geeignete Richtlinien, Prozesse und Technologien nicht implementiert haben.

Überprüfen Sie Ihre IAM-Strategie jetzt. Handeln Sie, um die Wirksamkeit Ihrer Strategie für digitale Identitäten auf der Grundlage der derzeitigen Tools und Prozesse zu bewerten.



WHITEPAPER DOWNLOAD



Das Whitepaper umfasst 18 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download





**JETZT DEN NÄCHSTEN
KARRIERESCHRITT GEHEN
– MIT DER JOBBÖRSE VON**

 **it-daily.net**



**JETZT
ENTDECKEN!**

18. – 19. März

Secure Unified Endpoint Management

Eilenriedehalle | Stand E49

DEEP DIVE

Sicher. Sichtbar. Beherrschbar.

Wie gezieltes Unified Endpoint Management
Administratoren wirklich entlastet

18.03.2026 | 14:30 – 15:30 Uhr,
Workshopraum 17

Mehr Infos:
www.aagon.com/secit2026

