06/2025 /// WWW.DIGITALBUSINESS-MAGAZIN.DE

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

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG | Ausgabe-Nr.: 200

SECURITY INSIGHT

MEGA

MAKE EUROPE GREAT AGAIN

DIGITALE SOUVERÄNITÄT

DIE ÜBERLEBENSFRAGE FÜR UNTERNEHMEN?

KI IM SMART OFFICE

KI-Tools wie ChatGPT und Microsoft Copilot sind relativ neu. Jetzt gilt es, sie effizient und wertsteigernd einzusetzen.

HR

Nur integrierte KI mit Echtzeit-Zugriff auf HR-/Payroll-Daten schafft messbaren Nutzen – wie Teams pragmatisch starten.

CLOUD ERP

Eine praxisnahe Checkliste hilft zu entscheiden, ob ein Public-Cloud-ERP für Ihren Business Case sinnvoll ist.


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

EDITORIAL

Liebe Leserin, lieber Leser

• MEGA – Make Europe Great Again: Das klingt nach großem Anspruch, ist aber vor allem **ein Weckruf,** den wir mit der Titelstrecke dieser Ausgabe aufgreifen. Digitale Souveränität ist keine ideologische Vokabel und schon gar kein romantischer Rückzug in Autarkie. Sie ist zur **Überlebensfrage für Unternehmen** geworden – für Resilienz, Verhandlungsmacht und die Fähigkeit, Innovationen selbst zu steuern. Wer in Daten, Cloud und KI die Regie abgibt, gibt auch Wertschöpfung und Zukunftsfähigkeit ab.

Strategische Variable
Die Abhängigkeit von Hyperscalern hat einen Preis: Lock-in durch proprietäre Dienste, Preissprünge ohne echte Ausweichmöglichkeit, geopolitische Risiken und extraterritoriale Zugriffe auf Daten. API-Änderungen, Service-Abkündigungen und regionale Outages können ganze Lieferketten aus dem Takt bringen. In der KI-Ära verschärft sich das: Wer auf geschlossene Foundation-Modelle und proprietäre Pipelines setzt, bindet kritisches Know-how an fremde Plattformlogiken – und macht sich **abhängig von Lizenzbedingungen**, Trainingsdaten und Governance fremder Ökosysteme. Compliance, Datenschutz und IP-Schutz werden zur strategischen Variable.

Kontrolle zurückgewinnen
Souveränität heißt nicht: alles selbst bauen. Souveränität heißt: die Stellhebel der Kontrolle zurückgewinnen. **„Souveränität light“** ist ein pragmatischer Weg dorthin: Multi-Cloud-Architekturen mit echten Exit-Strategien, offene Standards und Portabilität (Kubernetes, OpenStack, OCI), Verschlüsselung und Schlüsselhoheit, Datenklassifikation mit klaren Workload-Policies, verbindliche SLAs und Audits, Vendor-Risiko-Management im Board. Die Leitfrage lautet: Können Unternehmen gleich morgen wechseln – technisch, vertraglich, organisatorisch – ohne das Geschäft zu gefährden?

Europas Antworten
Die gute Nachricht: Europa hat Antworten. Von europäischen Cloud-Providern wie IONOS, OVHcloud, Scaleway, Cleura oder Exoscale über souveräne Stacks wie Sovereign Cloud Stack bis zu Datenräumen à la GAIA-X und Catena-X, getragen von **offenen Komponenten** wie dem Eclipse Dataspace Connector. Diese Lösungen laufen – in Industrieprojekten, bei Mittelständlern, in der öffentlichen Hand. Sie verbinden Datenschutz, Compliance und Performance, zunehmend auch am Edge und in Rechenzentren mit grüner Energie. Es geht nicht um ein Entweder-oder zu Hyperscalern, sondern um ein Europa, das seine Regeln, seine Prioritäten und seine **Exit-Optionen** beherrscht.

In diesem Heft zeigen unsere Autorinnen und Autoren, wo die Abhängigkeiten wirklich liegen, wie „Souveränität light“ ohne Dogma gelingt und welche **europäischen Alternativen** bereits Mehrwert liefern. MEGA ist auch ein Arbeitsauftrag: Gestalten wir die digitale Wertschöpfung so, dass Europa – und Ihre Unternehmen – resilient, innovativ und frei bleiben.

Ich wünsche Ihnen eine inspirierende Lektüre.

Ihr
HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS

heiner.sieger@win-verlag.de

06

Titelstory / Digitale Souveränität

Dr. Julia Pergande von Microfin hebt im Interview die Bedeutung von Exit-Strategien in der Cloud hervor.

SECURITY INSIGHT

DIGITAL BUSINESS

06 2025

Cloud-Exit-Strategien: Ein Muss für Unternehmen

Dr. Julia Pergande* von Microfin hebt die Bedeutung von Exit-Strategien in der Cloud hervor. Sie erläutert, wie aktuelle Regulierungen Unternehmen zu einem wohlüberlegten Anbieternwechsel anregen und die Risiken von Hyperscalern minimieren. /// von Heiner Sieger

Wie kritisch sehen Sie die Abhängigkeit von US-Anbietern beim Thema Sovereign Cloud?
Dr. Julia Pergande | Die Abhängigkeit von US-Anbietern ist rechtlich und strukturell problematisch. US-Gesetze wie der Patriot Act oder Cloud Act erlauben US-Behörden Zugriff auf Daten, auch wenn diese außerhalb der USA gespeichert sind, wenn die Anbieter US-Muttergesellschaften haben. Zudem entstehen faktische Monopole, höhere Lizenzkosten und die Gefahr von sogenannten „Kill Switches", also eingebauten Hintertüren in proprietären Systemen. Daher setzen viele Sovereign Cloud Anbieter auf Open-Source-Lösungen, um diese Probleme zu vermeiden.

Sie haben eine aktuelle Marktübersicht zum europäischen Public-Cloud-Markt erstellt. Wir stellt er sich heute dar? Wer sind die relevanten Anbieter, und worin unterscheiden sie sich von Hyperscalern in Angebotstiefe, Betriebsmodellen und Compliance?
JP | Die europäische Public-Cloud-Landschaft ist heute deutlich vielfältiger und reifer als noch vor wenigen Jahren. Es hat sich ein Markt entwickelt, der zwar in der Breite nicht mit den US-Hyperscalern konkurrieren kann, aber in spezifischen Bereichen – insbesondere rund um Compliance, Datensouveränität und sektorale Anforderungen – überzeugende Alternativen bietet. In unserer Marktübersicht, die microfin im September 2025 veröffentlicht hat, analysieren wir Anbieter wie OVHcloud, Open Telekom Cloud, STACKIT, Scaleway, Cleura, Exoscale und andere, die sich gezielt auf europäische Anforderungen ausrichten. Sie unterscheiden sich von den Hyperscalern vor allem in folgenden Punkten:

- **Betriebsmodell:** Viele setzen auf Rechenzentren ausschließlich in der EU, überwiegend mit eigener Infrastruktur, eigenen Mitarbeitenden mit EU-Staatsbürgerschaft sowie soliden Basisdiensten und ohne Abhängigkeit von US-Mutterkonzernen.
- **Rechtsraum:** Die Anbieter unterliegen europäischem Recht und bieten – anders als viele „Sovereign Cloud"-Konzepte der US-Anbieter – keine Hintertüren über den CLOUD Act.
- **Transparenz und Compliance:** Europäische Anbieter kommunizieren ihre Datenschutz- und Sicherheitsarchitekturen oft klarer, bieten Auditunterstützung, Exit-Klauseln und zum Teil größeren Spielraum bei der Vertragsgestaltung.

DIE GESPRÄCHSPARTNERIN
Dr. Julia Pergande
ist Principal Consultant und Projektleiterin bei Microfin, einer deutschen Beratung, die sich auf Finanzdienstleistungen und digitale Transformation spezialisiert hat. Sie unterstützt Unternehmen bei der Umsetzung von Governance-, Risiko- und Compliance-Projekten und entwickelt systematische, toolgestützte Risikobewertungen zur Einhaltung rechtlicher Vorgaben.

Es gibt auch Hybrid-Modelle, bei denen Sovereign Clouds auf Produkten von Hyperscalern aufsetzen. Welche Risiken sehen Sie dabei?
JP | Diese „Sovereignty light"-Modelle sind abhängig von Updates und Sicherheits-Management der Hyperscaler. Verzögerungen bei Updates können die Betriebssicherheit gefährden und Zeitfenster für Cyberangriffe öffnen. Unternehmen haben dann eine sogenannte Achillesferse, in der ihre Systeme angreifbar sind.

Wie verbreitet ist der Gedanke an Exit-Strategien aus der Cloud?
JP | In der Finanzbranche ist der Mindset durch Regulierungen wie DORA und den Data Act gut angekommen. Diese fordern Exit-Strategien und deren Tests, etwa durch Tabletop-Tests, um einen geordneten Wechsel und Notfallressourcen zu gewährleisten. Cloud-Provider sind inzwischen verpflichtet, Schnittstellen und Wechselmöglichkeiten bereitzustellen.

- **Service-Tiefe:** In der Breite an PaaS-, ML- oder Edge-Services sind sie den Hyperscalern noch unterlegen, bieten weniger „out-of-the-box Integration" – in bestimmten Kernfunktionen jedoch absolut konkurrenzfähig.

Was bedeutet „digitale Souveränität" für Unternehmen ganz konkret – und wie machen Sie sie messbar? Welche Dimensionen und Metriken nutzen Sie?

JP | „Digitale Souveränität" beschreibt „die Fähigkeit eines Unternehmens, digitale Infrastrukturen und Dienste selbstständig, selbstbestimmt und sicher zu gestalten, zu betreiben und weiterzuentwickeln – ohne Abhängigkeiten von einzelnen Anbietern oder Drittstaaten (in Anlehnung an Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (Zendis), Whitepaper Souveränitäts-Washing bei Cloud-Diensten erkennen). Wir übersetzen „Digitale Souveränität" in konkrete, bewertbare Kriterien, die Unternehmen direkt in ihre Auswahlprozesse übernehmen können. In unserer Methodik betrachten wir unter anderem folgende Dimensionen:

- **Souveränität & Compliance:** Welche Datenkategorien mit welcher Schutzbedürftigkeit und welchen Anforderungen an Drittstaatenexposition gemäß DSGVO, eigene Schlüssel und Auditrechte umfasst der Workload?
- **Resilienz & Portabilität:** Muss ich providerunabhängig bleiben (DORA-Konzentrationsrisiko), Exit testen können oder RTO/RPO konservativ einhalten?
- **Passfähigkeit:** Welche Anforderungen an Latenz-/Edge, Netzfunktionen, Kompatibilität und Berechtigungsmanagement hat mein Workload?
- **Innovation:** Welche PaaS/AI-Tiefe, Ökosystem-Integrationen und Time-to-Value brauche ich?
- **Wirtschaftlichkeit:** Welchen TCO inkl. Egress bzw. Exit-Kosten, Betriebsaufwand und Lizenzen möchte ich mir leisten?

Wie beeinflussen DSGVO, NIS2, DORA und branchenspezifische Vorgaben (z. B. KRITIS) die Anbieterwahl? Reichen „Sovereign Cloud"-Angebote der Hyperscaler aus, um CLOUD Act-Risiken und europäische Zertifizierungen abzudecken?

JP | DSGVO, NIS2, DORA und Orientierungshilfen im Finanzdienstleistungsumfeld geben den Startschuss für mehr Souveränität. Die genannten Vorgaben führen im Grundsatz zur Erkenntnis, dass Unternehmen mehr Souveränität benötigen – damit rücken Souveränitätsmaßnahmen in den Fokus aufsichtsrechtlicher Prüfungen. Das hat unmittelbare Auswirkungen auf die Anbieterwahl:

- Für Unternehmen mit kritischen Infrastrukturen oder in regulierten Branchen ist es heute nicht mehr ausreichend, sich auf rein technische Sicherheitsfunktionen zu verlassen.
- Viele „Sovereign Cloud"-Angebote der Hyperscaler sind aufgrund proprietärer Services stark von den US-Plattformen abhängig – sie versprechen Autonomie, können diese aber rechtlich nicht garantieren, da der Zugriff durch US-Behörden (z. B. CLOUD Act) weiterhin möglich ist.
- Zertifizierungen wie C5, ISO 27001, EUCS (zukünftig) sind wichtige Nachweise, aber kein Ersatz für eine rechtliche und strategische Bewertung des Anbietermodells.

Unser Fazit:

Wer regulatorische Anforderungen ernst nimmt, sollte nicht nur auf Labels vertrauen, sondern auf echte Kontrollmöglichkeiten, Exit-Management, nachvollziehbare Betriebsmodelle und vollständige Datenkontrolle. •

MEHR ERFAHREN

Lesen Sie das ausführliche Interview mit **Dr. Julia Pergande** auf der Webseite von DIGITAL BUSINESS.

INFOKASTEN PRAXISFAHRPLAN

Welche Schritte sollten Unternehmen in den nächsten 12–24 Monaten gehen, um digitale Souveränität zu erhöhen?

Wir empfehlen einen klaren, schrittweisen Fahrplan:

1. Ist-Analyse der bestehenden Cloud-Nutzung:
   Wer hat heute Zugriff auf welche Daten – technisch und rechtlich?
2. Souveränitätsbewertung der eingesetzten Anbieter:
   Rechte, Rechtsräume, Portabilität, Exit-Potenzial – also Chancen und Risiken bewerten.
3. Festlegung strategischer Cloud-Ziele:
   Was soll souverän bleiben, was darf performant aber kontrolliert ausgelagert werden?
4. Auswahl geeigneter Anbieter – unter Nutzung strukturierter Marktübersichten, wie sie microfin bereitstellt, und klarer Architekturanforderungen
5. Governance- und Compliance-Fähigkeiten:
   angemessene Risikosteuerung, IT-Security und Cloud-Providermanagement etablieren
6. Pilotierung und schrittweise Migration, begleitet durch Architektur und FinOps

Typische Fehler sind:

Zu enge Bindung an einzelne Sourcing-Partner, fehlende Exit-Pläne, Unterschätzen regulatorischer Risiken mit Folgen für Auditprüfungen.

Quick Wins liegen oft in:

- konsolidierter Datenhaltung an einem zentralen Ort
- Exit-tauglicher Architektur mit Portabilität und Flexibilität
- interner Sensibilisierung der Mitarbeitenden für Lock-in-Risiken

Neben klassischen Verfügbarkeitskennzahlen lassen sich weitere aussagekräftige Metriken heranziehen, um Fortschritt und Reifegrad im Cloud-Kontext messbar zu machen – und damit die notwendige **Management-Akzeptanz** zu schaffen. Dazu zählen unter anderem der **Abdeckungsgrad eingesetzter Cloud-Lösungen mit definierten Exit-Konzepten**, die **Kostenentwicklung pro Workload oder Umgebung** sowie die **Anzahl aktiver Cloud-Projekte je Betriebsumgebung** (z.B. Anzahl Cloud-Projekte in Entwicklung, Test, Produktion).
Solche Kennzahlen ermöglichen eine faktenbasierte Steuerung und helfen, Cloud-Ziele transparent zu verankern.

Digitale Souveränität als Überlebensstrategie für deutsche Unternehmen

Der Wechsel in eine souveräne Cloud ist keine technische Entscheidung, sondern eine strategische Notwendigkeit. Wer digitale Abhängigkeiten in Kauf nimmt, riskiert Compliance, Innovationskraft und Handlungsfähigkeit. Der aktuelle EuroCloud Pulse Check 2025 belegt: Souveränität wird zum Schlüssel für Resilienz. /// von Andreas Kadler

Abhängigkeit als strategisches Risiko

Lange galt die Nutzung globaler Hyperscaler als Garant für Stabilität und Skalierbarkeit. Doch wer seine Daten und Prozesse außerhalb des europäischen Rechtsraums betreibt, gibt ein Stück Kontrolle ab. Der EuroCloud Pulse Check 2025 zeigt deutlich, wie sehr Unternehmen diese Risiken inzwischen wahrnehmen. 71 Prozent der befragten IT-Entscheider stufen digitale Souveränität und Resilienz heute als zentrale Faktoren ihrer Cloud-Strategie ein. Vor fünf Jahren waren es nur 25 Prozent. Geopolitische Krisen, Handelskonflikte und rechtliche Unsicherheiten haben laut der Studie das Vertrauen in außereuropäische Cloud-Infrastrukturen erschüttert. 57 Prozent der Unternehmen geben an, dass die aktuelle US-Außenpolitik sie bezüglich ihrer Infrastrukturstrategie verunsichert.

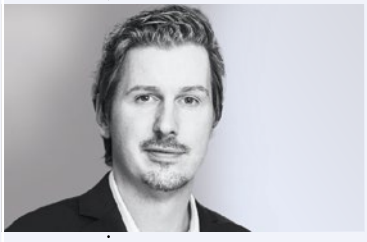
Was digitale Souveränität wirklich bedeutet

Digitale Souveränität beschreibt die Fähigkeit, Daten, Technologien und Prozesse eigenständig zu steuern. Es geht darum, zu wissen, wo Daten liegen, wer darauf zugreifen darf und welche Systeme den eigenen Betrieb tragen. Ebenso umfasst sie die Freiheit, Anbieter zu wechseln oder Infrastrukturen selbst weiterzuentwickeln. Daraus hat sich das Konzept der souveränen Cloud entwickelt. Sie basiert auf offenen Technologien und wird in Rechenzentren innerhalb der EU und somit im europäischen Rechtsraum betrieben. Was viele aber nicht wissen: Entscheidend ist vor allem der Unternehmenssitz des Anbieters. Nur wenn dieser ebenfalls in Europa liegt, bleiben der US CLOUD Act oder ähnliche extraterritoriale Regelungen ausgeschlossen.

Wirtschaftliche und strategische Vorteile

Rechtliche Sicherheit und langfristige Innovationsfreiheit sind wichtige Säulen für Unternehmen, um langfristig im Wettbewerb zu bestehen. Doch ein Wechsel in eine souveräne Cloud hat noch weitere Vorteile. Zum Beispiel klar ausgewiesene und planbare Kosten, während die Hyperscaler oft mit komplexen und intransparenten Preismodellen arbeiten.

Viele unterschätzen dabei die sogenannten Egresskosten, also die Gebühren, die beim Datentransfer aus einer Hyperscaler-Cloud anfallen. Wer Workloads migrieren möchte, zahlt oft hohe Summen für den Ausstieg.



DER AUTOR
Andreas Kadler
Andreas Kadler ist CEO von plusserver.

> „ Was viele Unternehmen nicht wissen: **Entscheidend ist vor allem der Unternehmenssitz des Anbieters.** Nur wenn dieser ebenfalls in Europa liegt, bleiben der US CLOUD Act oder ähnliche extraterritoriale Regelungen ausgeschlossen.
>
> *Andreas Kadler*

6 SCHRITTE IN RICHTUNG DIGITALE SOUVERÄNITÄT

1. **Machen Sie eine Bestandsaufnahme:** Erfassen Sie, welche Daten und Systeme kritisch sind und unter welchen rechtlichen Rahmenbedingungen sie betrieben werden.
2. **Prüfen Sie Abhängigkeiten:** Analysieren Sie technische, vertragliche und finanzielle Bindungen an aktuelle Anbieter.
3. **Migrieren Sie schrittweise:** Beginnen Sie mit sensiblen Workloads und erweitern Sie sukzessive die souveräne Infrastruktur.
4. **Nutzen Sie offene Standards:** Setzen Sie auf interoperable T echnologien und APIs, um künftige Migrationen zu erleichtern.
5. **Verankern Sie Compliance und Kontrolle:** Definieren Sie klare Zuständigkeiten und regelmäßige Audits für Ihre Cloud-Umgebung.
6. **Etablieren Sie eine Exit-Strategie:** Testen Sie regelmäßig, ob Daten und Anwendungen ohne Abhängigkeiten exportiert werden können.

Diese Kosten verstärken den Lock-in-Effekt und erschweren die Entscheidung für Alternativen. Jedoch lohnt sich der finanzielle und organisatorische Aufwand. Eine souveräne Cloud bietet langfristige Kostentransparenz statt versteckter Gebühren, ermöglicht rechtliche Kontrolle und stärkt die unternehmerische Resilienz.

Auch im operativen Bereich können sich langfristige Verbesserungen ergeben. Der direkte persönliche Support und die Möglichkeit, das eigene IT-Team durch Managed Services zu entlasten, schaufelt Kapazitäten frei, die beispielsweise für die Weiterentwicklung des digitalen Geschäftsmodells genutzt werden können.

Der Weg aus der Abhängigkeit

Für viele IT-Entscheider stellt sich heute nicht mehr die Frage, ob sie migrieren, sondern wie sie sich aus bestehenden Abhängigkeiten lösen können, ohne den laufenden Betrieb zu gefährden.

Der Schlüssel? Liegt in einer schrittweisen Strategie: Zunächst können besonders kritische Daten und Anwendungen, die sensibel oder regulatorisch relevant sind, in eine rechtssichere europäische Umgebung überführt werden. Dies hat auch den Vorteil, dass die neue Umgebung in einem Proof of Concept getestet werden kann, bevor sie zum produktiven Fundament des Unternehmens wird. Erst danach folgen weniger kritische Workloads, die sukzessive migriert werden.

Laut der Studie planen mehr als die Hälfte der befragten Unternehmen, zukünftig eine Hybrid-Cloud-Strategie zu verfolgen. Dieses Modell bietet einen praktikablen Mittelweg: Neue Anwendungen werden direkt in souveränen Infrastrukturen aufgebaut, während bestehende Systeme schrittweise folgen. So entsteht ein kontrollierter Übergang ohne Betriebsrisiko.

Wer im Zuge der Migration zudem auf offene Standards und kompatible Schnittstellen setzt, kann Datenportabilität sicherstellen und Lock-in-Effekte von vornherein ausschließen. Konkret bieten sich Technologien wie Kubernetes oder auch S3-kompatible Schnittstellen an, um die gewünschte Portabilität zu erreichen. Auch vertragliche und organisatorische Grundlagen spielen eine zentrale Rolle: Verträge sollten Exit-Klauseln, transparente Support-Bedingungen und eindeutige Datenrückführungsrechte enthalten.

Den richtigen Partner finden

Europa verfügt über ein breites Angebot souveräner Cloud-Lösungen, und diese sind oft leistungsfähiger als gemeinhin angenommen. Aber wie finden Unternehmen nun den richtigen Anbieter für ihre Anforderungen? Bei der Auswahl eines Cloud-Partners sind weniger die Größe oder die Markenbekanntheit entscheidend als die Qualität der Zusammenarbeit. Auch die reine Preisfrage sollte nicht im Vordergrund stehen.

Im Kontext der Studie gab die Mehrheit an, dass spezialisierte Dienstleistungen für Bereiche wie KI oder Data Analytics sowie ein umfangreiches Produktportfolio im Auswahlprozess eines geeigneten Partners mit großem Abstand am relevantesten seien. Es geht also darum, nicht nur „irgendeinen" Cloud-Anbieter zu finden, sondern einen strategischen Partner, mit dessen Infrastruktur und Know-how sie ihre digitale Zukunft sichern und durch souveräne Datenkontrolle langfristige Resilienz erreichen.

Digitale Souveränität entsteht nicht automatisch durch Technologie. Maßgeblich ist, ob der Anbieter nachvollziehbar darlegen kann, wie er Daten schützt, Zugriffe kontrolliert und Migrationen ermöglicht. •

Open Source als Grundpfeiler:

So sichern Unternehmen digitale Souveränität

Digitale Souveränität ist mehr als ein Label: Peter H. Ganten von der Open Source Business Alliance warnt vor Scheinlösungen und setzt auf Open Source und offene Standards.

/// von Konstantin Pfliegl

DIGITALE SOUVERÄNITÄT IST KEIN MODEBEGRIFF, SONDERN EINE ZENTRALE FÜHRUNGSFRAGE: Wer sie besitzt, behält die Kontrolle über Daten, Prozesse und Abhängigkeitsstrukturen – vor allem in einem Umfeld von Cloud-Hyperscalern, KI-Ökosystemen und zunehmender Regulatorik. Open Source gilt dabei als Hebel: Transparenz, Auditierbarkeit und offene Standards reduzieren Lock-ins, fördern Interoperabilität und beschleunigen Innovationen. Für Entscheider heißt das: Nicht „Open Source – ja oder nein?", sondern „wie".

Wie lässt sich Open Source so einsetzen, dass sie Souveränität wirklich stärkt? DIGITAL BUSINESS spricht darüber mit Peter H. Ganten, Vorstandsvorsitzender der Open Source Business Alliance (OSBA) – Bundesverband für digitale Souveränität.

Herr Ganten, sind wir aktuell zu abhängig von großen außereuropäischen IT-Anbietern, etwa aus den USA?
Peter H. Ganten | Ja, definitiv, auch wenn wir bereits Alternativen für mehr digitale Souveränität aufbauen, ist die bestehende Abhängigkeit ein riesiges Problem. Bereits im Jahr 2019 hat eine von der damaligen Bundesregierung beauftragte Studie eine erhebliche, ja schmerzhafte, Abhängigkeit der deutschen Verwaltung von großen außereuropäischen IT-Anbietern und deren Closed-Source-Angeboten festgestellt.

Und wie sieht es in der Wirtschaft aus?
PG | In der Wirtschaft sieht es genauso dramatisch aus: Eine Bitkom-Studie aus diesem Jahr hat ergeben, dass 90 Prozent der deutschen Unternehmen abhängig sind von digitalen Technologien und Services aus dem Ausland.

Die Anstrengungen, die seitdem unternommen wurden, waren vielfach zu gering, es scheint oft noch an dem entschlossenen politischen Willen zu fehlen, eine ernsthafte Open-Source-Transformation in der Verwaltung anzustoßen. Jahr für Jahr fließen aus öffentlichen Geldern weiterhin Milliarden-Beträge an große, vor allem US-amerikanische Konzerne, statt in digital souveräne Lösungen aus Deutschland und Europa investiert zu werden. Und diese Milliardenbeträge an monopolartige Closed-Source-Hersteller werden von diesen Unternehmen dafür verwendet, um die bestehenden Abhängigkeiten immer weiter auszubauen.

Aber ist die Abhängigkeit von außereuropäischen IT-Anbietern nicht schon viel zu weit vorgeschritten? Kann man überhaupt noch gegensteuern?
PG | Wissen Sie was, das ist ein Narrativ, das die großen US-amerikanischen Anbieter ganz bewusst verbreiten: Wir wären bereits viel zu abgehängt, der Innovationsabstand schon viel zu groß. Wir sollten also gleich aufgeben und die Abhängigkeiten einfach so hinnehmen, da wir ja ohnehin nichts ändern könnten. Das ist Quatsch.

Gerade in der IT sehen wir, dass alle paar Jahre unerwartete und erstaunliche Disruptionen passieren. Der IT-Markt kann sich jederzeit grundlegend durch das Aufkommen neuer Technologien ändern. Und wir haben bereits viel an Knowhow und an leistungsfähigen Open-Source-Alternativen in Deutschland und Europa, wir müssen diese nur entschlossen weiter ausbauen. Und selbstverständlich müssen wir bei den bestehenden Abhängigkeiten gegensteuern.

Was wäre denn die Alternative: Dass wir uns in unser Schicksal ergeben, unsere Daten, unsere Wettbewerbsfähigkeit, ja die Kontrolle über die kommunikativen Grundlagen unserer Demokratie einfach aufgeben, und die zukünftige Entwicklung im Digitalen vollständig anderen überlassen? Wir haben die Gestaltung unserer digitalen Zukunft selbst in der Hand und ich glaube, allen ist bewusst, dass es einen enormen Handlungsdruck gibt. Wir müssen noch viel für unsere digitale Souveränität tun, aber der Zeitpunkt um damit anzufangen ist so günstig wie nie.

Viele sehen Open Source als Schlüssel für eine digitale Souveränität. Welche Vorteile bietet Open-Source-Software im Gegensatz zu Lösungen, die einzelne Unternehmen entwickeln?
PG | Da Sie das „einzeln" erwähnen: Bei Open-Source-Software gibt es oft eine große internationale Community, die gemeinsam an der Weiterentwicklung und Verbesserung einer Software arbeitet. Diese Kooperation ist ein immenser Vorteil. Entwicklungskosten können geteilt werden, jeder kann sich den Quellcode anschauen und Fehler finden oder Verbesserungen vorschlagen und einbringen. Zugleich muss man nicht immer bei Null anfangen: Open Source bietet die Möglichkeit, auf bestehenden Lösungen aufzusetzen, und diese je nach Bedarf anzupassen und bewahrt dabei zugleich eine erhebliche Skalierbarkeit.

DER GESPRÄCHSPARTNER

Peter H. Ganten

ist Vorstandsvorsitzender der Open Source Business Alliance (OSBA) – Bundesverband für digitale Souveränität.

Bild: OSBA

MEHR ERFAHREN

Lesen Sie das ausführliche Interview mit Peter H. Ganten auf der Webseite von DIGITAL BUSINESS.

> „ Das ist ein Narrativ, das **die großen US-amerikanischen Anbieter ganz bewusst verbreiten:** Wir wären bereits viel zu abgehängt, der Innovationsabstand schon viel zu groß.
>
> *Peter H. Ganten*

Nicht zuletzt ermöglichen die Transparenz des Quellcodes und die Freiheiten, die die Open-Source-Lizenzen gewähren, eine Kontrolle über die Software, und eine Herstellerunabhängigkeit. Geht mein Dienstleister insolvent, wird aufgekauft oder erhöht die Preise zu sehr, kann ich die gleiche Software-Lösung auch von einem anderen Unternehmen betreiben und weiter entwickeln lassen. Aufgrund der Kontrolle, Gestaltungsfähigkeit und Herstellerunabhängigkeit ist Open-Source-Software eine entscheidende Grundvoraussetzung für digitale Souveränität.

Laut dem Digitalverband Bitkom nutzen drei von vier Unternehmen in Deutschland bereits Open-Source-Software und 73 Prozent sehen in Open Source eine Chance für mehr digitale Souveränität. Das mag bei so mancher Nischen-Software zutreffen. Aber ist es in der Praxis nicht so, dass viele Unternehmen – etwa mit Microsoft 365 und Cloud-Diensten etwa von Amazon – von Open Source für relevante Dienste noch weit entfernt sind?

PG | Zunächst mal würde ich vermuten, dass deutlich mehr Unternehmen bereits Open-Source-Software nutzen, vermutlich wissen sie das einfach nicht. Von Datenbankmanagement-Software über Betriebssysteme, in denen der Linux-Kernel verwendet wird: Studien zufolge stecken heute in circa 95 Prozent der Software-Lösungen Open-Source-Komponenten.

Es ist natürlich richtig, dass in einigen Bereichen die Open-Source-Alternativen schon weiter entwickelt sind als in anderen. Aber dort, wo es noch an digital souveränen Lösungen mangelt, werden diese entwickelt – oftmals sogar gemeinschaftlich von Marktbegleitern. Ein gutes Beispiel dafür ist die Autoindustrie, wo sich in dem Projekt Catena-X mehrere Unternehmen in einem Bündnis zusammengefunden haben, um passende Open-Source-Lösungen zu entwickeln. Denn mehr und mehr Unternehmen sehen inzwischen die Bedeutung von digitaler Souveränität für Ihr eigenes Geschäft und erkennen dass es unerlässlich ist, sich aus bestehenden Abhängigkeiten zu lösen. Denn diese Abhängigkeiten verursachen zunehmend erhebliche Kosten und bedrohen ihre Geschäftsgrundlage.

Die Unternehmen verstehen immer mehr, dass Open Source ein wichtiger Schlüssel für den Wandel ist. Gerade in der Industrie geht es häufig um hochspezialisierte Software, und dabei kann Open-Source-Software seine Vorzüge ausspielen.

Wenn wir uns Cloud-Dienste von Amazon & Co. ansehen: Zum Beispiel umfangreiche Services für Big Data oder künstliche Intelligenz – sind da vergleichbare Open-Source-Alternativen überhaupt absehbar?

PG | Auf jeden Fall. Mit Unternehmen wie beispielsweise Ionos, Schwarz IT, Plusserver, Syseleven, Nextcloud, B1 oder Opencloud gibt es bereits eine Reihe von Cloud-Anbietern, die auf Open-Source-Software setzen. Hier gibt es bereits eine Reihe sehr guter und am Markt erfolgreicher Angebote, Tendenz steigend. Auch hier sollten wir aber nicht anstreben, einen einzelnen Anbieter von vergleichbarer Hyperscaler-Dimension zu schaffen, oder deren Angebote oder Geschäftsmodelle eins zu eins zu kopieren. Offene Clouds ermöglichen eine ganz andere Flexibilität und Interoperabilität. Mit der Open Source Business Alliance waren wir übrigens maßgeblich daran beteiligt, mit dem Sovereign Cloud Stack (SCS) offene Cloud-Standards zu entwickeln, die diesen interoperablen, europäischen Ansatz erst ermöglichen. Und SCS wird heute schon produktiv von etlichen Unternehmen und Behörden genutzt. •

Europas Suche nach digitaler Freiheit:

Zwischen Anspruch und Realität

Geopolitischen Spannungen, Regulierungswelle in Europa und wachsender Druck zurDatenunabhängigkeit verändern die IT-Strategien von Unternehmen radikal. Kaum eine Organisation kommt heute noch am Thema digitale Souveränität vorbei. Doch was bedeutet das konkret – und wie souverän kann man in einer global vernetzten Welt überhaupt sein? Ein Gespräch mit Daniel Wagenknecht*, Partner bei KPMG in Deutschland, über den „Cloud Monitor“, regulatorische Zwänge und die Frage, wie viel Unabhängigkeit realistisch ist. /// von Heiner Sieger

Herr Wagenknecht, laut dem aktuellen KPMG Cloud Monitor wird digitale Souveränität zunehmend zur strategischen Priorität – vor allem im Finanzsektor. Wie erklären Sie sich diesen Trend?
Daniel Wagenknecht | Wir sehen in allen Branchen, dass das Thema digitale Souveränität durch geopolitische Unsicherheiten stark an Bedeutung gewonnen hat. Besonders im Finanzsektor, wo Regulatorik und Aufsicht eine große Rolle spielen, ist das Bewusstsein für Kontroll- und Sicherheitsmechanismen sehr ausgeprägt. Aber letztlich betrifft es alle, die mit sensiblen oder personenbezogenen Daten umgehen – also praktisch jedes Unternehmen. Es geht darum, sich unabhängiger zu machen und Risiken resultierend aus der Geopolitik zu steuern.

Laut Ihrer Studie sind 59 Prozent der Finanzunternehmen bereit, 20 bis 30 Prozent mehr für souveräne Cloud-Lösungen zu bezahlen. Spiegelt das echte Zahlungsbereitschaft oder eher Absichtserklärungen wider?
DW | Diese Zahlen sind zunächst hypothetisch – vergleichbar mit der Frage, ob jemand für Bio-Lebensmittel mehr zahlen würde. In der Praxis zeigt sich dann doch ein Unterschied zwischen Anspruch und Verhalten. Trotzdem ist klar: Souveräne Lösungen sind teurer, weil sie zusätzliche Kontrollinstanzen, Sicherheitsmechanismen und Beschränkungen beim Datenzugriff mitbringen. Unternehmen wissen, dass Unabhängigkeit ihren Preis hat – und der wird zunehmend akzeptiert, auch über den Finanzsektor hinaus.

Was verstehen Sie persönlich unter digitaler Souveränität?
DW | Souveränität bedeutet nicht, völlig unabhängig zu sein – das wäre illusorisch und wirtschaftlich ineffizient. Es geht darum, die Abhängigkeiten bewusst zu steuern und zu begrenzen. Unternehmen sollten vermeiden, in einen vollständigen „Lock-in“ bei einem Anbieter zu geraten, insbesondere bei großen Hyperscalern. Digitale Souveränität kann sich auf verschiedene Ebenen beziehen: technologische, servicebezogene oder datenspezifische. Jede verlangt andere Maßnahmen.

Gerade bei der Datensouveränität scheint der Markt noch eingeschränkt. Viele Lösungen gelten nur als „Light-Version“. Wie beurteilen Sie das?
DW | Das ist tatsächlich ein Spannungsfeld zwischen Souveränität und Innovationsfähigkeit. Je stärker ich den Regler in Richtung Unabhängigkeit schiebe, desto mehr schränke ich den Zugriff auf innovative Services ein – etwa auf KI-Angebote großer US-Provider. Europäische Anbieter gibt es, aber ihre Funktionsvielfalt liegt derzeit bei etwa einem Drittel dessen, was internationale Technologiekonzerne bieten. Unternehmen müssen deshalb abwägen: Wo brauche ich das „Luxusauto“ mit allen Features – und wo reicht ein solider „Kleinwagen“, der mir volle Datensouveränität in Europa garantiert?

Welche Kriterien sollten Unternehmen erfüllen, um wirklich souverän handeln zu können?
DW | Wenn wir bei der Datensouveränität bleiben, dann ist ein entscheidendes Kriterium, dass Daten ausschließlich in europäischen Rechenzentren gespeichert und verarbeitet werden – ohne jegliche Zugriffsmöglichkeiten von außen. Das betrifft insbesondere den US Cloud Act, der theoretisch den Zugriff amerikanischer Behörden erlaubt. Wer Datensouveränität ernst nimmt, sollte sicherstellen, dass diese Zugriffe technisch und organisatorisch ausgeschlossen sind.

Welche konkreten Vorteile bringt ein souveräneres Cloud-Setup über die reine Compliance hinaus?
DW | Im Finanzsektor schafft es vor allem Vertrauen – bei Aufsichtsbehörden, aber auch bei Kundinnen und Kunden. Wenn Banken oder Versicherungen zeigen können, dass ih-

DER GESPRÄCHSPARTNER

Daniel Wagenknecht ist Partner bei KPMG Deutschland und verantwortet den Bereich Financial Services Technology. Er berät Banken, Versicherungen und Aufsichtsbehörden in Fragen der Cloud-Transformation, IT-Governance und digitalen Souveränität.

> „ Europäische Anbieter gibt es, aber ihre Funktionsvielfalt liegt derzeit bei etwa 20 Prozent dessen, was internationale Hyperscaler bieten. Unternehmen müssen deshalb abwägen: Wo brauche ich den „Mercedes“ mit allen Features – und wo reicht ein solider „Kleinwagen“, der mir **volle Datensouveränität in Europa** garantiert?
>
> *Daniel Wagenknecht*

re Datenströme nachvollziehbar und abgesichert sind, stärkt das ihre Reputation. Darüber hinaus ermöglicht eine klare Exit-Strategie – also die Möglichkeit, im Krisenfall den Anbieter zu wechseln – eine größere Resilienz gegenüber Störungen und Sanktionen. Das ist auch für andere Branchen wie Pharma oder Fertigungsindustrie zunehmend relevant.

Viele Unternehmen setzen inzwischen auf Multi-Cloud- oder Sovereign-Cloud-Modelle. Wo liegen die größten technischen Herausforderungen?

DW | Meist starten Unternehmen nicht mit einem kompletten Wechsel, sondern ergänzen ihre bestehende Landschaft um einen souveränen Anbieter – oft zunächst in Pilotprojekten. Das erhöht aber die Komplexität: zusätzliche Technologien, mehr Integrationsaufwand, neue Kompetenzen. Die IT-Abteilungen müssen lernen, mit hybriden Architekturen umzugehen und Datenflüsse über mehrere Clouds hinweg sicher zu managen. Das kostet Geld und Know-how, ist aber der Preis für mehr Kontrolle.

Welche Rolle spielen Verträge und Service Level Agreements, wenn es um digitale Souveränität geht?

DW | Eine sehr große. Gerade im Finanzsektor sind umfangreiche Prüf- und Informationsrechte, Exit-Klauseln und Kündigungsrechte mittlerweile Standard. Dienstleister müssen diese Bedingungen akzeptieren, um überhaupt am Markt bestehen zu können. Aber selbst der beste Vertrag schützt nicht vor geopolitischen Risiken. Wenn morgen eine Sanktion kommt, die US-Anbietern das Geschäft in Europa verbietet, hilft kein Paragraph weiter. Das ist das berühmte „Worst-Case-Szenario“, das man zwar durchspielen, aber nicht komplett verhindern kann.

Die neuen europäischen Regulierungen wie DORA oder NIS2 sollen die Widerstandsfähigkeit erhöhen. Fördern sie auch digitale Souveränität?

DW | Grundsätzlich ja, weil sie Unternehmen zwingen, sich intensiver mit Risiken, Abhängigkeiten und Resilienz zu beschäftigen. Allerdings nimmt der regulatorische Druck immer weiter zu – besonders für Banken und Versicherungen. Die Umsetzung ist teuer und aufwendig, und manchmal geht der eigentliche Zweck, nämlich die Stärkung der IT-Widerstandsfähigkeit, in Detailvorgaben verloren. Es braucht hier an manchen Stellen mehr Pragmatismus und klare Prioritäten.

Wie können Unternehmen in Zeiten geopolitischer Unsicherheit ihre Handlungsfähigkeit sichern?

DW | Der wichtigste Rat ist: Ruhe bewahren. Panikreaktionen helfen niemandem. Stattdessen sollten Unternehmen ihre aktuelle Dienstleisterlandschaft analysieren: Wo liegen die größten Risiken und Abhängigkeiten? Welche (Cloud-)Provider nutze ich, und wo ist mein Grad an Souveränität zu niedrig? Auf dieser Basis lassen sich gezielte Maßnahmen ableiten – etwa der Aufbau eines weiteren, souveränen Providers oder die stärkere Diversifizierung von Anwendungen. Absolute Risikomitigation gibt es nicht, aber Transparenz ist der erste Schritt.

Was braucht es, um digitale Souveränität in Europa langfristig zu stärken – über einzelne Unternehmen hinaus?

DW | Jetzt ist der richtige Moment, um gemeinsam zu handeln. Politik, Wirtschaft und Anbieter sollten den Rückenwind nutzen, um echte europäische Alternativen aufzubauen. Die Idee von Gaia-X war ein Anfang, aber sie ist ins Stocken geraten. Wenn sich Branchen, Technologieanbieter und Regierungen jetzt zusammenschließen, könnten aus Kooperationen tragfähige, souveräne Cloud-Lösungen entstehen.

Dafür braucht es Mut, Investitionen – und die Bereitschaft, kurzfristige Konkurrenzgedanken beiseitezulegen. •

Souveräne Daten, starke Industrie

Europas Industrie steht vor der Herausforderung, Innovation und den Schutz sensibler Daten in Einklang zu bringen. Datensicherheit und digitale Souveränität sind dabei keine Option mehr, sondern die Grundlage nachhaltiger Wettbewerbsfähigkeit – insbesondere in einem Umfeld, das von globalen Abhängigkeiten und wachsenden Cyberrisiken geprägt ist. /// von Andreas Dangl

Cyberrisiken und globale Abhängigkeiten wachsen
Aktuelle Entwicklungen zeigen, wie verletzlich digitale Wertschöpfung geworden ist. Cyberangriffe auf industrielle Steuerungssysteme, gezielte Sabotage oder Datenmanipulation in Lieferketten haben reale wirtschaftliche Auswirkungen. Gleichzeitig dominieren außereuropäische Cloud-Anbieter weiterhin den Markt. Diese Konzentration führt zu strukturellen Abhängigkeiten, die über rein technische Aspekte hinausgehen. Immer mehr europäische Unternehmen befassen sich mit der Frage: Wer hat Zugriff auf die eigenen Daten – und wo sind diese tatsächlich gespeichert?

Der US CLOUD Act verpflichtet amerikanische Betriebe, gespeicherte Daten auf Anfrage an US-Behörden herauszugeben – selbst wenn sie sich physisch in Europa befinden. Damit verliert jede Organisation, die auf US-basierte Cloud-Dienste setzt, ein Stück ihrer Kontrolle über vertrauliche Informationen. Digitale Souveränität wird so zu einer Frage der Selbstbestimmung: Wer eigene Handlungsspielräume sichern will, entscheidet sich bewusst für europäische IT-Infrastrukturen und Rechtsrahmen.

Industrie braucht transparente und vertrauenswürdige Systeme
In der Industrie spielt der Schutz von Konstruktionsdaten, Stücklisten, Prüfzertifikaten und Projektdokumentationen eine zentrale Rolle. Diese Informationen bilden das Rückgrat technischer Prozesse und sind entscheidend für Qualität, Sicherheit und Nachweisführung.

DER AUTOR
Andreas Dangl
ist Entrepreneur und Geschäftsführer der Fabasoft Approve GmbH.
In seiner Funktion unterstützt er Unternehmen aus der Industrie bei der Einführung von KI-gestütztem Dokumenten- und Qualitätsmanagement.

Ziel ist es, klare Strukturen für Zugriffsrechte und Verantwortlichkeiten zu etablieren. Ein präzises Rollen- und Berechtigungskonzept regelt, wer welche Daten einsehen, bearbeiten oder freigeben darf. Jede Änderung lässt sich nachvollziehen, jeder Bearbeitungsschritt dokumentieren. So entsteht Transparenz über den gesamten Lebenszyklus eines Dokuments, auch in Zusammenarbeit mit Partnern wie Lieferanten und Kunden entlang der gesamten Supply-Chain.

Versionierung und Wiederherstellung älterer Stände ermöglichen, Entwicklungen exakt nachzuvollziehen. Damit behalten Organisationen die Kontrolle über ihre Informationshistorie und können Compliance-Anforderungen effizient erfüllen.

Künstliche Intelligenz mit Verantwortung nutzen
Künstliche Intelligenz verändert das industrielle Datenmanagement grundlegend. Richtig integriert, steigert sie Effizienz und Qualität – etwa durch automatisierte

„ Digitale Souveränität wird zu einer **Frage der Selbstbestimmung**: Wer eigene Handlungsspielräume sichern will, entscheidet sich bewusst für europäische IT-Infrastrukturen und Rechtsrahmen. *Andreas Dangl*

Klassifizierung technischer Unterlagen, intelligente Suchfunktionen oder Unterstützung bei mehrsprachiger Kommunikation.

Large Language Models (LLMs) wie ChatGPT oder Claude zeigen eindrucksvoll, wie leistungsfähig generative KI heute ist. Trainiert mit riesigen Mengen an Text-, Code- und Bilddaten, können diese Systeme Inhalte analysieren, zusammenfassen oder neu formulieren.

So hilfreich diese Modelle für Forschung, Kommunikation oder Prototyping sein mögen, so groß bleiben die Unsicherheiten im Hinblick auf Datensouveränität. Nutzer können in der Regel nicht nachvollziehen, wo und wie ysteme ihre eingegebenen Informationen verarbeiten oder speichern. In vielen Fällen verlassen die Daten den europäischen Rechtsraum und unterliegen damit nicht mehr der Kontrolle der EU-Datenschutzgrundverordnung. Für Unternehmen, die mit vertraulichen oder geschäftsrelevanten Informationen arbeiten, entsteht dadurch ein erhebliches Risiko. Der bewusste Einsatz von KI in geschützten, europäischen Umgebungen wird zu einer Grundvoraussetzung für Rechtssicherheit.

Mandantenreine Modelle hingegen arbeiten innerhalb abgeschotteter Umgebungen ohne Verbindung zum Internet, lernen ausschließlich aus den Daten der jeweiligen Organisation und geben keine Informationen nach außen. Auf diese Weise kombiniert KI Geschwindigkeit mit Sicherheit und stärkt die Wettbewerbsfähigkeit, ohne das Unternehmenswissen zu gefährden.

Europäische Cloud als Fundament der Souveränität

Digitale Selbstbestimmung basiert auf Infrastruktur, die europäischen Werten, Gesetzen und Datenschutzprinzipien folgt. Vollständig in Europa betriebene, Cloud-native Plattformen schaffen genau diese Grundlage. Sie unterliegen dem europäischen Rechtsrahmen und sind damit verpflichtet, dass Datenhaltung, Entwicklung und Betrieb transparent, überprüfbar und sicher erfolgen. Unternehmen profitieren nicht nur von der rechtlichen Klarheit, sondern auch von der technischen Flexibilität moderner Cloud-Architekturen. Die Möglichkeit, den Datenstandort gezielt zu wählen, stärkt zusätzlich das Vertrauen in die eigene digitale Infrastruktur und verhindert Abhängigkeiten von außereuropäischen Anbietern.

Zertifizierte Sicherheit schafft Vertrauen

Souveränität braucht überprüfbare Sicherheit. Europäische Cloud-Anbieter setzen auf international anerkannte Standards, um Datenschutz und Informationssicherheit messbar zu machen. Zertifizierungen nach BSI C5, ISO 27001/27018, ISAE 3000 SOC2 und dem EU Cloud Code of Conduct (Level 3) belegen die Einhaltung strengster Vorgaben.

Regelmäßige Audits schaffen Transparenz und Nachvollziehbarkeit. Unternehmen wissen damit genau, unter welchen Bedingungen sie ihre Daten verarbeiten– ein wesentlicher Aspekt, um Vertrauen innerhalb globaler Lieferketten zu festigen.

Sicherheit, Kontrolle und Innovation vereinen

Datensicherheit und digitale Souveränität sind weit mehr als technische Schutzmechanismen. Sie stehen für Eigenständigkeit, Innovationskraft und die Fähigkeit, Verantwortung für das eigene Wissen zu übernehmen. Eine gemeinsame Datenumgebung in einer europäischen Cloud verbindet maximale Datensicherheit mit praxisorientierter Unterstützung für Dokumentations- und Qualitätsprozesse.

Europas Industrie kann ihre digitale Zukunft nur dann gestalten, wenn sie Technologien nutzt, die Kontrolle und Fortschritt in Einklang bringen. Eine souveräne Datenstrategie schafft Resilienz gegenüber äußeren Einflüssen und sichert den langfristigen Erfolg. Wer Datenhoheit, Compliance und Effizienz miteinander verbindet, legt den Grundstein für eine starke, selbstbestimmte und zukunftsfähige Industrie in Europa. •

Exit aus den US Wolken:

Wie Unternehmen Kontrolle, Kosten und Compliance vereinen

Bernd Korz*, CEO von Alugha erklärt, wie der Umstieg auf europäische Clouds und OpenSourceStacks gelingt: Von Hosting und Streaming bis KI – mit nachprüfbaren Datenflüssen, ISOZertifikaten und Geoblocking. Ein Praxisfahrplan, der Kosten senkt, Risiken minimiert und Unternehmen die Hoheit über Inhalte zurückgibt. /// von Heiner Sieger

Bernd, Du gilst als Verfechter europäischer digitaler Souveränität. Was gehört für Dich konkret dazu?
Bernd Korz | Souveränität heißt: Datenhoheit, Transparenz und Unabhängigkeit von US-Hyperscalern, die dem CLOUD Act unterliegen. Wer „100 % DSGVO-konform" wirbt und gleichzeitig YouTube, Google Tag Manager oder Analytics einbindet, gibt Kontrolle ab. Auch scheinbares EU-Hosting bei US-Konzernen ändert daran wenig. Untersuchungen zu Microsoft 365 im Bildungsbereich zeigen Datenflüsse in die USA. Wenn Konzerne KI-Dienste via OpenAI auf Azure betreiben, wandert Trainingsmaterial außer Landes – mit unklaren Konsequenzen für IP-Schutz, Compliance und Nachvollziehbarkeit.

Wie setzt Ihr dieses Prinzip im Alltag um – von Kollaboration bis KI?
BK | Wir arbeiten konsequent europäisch: Hetzner, OVHcloud und Exoscale für Hosting, Storage und Compute. Für KI nutzen wir Mistral (Frankreich) – direkt oder selfhosted –, erzeugen Transkriptionen, Übersetzungen und Metadaten und verfeinern Modelle mit eigenen Datensätzen. Kollaboration läuft über OpenTalk (selfhosted) und Element/Matrix; Dokumente liegen in Nextcloud, Office-Funktionen kommen via LibreOffice. Das größte Hindernis ist Bequemlichkeit: Wer in Schule und Studium nur Microsoft-Tools lernt, wechselt später selten. Das ist ein kulturelles, kein technisches Problem.

Kannst Du Eure technische Architektur skizzieren – vom Upload bis zum Stream?
BK | Der Videoupload landet zunächst bei Hetzner in der EU. Für kosteneffizientes Encoding verteilen wir Workloads auf europäische Standorte (u. a. Finnland) und verarbeiten bei OVHcloud und Exoscale. Encoding-Kapazitäten mieten wir im Minutentakt zu, legen fertige Assets in Object Storage ab und liefern über Bunny CDN (Tschechien) aus – optional als Open-Source-Variante. Unsere Kundschaft entscheidet selbst: EU-only, Geoblocking oder Auslieferung in den USA für geringere Latenz. Für Sprachverarbeitung setzen wir auf Mistral und eigene Pipelines.

Man hört am Markt oft: Europäische Alternativen kosten mehr und können weniger. Was entgegnest Du?
BK | Die Wirklichkeit sieht anders aus. CDN, Storage und Compute sind bei europäischen Anbietern häufig deutlich günstiger als S3 & Co. Mistral kostet pro Million Tokens weniger als ChatGPT und ist für 90 Prozent der Anwendungsfälle stark genug. Für Speech-to-Text betreiben wir ein auf Whisper basierendes, eigens trainiertes Modell: Was bei Azure schnell dreistellige Eurobeträge pro Monat kostet, liegt selfhosted ungefähr bei einem Zehntel – mit voller Datenkontrolle. Auch für Bilder und Video gibt es produktionsreife Open-Source-Stacks.

> „ Wir entscheiden technisch und strategisch ohne Fremdvorgaben. Das erlaubt uns, langfristig auf europäische Infrastruktur zu setzen, **Features nach Kundennutzen statt nach Investorenlogik** zu priorisieren und sensible Services – wie KIPipelines – selbst zu betreiben.
>
> *Bernd Korz*

Wo steht Ihr beim Thema Skalierung – ohne Hyperscaler?
BK | Wir stoßen nicht an Grenzen. Hetzner, OVHcloud und Exoscale sind leistungsfähig und preislich attraktiv. In starken Monaten streamen wir 100 bis 150 Millionen Videominuten – stabil, weltweit. Große Workloads funktionieren auf europäischer Infrastruktur, wenn die Architektur

DER GESPRÄCHSPARTNER
Bernd Korz
ist CEO und CoFounder der Alugha GmbH, einer mehrsprachigen Videoplattform für Hosting, Encoding und Streaming mit KIFunktionen für Transkription, Übersetzung und Metadaten. Korz engagiert sich in der Bundesfachkommission KI des Wirtschaftsrats und setzt sich öffentlich für europäische digitale Souveränität ein. Seine Expertise in KI und Mehrsprachigkeit macht ihn zu einem gefragten Diskussions- und Interviewpartner in den Medien.

stimmt: Multi-Provider-Setup, offene Standards, Automatisierung, observability-getriebene Skalierung und klare Exit-Strategien. So vermeiden wir Lockin und behalten die Kosten im Griff.

Wie adressiert Ihr Datenschutz, Security by Design und Compliance?
BK | Mit allen Infrastrukturpartnern bestehen Auftragsverarbeitungsverträge; die Anbieter sind ISOzertifiziert. Wir minimieren personenbezogene Daten, speichern keine Zahlungsinformationen und trennen kritische Systeme strikt. Payments laufen derzeit über Paddle (UK), wir wechseln aber in Kürze zu einem Anbieter aus Heidelberg, um vollständig in der EU zu bleiben. Kundinnen und Kunden erhalten vollständige AV-Verträge. Standard sind transparente Datenflüsse, Zugriffsmanagement nach Least-Privilege und Verarbeitung in europäischen Rechenzentren.

Welche Rolle kann Alugha in Bildung, Verwaltung und regulierten Branchen spielen?
BK | Mit Alucation bieten wir tausende frei zugängliche, gemeinfreie Bildungsvideos – wirklich kostenlos und ohne Werbetracking. Problematisch ist, wenn Behörden YouTube zur Norm machen. So zwingen wir Bürgerinnen und Bürger faktisch in ein US-Ökosystem – inklusive Datenerhebung und möglicher Trainingsnutzung. Viele Unternehmen trennen deshalb bereits bewusst: Öffentlichkeitsarbeit kann auf YouTube bleiben, doch interne Schulungen, Wissensbestände und sensible Inhalte hosten sie bei Alugha – aus Compliance, IP und Reputationsschutzgründen.

Ihr seid seit zwölf Jahren am Markt und vollständig eigenfinanziert. Welche Vorteile hat diese Unabhängigkeit?
BK | Wir entscheiden technisch und strategisch ohne Fremdvorgaben. Das erlaubt uns, langfristig auf europäische Infrastruktur zu setzen, Features nach Kundennutzen statt nach Investorenlogik zu priorisieren und sensible Services – wie KI-Pipelines – selbst zu betreiben. Unabhängigkeit erhöht Glaubwürdigkeit: Wir kritisieren Big-Tech-Abhängigkeiten nicht nur, wir zeigen täglich, dass es anders geht – mit Kunden wie Rheinmetall, Meet Your Master, Oliver Kahn und internationalen Hochschulen.

Was müssen Organisationen tun, die „raus aus dem Lockin" wollen – Dein Fahrplan in fünf Schritten?
BK | Erstens: Datenflüsse und Hyperscaler-Abhängigkeiten erfassen. Zweitens: europäische Alternativen mappen (Hosting, Kollaboration, Video, KI). Drittens: AV-Verträge, ISO-Nachweise, Exit-Strategien prüfen. Viertens: Pilotmigrationen (z. B. Nextcloud, Matrix, Mistral) mit klaren KPIs aufsetzen. Fünftens: Teams schulen, Governance und Prozesse anpassen, dann skalieren. Wichtig ist ein iteratives Vorgehen mit Quick Wins – so entsteht Souveränität Schritt für Schritt.

Welche politischen und kulturellen Weichenstellungen sind aus Deiner Sicht für mehr digitale Souveränität in Europa nötig?
BK | Für mich gilt: Mindset first. Nicht auf „den Staat" warten, sondern selbst europäische Alternativen nutzen. Frankreich macht vor, was Investitionen, Technologie-Stolz und Beschaffung angeht. Gleichzeitig sollten Regierungen und öffentliche Einrichtungen mit gutem Beispiel vorangehen: Kollaboration, Dokumentenmanagement, Video-Hosting und KI europäisch aufsetzen. Das schafft Orientierung, reduziert Risiko und stärkt ein Ökosystem, das wettbewerbsfähig ist.

Braucht es eine Allianz für digitale Unabhängigkeit – und wie könnte sie wirken?
BK | Ja. Anbieter, Vordenker und Anwender sollten sich zu einer sichtbaren, handlungsorientierten Koalition verbinden. Aufgaben: Best Practices bündeln, Referenzarchitekturen publizieren, kuratierte Tool-Stacks bereitstellen, Migrationsteams für den Mittelstand aufbauen und Schulungen fördern. Der Bedarf ist groß, die Lösungen existieren – oft fehlt nur Sichtbarkeit und Anleitung.

Zum Schluss: Was sagst Du denen, die meinen „Es gibt doch YouTube – wozu Alugha?"
BK | Es geht nicht um „YouTube oder nichts", sondern um Wahlfreiheit, Datenschutz, IP-Schutz und Unabhängigkeit. Wer Markenwerte, interne Inhalte und Compliance ernst nimmt, braucht eine europäische Alternative. Wir zeigen täglich: Hochwertige Video-Workflows funktionieren souverän, sicher und kosteneffizient – ohne Big-Tech-Abhängigkeit. •

Digitale Souveränität und Cloud-Innovation:

Kein Widerspruch, sondern eine Frage der Strategie

Wie können europäische Unternehmen die Innovationskraft globaler Cloud-Plattformen nutzen und gleichzeitig die volle Kontrolle über ihre Daten behalten? Souveränität ist kein Alles-oder-Nichts-Prinzip. Von Datenlokalisierung bis hin zu komplett isolierten Umgebungen – die richtigen strategischen Entscheidungen muss jedes Unternehmen für sich treffen. /// von Marianne Janik

DIGITALE SOUVERÄNITÄT IST KEIN NEUES KONZEPT; aktuell gewinnt es jedoch deutlich an Momentum. Zurecht ist dies ein zentrales Thema, mit dem sich Unternehmen und öffentliche Einrichtungen beschäftigen. Cloud-Anbieter, die ihre Verantwortung ernst nehmen, beschäftigen sich seit vielen Jahren mit den Kernanforderungen: Sicherheit, Vertrauen und Kontrolle. Entscheidend ist, die individuellen Bedürfnisse der Kunden zu verstehen und Flexibilität durch Wahlmöglichkeiten zu bieten. Letzteres ist von immenser Bedeutung, denn Souveränität in der Cloud ist keine Einheitslösung. Sie ist ein Spektrum, das von regulatorischen Minimalanforderungen bis hin zu sogenannten Air-Gapped Lösungen reicht, die auch ohne Verbindung zum Internet oder zu Cloud-Anbietern eingesetzt werden können.

Der Spagat als strategische Notwendigkeit

Die aktuelle Debatte stellt Unternehmen vor einen strategischen Spagat. Einerseits wollen sie – und müssen sie, um global wettbewerbsfähig zu bleiben – an der Spitze der technologischen Innovation teilhaben, sei es bei KI, Datenanalyse oder globaler Skalierbarkeit. Gleichzeitig wachsen Anforderungen an Datenschutz, Compliance und Kontrolle über kritische Datenbestände. Dieser Spagat ist real, und er betrifft nicht nur die Anbieter von Hyperscale-Clouds, sondern in gleichem Maße die Kunden selbst. Jedes Unternehmen muss für sich definieren, welches Maß an Digitaler Souveränität es benötigt, und diese Anforderung gegen Kosten, Innovationsgeschwindigkeit und Funktionalität abwägen. Die Annahme, es gäbe eine einzige „reine" Lehre der Digitalen Souveränität, ignoriert die Realität der global vernetzten Wirtschaft.

Wahlfreiheit statt Dogma: Ein Portfolio für Digitale Souveränität

Um diesen Spagat zu meistern, braucht es technologische Wahlfreiheit statt Dogmatismus. Ein starrer „One-size-fits-all"-Ansatz wird den unterschiedlichen Risikoprofilen und regulatorischen Erfordernissen von Unternehmen nicht gerecht. Wir setzen daher auf ein Portfolio an Lösungen, das Kunden eine granulare Steuerung ermöglicht. Konkret adressieren wir Digitale Souveränität technisch über ein Portfolio von drei Optionen.

> „ Die Annahme, es gäbe eine einzige „reine" Lehre der Digitalen Souveränität, ignoriert die **Realität der global vernetzten Wirtschaft**. *M. Janik*

Die erste Option, unsere „Google Cloud Data Boundary", bietet umfassende Datenlokalisierung – gepaart mit starker Verschlüsselung und Hoheit der Kunden über die kryptografischen Schlüssel. Für viele Unternehmen ist dies die ideale Balance aus Datensouveränität sowie Agilität, Elastizität, Skalierbarkeit und Innovationskraft der Public-Cloud. Die zweite Option, „Google Cloud Dedicated", geht einen Schritt weiter und wird auf einer dedizierten Infrastruktur mit eigenen, unabhängigen Abläufen bereitgestellt, die von einem lokalen Partner betrieben wird, wie etwa mit S3NS in Frankreich. Für Unternehmen mit höchsten Anforderungen, etwa im öffentlichen Sektor oder der kritischen Infrastruktur, gibt es die dritte Option: die „Google Cloud Air-Gapped". Diese Lösung benötigt keine Verbindung zu Google Cloud oder dem öffentlichen Internet und wird im Rechenzentrum des Kunden oder eines Partners betrieben. Kunden, die diesen Weg wählen, erhalten maximale Kontrolle. Dies geht naturgemäß einher mit einem geringeren Serviceumfang, geringerer Innovationsgeschwindigkeit und niedrigerer Skalierbarkeit im Vergleich zur Public Cloud. Auch kostenseitig unterscheiden sich die drei Optionen entsprechend. Diese Abwägungen – Kontrolle, versus Funktionsumfang, versus Kosten – muss jedes Unternehmen für sich treffen.

Vertrauen durch Technik, Transparenz und Regulierung

Eine der größten Sorgen von Kunden ist der potenzielle, ungewollte Zugriff auf ihre Daten durch Dritte, etwa ausländische Behörden – ein Anliegen, das oft im Kontext von Regularien wie

dem US CLOUD Act oder dem Digital Services Act (DSA) zur Sprache kommt. Unsere Antwort darauf ist primär technisch und vertraglich geregelt:

Als globales Unternehmen umfasst unser Ansatz zum einen vertragliche Regelungen, die unsere Kunden schützen, zum anderen aber vor allem technische Lösungen. Im Falle einer behördlichen Anfrage wird diese streng geprüft; und es ist unsere Policy, die Anfrage an den betreffenden Kunden weiterzuleiten. Viel wichtiger sind für uns die technischen Lösungen. In allen drei unserer Sovereign-Cloud-Ansätze gibt es unterschiedliche technische Lösungen. Zum Beispiel: Im Falle einer isolierten Umgebung, wie etwa bei der Google Cloud Dedicated, in der die kryptographischen Schlüssel, die Identitäten, die Netzwerkadressen und auch die Domainnamen in dieser Umgebung von einem Partner verwaltet werden, ist es objektiv und technisch unmöglich, dass Google unbefugten Zugang zu den Daten erhält.

Zusätzlich schaffen wir Transparenz durch die Zusammenarbeit mit lokalen Partnern und Behörden wie dem BSI. Eine Herausforderung bleibt jedoch. In Deutschland fehlt, anders als etwa in Frankreich, ein einheitlicher, staatlich definierter Anforderungskatalog für souveräne Clouds. Ohne diese klaren regulatorischen Rahmenbedingungen bleibt Unternehmen oft nur die individuelle Abwägung von Kosten, Funktionalität und Risiko. Als Cloud-Anbieter wird es unsere Kernaufgabe bleiben, ein Umfeld des Vertrauens zu schaffen. Die enge Zusammenarbeit mit Kunden, Partnern und politischen Entscheidungsträgern ist essentiell, um Technologien bereitzustellen, die den jeweiligen Anforderungen Europas entsprechen. Technische Durchsetzung von Souveränität, ergänzt um transparente Zertifizierungen, schafft Vertrauen und wird die Adoption sicherer Cloud-Lösungen beschleunigen – als wichtiger Wegbereiter für die Zukunftsfähigkeit im globalen Wettbewerb, speziell im Zeitalter der künstlichen Intelligenz. •

DIE AUTORIN
Marianne Janik
ist VP EMEA North bei Google Cloud.

Nachhaltige Rechenzentren als Schlüssel zu digitaler Souveränität

Warum Betreiber, Unternehmen und Investoren jetzt in resiliente und klimafreundliche Infrastruktur investieren müssen. /// von Ralf Siefen, CEO und Sonja Philipp

DIE DIGITALE TRANSFORMATION TREIBT WIRTSCHAFT UND GESELLSCHAFT IN EIN NEUES ZEITALTER und verschärft zugleich ein altes Dilemma: Künstliche Intelligenz und datengetriebene Geschäftsmodelle erzeugen einen immensen Bedarf an Rechenleistung, während geopolitische Spannungen den Ruf nach regionaler Unabhängigkeit und Klimaziele nach effizienteren Lösungen lauter werden lassen.

Die Bitkom-Studie „Rechenzentren in Deutschland 2024“ verdeutlicht, wie groß der Handlungsdruck ist: Innerhalb einer Dekade hat sich die IT-Anschlussleistung deutscher Rechenzentren auf rund 2,7 Gigawatt verdoppelt. Der Stromverbrauch stieg auf etwa 20 Milliarden Kilowattstunden und könnte bis 2030 auf über 30 Milliarden anwachsen. Gleichzeitig hinkt Deutschland im internationalen Vergleich hinterher: Die USA verfügen bereits über fast 48 Gigawatt Kapazität, China über rund 38 Gigawatt.

Für Unternehmen und Betreiber bedeutet das: Wer die wachsenden Datenmengen der KI-Ära zuverlässig verarbeiten will, darf sich nicht allein auf Hyperscaler aus den USA oder China verlassen. Abhängigkeiten von ausländischen Cloud-Giganten bergen Risiken: Von Preisgestaltung und Lieferketten über Datenschutz bis hin zu Cyberangriffen oder politisch motivierten Zugriffsbeschränkungen. Digitale Souveränität und wirtschaftliche Resilienz werden damit zu Standortfaktoren.

Das Spannungsfeld aus Wachstum, Sicherheit und Nachhaltigkeit

Die Herausforderungen sind mehrdimensional. Auf der einen Seite steht der ungebremste Datenhunger moderner Anwendungen: Echtzeit-Analysen, KI-gestützte Produktionsprozesse und neue Geschäftsmodelle erhöhen den Druck auf bestehende IT-Infrastrukturen. Auf der anderen Seite steigen die gesetzlichen Anforderungen an Energieeffizienz und Klimaschutz. Das Energieeffizienzgesetz (EnEfG) schreibt konkrete Einsparziele vor, während Kommunen, Investoren und nicht zuletzt die Endkunden zunehmend auf ESG-Kriterien achten.

Gleichzeitig wächst die Bedrohungslage: Cyberangriffe, Sabotage und Stromausfälle sind längst keine theoretischen Szenarien mehr. Kritische Infrastrukturen müssen gegen physische und digitale Angriffe gewappnet sein, während die Verfügbarkeit rund um die Uhr garantiert werden muss. Es reicht nicht mehr, Rechenzentren einfach nur leistungsstark zu bauen – sie müssen zugleich effizient, resilient und unabhängig sein. Nur so kann Deutschland im internationalen Vergleich nicht nur mithalten, sondern eine führende Rolle übernehmen.

Nachhaltigkeit beginnt beim Fundament

Wer diese Ziele erreichen will, muss Rechenzentren von Grund auf anders denken. Nachhaltigkeit ist kein nachträglicher Bonus, sondern Planungsprinzip. Schon bei der Standortwahl lässt sich festlegen, wie sich Energiequellen nutzen, Abwärme einspeisen und zukünftige Erweiterungen umsetzen lassen.

Nachhaltiges Design, recycelbare Baustoffe und modulare Bauweisen reduzieren den Energiebedarf beim Bau und auch später im Betrieb sind entsprechende Einsparungen möglich. Intelligente Kühlung – etwa durch Freikühlung oder Flüssigkühlung – senkt den Stromverbrauch erheblich. Ein intelligentes Energiemanagement identifiziert Schwachstellen und spart Kosten.

Besonders großes Potenzial bietet die Abwärmenutzung: Die von Servern erzeugte Wärme kann in Nah- und Fernwärmenetze eingespeist werden und so ganze Quartiere oder andere nahegelegene Abnehmer versorgen. Solche Modelle sind ökologisch wie ökonomisch attraktiv und stärken zugleich die regionale Infrastruktur.

Verfügbarkeit und Zertifizierung als Vertrauensanker

Neben Effizienz zählt vor allem Verlässlichkeit. Kritische Datenverarbeitung erfordert maximale Ausfallsicherheit. Zertifizierungen nach EN 50600 oder Uptime, ergänzt durch Nachhaltigkeitslabels wie DGNB, LEED oder Blauer Engel, dokumentieren die Qualität eines Rechenzentrums und sind für viele Auftraggeber und Endkunden mittlerweile Voraussetzung.

Unsere Kunden erwarten Lösungen, die messbare ökologische Effekte nachweisen und nicht nur gut klingen.Transparenz und konkrete Kennzahlen sind für Investoren und Betreiber entscheidend, um Vertrauen zu schaffen.

Investition in die eigene Handlungsfähigkeit

Für Unternehmen und öffentliche Einrichtungen geht es nicht allein um Klimaschutz, sondern um die Fähigkeit,

ihre digitale Zukunft selbst zu gestalten. Wer eigene, effiziente und sichere Rechenzentren betreibt oder in solche Projekte investiert, reduziert Abhängigkeiten von globalen Hyperscalern, behält die Kontrolle über sensible Daten und sichert sich gegen geopolitische Risiken ab.

Gleichzeitig sind die ökonomischen Argumente klar: Niedrigere Betriebskosten, planbare Energiekosten und ein nachweisbar kleinerer CO2-Fußabdruck verschaffen Wettbewerbsvorteile. Investoren und Kunden bewerten nachhaltige Infrastruktur zunehmend als wertstabil und zukunftssicher.

Zukunft braucht Partner

Die Umsetzung solcher Projekte erfordert Erfahrung und ganzheitliche Konzepte – von der Bedarfsanalyse über die Planung und Bau bis zum Betrieb. Dienstleister wie die Data Center Group begleiten diesen Prozess mit individuell zugeschnittenen Lösungen: Von der bedarfsgerechten, intelligenten Planung über die Auswahl nachhaltiger Baustoffe, energieeffizienter Kühl- und Abwärmenutzungs-Konzepte bis hin zur Vorbereitung auf Zertifizierungen. Ziel ist es, höchste Verfügbarkeit mit minimalem ökologischen Fußabdruck zu verbinden und gleichzeitig die digitale Souveränität der Kunden zu stärken.

Deutschland steht an einem Wendepunkt. Die Nachfrage nach Rechenleistung wird weiter steigen, KI-Trends beschleunigen diese Entwicklung. Wer jetzt handelt, kann digitale Unabhängigkeit, Klimaschutz und wirtschaftliche Resilienz in Einklang bringen. Unternehmen, die ihre Rechenzentren modernisieren oder neu aufbauen, sollten daher frühzeitig den Dialog mit erfahrenen Partnern suchen, um ihre Datenhoheit zu sichern, regulatorische Vorgaben zu erfüllen und die Chancen der digitalen Transformation langfristig zu nutzen. •

DIE AUTOREN

Ralf Siefen

ist CEO und Vorsitzender der Geschäftsführung der Data Center Group.

Sonja Philipp

ist Head of Marketing & Communications der Data Center Group.

„ Abhängigkeiten von ausländischen Cloud-Giganten bergen **Risiken**: Von Preisgestaltung und Lieferketten über Datenschutz bis hin zu Cyberangriffen oder politisch motivierten Zugriffsbeschränkungen. Digitale Souveränität und wirtschaftliche Resilienz werden damit zu **Standortfaktoren**.

Ralf Siefen und Sonja Philipp

Gaia-X:

Der europäische Ansatz für digitale Souveränität

Wie werden Deutschland und Europa unabhängiger von Dienstleistern etwa aus den USA? Ulrich Ahle, CEO von Gaia-X, erklärt im Interview, wie Datensouveränität in Europa gelingt und welche Rolle Gaia-X spielt. /// von Konstantin Pfliegl

DIGITALE SOUVERÄNITÄT IST AKTUELL IN EUROPA EINES DER WICHTIGEN POLITISCHEN SCHLAGWÖRTER. Lieferketten-Schocks, geopolitische Spannungen und die rasante Einführung von künstlicher Intelligenz haben gezeigt: Kontrolle über Daten, Infrastruktur und Compliance ist heute so entscheidend wie Energie oder Logistik. Genau hier setzt Gaia-X an: keine „europäische Cloud", sondern ein offenes, föderiertes Ökosystem, in dem jede Cloud und jeder Datendienst nach europäischen Regeln betrieben werden kann – mit Kontrolle, Datenhoheit und Compliance in europäischer Hand.

Im Interview mit DIGITAL BUSINESS erklärt Gaia-X-CEO Ulrich Ahle, wie Europa globale Technologien selbstbewusst nutzt – und zugleich die Spielregeln definiert.

Herr Ahle, in den vergangenen Monaten hat die Bedeutung von digitaler Souveränität enorm zugenommen. Teilen Sie diesen Eindruck? Und wie kam es dazu, dass wir plötzlich alle darüber sprechen?
Ulrich Ahle | Ja. Was sich verändert hat, ist, dass digitale Fähigkeiten heute Wettbewerbsfähigkeit und Resilienz ebenso bestimmen wie Energie oder Logistik. Lieferketten-Schocks, geopolitische Spannungen und die rasante Einführung von KI haben die Kontrolle über Daten, Infrastruktur und Compliance zu nicht verhandelbaren Themen auf Vorstandsebene gemacht. Europa hat erkannt, dass Offenheit ohne überprüfbares Vertrauen zu Abhängigkeit führt. Deshalb müssen wir Offenheit mit durchsetzbaren Regeln für Transparenz, Portabilität und Interoperabilität verbinden. Wir setzen uns seit Beginn für diese Prinzipien ein, und es ist gut zu sehen, dass sie inzwischen auf allen Agenden stehen.

Digitale Souveränität ist von einem politischen Schlagwort zu einem strategischen Imperativ für Europa geworden. Der Zugang zu Daten, Rechenleistung und KI-Fähigkeiten definiert heute nicht nur Wettbewerbsfähigkeit, sondern auch Resilienz und demokratische Stabilität. Die Diskussion hat sich intensiviert, weil Unternehmen und Regierungen gleichermaßen verstehen, dass Autonomie im digitalen Raum ebenso essenziell ist wie Energie- oder Verteidigungssouveränität.

Digitale Souveränität bedeutet keine Abschottung. Sie bedeutet, Partner, Technologien und Dienste frei wählen zu können – auf der Grundlage von überprüfbarem Vertrauen, Transparenz und Interoperabilität. Genau diese Vision setzt Gaia-X in die Praxis um.

Ist es angesichts der Dominanz außereuropäischer Anbieter denn überhaupt möglich, digitale Souveränität in Europa zu erreichen?
UA | Ich sehe das nicht als Frage des „Aufholens", sondern als Frage der Neugestaltung des Spielfelds. Hyperscaler haben beeindruckende Infrastrukturen aufgebaut, doch ihre Dominanz beruht auf Integration – nicht allein auf Technologie. Sie sind nur dann unersetzlich, wenn man geschlossene, nicht-portable Architekturen akzeptiert.

Europas Stärke liegt in der industriellen und öffentlichen Datennutzung im großen Maßstab – von der Fertigung über das Gesundheitswesen bis zur Energie. Indem wir Identitäten, Richtlinien und Schnittstellen über Anbieter und Edge-Systeme hinweg standardisieren, machen wir den Markt wieder wettbewerbsfähig. Dieser Wettbewerb verbessert Preise, Innovation und Compliance für europäische Nutzer und schafft Raum für neue europäische Angebote.

Und wie kann das gelingen?
UA | Das kann nur durch föderierte, offene Ökosysteme gelingen, die große und kleine Anbieter über gemeinsame Standards und Vertrauensmechanismen verbinden. Genau das ermöglicht Gaia-X.

Unser Ansatz macht den Markt wieder anfechtbar. Er erlaubt KMU, Forschungseinrichtungen und öffentlichen Institutionen, auf Augenhöhe teilzunehmen. Zugleich stellt er sicher, dass kritische Daten – etwa aus den Bereichen Gesundheit, Mobilität oder Industrie – unter europäischer Governance bleiben.

Hyperscaler sind wichtige Akteure, aber sie müssen innerhalb eines von Europa definierten Rahmens aus Transparenz und Vertrauen agieren. Dieses Gleichgewicht aus Offenheit und Kontrolle macht unser Modell nachhaltig.

DER GESPRÄCHSPARTNER
Ulrich Ahle ist CEO von Gaia-X.
Bild: Gaia-X

MEHR ERFAHREN
Lesen Sie das ausführliche Interview mit **Ulrich Ahle** auf der Webseite von **DIGITAL BUSINESS**.

Welche Rolle spielt hier Ihrer Meinung nach der Gesetzgeber? Wie kommen Deutschland beziehungsweise die EU zu mehr digitaler Unabhängigkeit? Braucht es strengere Regulierungen und Vorschriften?
UA | Regulierung gibt die Richtung vor, aber Technologie macht sie umsetzbar. Europa hat mit dem EU Data Act, dem Data Governance Act, NIS-2 und dem AI Act bereits eine starke politische Basis geschaffen. Diese Regelwerke bilden einen Rahmen, der Rechte und Wettbewerb schützt. Der nächste Schritt besteht darin, diese Prinzipien automatisch überprüfbar zu machen – nicht durch Papierarbeit, sondern durch maschinenlesbare Regeln und Compliance-Mechanismen.

Gaia-X liefert genau das über unser Trust Framework. Unser Trust Framework übersetzt europäische Vorschriften in technische Realität: Daten-Nutzungsrichtlinien, Zugriffsbedingungen und Compliance-Anforderungen werden direkt in die Systeme eingebaut. Europa braucht also nicht mehr Regulierung, sondern deren technische Umsetzung und Interoperabilität – damit jede Vorschrift in der Praxis überprüfbar wird. Gaia-X hilft, rechtliche Souveränität in technologische Autonomie zu überführen.

Viele Hyperscaler bieten mittlerweile Cloud-Dienste ausschließlich aus Europa an, etwa Microsofts Sovereign Cloud. Wie sehen Sie diese Dienste? Ist das Souveränität Light oder eine echte Alternative für europäische Unternehmen?
UA | Sie können ein wichtiger Teil des Ökosystems sein – aber nur, wenn ihre Versprechen überprüfbar sind. Souveränität darf kein Marketingbegriff sein, sie muss durch transparente Kriterien nachgewiesen werden. Unser Compliance Framework und die Gaia-X-Labels legen klare, messbare Anforderungen fest – etwa zur Datenlokation, zur rechtlichen Kontrolle, zur Portabilität und Interoperabilität. Diese lassen sich über Gaia-X verifizieren. Allein die höchste Sicherheitsstufe, das „Gaia-X Label Level 3", kann ausschließlich durch Anbieter erbracht werden, die ihren Hauptsitz in Europa haben und nicht durch außereuropäische Unternehmen bestimmt werden. Hierdurch kann sichergestellt werden, dass die Daten keinen extraterritorialen Regelungen unterliegen.

Gaia-X bewertet keine Marken, sondern überprüft Eigenschaften. Wenn ein Cloud-Dienst – egal ob europäisch oder global – diese Kriterien erfüllt, seine Compliance über ein Gaia-X Digital Clearing House nachweist und portabel bleibt, dann ist er tatsächlich souverän und eine valide Option. Wenn nicht, bleibt es Marketing.

Wie muss man sich das in der Praxis vorstellen: Als europäisches Unternehmen bin ich auf der Suche etwa nach einem KI-Cloud-Dienst – und Gaia-X hilft mir dabei, einen entsprechenden Anbieter aus Europa zu finden, bei dem ich mir sicher sein kann, dass meine digitale Souveränität gewahrt bleibt?
UA | Genau. Über das Gaia-X-Ökosystem können Sie Anbieter finden, die Gaia-X-konform sind – also europäischen Standards für Datenschutz, Transparenz und Interoperabilität entsprechen. Jeder Dienst wird durch überprüfbare digitale Nachweise beschrieben, die angeben, wo Daten gespeichert werden, welches Recht gilt, welche Interoperabilitätsschnittstellen bestehen und wie ein Datenwechsel möglich ist.

Als Unternehmen können Sie diese Nachweise vor der Beschaffung oder während des Betriebs automatisch prüfen. Das reduziert Risiken und Compliance-Kosten erheblich und stellt sicher, dass Ihre KI-Anwendungen unter europäischer Governance bleiben. Das funktioniert bereits in realen Anwendungsfällen, etwa bei KI-Modellen in vertrauenswürdigen Datenräumen für Mobilität oder Gesundheit, in denen mehrere europäische Partner sicher nach Gaia-X-Prinzipien zusammenarbeiten. •

> „ Hyperscaler haben beeindruckende Infrastrukturen aufgebaut, doch **ihre Dominanz beruht auf Integration – nicht allein auf Technologie**.
>
> *Ulrich Ahle*

Schützen die EU-Clouds der Hyperscaler vor US-Behörden?

Europäische Unternehmen machen sich Sorgen um ihre digitale Souveränität. Die US-Hyperscaler begegnen den Bedenken mit eigenen EU-Clouds. Sicherer Schutz für Daten – oder nur Souveränität light? /// von Konstantin Pfliegl

DIGITALE SOUVERÄNITÄT ENTSCHEIDET DARÜBER, OB UNTERNEHMEN IN DEUTSCHLAND UND EUROPA ihre Daten, Anwendungen und Wertschöpfungsketten eigenständig steuern können. Es geht um Kontrolle: über Datenflüsse, Speicherorte, Schlüssel und Betriebsprozesse – im Einklang mit DSGVO, NIS-2 und weiteren europäischen Vorgaben.

Die großen Hyperscaler sind sich des Problems bewusst und bieten ihren europäischen Kunden mit eigenen Cloud-Angeboten aus europäischen Rechenzentren entsprechende Angebote an. Doch lassen sich mit diesen Angeboten wirklich regulatorische Vorgaben wie die DSGVO einhalten? Und welche Rolle spielt der US Cloud Act, der US-Behörden Zugriff auf Daten von US-amerikanischen Unternehmen ermöglicht – auch bei Tochterunternehmen im Ausland?

Im Gespräch mit Mustafa Isik, Chief Technologist Digital Sovereignty bei Amazon Web Services (AWS), wollen wir klären, wie Unternehmen technische Freiheit und regulatorische Sicherheit vereinen können.

Herr Isik, in der deutschen IT-Landschaft spricht aktuell fast jeder von einer digitalen Souveränität – wir müssen uns unabhängig machen von außereuropäischen Diensten. Wie stehen Sie als US-amerikanischer Anbieter dazu?

Mustafa Isik | Für AWS bedeutet Souveränität, unseren Kunden volle Kontrolle und Transparenz über ihre Daten zu geben. Kunden entscheiden, wo ihre Daten gespeichert und verarbeitet werden, wer zugreifen kann und wie sie verschlüsselt werden. Alle AWS-Regionen sind „sovereign-by-design" und „secure-by-design" konzipiert und erfüllen die Anforderungen der meisten Workloads unserer Kunden. Für Kunden aus besonders stark regulierten Branchen und der öffentlichen Verwaltung haben wir im Oktober 2023 die AWS European Sovereign Cloud angekündigt. Sie erhalten damit mehr Auswahl und Flexibilität, um den steigenden Anforderungen an den Ort der Datenverarbeitung und die operative Souveränität in der Europäischen Union besser gerecht zu werden. Der Start der ersten Region der AWS European Sovereign Cloud ist in Brandenburg bis zum Jahresende 2025 geplant.

Sie haben die AWS European Sovereign Cloud angesprochen. Vielleicht können Sie kurz umreißen, wie Sie damit eine digitale Souveränität für Ihre europäischen Kunden schaffen wollen?

MI | Mit der AWS European Sovereign Cloud schaffen wir eine neue, unabhängige Cloud für Europa, die physisch und logisch von bestehenden AWS-Regionen getrennt ist und ausschließlich innerhalb der EU betrieben wird. Sie bietet dabei die gleiche Sicherheit, Verfügbarkeit und Leistung wie bestehende AWS-Regionen.

Die Besonderheiten dieser Cloud manifestieren sich in einer neuen deutschen Unternehmensstruktur mit einer von EU-Bürgern geführten Muttergesellschaft sowie einem unabhängigen Beirat mit vier EU-Bürgern. Hinzu kommen ein eigenes europäisches Security Operations Center und ein dedizierter European Trust Service Provider für autonome Trust Service Operations. Der Betrieb erfolgt zunächst durch in der EU ansässige Mitarbeiter und wird nach einer Übergangsphase vollständig von in der EU ansässigen EU-Bürger übernommen. Zudem haben autorisierte AWS-Mitarbeiter der European Sovereign Cloud Zugriff auf eine Kopie des Quellcodes, um selbst unter extremen Umständen einen unabhängigen Weiterbetrieb gewährleisten zu können.

> „ Wir geben Kundendaten auf keinerlei behördliche Anfragen heraus, **es sei denn, wir sind dazu durch eine rechtlich gültige und verbindliche Anordnung verpflichtet**.
>
> *Mustafa Isik*

Das souveräne Cloud-Angebot hat aber doch keinerlei Auswirkungen auf die Anwendbarkeit des US Cloud Act...

DER GESPRÄCHSPARTNER

Mustafa Isik

ist Chief Technologist Digital Sovereignty bei Amazon Web Services (AWS).

Bild: AWS

MEHR ERFAHREN

Lesen Sie das ausführliche Interview mit **Mustafa Isik** auf der Webseite von **DIGITAL BUSINESS.**

MI | Bei AWS haben Kundendatenschutz und -sicherheit höchste Priorität. Der Cloud Act von 2018 hat der US-Regierung keinerlei neue Befugnisse eingeräumt, Daten von Anbietern anzufordern. Vielmehr schafft er wichtige rechtliche Leitplanken zum Schutz von Inhalten. Das Ziel des Cloud Act ist, bei schweren Straftaten Zugang zu elektronischen Beweismitteln für die Ermittlungen zu erhalten, unabhängig vom Speicherort der Beweise. Dabei gilt der Cloud Act nicht nur für Unternehmen mit Hauptsitz in den USA, sondern für alle Anbieter, die Geschäfte in den Vereinigten Staaten tätigen. Beispielsweise unterliegen Cloud-Anbieter mit Hauptsitz in Europa, die Geschäfte in den USA tätigen, genauso den Anforderungen des Gesetzes.

AWS erkennt die legitimen Bedürfnisse von Strafverfolgungsbehörden bei der Untersuchung krimineller und terroristischer Aktivitäten an, aber diese müssen die rechtlichen Schutzmaßnahmen für solche Ermittlungen beachten. Wir geben Kundendaten auf keinerlei behördliche Anfragen heraus, es sei denn, wir sind dazu durch eine rechtlich gültige und verbindliche Anordnung verpflichtet. Dies haben wir in unseren rechtlichen Bedingungen öffentlich zugesichert. Darüber hinaus werden wir behördliche Anfragen anfechten, die gegen das Gesetz verstoßen, zu weitreichend oder anderweitig unangemessen sind.

Es hat also niemand Zugriff auf die Daten europäischer Kunden?

MI | AWS verfügt über eine Reihe von Produkten und Services, die sicherstellen, dass niemand – nicht einmal Mitarbeiter von AWS – auf Kundeninhalte zugreifen können. AWS-Kunden verfügen auch über eine Reihe zusätzlicher technischer Maßnahmen und operativer Kontrollen, um den Zugriff auf Daten zu verhindern. Beispielsweise sind viele der AWS-Kernsysteme und Services mit Zero-Operator-Zugriff konzipiert, was bedeutet, dass die Services keine technischen Möglichkeiten für AWS-Mitarbeiter bieten, auf Kundendaten als Reaktion auf eine rechtliche Anfrage zuzugreifen.

Ein deutlicher Beleg für die Wirksamkeit unserer Maßnahmen und der strengen gesetzlichen Anforderungen ist die Tatsache, dass AWS seit Beginn der statistischen Erfassung im Jahr 2020 keine außerhalb der USA gespeicherten Kundeninhalte von Unternehmens- oder Regierungskundendaten an die US-Regierung weitergegeben hat.

Aber was macht Amazon Web Services, wenn die US-Behörden mal einen Blick in die AWS European Sovereign Cloud werfen wollen?

MI | Der Zugriff auf Daten durch US-Behörden ist bei weitem nicht uneingeschränkt oder automatisch möglich, und Strafverfolgungsbehörden müssen strenge rechtliche Standards erfüllen. Seit Beginn unserer statistischen Erfassung von Anfragen im Jahr 2020 hat es keine Datenanfrage an AWS gegeben, die zur Offenlegung von außerhalb der USA gespeicherten Kundeninhalten von Unternehmens- oder Regierungsdaten gegenüber der US-Regierung geführt haben.

Wir haben mehrschichtige Schutzmaßnahmen implementiert, um die Daten unserer Kunden zu schützen und prüfen jede behördliche Anfrage auf ihre Rechtmäßigkeit. Hinzu kommen technische Schutzmaßnahmen: Eine Vielzahl unserer Produkte und Services gewährleisten, dass niemand – also nicht einmal AWS Mitarbeiter – Zugriff zu Kundeninhalten haben.

Im Übrigen ist der Cloud Act kein rein amerikanisches Phänomen. Viele Länder verlangen bei schweren Straftaten die Offenlegung von Kundendaten, unabhängig vom Speicherort. So ermöglicht beispielsweise der britische Crime (Overseas Production Orders) Act britischen Strafverfolgungsbehörden auf elektronische Daten zuzugreifen, die außerhalb des Vereinigten Königreichs gespeichert sind. Tatsächlich kommt seit 2023 die Mehrheit der Strafverfolgungsanfragen, die AWS erhält, von Behörden außerhalb der Vereinigten Staaten.

Handelt es sich aber bei diesen Sovereign Clouds dennoch nicht vielmehr um eine Art Souveränität light?

MI | Nein. Die AWS European Sovereign Cloud wird die einzige vollumfängliche, unabhängig betriebene souveräne Cloud sein, die durch starke technische Kontrollen, souveräne Zusicherungen und rechtliche Schutzmaßnahmen abgesichert ist. •

CRM und KI: Umsatzziele nachhaltig sichern

In dynamischen Märkten mit steigendem Wettbewerbsdruck, unsicheren Exportbedingungen und wachsendem Kostendruck stehen Unternehmen vor der Herausforderung, ihre Umsatzziele nachhaltig zu sichern. Der Schlüssel liegt im proaktiven Vertrieb – einem Ansatz, der nicht auf Zufälle oder spontane Reaktionen setzt, sondern auf strukturierte Daten, Reports, automatisierte Prozesse und eine intelligente Vertriebs- und Aufgabensteuerung direkt im CRM. /// von Patrick Roth

DER AUTOR
Patrick Roth
ist Sales Division Manager CRM bei der Kumavision BSO GmbH.
Bild: Kumavision

VIELE UNTERNEHMEN KÄMPFEN MIT VERALTETEN VERTRIEBSSTRUKTUREN: Prozesse sind inkonsistent, Daten liegen verstreut und unstrukturiert in unterschiedlichen Dateien, Reports sind wenig aussagekräftig, moderne Tools fehlen. Die Folge: Vertriebsaktivitäten lassen sich nicht skalieren, vom Marketing generierte Leads versanden beim Vertrieb, Potenziale bei Neu- und Bestandskunden bleiben ungenutzt.

Frühzeitig mit Systemunterstützung handeln statt verspätet reagieren

Auch wenn ein proaktiver Vertrieb zuerst immer auch eine zielführende Haltung widerspiegelt, geht es nicht ohne moderne Technologie. Denn um proaktiv handeln zu können, braucht es eine klare Sicht auf Geschäftsfelder. Eine Segmentierung im Customer Relation Management, die Verbindung von ERP- und CRM-Daten sowie die Abbildung aktueller Geschäftsprozesse sind unverzichtbar.

Nur mit dieser Transparenz lassen sich belastbare Forecasts erstellen und Potenziale bei Bestandskunden frühzeitig erkennen. Beispielsweise durch die systemgesteuerte Überwachung von Vertragslaufzeiten, Produktlebenszyklen oder Ersatzteilbedarf im CRM. Das CRM kann auf Basis dieser Daten automatisiert Maßnahmen ableiten, wie etwa das Anlegen von Aufgaben für den Vertrieb.

Vom unbekannten Kontakt zur margenträchtigen Verkaufschance

Eine enge Verzahnung von Marketing und Sales erleichtert die Gewinnung von Neukunden und vermeidet Reibungsverluste. Microsoft Dynamics 365 ermöglicht beispielsweise die Erstellung individueller, datenbasierter Customer Journeys und automatisiert die Lead-Generierung, etwa über Events oder White Paper als Lead-Magneten. Externe Tools und B2B-Datenbanken lassen sich integrieren, um Website-Besucher direkt als Leads ins CRM zu überführen – inklusive automatischer Anreicherung der Daten und Aufgabenverteilung im Vertriebsteam.

Ein zentrales Element ist dabei das Lead Scoring: Es bewertet Leads anhand definierter Trigger wie Website-Besucher, Webinar-Teilnahmen, Downloads oder E-Mail-Reaktionen. So wird sichergestellt, dass der Vertrieb sich auf die vielversprechendsten Kontakte konzentriert. Gleichzeitig lassen sich Marketing-Kampagnen skalieren, ohne dass zusätzliches Personal erforderlich ist.

KI als Vertriebsassistent für maximale Performance des Vertriebsteams

Microsoft Copilot unterstützt die Mitarbeiter, die Vertriebsaufgabe mit maximaler Effizienz zu erfüllen. In Vorbereitung auf einen Kundentermin beantwortet der Copilot allwissend jegliche Fragen zum Kunden, wie beispielsweise die historische Verkaufsmenge, aktuelle Verkaufschancen oder offene Service-Tickets. Darüber hinaus erstellt der Copilot Zusammenfassungen, Marketing-Content und erledigt automatisiert Routineaufgaben. Im Lead Management unterstützt der Copilot bei der Anreicherung von Kundendaten. In Microsoft Teams integriert unterstützt künstliche Intelligenz so eine zentrale Kommunikation und Dokumentation vom Angebot bis zur Nachbereitung.

Proaktivität als Wettbewerbsvorteil

Unsere Erfahrung bei Kumavision zeigt: Unternehmen, die auf einen proaktiven Vertrieb setzen, stärken ihre Resilienz, um auch unter herausfordernden Bedingungen ihre Umsatzziele sicher zu erreichen. Sie erkennen Handlungsbedarf frühzeitig, nutzen ihre Ressourcen effizienter und steigern ihre Abschlussquoten. Der Weg dorthin führt über moderne CRM-Systeme mit intelligente Datenstrukturen und automatisierte Workflows sowie dem gezielten Einsatz von KI: für mehr Umsatz, mehr Marktanteile und mehr Zukunftssicherheit. •

PROAKTIVER VERTRIEB

Viele B2B-Vertriebe leiden unter zersplitterten Daten, inkonsistenten Prozessen und fehlenden Tools – Leads versanden, Skalierung scheitert.

Proaktivität gelingt nur mit moderner Systemunterstützung:
Ein segmentiertes CRM, die Verknüpfung von ERP- und CRM-Daten sowie die Abbildung realer Prozesse schaffen Transparenz für belastbare Forecasts und frühe Cross-/Upsell-Impulse (zum Beispiel Vertragslaufzeiten, Produktzyklen, Ersatzteile). Marketing und Sales verzahnen sich über Dynamics 365 mit datenbasierten Customer Journeys, automatisierter Lead-Generierung und Lead Scoring.

Ergebnis: höhere Resilienz, bessere Abschlussquoten und mehr Umsatz.

> „Auch wenn ein proaktiver Vertrieb zuerst immer auch eine zielführende Haltung widerspiegelt, geht es nicht ohne moderne Technologie. Denn **um proaktiv handeln zu können, braucht es eine klare Sicht** auf Geschäftsfelder."
>
> *Patrick Roth*

Welche Tools sind für mein Unternehmen die richtigen?

KI-Tools wie ChatGPT und Microsoft Co-Pilot sind noch relativ neu. Arbeitgeber*innen wie auch Angestellte stehen vor der Herausforderung, diese Werkzeuge verstehen und effizient einsetzen zu müssen. Michael Hofmann* von Cosmo Consult erklärt, wie dies gelingen kann. /// von Heiner Sieger

Programme wie ChatGPT, Copilot, sowie Claude sind inzwischen zu gängigen Werkzeugen in Firmen geworden. Welche Zwischenbilanz ziehen Sie, was den Umgang mit diesen Tools angeht?

Michael Hofmann | KI – beispielsweise der Copilot und ChatGPT – ist noch eine junge Technologie. Eine Innovation erfordert immer ein neues Mindset. Bislang sind viele Funktionen den Nutzern unklar. Das führt unter anderem dazu, dass sie Ergebnisse erhalten, nach denen sie nicht gesucht haben. Oft heißt es entsprechend: „Die KI macht Dinge, die ich nicht verstehe."

Woran liegt das?

MH | Unter anderem an der Tatsache, dass es sich schlicht um eine neue Technologie handelt. Es hat Zeit gebraucht, bis Leute verstanden haben, was bei ihren regelmäßigen iPhone-Updates passiert.

Fragen und Sorgen haben sich langsam aufgelöst, weil Menschen verstanden haben, dass ihre Daten in einem Bereich des Handys abgelegt sind, die Daten der Applikationen wiederum in einem anderen. Uns werden Werkzeuge angeboten, von denen wir noch nicht ahnen, was genau sie tun.

DER GESPRÄCHSPARTNER
Michael Hofmann
ist Clusterlead Modern Work bei Cosmo Consult.

Wie kann diese Aufklärung stattfinden?
MH | Hier setzt das Erwartungsmanagement an. Es existiert eine Dissonanz zwischen den Herstellern und den Nutzern – ihre Erwartungen liegen auf unterschiedlichen Wellenlängen. Genauer gesagt: was die Hersteller sich von ihren Programmen erhoffen, stimmt nicht mit dem überein, was ihre Kund*innen damit anfangen können oder wollen. Nur durch gezielte Information und Schulung lässt sich diese Lücke schließen. Dann erst kann effizient gearbeitet werden.

Ein Beispiel: Ein großer Arbeitgeber führte vor kurzem eine KI-Lösung ein. Als ich ihn nach seinem Eindruck fragte, sagte er offen, dass er enttäuscht sei: „Es ist nicht das, was uns verkauft wird. Es kann gar nicht alles." KI-Tools wie Copilot oder ChatGPT werden präsentiert wie ein neuer Kollege, der an seinem ersten Tag durchstarten soll, ohne eingeführt worden zu sein. Es braucht Vorarbeit, bevor diese Werkzeuge effizient genutzt werden können.

Dissonanz zwischen Arbeitgebern und Arbeitnehmern gilt es ebenfalls aufzulösen.

Viele Angestellte empfinden vorkonfigurierte KI-Tools als undurchsichtig und haben das Gefühl, sie nicht zu verstehen.
MH | Das stimmt. KIs sind so programmiert, dass sie versuchen, aus vorhandenen Informationen einen Sinn zu generieren. Sie liefern das, was aus ihrer Sicht am wahrscheinlichsten richtig ist. Manchmal funktioniert das gut. Manchmal kommt es zu Halluzinationen, weil die KI rät.

Claude beispielsweise nutzt das Vorwissen aus bereits gestellten Fragen und aus Rückmeldungen, die sie zu ihren Antworten bekommen hat. Dadurch sind die Resultate oft treffsicherer als bei ChatGPT. ChatGPT ist laut Selbstbeschreibung unvoreingenommen – gewissermaßen „blank". Es bezieht sich innerhalb eines Gesprächs zwar auf den bisherigen Verlauf, lernt aber nicht dauerhaft aus einzelnen Interaktionen. Ein kontinuierliches Lernen

> „ Wir müssen Menschen schulen, damit sie verstehen, was in der KI passiert. **Damit nehmen wir ihnen auch die Angst.** Das ist eine große Baustelle.
>
> *Michael Hofmann*

Halten Sie Schulungen für eine geeignete Möglichkeit, diese Souveränität zu erlangen?
MH | Absolut. Wir müssen Menschen schulen, damit sie verstehen, was in der KI passiert. Damit nehmen wir ihnen auch die Angst. Das ist eine große Baustelle. Wie erreichen wir, dass die Ausgabe der KI für jeden verständlich ist? Das wiederum führt uns zum nächsten Thema: Nicht jedes Tool ist für alles geeignet. Einige Ergebnisse sind missverständlich oder irritierend, wenn man ein ungeeignetes Tool genutzt hat. Niemand benutzt eine Bohrmaschine, um einen Nagel in die Wand zu schlagen. Es gibt Unterschiede zwischen den einzelnen Tools.

Der Copilot ist das klassische Cloud-Tool. Ich gebe ihm meine Daten und weise ihn vielleicht noch an, in das Repository zu schauen, um davon zu lernen. Dann gebe ich ihm mit, was ich haben möchte. Das sind die Prompts. Ich gehe davon aus, dass die meisten Menschen ihre Prompts sammeln und jene immer wieder nutzen, die sich als nützlich erwiesen haben. Mit dem Copilot Studio oder ChatGPT Enterprise kann man mehr steuern. Wenn ich eine Maschine haben möchte, die für sehr spezielle Zwecke geeignet ist und entsprechend schnell und präzise funktioniert, muss ich sie herstellen. Sie ist komplizierter zu bedienen und auch teurer. Firmen, die mit einer Custom KI arbeiten, beschäftigen Menschen, die darin geschult sind. Diese Programmierer sind allerdings nicht die, die die Strategie verantworten oder das Geld bereitstellen. Diese im Sinne eines ständigen Prüfens und Verfeinerns findet derzeit nicht statt. Trotzdem funktionieren die KI-Tools sehr ähnlich. Die wesentlichen Unterschiede sind die Fragen: Welche Kontrolle übe ich aus? Mit welchen Daten arbeite ich? Wie leistungsfähig muss das Werkzeug sein?

Wie gestalten Sie diese Schulungen konkret?
MH | Zunächst erklären wir den Mitarbeitern, wie Algorithmen grundsätzlich funktionieren: Eine KI durchsucht Datenquellen, sammelt Informationen, schaut nach Keywords, analysiert Wahrscheinlichkeiten und bildet Vernetzungen, auf deren Basis sie ein Ergebnis liefert. Im nächsten Schritt erklären wir, wie man richtig fragt. Um Ängste zu nehmen, entwickeln wir zusammen mit unseren Kunden Basic Prompts. Was sind Dinge, die sie beschäftigen? Was sind oft wiederkehrende Aufgaben, die ihnen Zeit rauben? Kurz: Wie füttere ich die KI mit meinen Erwartungen, damit das Ergebnis für mich passt?

Daraus wiederum bauen wir einen Agenten, einen Bot. So verstehen die Mitarbeiter besser, wie eine KI in Ansätzen funktioniert. Auf diese Weise ist Transparenz gegeben und die Kunden müssen sich keine Sorgen um die Sicherheit ihrer Daten machen.

Manchmal habe ich den Eindruck, dass bei all der Begeisterung über die neue Technologie der Mensch in Vergessenheit gerät. Da müssen wir hin. Der Mensch sollte immer im Mittelpunkt stehen. •

ON TOP statt auf Tauchstation

Das Prompt-Volumen wächst rasant, Shopping-Anfragen verdoppeln sich und die Klickzahlen steigen deutlich: Immer mehr Verbraucher greifen auf ChatGPT & Co. zurück, um Produkte zu suchen oder Preise zu vergleichen – mit direktem Einfluss auf ihre Kaufentscheidungen. Unternehmen, die ihre Inhalte nicht durch Artificial Intelligence Optimization (AIO) aufbereiten, riskieren, in der neuen Suchlandschaft unsichtbar zu werden. /// von Dr. Florian Mueller

TECHNOLOGISCHE UMBRÜCHE ZEICHNEN SICH SELTEN SO KLAR AB WIE DERZEIT im Bereich der durch künstliche Intelligenz (KI) gestützten Suche. Laut Daten des Marktforschers Sensor Tower stieg das Volumen der ChatGPT-Prompts zwischen Januar und Juni 2025 um fast 70 Prozent. Besonders dynamisch entwickelt sich dabei der Bereich Shopping. Innerhalb von sechs Monaten hat sich der Anteil der Einkaufsanfragen verdoppelt. Eine aktuelle Bain-Befragung zeigt zudem: In den USA haben schon 73 Prozent der Verbraucher KI für Produktrecherchen oder Preisvergleiche genutzt – oder sind dazu bereit.

Parallel dazu wächst auch die Zahl der Klicks auf eingebundene Links in ChatGPT rasant: Zwischen März und Juni 2025 ist die Click-Through-Rate von 2,2 auf 5,7 Prozent gestiegen. Damit entwickelt sich KI nicht nur zur Antwortmaschine, sondern zu einer Plattform, die Kaufentscheidungen unmittelbar beeinflussen kann. Für Unternehmen bedeutet das: Eine bloße Nennung reicht nicht mehr. Erst wenn die eigene Seite aktiv in den Antworten der KI verlinkt ist, eröffnen sich echte Chancen auf Reichweite und Umsatz.

AIO gilt als neue Pflichtdisziplin

Analog zur klassischen Suchmaschinenoptimierung (SEO), die im Laufe der Zeit eigene Berufsrollen und spezialisierte Agenturen hervorgebracht hat, entsteht nun ein neues Feld: Artificial Intelligence Optimization (AIO), auch als Generative Engine Optimization (GEO) bezeichnet. Im Kern geht es darum, Inhalte so aufzubereiten, dass sie von ChatGPT, Perplexity und anderen KI-Suchsystemen nicht nur verstanden, sondern auch als Quelle herangezogen werden. Die Logik ähnelt zwar der SEO, aber die Mechanik verändert sich grundlegend. Klassische Suchmaschinen priorisieren Keywords und Backlinks, während KI-Systeme Antworten aus Texten ziehen, die maschinenfreundlich strukturiert, klar formuliert und mit vertrauenswürdigen Quellen versehen sind. Unternehmen, die ihre Inhalte entsprechend ausrichten, können von dieser Dynamik profitieren. Wer hingegen abwartet, läuft Gefahr, in der neuen Suchlandschaft nicht mehr stattzufinden.

Auf Zugänglichkeit, Struktur und Inhalte fokussieren

Handeln ist jetzt gefragt. Der erste Schritt ist technischer Natur: KI-Modelle können Inhalte nur dann verarbeiten, wenn sie frei zugänglich sind.

> „ Produktinformationen sollten mit **Schema.org-Markup angereichert** und durch aktuelle Feeds zu Preisen, Verfügbarkeiten und Bewertungen ergänzt werden. Nur so lassen sich Inhalte verlässlich in Shopping-Antworten integrieren.
>
> *Dr. Florian Mueller*

DER AUTOR
Dr. Florian Mueller
leitet bei Bain & Company die Praxisgruppe AI, Insights & Solutions in der EMEA-Region.

Crawler wie GPTBot müssen in den Website-Einstellungen ausdrücklich zugelassen werden, zudem dürfen Inhalte nicht hinter Paywalls oder technischen Sperren verborgen sein.

Doch Zugänglichkeit allein genügt nicht. Ebenso entscheidend ist die richtige Struktur. Inhalte sollten so aufbereitet sein, dass Modelle sie schnell erfassen und verarbeiten können. Formate wie FAQs, How-to-Artikel oder klare Schritt-für-Schritt-Anleitungen haben deutlich bessere Chancen, als Quelle in Antworten aufgenommen zu werden. Besonders wichtig: die Kernbotschaft gleich zu Beginn – nach der sogenannten Answer-first-Logik. Für den Handel und die Konsumgüterindustrie spielen strukturierte Daten ebenfalls eine Schlüsselrolle. Produktinformationen sollten mit Schema.org-Markup angereichert und durch aktuelle Feeds zu Preisen, Verfügbarkeiten und Bewertungen ergänzt werden. Nur so lassen sich Inhalte verlässlich in Shopping-Antworten integrieren. Auch die Inhalte selbst verändern sich. KI-Systeme bevorzugen originäre Daten, klar definierende Artikel und praxisnahe Leitfäden. Unternehmen, die eigene Studien oder Benchmark-Reports veröffentlichen, steigern ihre Chancen erheblich, als Primärquelle verlinkt zu werden. Entscheidend ist dabei Transparenz: Angaben zu Autorenschaft, Aktualisierungsdatum und Quellen erhöhen die Glaubwürdigkeit – und damit die Wahrscheinlichkeit einer Verlinkung.

Strategische Weichen stellen

Noch ist offen, wie schnell sich die KI-Suche durchsetzen wird. Sicher ist: Sie verschiebt das Kräfteverhältnis zwischen Suchmaschinen, Plattformen und Unternehmen. Erste Anbieter testen neue Geschäftsmodelle wie gesponserte Links oder Revenue-Share-Programme für Publisher. Für Unternehmen bedeutet das, ihre Marketing- und Kommunikationsbudgets neu auszurichten. Frühe Investitionen in AIO bringen nach Bain-Erfahrungen bereits messbare Vorteile. Wer jetzt die Grundlagen schafft, profitiert langfristig: durch erhöhte Reichweite in einem wachsenden Kanal und durch Erfahrungswerte in einem Feld, das in den kommenden Jahren weiter an Bedeutung gewinnen wird. •

So unterstützen Agenturen KI-Integration entlang der Wertschöpfungskette

Unternehmen professionalisieren den Einsatz von künstlicher Intelligenz (KI) zunehmend. Die ersten Integrationen erfolgten maximal agil, kreativ, oft improvisiert. Sie haben gezeigt: KI-Technologie senkt Kosten punktuell und beschleunigt Prozesse. Heute kann sie jedoch mehr als nur Einzelerfolge erzielen. /// von Jens-Christian Jensen und Kai Ebert

FÜR UNTERNEHMEN GILT ES DAHER AKTUELL, KI ENTLANG der gesamten Wertschöpfungskette zu implementieren. Langfristig, flächendeckend und messbar. Tech-Agenturen nehmen bei dieser Aufgabe eine Schlüsselfunktion ein.

Von der Einzelanwendung zum Querschnittsthema

Der Nutzen und die Dynamik von KI haben die Perspektive auf die Technologie verändert. Unternehmen denken zunehmend in Arbeitsabläufen. Ziel ist es, Prozesse über mehrere Abteilungen hinweg zu verstehen, standardisieren und orchestrieren. KI nimmt so eine Querschnittsfunktion ein und wird zum Bestandteil der Wertschöpfung. In der Praxis stehen mittelständische Unternehmen jedoch vor einer Herausforderung: Sie verfügen zwar über funktionierende digitale Strukturen. Ihnen fehlt jedoch das nötige Know-how, um Technologie, Organisation und Kommunikation zusammenzuführen. KMUs brauchen einen Sparringspartner, der ihre komplexen Prozesse versteht und sie bei der Integration von KI in bestehende Wertschöpfungssysteme unterstützt.

Agenturen werden zum KI-Koordinator

Tech- und Digitalagenturen nehmen in diesem Zusammenhang eine Koordinatoren-Rolle ein. Sie verstehen Datenströme, Systemlogiken und Nutzerinteraktionen gleichermaßen. Sie überführen technische Komplexität in überschaubare, ergebnisorientierte Schritte. Im Dialog mit Unternehmen liefern sie KI-Trainings, erstellen Leitlinien und begleiten die KI-Integration eng im laufenden Betrieb. In der Praxis manifestiert sich die Zusammenarbeit vor allem entlang von zwei Schritten:

- **Hebel identifizieren:** Welche Prozesse innerhalb der Wertschöpfungskette sind es, die maßgeblich auf den Unternehmenserfolg einzahlen? Gemeinsam machen Agenturen und Unternehmen vorhandenes Datenmaterial nutzbar und schaffen erste Use Cases. Relevante Prozesse sollten durch KI-Tools neu prototypisiert werden, um reale Mehrwerte und Effizienzgewinne zu schaffen. Nur so kann KI als Hebel wirken.
- **Framework etablieren:** Funktionierende Prototypen müssen in wiederholbare Frameworks überführt werden. Diese reichen von integrierten Suite-Plattformen bis zu schlanken Agentenlösungen. Agenturen helfen in dieser Phase, die passenden Werkzeuge auszuwählen und den Übergang in den Regelbetrieb sicherzustellen. So bringen sie Organisation, Kommunikation und Technologie in Einklang und helfen Unternehmen, ihre Wertschöpfung schrittweise durch KI zu erweitern.

Zukunft KI: Vom Einzeltool zum Ökosystem

Für den Mittelstand eröffnet sich damit eine echte Zukunftschance – und ein klares Leitbild: Wer jetzt vernetzte Strukturen für eine integrierte, sichere und transparente KI-Nutzung schafft, legt den Grundstein für langfristige Wettbewerbsfähigkeit. Agenturen stehen KMUs dabei als strategischer Wegbegleiter und praxisnaher Innovationspartner zur Seite. •

Die AUTOREN

Jens-Christian Jensen (l.) (Plan.Net Group) & **Kai Ebert** (SYZYGY) sind beide Lableiter des Labs „Value Chain" der Working Group „Künstliche Intelligenz" im BVDW. Das Lab behandelt die chancen-orientierte Veränderung der Wertschöpfungskette der digitalen Wirtschaft.

Digitales Vertragsmanagement mit Köpfchen

Das Contract Lifecycle Management (CLM) genießt in vielen Unternehmen einen eher schlechten Ruf, weswegen – gerade auf LinkedIn – sogar schon der „Tod des CLM" vorhersagt wurde. Die gängige Kritik fokussiert sich auf die eingeschränkte Flexibilität, mangelnde Anwenderfreundlichkeit und fehlende Intelligenz vieler Systeme. Gleichzeitig wird häufig behauptet, dass Unternehmen keinen Bedarf an einem smarten digitalen Vertragsmanagement mehr hätten. Die aktuelle Studie „Smartes Vertragsmanagement: Wo Unternehmen heute stehen" von techconsult und Ceyoniq zeigt klar, dass dem nicht so ist.

VON DEN 221 UNTERNEHMEN, DIE IM RAHMEN DER STUDIE BEFRAGT WURDEN, NUTZT AKTUELL NUR JEDES DRITTE EIN ENTSPRECHENDES CLM-TOOL. Das führt dazu, dass z.B. im Finanzgewerbe mehr als die Hälfte der Unternehmen (59%) keinen zentralen Überblick über ihre laufenden Verträge haben – gerade in dieser hochregulierten Branche eigentlich undenkbar. Insgesamt 49 Prozent aller befragten Firmen setzt auf simple Tools wie Excel oder ähnliches, um die laufenden Verträge zu verwalten.

Vertragschaos in den Griff bekommen mit nscale CLM

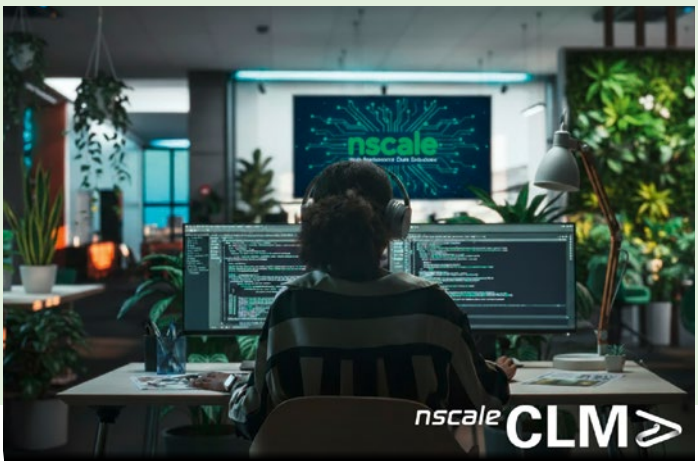
Dabei könnte es einfacher sein, wenn Unternehmen eine intelligente Vertragsmanagementlösung einsetzen würden wie das neue **nscale CLM** von **Ceyoniq**. **nscale CLM** ist mit Blick auf die tägliche Arbeit mit Verträgen entwickelt worden und schafft für Unternehmen volle Transparenz über den gesamten Vertragslebenszyklus. **nscale CLM** unterstützt bspw. bei der ungeliebten Organisationsarbeit, indem eingehende Verträge geprüft werden und eine voll automatisierte Fristenverwaltung intelligente Benachrichtigungen zu Terminen sendet. Schluss mit verpassten Zahlungs-, Kündigungs- oder Verhandlungsterminen!

Außerdem verfügt **nscale CLM** standardmäßig über eine revisionssichere Archivierung, nachvollziehbar, unveränderbar und fälschungssicher. Somit sind Unternehmen jederzeit voll auditfähig, regelkonform und selbst höchste Compliance-Vorgaben können ganz ohne Probleme erfüllt werden. Eine echte Unterstützung zur Vertragsanalyse bietet die eingebaute KI auf Basis von sogenanntem Natural Language Processing. So können die Anwender innerhalb von **nscale CLM** beispielsweise über einen Chat ganz natürlich mit der integrierten Künstlichen Intelligenz interagieren und diese nach Details der Verträge fragen oder lange Dokumente zusammenfassen lassen.

Sicherheit wird großgeschrieben – genauso wie Komfort

nscale CLM basiert auf einer modernen Cloud-Lösung, die ausschließlich innerhalb von Deutschland gehostet wird. Unternehmen können sich also sicher sein, dass ihre vertraulichen Daten nicht die Landesgrenzen überqueren. Das ist gerade angesichts aktueller EU-Gesetzgebungen wie dem EU Data Act für viele Unternehmen unabdingbar. Die Cloud Lösung ist außerdem flexibel skalierbar und fügt sich nahtlos in bestehende ITLandschaften ein.

nscale CLM ist Teil der „nscale Familie" aus dem Hause **Ceyoniq**. Mit Lösungen „Made in Germany" – und vor allem ausschließlich in Deutschland gehostet – sind Unternehmen damit optimal aufgestellt, um alle Anforderungen nicht nur zu erfüllen, sondern sogar zu übertreffen. Ganz egal, welche Regularien aus Brüssel kommen mögen. •



CEYONIQ Technology
A KYOCERA GROUP COMPANY

Dokumentationsfrust? Lass die KI ran

In deutschen Krankenhäusern fallen täglich pro Patient rund 27 Seiten Dokumentation an. Zwei Kliniken, das Robert-Bosch-Krankenhaus und das Klinikum Rheine, testen nun eine KI, die diese Datenflut bündelt und durchsuchbar macht. Erste Ergebnisse zeigen: Ärzte finden relevante Informationen fünfmal schneller und können Entscheidungen deutlich effizienter treffen. /// von Patrick Oestringer

IN DEUTSCHEN KRANKENHÄUSERN GEHÖRT DIE FLUT AN PATIENTENDATEN längst zum Alltag. Befunde, Laborwerte und Arztbriefe summieren sich schnell zu ganzen Aktenbergen. Wer eine bestimmte Information sucht, verliert dabei wertvolle Minuten – Zeit, die in der Patientenversorgung fehlt. Künstliche Intelligenz kann diesen Prozess entscheidend vereinfachen. Moderne Systeme strukturieren Daten automatisch, erstellen Zusammenfassungen und liefern gezielte Antworten auf Fragen. Das Ziel: Ärzte nicht mit zusätzlicher Bürokratie zu belasten, sondern ihnen mehr Zeit für die Behandlung ihrer Patienten zurückzugeben.

KI im Regelbetrieb – Erfahrungen für die Praxis

Zu den Vorreitern gehört das Robert-Bosch-Krankenhaus in Stuttgart. Als Teil des Bosch Health Campus treibt es Innovationen in der medizinischen Versorgung voran. Dafür hat der Campus das vom Land geförderte KI-Reallabor Gesundheit BW etabliert – ein geschützter Raum, in dem KI-Innovationen unter realen Bedingungen erprobt und regulatorisch begleitet werden. In diesem Rahmen testet das Krankenhaus die Anwendung Medical Summary des deutschen Unternehmens Averbis. Sie bündelt alle verfügbaren Patienteninformationen, beantwortet ärztliche Fragen in Sekunden und verweist direkt auf die Quelle. Perspektivisch lassen sich auch Daten aus der elektronischen Patientenakte (ePA) einbeziehen.

„Gemeinsam mit Averbis gelingt es uns, medizinische Informationen mithilfe von KI sogar aus unstrukturierten Daten wie PDF-Dokumenten zu extrahieren und sie gezielt für Patientenversorgung und Forschung nutzbar zu machen“, sagt Prof. Dr. med. Oliver Opitz, Leiter des Bosch Digital Innovation Hubs.

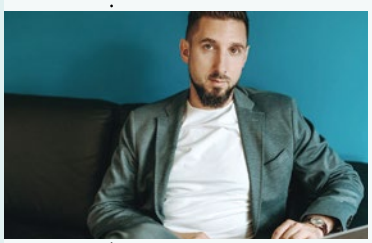
Daten als Engpass

Das größte Hindernis für den Einsatz von KI: Rund 90 Prozent der Patientendaten liegen unstrukturiert in Freitexten oder PDFs vor. Bevor eine KI Antworten geben kann, müssen diese Informationen in eine maschinenlesbare Form gebracht werden. Genau hier setzt Medical Summary an. Die Technologie ordnet die verfügbaren Daten so, dass die Krankheitsgeschichte in einer einheitlichen Datenbasis zur Verfügung steht. Daraus entstehen automatisch Zusammenfassungen nebst Chatbot-Funktion.

Erste Ergebnisse zeigen: Ärzte sichten relevante Daten bis zu fünfmal schneller. „Wir müssen die Ressourcen möglichst effektiv nutzen, das muss der Anspruch an digitale Lösungen sein. Mit der Lösung aus unserem Reallabor und mit Averbis haben wir genau die Chance, die Effizienz zu erhöhen”, sagt Prof. Dr. med. Mark Dominik Alscher, Geschäftsführer des Robert-Bosch-Krankenhauses am Bosch Health Campus.

Der Weg zur KI-Implementierung

Zentrale Voraussetzung für den Einsatz von KI ist die Anbindung an das Krankenhaus-Informationssystem, das wichtigste Gateway für Daten aus Archiv, ePA und weiteren Dokumentationssystemen. Bewährt hat sich dabei ein schrittweises Vorgehen: Zunächst wird die Lösung auf einer motivierten Pilotstation eingeführt, um Erfahrungen zu sammeln und Vorbehalte abzubauen – oft ist die Sorge groß, dass neue Software mehr Arbeit bedeutet. Am Ro-



DER AUTOR

Patrick Oestringer

ist Geschäftsführer von Averbis, einem KI-Vorreiter im Bereich Medizin. Das deutsche Unternehmen bereitet Gesundheitsdaten in Krankenhäusern so auf, dass sie Ärzten übersichtlich und intuitiv zur Verfügung stehen.

bert-Bosch-Krankenhaus soll noch dieses Jahr die erste Abteilung produktiv starten, bevor die Klinik schrittweise folgt. Alle Daten verbleiben in der Infrastruktur des Krankenhauses. Für die notwendige Rechenleistung wird zusätzlich der Cloud-Anbieter StackIT in Baden-Württemberg genutzt. Die Anbindung erfolgt verschlüsselt, die Daten werden dort lediglich verarbeitet, aber nicht gespeichert.

Mindestens eine Stunde Zeitersparnis – pro Arzt und Tag

KI entlastet nicht nur bei der Auswertung von Patientenakten, sondern auch bei der Dokumentation. Arzt-Patienten-Gespräche können automatisch protokolliert, Diagnosen erkannt und direkt im KIS dokumentiert werden. Ärzte prüfen nur noch und korrigieren bei Bedarf. Auch Arztbriefe lassen sich intelligent erstellen. Im Hausarztzentrum Wiesloch reduziert diese Automatisierung den Aufwand bereits erheblich: „So sparen wir pro Arzt täglich rund eine Stunde“, berichtet Dr. med. Rita Bangert-Semb. Hochgerechnet entspricht das Millionen gewonnener Stunden pro Jahr – ein enormes Potenzial für mehr Zeit bei den Patienten. Entscheidend bleibt jedoch das Vertrauen des Personals: Sobald der Eindruck entsteht, dass die KI fehlerhaft arbeitet, wird sie nicht genutzt. Ziel ist daher nicht nur Effizienz, sondern vor allem eine verlässliche Unterstützung, die die Qualität der Versorgung stärkt.

Zuverlässigkeit als Knackpunkt – so lässt sich die Qualität der KI sicherstellen

Für den Erfolg von KI im Klinikalltag ist ihre Verlässlichkeit entscheidend. Da einzelne Sprachmodelle (LLMs) unterschiedliche Stärken und Schwächen haben, setzt Averbis auf eine Kombination mehrerer Modelle. Es geht jedoch nicht darum, dem medizinischen Personal Entscheidungen abzunehmen oder Diagnosen zu automatisieren – schon gar nicht darum, sie zu ersetzen. Ziel ist vielmehr, Informationen so aufzubereiten, dass Ärzten und Pflegekräfte bessere Entscheidungen treffen können. Es geht darum, sie die besten Experten sein zu lassen, die sie sein können. •

Digitale Helfer gegen Termin-Ausfälle

Fast jeder fünfte Arzttermin in Deutschland wird nicht wahrgenommen. Das hat Folgen für alle Beteiligten: Wartezimmer bleiben leer, während andere Patientinnen und Patienten dringend auf Termine warten. Praxisteams verlieren Zeit, Abläufe geraten durcheinander, Vorsorge bleibt liegen. /// von Susanne Dubuisson

DIE URSACHEN SIND VIELFÄLTIG UND OFT TEIL DES HEKTISCHEN ALLTAGS: Ein wichtiger Arbeitstermin überschneidet sich plötzlich mit dem Vorsorgetermin, das kranke Kind braucht Aufmerksamkeit, oder der Termin wird zwischen Homeoffice und einem Besuch bei den Großeltern schlicht versehentlich vergessen. Manchmal macht auch eine spontane Erkrankung den geplanten Kontrolltermin unmöglich, oder die Anfahrt zur Praxis wird durch einen Stau erschwert. Was als einzelne, verständliche Situation beginnt, entwickelt sich schnell zu einem strukturellen Versorgungsproblem.

Digitale Erinnerungen als einfache Hilfe

Genau hier können digitale Lösungen unterstützen. Eine Erinnerung zum richtigen Zeitpunkt senkt die Wahrscheinlichkeit, dass ein Termin versäumt wird. Gerade wenn Vorsorgeuntersuchungen nur alle paar Jahre anstehen, ist es hilfreich, im passenden Moment einen Hinweis zu bekommen. Und wenn aus dieser Erinnerung direkt eine Buchung möglich ist, wird der Weg zur Vorsorge spürbar kürzer. Wie groß der Effekt sein kann, zeigt ein aktuelles Beispiel: Unsere neuen Gesundheitserinnerungen haben in nur acht Wochen mehr als 150.000 Vorsorgetermin-Buchungen ausgelöst. Über zwei Millionen Gesundheitserinnerungen wurden in diesem Zeitraum allein gelesen, und eine halbe Million Menschen hat sofort reagiert – sei es durch die Online-Buchung eines individuellen Vorsorgetermins oder das Abhaken einer erledigten Untersuchung.

Vorsorge in den Alltag integrieren

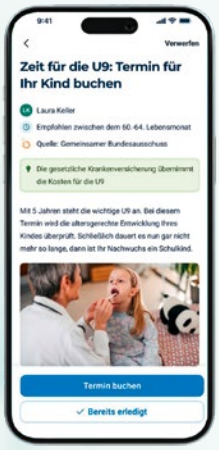
Der Erfolg liegt nicht allein in der Technik, sondern in der Haltung dahinter: Prävention darf kein zusätzlicher Aufwand sein, sondern muss selbstverständlich in den Alltag der Patienten passen. Deshalb wurde die Funktion bewusst schlank und intuitiv entwickelt. In der Praxis bedeutet das z. B.: Eltern erhalten rechtzeitig eine Erinnerung an die nächste U-Untersuchung ihres Kindes. Der Vater wird an die anstehende Darmkrebsvorsorge erinnert und die Mutter erhält den Hinweis auf die nächste Mammographie. Die Grundlage bilden die offiziellen Empfehlungen des Gemeinsamen Bundesausschusses und des Robert Koch-Instituts. Hier wird ein breites Spektrum abgedeckt: von Krebsfrüherkennungen über Impfungen und Check-ups bis zu Zahnkontrollen. Für Praxen bedeutet das weniger Ausfälle und verlässlichere Abläufe. Für Patienten heißt es: ein kleiner Impuls, der große Wirkung entfalten kann.

Prävention statt Reaktion

Digitale Gesundheitserinnerungen zeigen, dass Digitalisierung im Gesundheitswesen mehr sein kann als das Verwalten von Terminen. Sie kann dabei helfen, das System neu auszurichten – weg von einer reaktiven Versorgung, die erst bei akuten Beschwerden greift, hin zu einer präventiven Logik. Jeder wahrgenommene Vorsorgetermin bedeutet, dass eine Krankheit vielleicht gar nicht erst entsteht. Und gleichzeitig werden Ressourcen frei, die Ärztinnen und Ärzte für akute Fälle einsetzen können.

Technik, die Nutzen schafft

Das persönliche Gespräch und die ärztliche Fürsorge werden gebraucht. Technik kann den Rahmen dafür schaffen, dass mehr Zeit genau dafür bleibt. Entscheidend ist, dass digitale Lösungen sicher sind, den Alltag der Menschen ernst nehmen und spürbaren Mehrwert bringen. Gerade im Gesundheitswesen ist Vertrauen die wichtigste Grundlage. •



Ergebnisse der neuen Gesundheitserinnerungen. Bild: Doctolib GmbH

DIE AUTORIN

Susanne Dubuisson ist Product Director bei Doctolib. Bild: Doctolib GmbH

SECURITY INSIGHT

NIS-2 & CRA:

ITK VOR CYBERATTACKEN SCHÜTZEN

KMU werden immer öfter Opfer von Cyber-Attacken – oft mit fatalen Folgen. Die EU steuert mit NIS-2 oder CRA dagegen und erhöht so den Handlungsdruck: Neben dem Datenverlust drohen hohe Strafen. Wie können KMU die Security im ITK-Bereich sichern, ohne sich finanziell zu übernehmen? Ein Ansatz sind zertifizierte, in Deutschland produzierte Produkte. /// von Christian Auerswald

DARUM GEHT'S

- Neue Vorgaben durch NIS-2 und CRA: Unternehmen müssen ihre ITK-Systeme an verschärfte EU-Sicherheitsstandards anpassen – sonst drohen hohe Strafen und Produktverbote.
- Gefährdete Unternehmenskommunikatiown: Veraltete Telefonanlagen sind Einfallstore für Cyberattacken – moderne, konforme Lösungen sind Pflicht.
- Kosteneffizient schützen: Mit Soft-PBX-Lösungen „Made in Germany" lassen sich bestehende Anlagen absichern, Schritt für Schritt modernisieren und zugleich sensible Daten zuverlässig schützen.

DER AUTOR
Christian Auerswald
ist Geschäftsführer der Auerswald GmbH & Co. KG.

> „ Made in Germany ist noch immer ein **Gütesiegel für Zuverlässigkeit und Sicherheit**. Wer hier produziert, ist etwa nicht dazu verpflichtet, versteckte Backdoors einzubauen, wie es in bestimmten Ländern der Fall wäre.
>
> *Christian Auerswald*

Frankenstein, The Shining und Co. haben sicher zurecht ihre Fangemeinde – wenn ich mich gruseln möchte, schaue ich mir einfach die Honeypots der Deutschen Telekom an, die tagtäglich massenhaft Angriffe registrieren. Minütlich prasseln bis zu 40.000 Attacken auf die Hacker-Fallen ein, deren Zweck es ist, ein Ziel für Hacker zu simulieren, um deren Vorgehensweise zu erforschen. Die Zahlen zeigen, wie realistisch das Horrorszenario „Cyberangriff" heute ist. Gerade Kommunikationslösungen stellen durch den ständigen Ein- und Ausgang von Daten und dem Austausch zwischen internen und externen Quellen ein potenziell verwundbares Ziel dar.

IT-Security muss Priorität haben

Fragt man Unternehmensverantwortliche landauf landab nach Technologietrends und ihren aktuellen Herausforderungen, ist die Antwort oft die sinnvolle Integration von KI-Anwendungen im Geschäftsalltag. Dafür gibt es meine volle Zustimmung, denn eine KI-gestützte Kommunikation bietet zahlreiche Mehrwerte wie die Entlastung der Beschäftigten und Effizienzgewinne. Zentral, weiterhin zunehmend und alle Branchen betreffend ist jedoch das Thema IT-Security. Deshalb reagiert die Politik mit Vorgaben wie der NIS-2-Richtlinie oder dem Cyber Resilience Act (CRA), die die Sicherheit in Unternehmen steigern sollen. Diese nicht zu beachten kann teuer werden. Neben dem Daten-Diebstahl drohen empfindliche Strafen: Ein Verstoß kann bis zu 15 Millionen Euro oder 2,5 Prozent des

weltweiten Jahresumsatzes kosten. Auch Produktverbote sind möglich.

Unternehmenskommunikation schützen

Gerade im Bereich der Businesskommunikation ist es ratsam, das Thema IT-Security ernst zu nehmen und sich auf Partner zu verlassen, die langjährige Erfahrung auf dem Gebiet vorweisen können. Zudem gilt es, die Widerstandsfähigkeit der ITK-Anlage zu überprüfen. Nur Lösungen auf dem Stand der Technik bieten die Basis für einen guten Schutz und entsprechen den Gesetzen. Ältere Systeme stellen hingegen ein Einfallstor für Cyberattacken dar.

Was heißt das konkret? Eine hochwertige Telekommunikationsinfrastruktur funktioniert zwar auch nach 20 Jahren noch einwandfrei. Den aktuellen und strengen künftigen Sicherheitsanforderungen wird sie jedoch nicht mehr vollends entsprechen, sodass ein Wechsel auf ein moderneres System unumgänglich wird. An so einem Punkt stehen wir aktuell. Unternehmen in Deutschland sollten daher einerseits ihren Bedarf prüfen, auf eine gesetzeskonforme und sichere Anlage zu wechseln. Zugleich ist zu empfehlen, gezielte Schulungen und fundierte Beratung zu Security-Themen in Anspruch zu nehmen. Die Nutzung konformer Technologie allein ist keine Sicherheitsgarantie. Es gilt, das Bewusstsein für potenzielle Gefahren der gesamten Belegschaft zu schärfen und, wo nötig, auch juristische Unterstützung einzuholen. Zum Beispiel, wenn es um die praktische technologische Umsetzung von Datenschutz-Anforderungen oder dem CRA geht.

Bestehende Anlage erhalten, Kosten einsparen

Dass Beratungsbedarf besteht, wird im Austausch mit dem Markt spürbar: Viele gehen davon aus, nicht von NIS-2 betroffen zu sein, weil die Zahl ihrer Beschäftigten unter 50 liegt. Doch muss das nicht das ausschlaggebende Kriterium sein. So sind zum Beispiel Arztpraxen oder Anwaltskanzleien zwar häufig eher klein, doch gehen sie mit sehr sensiblen Daten um und unterliegen letztlich doch den Vorgaben.

Wie können sich also auch kleinere Unternehmen in kurzer Zeit sicher aufstellen, ohne dafür einen hohen finanziellen Aufwand zu betreiben? Die Lösung ist ein schrittweises Vorgehen, das Kosten spart und gleichzeitig zur Einhaltung aktueller Sicherheitsstandards beiträgt: Die bestehende Anlage bleibt erhalten und wird dadurch geschützt, dass eine CRA- und NIS-2-konforme Soft-PBX vorgeschaltet wird, um das System in Richtung Netz abzusichern. So ist auf einen Schlag zuverlässiger Schutz gewährleistet. Um die Kosten einfach im Griff halten zu können, empfiehlt sich ein Lizenzmodell, dass bereits ab fünf Usern startet. Bei Bedarf können weitere Teilnehmer nach und nach auf die neue Anlage migriert werden.

Auswahlkriterien:
Welche Soft-PBX ist geeignet?

Entscheidend bei der Auswahl einer entsprechenden Lösung ist ihre Kompatibilität mit Standard SIP-Telefonen, um sicherzustellen, dass die bestehende Anlage erhalten bleiben kann. Auch der Funktionsumfang spielt eine Rolle, denn nur wenige Soft-PBX-Lösungen unterstützen Kommunikationsprozesse so, wie es die Beschäftigten von der herkömmlichen Telefonie kennen. Vor dem Hintergrund der aktuellen geopolitischen Umwälzungen bieten Produkte, die hierzulande entwickelt und hergestellt werden und deren Dienste ebenfalls hier gehostet werden, das höchstmögliche Maß an Sicherheit. Made in Germany ist noch immer ein Gütesiegel für Zuverlässigkeit und Sicherheit. Wer hier produziert, ist etwa nicht dazu verpflichtet, versteckte Backdoors einzubauen, wie es in bestimmten Ländern der Fall wäre.

So können Vorgaben wie die DSGVO ohne Probleme eingehalten werden, weil die Datenverarbeitung lokal stattfindet. Politisch instabile Vereinbarungen wie das Transatlantic Data Privacy Framework, das die Verarbeitung in den USA regelt, haben folglich keinen Einfluss. Theoretisch könnte Trump es von einem auf den nächsten Tag kippen, die Auswirkungen wären schwer absehbar. Das Risiko lässt sich für deutsche Unternehmen leicht umgehen, indem sie auf hier produzierte Lösungen setzen. Diese müssen nicht teurer sein. Die Produktion in Deutschland ist problemlos wirtschaftlich umsetzbar, wenn sie geschickt gestaltet wird.

Unternehmen müssen handeln

Die Bedrohung ist real, es ist Zeit zu handeln. Es gilt, die ITK-Anlage vor Angriffen und Cyberkriminalität zu schützen, um Business Continuity zu gewährleisten und gesetzliche Vorgaben einzuhalten. Mit intelligenten Lösungen Made in Germany kann dies zuverlässig und kostengünstig gelingen. •

MEHR ERFAHREN

Echtzeit-Übersicht zu weltweiten Cyberangriffen in Form einer interaktiven Karte und eines Statistik-Dashboards.

CYBERSECURITY UND DIGITALE SOUVERÄNITÄT
miteinander verbinden

Digitale Souveränität bedeutet, dass Fimen die Kontrolle über die eigene IT-Infrastruktur sowie über Daten und Technologien behalten. Dadurch können sie unabhängig im digitalen Raum handeln, ohne von externen Akteuren abhängig zu sein. Wir haben Experten folgende Fragen gestellt: Welche Auswirkungen hat die digitale Souveränität auf die Cybersicherheit? Und wie lassen sich beide Ansätze effizient miteinander verbinden? /// von Stefan Girschner

MICHAEL HEUER

Area VP Central Europe/DACH bei Keepit

• Digitale Souveränität und Cybersicherheit sind untrennbar – denn echte Souveränität setzt technologische Sicherheit und volle Kontrolle über Daten voraus. Unternehmen müssen also wissen, wo ihre Daten liegen, welcher Rechtsordnung sie unterstehen und wer Zugriff darauf hat. Erst wenn diese Fragen geklärt sind, kann eine Organisation regulatorische Anforderungen erfüllen. Ein zentraler Hebel ist dabei eine Infrastruktur, die auf europäische Werte und Datenschutz-Prinzipien ausgerichtet ist. Eine unabhängige Cloud-Backup-Architektur schafft diese Grundlage. Durch ein europäisches Netzwerk von Rechenzentren wird gewährleistet, dass Daten regional gespeichert und technisch von anderen Rechtsräumen isoliert bleiben. Eine No-Transmission-Garantie und die Unabhängigkeit von Hyperscalern schützen vor indirekten Zugriffspfaden.

Kombination von Schutzmechanismen und Compliance

Die Verbindung von digitaler Souveränität und Cybersicherheit gelingt, wenn Schutzmechanismen, Transparenz und Compliance ineinandergreifen. Zertifizierte Sicherheitsverfahren, Audit-Logs und regelmäßige Recovery-Tests stärken nicht nur die technische Resilienz, sondern auch das Vertrauen in die eigene Datenhoheit. Datenschutz, Ausfallsicherheit und regulatorische Konformität werden so zu einem gemeinsamen Fundament. •

TOM MOLDEN

CIO Global Executive Enagament bei NinjaOne

• Digitale Souveränität bedeutet, die Kontrolle über eigene IT-Systeme, Daten und Sicherheitsprozesse zu behalten – unabhängig von externen Abhängigkeiten. Ein zentraler Bestandteil dabei ist die Fähigkeit, Risiken schnell zu erkennen, zu priorisieren und zu beheben. Genau hier setzt Autonomous Patch Management von NinjaOne an: Es kombiniert KI-gestützte Entscheidungsintelligenz mit automatisierter Ausführung und schafft so die Grundlage für eine resiliente und souveräne IT-Infrastruktur.

Priorisierung der Patches aufgrund von Bedrohungsdaten

In einer Zeit, in der Cyberbedrohungen in Stunden statt Wochen entstehen, ist manuelles Patchen keine Option mehr. NinjaOne integriert Bedrohungsdaten aus verschiedenen Quellen, bewertet deren Relevanz und priorisiert automatisch die Patches. So wird sichergestellt, dass kritische Schwachstellen umgehend geschlossen werden, ohne die Stabilität des IT-Betriebs zu gefährden. Diese intelligente Automatisierung stärkt nicht nur die Cybersicherheit, sondern auch die digitale Handlungsfähigkeit: IT-Teams gewinnen Zeit und Ressourcen zurück. Sie behalten die Hoheit über ihre Systeme, während Prozesse standardisiert und nachvollziehbar ablaufen. Damit wird autonomes Patch Management zu einem strategischen Instrument für digitale Souveränität und Cyberresilienz. •

Michael Heuer
Bild: Keepit

Tom Molden
Bild: NinjaOne

JOACHIM ASTEL

Co-Gründer und Mitglied des Vorstands, noris network AG

• Digitale Souveränität und IT-Sicherheit sind untrennbar miteinander verbunden. Unternehmen, die ihre Zukunft selbst gestalten wollen, müssen technologische Abhängigkeiten verringern, Datenhoheit steigern und zugleich ein belastbares Sicherheitsniveau etablieren. Das bedeutet: weg von rein vertrauensbasierten Modellen und hin zu überprüfbaren, kontrollierbaren Infrastrukturen und damit zu nachweislich geprüften Qualitäts- und Sicherheitsstandards.

Kontrolle von Technologien, Datenräumen und Lieferketten

Gerade in Zeiten geopolitischer Spannungen und KI-getriebener Wertschöpfung wächst der Druck, Kerntechnologien, Datenräume und Lieferketten unter eigener Kontrolle zu halten. Doch digitale Selbstbestimmung verlangt Verantwortung: Je stärker Systeme entkoppelt und eigenständig betrieben werden, desto wichtiger werden Schutz, Wartung und kontinuierliche Überwachung. Hilfestellung leisten dabei Managementsysteme wie ISO 27001 und BSI C5. Wichtig ist jedoch gleichermaßen Security-by-Design, sonst kann gewonnene Unabhängigkeit zur trügerischen Sicherheit werden. Die Zukunft liegt in einer integrierten Strategie, die Souveränität und Sicherheit nicht als Gegensätze, sondern als Verstärker begreift.

Bei noris network denken wir Sicherheit von Anfang an mit: von der Rechenzentrumsarchitektur über zertifizierte Prozesse bis hin zu europäischen Cloud-Ökosystemen unter deutscher Datenhoheit. So entsteht Vertrauen auf einer überprüfbaren Grundlage. Wer Souveränität als Sicherheitsarchitektur versteht und sie mit klaren Standards untermauert, stärkt im Übrigen nicht nur seine digitale Handlungsfähigkeit, sondern leistet auch einen Beitrag zu einem resilienten, unabhängigen Europa im digitalen Zeitalter. •

SVEN KNIEST

Vice President Central & Eastern Europe bei Okta

• Diese Frage beschäftigt in der Tat viele Unternehmen, mit denen ich spreche. Auf den ersten Blick scheint digitale Souveränität ein Rückzug zu sein: Daten zurück ins eigene Rechenzentrum, weg von externen Clouds, hin zur maximalen Kontrolle. Cybersicherheit hingegen erfordert vernetzte Datenzugriffe und interoperable Cloud-Architekturen für wirksamen Echtzeitschutz. Meine Antwort: Nur eine konsequent gelebte Sicherheitsarchitektur bietet die sichere Grundlage für echte Datensouveränität. Denn echte Souveränität definiert sich nicht darüber, wo die Daten liegen – sondern über die Kontrolle, wer darauf zugreift.

Identitätsmanagement mit Zero-Trust-Ansatz

Viele Unternehmen haben diese Kontrolle längst verloren. Nicht wegen der Cloud, sondern wegen fragmentierter IT-Landschaften, unkontrollierter Zugriffsrechte und proprietärer Systemlösungen. Modernes Identitätsmanagement mit Zero Trust liefert die Antwort für beide Herausforderungen: Vertraue niemandem, verifiziere alles – unabhängig von Standort oder Netzwerk. Wer weiß, welche Identitäten – von Mitarbeitenden bis zu KI-Agenten – auf welche Systeme zugreifen, schafft die Grundlage für Souveränität und Sicherheit. Moderne Identitätsverwaltung macht alle Zugriffe transparent, kontrollierbar und anpassungsfähig, um auch Compliance mit NIS2, DORA oder dem EU Data Act zu garantieren. Mein Fazit: Digitale Souveränität und Cybersicherheit sind zwei Seiten einer Medaille. Modernes Identitätsmanagement ist das verbindende Element, ohne das beide nicht auskommen. •

Joachim Astel
Bild: Noris Network

Sven Kniest
Bild: Okta

PHILIPP BEHRE

Field CTO & Strategic Advisor Technology & Innovation bei Splunk

• Digitale Souveränität bedeutet für Unternehmen heute weit mehr als die Kontrolle über Daten und Systeme – sie wird zum Fundament wirtschaftlicher Handlungsfähigkeit. Doch echte Souveränität ist ohne robuste Cybersicherheit nicht denkbar. Unternehmen, die aus Gründen der Souveränität ihre Daten und Infrastruktur unter ihre Kontrolle bringen, müssen auch sicherstellen, dass sie die erforderlichen Cyberfähigkeiten als Kernbestandteil ihrer Strategie entwickeln. Cybersicherheit schützt die Fähigkeit eines Unternehmens, die Kontrolle über digitale Prozesse und Assets nicht zu verlieren und damit handlungsfähig zu bleiben. Cybersicherheit ist also auch ein geschäftskritischer Erfolgsfaktor.

Digitale Resilienz wird zum Wettbewerbsvorteil

Mit der zunehmenden Vernetzung und dem Einsatz von KI steigt der Druck, Sicherheitsrisiken in Echtzeit zu erkennen und zu beheben. Digitale Resilienz – also die Fähigkeit, Angriffe schnell zu erkennen, zu verstehen und darauf zu reagieren – wird zum strategischen Wettbewerbsvorteil. Gleichzeitig verändert KI die Arbeit von Security-Teams grundlegend, schafft neue Möglichkeiten für Verteidiger, aber auch neue Risiken. Wir müssen KI so einsetzen, dass sie die Cybersicherheit transformiert und wichtige Bereiche wie die KI-Infrastruktur vor Cyberbedrohungen schützt.

Unternehmen, die frühzeitig in Talentbindung und in die Rekrutierung neuer Cybersicherheits-Experten investieren, sichern sich einen Vorteil, wenn es darum geht, im Zeitalter von KI sicher und handlungsfähig zu operieren. In einer Welt des ständigen Wandels streben Unternehmen letztlich danach, die neuesten Technologien zu nutzen und gleichzeitig ihre Resilienz zu maximieren. Ohne Cybersicherheit ist dies nicht möglich. •

RICHARD WERNER

Security Advisor bei Trend Micro

• Digitale Souveränität ist in Deutschland ohne die nötige Cybersicherheit nicht zu erreichen. Denn IT-Sicherheit und Resilienz sind Voraussetzung und Verstärker souveränen Handelns in jedem Unternehmen. Denn nur wer Transparenz über die eigene IT-Landschaft hat, kann diese auch steuern. Ein aktuelles Lagebild über Assets, Softwareabhängigkeiten und Betriebszustände spielt dabei eine wichtige Rolle und wird durch Funktionen wie Asset-Discovery, Protokollierung, Monitoring und Incident Response ermöglicht. Um „Pseudosouveränität" durch Lock-in zu vermeiden, sollten Interoperabilität, offene Standards sowie technische und vertragliche Exit-Strategien verankert sein.

Operativ bedeutet das: Sicherheitsprinzipien wie Defense-in-Depth und Zero Trust umsetzen, auf erprobte Resilienz-Patterns setzen und regelmäßig Tests durchführen, um Schwachstellen frühzeitig zu erkennen und zu beheben. Governance-seitig braucht es gemeinsame Kennzahlen, mit denen sich IT-Sicherheit messbar vergleichen lässt – etwa Ausfallzeiten, Patch- oder Cyberrisiko-Status. Regelmäßige Architektur- und Lieferketten-Reviews stellen sicher, dass Systeme sicher aufgebaut sind.

Sicherheitslösungen müssen Audit standhalten

Da eine vollkommene Unabhängigkeit weder sinnvoll noch realistisch ist, sollte das Augenmerk bei der Umsetzung einer Souveränitätsstrategie auf dem bewussten Management von Abhängigkeiten, der Förderung von Wettbewerb und der Auswahl vertrauenswürdiger Geschäftspartner mit Lösungen liegen, die einem Audit jederzeit standhalten. Digitale Souveränität, Cyberresilienz und IT-Security sind also untrennbar miteinander verbunden. Souveränität entsteht dann, wenn sichere, transparente und resiliente Systeme echte Wahlfreiheit schaffen, Abhängigkeiten gemanagt und Wettbewerbs- und Transparenzprinzipien konsequent verankert werden. •

Phillip Behre
Bild: Lisa Hantke

Richard Werner
Bild: Trend Micro

PAUL MOLL

Senior Field Marketing Manager Central Europe bei WatchGuard Technologies

• Natürlich beschäftigt sich WatchGuard als US-amerikanischer IT-Security-Anbieter mit starker Präsenz im europäischen Markt intensiv mit diesem Thema und will Unternehmen bei der digitalen Souveränität unterstützen. Lösungen müssen international integriert werden und wenn dies in der Cloud geschieht, taucht die Frage nach der Datenhoheit automatisch auf.

Tatsache ist: Cloud-Lösungen sind aus gutem Grund verstärkt auf dem Vormarsch, auch wir setzen ganz bewusst auf die Cloud. Der vermehrte Einsatz sorgt jedoch für zunehmende Komplexität und stellt viele Datenschützer hinsichtlich der Bewertung vor Herausforderungen. Umso mehr zählt Transparenz.

Dreiteilung der Datenschutzräume in Amerika, Europa und Asien

Bei WatchGuard verfolgen wir eine grundsätzliche Dreiteilung der Datenschutzräume in den Regionen „Amerika“ (AMER), „Europa“ (EMEA) sowie „Asien“ (APAC). Je nachdem, wo sich ein Unternehmen befindet, wählt es seinen Datenschutzraum aus, dessen Sphäre die Daten nicht verlassen. Die Cloud-Server für Europa befinden sich beispielsweise in Frankfurt am Main. Entsprechende Dokumentationen sind im WatchGuard Trust Center hinterlegt. So schlagen wir effektiv eine Brücke zwischen Cybersicherheit und dem Aspekt der Datenhoheit.

IT-Sicherheit und Souveränität in Einklang bringen

Da digitale Souveränität kein Produkt von der Stange ist, spielt zudem die Zusammenarbeit mit unseren Partnern eine entscheidende Rolle. Diese bringen viel Expertise mit und kennen die lokalen Gegebenheiten und Cloud-Bedenken der Unternehmen. Daher können sie einen zusätzlichen Beitrag dazu leisten, IT-Sicherheit und digitale Souveränität in Einklang zu bringen. •

PANTELIS ASTENBURG

Vice President Global Sales DACH bei Versa Networks

• Digitale Souveränität bedeutet, dass Unternehmen ihre Daten und IT-Systeme selbstständig, transparent und sicher kontrollieren können. Dieser Ansatz hat direkten Einfluss auf die Cybersicherheit: Wer seine digitalen Systeme eigenständig verwalten will, muss auch in der Lage sein, sie aktiv zu schützen.

Die digitale Souveränität fordert entsprechend mehr Transparenz und Kontrolle: Unternehmen müssen wissen, wo ihre Daten liegen, wer darauf zugreift und welche Abhängigkeiten zu Drittanbietern bestehen. Souveräne Cloud- und Infrastrukturangebote verringern dabei geopolitische Risiken und stärken Datenschutz und Compliance – besonders durch geringere Abhängigkeit von nicht-europäischen Anbietern. Statt „nur“ Angriffe abzuwehren, geht es stärker um Resilienz und Nachvollziehbarkeit in der gesamten digitalen Lieferkette.

Kombination von souveräner Cloud und europäischen Standards

Dabei ist die Kombination der Schlüssel zum Erfolg: Zero Trust als Sicherheitsgrundlage, souveräne Cloud-Modelle mit klar zugeordneter Datenhoheit und europäische Standards wie Gaia-X oder ISO 27001. Digitale Souveränität und Cybersicherheit gehören zusammen. Nur wer souverän über seine Infrastruktur verfügt, kann sie auch dauerhaft sicher betreiben – und umgekehrt wird Sicherheit erst durch Souveränität wirklich gewährleistet. •

Paul Moll
Bild: WatchGuard

Pantelis Astenburg
Bild: Versa

FLEXIBILITÄT UND SICHERHEIT

IN ALLEN NETZWERKFACETTEN

Der Schutz hybrider Arbeitsumgebungen erfordert ein Umdenken. Eine Möglichkeit ist die Technologie-Architektur Secure Access Service Edge (SASE). /// von Paul Moll

DEZENTRALE ARBEITSMODELLE SOWIE CLOUD-MIGRATIONEN SIND AN DER TAGESORDNUNG und somit rückt die Umstellung auf adäquate Security-Strategien für Unternehmen jeder Größe auf der Aufgabenliste immer weiter nach oben. Der Begriff SASE (Secure Access Service Edge) steht für eine Technologie-Architektur, die softwaredefinierte Netzwerkfunktionalität und einschlägige Sicherheitskontrollen cloudbasiert zusammenführt. Dass SASE im Zuge der digitalen Transformation eine Schlüsselrolle zukommt, steht außer Frage. Schließlich lässt sich dem aktuellen Wandel durch die Kombination von Internetkonnektivität und Sicherheit auf dem funktionalen Fundament mehrerer verschiedener grundlegender Netzwerk- und Cybersicherheitstechnologien wie Software-defined Wide Area Network (SD-WAN), Firewall-as-a-Service (FWaaS) und Zero-Trust Network Access (ZTNA) effektiv Rechnung tragen.

Secure Access Service Edge selbst ist jedoch kein Allheilmittel. Es gibt verschiedene Arten von SASE, und Details können darüber entscheiden, ob der gewählte Ansatz für ein Unternehmen geeignet ist oder nicht. Hybrid-SASE gewinnt in dem Zusammenhang als Lösungsoption klar an Bedeutung, denn der Aufwand beim Umstieg auf eine Zero-Trust-Zugriffsarchitektur, deren Kernstück SASE bildet, sollte keinesfalls unterschätzt werden. Eine Strategie mit kleinen, effektiven Schritten kann entscheidend zum Erfolg beitragen und genau hier gehen mit einem Hybrid-Angebot, das genau diese Zwischenschritte ermöglicht, Vorteile einher.

DER AUTOR
Paul Moll
Paul Moll ist Senior Field Marketing Manager Central Europe bei WatchGuard Technologies.
Bild: Watchguard

Die Fallstricke des klassischen Secure Access Service Edge
Ausschließlich cloudzentrierte SASE-Modelle greifen oftmals zu kurz. Denn der Anspruch auf Unternehmensseite besteht gerade im KMU-Umfeld vor allem darin, sowohl lokale als auch cloudbasierte Systeme einheitlich verwalten zu können. Viele Anbieter von SASE-Lösungen übersehen den Stellenwert nahtloser Prozesse im Hinblick auf die On-Premises-Strukturen. Dadurch lässt sich der Mehrwert von SASE nicht vollumfänglich ausspielen. Bei mangelnder Integration entstehen isolierte Systeme, die separat verwaltet werden müssen, was zu unnötiger Komplexität und zusätzlicher Belastung führt. Sobald eine SASE-Lösung nur auf die Cloud ausgerichtet ist, wird es für Unternehmen schwierig, das Sicherheitsniveau zu erhöhen und den geplanten Return on Invest zu erreichen. Wichtig ist also, dass sich eine SASE-Lösung ans Unternehmen anpasst.

Vorteile von Hybrid-SASE
Hybrid-SASE kombiniert Technologien aus mehreren Netzwerkarchitekturen, um alle entsprechenden Endpunkte sowie Ressourcen abbilden zu können. Auf diese Weise lässt sich höhere Sicherheit und ein verbessertes Management über vielfältige Umgebungen hinweg gewährleisten – egal ob es sich um Zero-Trust-Modelle, cloudbasierte oder traditionelle lokale, perimeterbasierte Strukturen handelt. Dank mehr Transparenz über alle Systeme und konsistenterer Sicherheitskontrollen fallen die Kosten in den Reihen von IT-Teams und Managed Service Providern (MSP) spürbar geringer aus.

Die Bereitstellung gestaltet sich ebenfalls einfach: Administratoren können Sicherheitsrichtlinien über eine einzige Schnittstelle konfigurieren und durchsetzen. Die Verwaltung erfolgt auf Grundlage einheitlicher Richtlinienstrukturen und Terminologie. Gerade für Unternehmen, die dabei sind, auf Zero-Trust-Konzepte umzustellen, liefert Hybrid-SASE eine optimale Lösung: Denn wer in der Lage ist, sowohl lokale als auch cloudbasierte Systeme zu verwalten, muss nach Abschluss der Zero-Trust-Umstellung keine zusätzliche Zeit, kein zusätzliches Budget und keine zusätzlichen Ressourcen für die Implementierung einer weiteren SASE-Lösung aufwenden. •

SMARTES ITSM BEGINNT MIT ZUVERLÄSSIGER KI

In unserer heutigen hypervernetzten Welt stehen IT-Verantwortliche einer doppelten Herausforderung gegenüber: Sie müssen die transformative Kraft künstlicher Intelligenz einführen und gleichzeitig die Daten ihres Unternehmens schützen. Während sich KI zunehmend vom Hype zur Realität entwickelt, sind Fragen der Datenhoheit und Compliance für europäische Organisationen zentral. /// von Santeri Jussila

DAS KLASSISCHE IT SERVICE MANAGEMENT, DAS AUF DIE MANUELLE BEARBEITUNG von Tickets setzt, stößt zunehmend an seine Grenzen. KI-gestützte Automatisierung eröffnet hier neue Möglichkeiten: Sie erkennt Muster, antizipiert Probleme und hilft, diese zu lösen, bevor sie die Produktivität der Nutzer beeinträchtigen. Gleichzeitig entlastet sie IT-Teams – durch schnellere Bearbeitungszeiten und durch einen intelligenten, kontextsensitiven Selbstservice, der die Benutzererfahrung verbessert.

Der Wandel vom reaktiven Ticketing-System hin zu intelligenten, proaktiven Abläufen ist entscheidend für ein zukunftsfähiges, intelligentes Service Management.

Wie dieser Wandel beginnen kann, zeigt das Beispiel einer europäischen Universität mit über 18.000 Nutzern aus 88 Ländern: Die IT-Abteilung stand täglich vor der Herausforderung, dass rund 30 Prozent der eingehenden E-Mails in Sprachen geschrieben waren, die die meisten Mitarbeiter nicht beherrschten, und Anfragen enthielten, die nicht IT-bezogen waren. Mithilfe eines kontextbasierten KI-Assistenten konnte das Team in Echtzeit Texte generieren, korrigieren und übersetzen. Besonders hilfreich bei dringenden Anfragen aber auch für weniger erfahrene IT-Agenten.

Das Ergebnis? Eine spürbare Qualitätssteigerung im (Self-)Service und eine Zeitersparnis von bis zu einem Arbeitstag pro Agent und Monat. Der Case zeigt, wie KI bestehende Prozesse entlastet und aktiv dazu beiträgt, Produktivität und Nutzerzufriedenheit zu steigern – und damit den Weg für eine neue Ära im Service Management ebnet.

Verantwortungsvolle KI bietet Sicherheit und Flexibilität

Doch IT-Entscheider stehen vor einem Dilemma: Laut einer Untersuchung der Bertelsmann Stiftung stammen rund 70 Prozent der weltweit eingesetzten KI-Grundmodelle aus den USA. Diese Dominanz steht im Spannungsfeld zu einem wachsenden Bedürfnis nach Datensicherheit und digitaler Souveränität – befeuert durch geopolitische Entwicklungen und Regularien wie den EU AI Act.

Zentrale Aspekte bei der Wahl der KI

Europäische Organisationen, die das Potenzial von künstlicher Intelligenz nutzen und den Weg zu einem proaktiven Service Management einschlagen wollen, sollten bei der Auswahl ihrer Anbieter vier zentrale Aspekte berücksichtigen: die Herkunft sowie den Betrieb der Lösung, ihre Wertekompatibilität, die Kontrolle über Daten und die Flexibilität im Einsatz.

Denn KI darf kein Selbstzweck sein: Sie muss die unternehmenseigenen Standards respektieren und gleichzeitig echten Mehrwert schaffen.

Ob künstliche Intelligenz IT und Geschäftsprozesse wirksam transformiert, hängt nicht allein vom technologischen Einsatz ab, sondern von der Fähigkeit, sie verantwortungsvoll einzusetzen – für ein intelligentes Service Management, das Produktivität steigert, Nutzer überzeugt und die digitale Souveränität aktiv stärkt. •

> „Der Wandel vom reaktiven Ticketing-System hin zu intelligenten, proaktiven Abläufen ist **entscheidend für ein zukunftsfähiges, intelligentes Service Management**."
>
> *Santeri Jussila*

DER AUTOR
Santeri Jussila
ist Chief Product Officer bei Matrix42.
Bild: Matrix42

INTEGRATION
IST DER NEUE SCHLÜSSEL IN DER CYBERSECURITY

Die IT-Sicherheitslandschaft vieler Unternehmen gleicht einem Puzzle aus Einzellösungen. Über Jahre wurden für jede neue Bedrohung eigene Tools eingeführt. Doch Sicherheit sollte man als System sehen – nicht als Sammlung. Denn konsolidierte Systeme bieten nicht nur mehr Sicherheit, sondern auch mehr Effizienz.l /// von Thorsten Henning

VIELE UNTERNEHMEN VERFÜGEN ÜBER ZAHLREICHE SECURITY-TOOLS: Firewalls, Endpoint-Schutz, Cloud-Gateways, Monitoring-Systeme. Zwar erfüllt jede Komponente ihren Zweck, doch das Zusammenspiel ist oft brüchig. Schnittstellen, Überschneidungen und manuelle Prozesse schaffen nicht nur Ineffizienzen, sondern auch neue Angriffsflächen.

Diese Komplexität ist zu einem der größten Cybersecurity-Risiken geworden. Wenn Alarme aus mehreren Quellen erst manuell korreliert werden müssen, verlängert das Reaktionszeiten – genau in dem Moment, in dem Angreifer jede Millisekunde ausnutzen. Hinzu kommen steigende Betriebskosten, Fachkräftemangel und der wachsende Druck, hybride und Cloud-Umgebungen zuverlässig abzusichern.

Security und Netzwerk wachsen zusammen

Immer mehr Unternehmen erkennen: Mehr Tools bedeuten nicht automatisch mehr Cybersecurity. Der Fokus liegt deshalb auf Konsolidierung, also dem Übergang von vielen isolierten Einzellösungen zu integrierten Plattformen, die Netzwerke und Sicherheit eng verzahnen. Eine konsolidierte Architektur reduziert nicht nur den Verwaltungsaufwand, sondern schafft Transparenz und Konsistenz. Wenn Security-Funktionen über ein gemeinsames Betriebssystem, einheitliche Richtlinien und eine zentrale Datenbasis gesteuert werden, lassen sich Bedrohungen schneller erkennen und bekämpfen.

Die klassische Trennung zwischen Netzwerkbetrieb und Sicherheitsarchitektur hat ausgedient. Moderne Ansätze wie Secure Access Service Edge (SASE) oder Secure SD-WAN führen beide Welten in einer gemeinsamen Plattform zusammen. So entsteht ein System, das Datenverkehr steuert, überwacht und absichert – unabhängig davon, ob Benutzer im Büro, zu Hause oder in der Cloud arbeiten. Fortinet spricht in diesem Zusammenhang von einer Security Fabric, die alle Komponenten eines Unternehmensnetzwerks miteinander verknüpft. Im Mittelpunkt steht dabei eine gemeinsame Betriebsebene, auf der Netzwerk, Security-Funktionen und Analysen nahtlos zusammenarbeiten. Das Ziel: weniger Komplexität, konsistente Richtlinien und ein ganzheitlicher Schutz über alle Umgebungen hinweg.

Sicherheit als System, nicht als Sammlung

Konsolidierte Systeme bieten nicht nur mehr Sicherheit, sondern auch mehr Effizienz. Eine gemeinsame Verwaltungsoberfläche und einheitliche Automatisierungsfunktionen entlasten IT-Teams, vereinfachen Updates und verhindern Konfigurationsfehler. KI-gestützte Analysen können auf konsistente Telemetriedaten zugreifen und so präziser reagieren.

Angesichts verteilter Infrastrukturen, KI-gestützter Angriffe und steigender Compliance-Anforderungen führt an einem integrierten Cybersecurity-Ansatz kaum ein Weg vorbei. Wer auf gewachsene, uneinheitliche Architekturen setzt, erkauft sich kurzfristige Flexibilität auf Kosten der Stabilität. Eine konsolidierte Plattformstrategie funktioniert hingegen wie ein geschlossenes System: Sie verbindet Netzwerke, Clouds und Benutzer über einheitliche Steuerungslogik, anstatt sie nur lose zu verknüpfen. Cybersecurity entwickelt sich damit von vielen einzelnen Abwehrmechanismen hin zu einer konsistenten, intelligenten Verteidigungslinie. •

DER AUTOR
Thorsten Henning
ist Regional Director Pre-Sales and Business Development DACH bei Fortinet.
Bild: Fortinet

> „ Immer mehr Unternehmen erkennen: Mehr Tools bedeutet nicht automatisch mehr Cybersecurity. *Thorten Henning*

Blindflug mit Algorithmus:

Wenn fehlendes KI-Wissen zum Risiko wird

Künstliche Intelligenz ist im Alltag angekommen. Doch häufig fehlt das Verständnis dafür, was sie eigentlich tut. Entscheidungen werden akzeptiert, Ergebnisse vertraut – Hauptsache, es funktioniert. Die EU will diesen Blindflug beenden: Mit der KI-Verordnung und einer neuen Pflicht zur „KI-Literacy" sollen Mitarbeiter Systeme kritisch hinterfragen. /// von Melanie Ludolph

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

Bild: Fieldfisher

KI-SYSTEME SIND LÄNGST KEINE REINEN TOOLS MEHR. Sie treffen Vorentscheidungen, priorisieren Aufgaben, filtern Informationen. Das Problem: Selbst gut geschulte Fachkräfte wissen oft nicht genau, nach welchen Regeln das passiert. Die Folge sind unbewusste Fehlerketten – von der Datenauswahl bis zur Ergebnisbewertung. Datenschutzrechtlich wird das brisant. Denn wer personenbezogene Daten in KI-Prozesse einspeist, trägt Verantwortung für deren Verarbeitung. Eine „automatische Entscheidung" entbindet niemanden von der Pflicht, sie nachvollziehbar zu machen. Ohne technisches Verständnis wird Compliance zur Glückssache.

Kompetenz statt Kontrollillusion

Die EU-Kommission will, dass Unternehmen ihre Belegschaften für KI sensibilisieren – technisch, rechtlich und ethisch. „KI-Literacy" lautet das Schlagwort. Es geht nicht darum, dass alle programmieren können, sondern darum, Risiken zu erkennen: Woher stammen Trainingsdaten? Wie transparent ist ein Modell? Welche Informationen verlassen das Unternehmen? Fehlt dieses Wissen, entstehen unbemerkt Haftungsrisiken. Etwa wenn ein Chatbot sensible Kundendaten speichert oder eine Analyse-Software diskriminierende Muster übernimmt. Unternehmen, die nur auf die vermeintliche Neutralität von Algorithmen vertrauen, übersehen schnell, dass Verantwortung nicht automatisiert werden kann.

Schulung ist keine Kür

Die gute Nachricht: KI-Kompetenz lässt sich vermitteln. Workshops, interne Leitlinien und Schulungen schaffen Bewusstsein für Chancen und Grenzen. Wer seine Mitarbeiter befähigt, KI-Ergebnisse kritisch zu prüfen, gewinnt mehr als nur Rechtssicherheit – nämlich Qualität in den Entscheidungen.

Das gilt besonders für Datenschutzbeauftragte, Compliance-Teams und Marketingabteilungen, die zunehmend mit KI-Systemen arbeiten. Ein fundiertes Grundverständnis verhindert Fehlkonfigurationen, Datenlecks oder unzulässige Automatisierungen.

Verantwortung bleibt analog

So smart KI-Systeme auch sind – die Verantwortung bleibt beim Menschen. Ein Algorithmus kennt keine Ethik, kein Urheberrecht, kein Datenschutzrecht. Er folgt Mustern, nicht Werten. Deshalb braucht digitale Verantwortung beides: Technologiekompetenz und Urteilsfähigkeit. Unternehmen, die das erkennen, handeln nicht nur regelkonform, sondern zukunftssicher. Denn wer versteht, wie KI funktioniert, kann sie besser steuern – und vermeidet, dass Innovation zur Blackbox wird.

Wissen ist die beste Absicherung

KI kann viel, aber sie nimmt uns nicht das Denken ab. Wer Systeme blind nutzt, läuft Gefahr, Verantwortung auszulagern – an Software, die selbst keine Verantwortung kennt. Der Weg aus dem Blindflug führt über Aufklärung, Schulung und Transparenz.

Denn am Ende gilt: Wer KI verstehen will, muss sie nicht fürchten, nur beherrschen. •

Mehr Zeit für Wertschöpfung

KI nimmt der Personalabteilung viel Arbeit ab: Dokumente, Fristen, Onboarding, Abstimmungen. Oliver Rozić (Sage) erklärt, warum erst integrierte KI mit Echtzeit-Zugriff auf HR-/Payroll-Daten messbaren Nutzen schafft – und wie Teams jetzt pragmatisch starten. /// von Heiner Sieger

Herr Rozić, Sie sagen, KI im HR steckt noch in den Kinderschuhen. Woran liegt das – Technologie, Daten oder Mindset?
Oliver Rozić | Von allem etwas. Der Reifegrad bleibt niedrig: Laut Kienbaum-Studie 2024 haben erst rund 20 Prozent der Unternehmen generative KI im HR-Bereich eingeführt, etwa 40 Prozent berücksichtigen sie in der HR-Strategie. In Gesprächen hören wir häufig: „Wir reden über KI, aber digitalisieren gerade erst Aktenordner." Es fehlt an Wissen, Sicherheit und Vertrauen. Seit Februar 2025 verpflichtet der EU AI Act zudem Anbieter und Anwender, KI-Kompetenz im Unternehmen nachzuweisen. Das beschleunigt den Kompetenzaufbau – ersetzt aber nicht die nötige Kultur- und Wissensarbeit.

Ist der technische Fortschritt denn schon weit genug – oder scheitert es an den Daten?
OR | Die Modelle sind leistungsfähig. Entscheidend ist der Anschluss an Unternehmensdaten. Ohne saubere, aktuelle Daten liefert KI nur generische Antworten. Ein Beispiel: Eine Präsentation zum Gender Pay Gap in Deutschland erstellt ein Modell problemlos. Will ich aber die Gehaltsunterschiede in meinem Unternehmen analysieren, braucht die KI Zugriff auf interne, korrekte und vollständige Daten. Genau hier liegt oft das Problem: Die Schnittstellen zwischen KI und HR-Daten fehlen oder sind unzureichend.

Was müssen Unternehmen konkret tun, um KI in HR nutzbar zu machen?
OR | Daten aufbereiten, integrieren und eine sichere Verbindung zur KI herstellen. Viele aktuelle HR-Chatbots sind mit FAQs manuell gefüttert und nicht direkt mit der HR-Software verbunden. Das hilft bei Standardfragen, scheitert aber bei individuellen Anliegen, etwa einer Gehaltsabrechnung. Payroll-Daten ändern sich monatlich und sind hochsensibel – dafür braucht es einen eingebetteten, berechtigten Echtzeitzugriff. Erst wenn KI und HR-/Payroll-Systeme direkt sprechen, entsteht echter Nutzen.

In welchen HR-Bereichen sehen Sie kurzfristig die größten Effizienzgewinne?
OR | Erstens in der Administration und Dokumentenarbeit: Stammdatenpflege, Bescheinigungen, Verträge, Zeugnisse, Stellenausschreibungen – alles regelbasiert, ideal für KI. Zweitens in der Prozessautomatisierung: Fristen prüfen, Erinnerungen senden, fehlende Zeiten einholen, Onboarding orchestrieren – vom Terminplan bis zur Hardware-Bestellung. Drittens bei der Anomalieerkennung in der Gehaltsabrechnung: Ausreißer oder Plausibilitäten identifizieren, bevor Fehler passieren. Viertens in der Talententwicklung: Mit angebundenen Daten macht KI personalisierte Lernvorschläge und identifiziert Kompetenzlücken.

Viele Anbieter werben mit „KI drin". Was unterscheidet eine integrierte von einer aufgesetzten Lösung?
OR | Aufgesetzte Lösungen arbeiten oft mit statischen, manuell gepflegten Wissensbeständen. Nützlich, aber begrenzt. Integrierte KI sitzt im HR-System, kennt Berechtigungen, nutzt aktuelle Mitarbeiter-, Policy- und Payroll-Daten. Dann kann sie etwa eine Frage zur individuellen Abrechnung beantworten, Abweichungen erklären, Dokumente korrekt befüllen und Prozessschritte automatisiert anstoßen. Ohne Dateneinbettung bleiben Antworten generisch – und Nutzen und Vertrauen somit gering.

> „ KI ersetzt keine HR-Rollen, aber übernimmt sachbearbeitende Tätigkeiten. Dafür müssen HR und IT enger zusammenarbeiten; manche Unternehmen denken über organisatorische Zusammenführungen nach. Wer diesen Wandel aktiv gestaltet, löst sich vom Bild der reinen Verwaltung und positioniert **HR als strategischen Business Partner**. *Oliver Rosić*

DER GESPRÄCHSPARTNER
Oliver Rozić
ist Vice President Product Management bei Sage und verantwortet die internationale Business Unit HR & Payroll. Er treibt Produktentwicklung, Strategie und Marktausrichtung der HR- und Lohnlösungen voran. Als Sprecher und Autor setzt er sich für den praxisnahen, ethischen Einsatz von KI in HR ein.

Welche technische Entwicklung hat diese Integration erst möglich gemacht?
OR | Bis vor Kurzem fehlte ein Standard, der KI sicher und effizient mit externen Daten verbindet. Das ändert der offene Model Context Protocol (MCP) Standard. Er fungiert wie ein „USB-Stecker" für KI: Statt für jeden Use Case eigene Datenverknüpfungen zu bauen, bietet MCP eine einheitliche, skalierbare Anbindung von Tools und Datenquellen. Für Entwickler beschleunigt das die Umsetzung erheblich – inklusive klar definierter Rechte- und Sicherheitsmodelle.

Wo drückt HR-Teams denn der Schuh derzeit am meisten?
OR | Da gibt es einige wunde Punkte, um im Bild zu bleiben: Hohe Last durch Verwaltungsaufgaben, sinkende Motivation, bis hin zu Burnout-Risiken. Viele HR-Abteilungen werden als reine Administration wahrgenommen und kommen kaum zu strategischen Themen. In einer unserer Studien sagten rund 80 Prozent, sie wünschten sich weniger Prozesse und mehr Fokus auf Strategie und Menschen. Genau dort setzt KI an: Sie nimmt Routinearbeit ab, reduziert Fehler und schafft Zeitfenster für Wertschöpfung.

Bedeutet das in der Konsequenz auch eine Neudefinition der HR-Rolle?
OR | Auf jeden Fall – vor allem hin zu mehr Strategie, Organisationsentwicklung und People-Themen. KI ersetzt keine HR-Rollen, aber übernimmt sachbearbeitende Tätigkeiten. Dafür müssen HR und IT enger zusammenarbeiten; manche Unternehmen denken über organisatorische Zusammenführungen nach. Wer diesen Wandel aktiv gestaltet, löst sich vom Bild der reinen Verwaltung und positioniert HR als strategischen Business Partner.

Wie sieht Ihr aktueller Produktfahrplan aus – was können Unternehmen in Deutschland von Sage in nächster Zeit erwarten?
OR | In Großbritannien ist Sage Business Cloud Payroll mit KI-gestützter Anomalieerkennung seit Kurzem live. Für Deutschland planen wir ähnlich priorisiert: KI zur Erkennung von Ausreißern in der Lohnabrechnung. In Sage HR haben wir die KI-gestützte Dokumentenerstellung vorbereitet – Stellenbeschreibung, Vertrag oder Bescheinigung aus dem System heraus, auf Basis aktueller Daten, mehrsprachig und in passender Tonalität. Ebenfalls in Arbeit: ein KI-gestütztes Onboarding, das neue Mitarbeitende strukturiert durch die ersten Wochen führt. Die Rollouts sind für das kommende Jahr geplant.

Wo ziehen Sie Grenzen beim KI-Einsatz in HR – insbesondere mit Blick auf Fairness, Datenschutz und Transparenz?
OR | HR arbeitet mit besonders sensiblen Daten. Für Aufgaben wie Ethisches Urteilsvermögen, Konfliktlösung, Führungskräfte-Coaching, Kulturarbeit – dafür ist KI nicht geeignet. Juristisch gilt: Die DSGVO verbietet, Menschen ausschließlich automatisierten Entscheidungen zu unterwerfen, die rechtliche Wirkung entfalten. KI darf somit nicht über Einstellungs- oder Entlassungsentscheidungen befinden. Der EU AI Act konkretisiert zudem Transparenz- und Governance-Pflichten. Unternehmen sollten klare Leitlinien definieren, einen Ethikbeirat einbinden und die KI-Literacy des Personals nachweisbar erhöhen.

Was raten Sie einem HR-Team, das morgen mit dem Einsatz von KI starten will?
OR | Klein anfangen, schnell lernen. Ein datennaher, risikoarmer Use Case ist ideal: Dokumentenerstellung, Fristenmanagement oder Anomalie-Alerts in definierten Prozessschritten. Parallel Datenqualität und Berechtigungen klären, die Anbindung via Standard (z. B. MCP) planen, rechtliche Leitplanken setzen – und von Anfang an die Mitarbeitenden qualifizieren. So werden aus Pilotprojekten rasch skalierbare Routinen mit messbarem Nutzen. •

KI zwischen Entlastung und Bedrohung

Die Crux der gefühlten zwei Unternehmenskulturen: Was Frontline-Beschäftigte in Deutschland jetzt bewegt. /// von Russell Howe, Group Vice President EMEA bei UKG

DIE LAGE AN DER FRONTLINE IST EIN SEISMOGRAF FÜR DIE WIRTSCHAFTLICHE UND KULTURELLE STABILITÄT VON UNTERNEHMEN. Beschäftigte im Handel, in der Pflege, in der Produktion oder im Kundenservice sind die ersten, die Überlastung und strukturelle Defizite spüren. Die aktuelle Global Frontline Study von UKG, Anbieter für Human Capital Management, HR Service Delivery und Workforce Management, zeigt: Die Situation in Deutschland ist angespannt – und die Rolle von künstlicher Intelligenz (KI) wird dabei zwiespältig gesehen.

Zwischen Überlastung und Unzufriedenheit

70 Prozent der Befragten fühlen sich zumindest zeitweise ausgebrannt, 20 Prozent sogar oft oder dauerhaft. Mehr als ein Viertel sucht aktiv nach einer neuen Stelle, vor allem wegen niedriger Bezahlung, ungünstiger Arbeitszeiten und negativer Auswirkungen auf das Wohlbefinden. 40 Prozent sind mit ihrer Employee Experience insgesamt unzufrieden, also mit den Rahmenbedingungen, die ihr Arbeitgeber für ihre Arbeit schafft. Jeder Zweite sagt zudem, er müsse besonders lange arbeiten, um finanziell über die Runden zu kommen. Besonders alarmierend: 41 Prozent erleben zwei Unternehmenskulturen – eine für die Frontline, eine für alle anderen. Dieses Gefühl „zweiter Klasse“ schwächt nicht nur die Loyalität, sondern auch die Qualität der Kundeninteraktion.

KI als Hoffnungsträger – und als Risiko

Bezüglich der Rolle von KI zeigt die Studie ein ambivalentes Bild: Einerseits vertrauen über 80 Prozent einer KI, wenn es um faire Schichtplanung, fehlerfreie Gehaltsabrechnungen oder verständliche Zusammenfassungen von Richtlinien geht. Andererseits befürchten 41 Prozent, dass KI die Kundenerfahrung verschlechtern könnte. Und 80 Prozent halten es für einen schweren Fehler, Frontline-Mitarbeitende durch KI zu ersetzen.

Bemerkenswert ist auch: Für 79 Prozent hatte KI bislang keinerlei Einfluss auf den Arbeitsalltag. Die hohen Erwartungen an Entlastung stehen also bisher ungenutzten Möglichkeiten gegenüber.

Die entscheidende Weichenstellung

Ob KI als Partner oder als Bedrohung wahrgenommen wird, hängt davon ab, wie Unternehmen sie einsetzen. Sie kann helfen, Arbeitszeitplanung fairer zu gestalten, Routinen in der Personalabteilung zu übernehmen und Führungskräften Zeit für den Dialog mit ihren Teams zu verschaffen. Entscheidend ist, dass KI nicht als reines Sparinstrument gesehen wird, sondern als Werkzeug, Arbeit menschlicher zu machen.

Die Frontline ist das Gesicht eines Unternehmens. Wer hier Burnout, Unzufriedenheit und kulturelle Spaltung ignoriert, riskiert nicht nur höhere Fluktuation, sondern auch Einbußen bei Servicequalität und Kundenbindung. Umgekehrt eröffnet der verantwortungsvolle Einsatz von KI Chancen: Prozesse werden effizienter, Mitarbeitende entlastet, Wertschätzung sichtbar. Die Global Frontline Study macht deutlich: Der größte Erfolg entsteht dort, wo Technologie und Menschen zusammenspielen. •

DER AUTOR
Russell Howe
ist Group Vice President EMEA bei UKG.

> „ Besonders alarmierend: 41 Prozent erleben zwei Unternehmenskulturen – eine für die Frontline, eine für alle anderen. Dieses **Gefühl „zweiter Klasse“** schwächt nicht nur die Loyalität, sondern auch die Qualität der Kundeninteraktion.
>
> *Russell Howe*

Vom Papier zum smarten Workflow:

Die Rolle von KI im Mittelstand

Für kleine und mittelständische Unternehmen beginnt die digitale Transformation oft mit einer zentralen Frage: Wie können wir mit weniger mehr erreichen? Die Antwort lautet immer häufiger: KI und Automatisierung – nicht über komplexe Infrastrukturen, sondern über cloudbasierte Tools, die sich leicht einführen, verwalten und bezahlen lassen. Dabei geht es nicht nur darum, alte Systeme gegen neue auszutauschen. Es geht darum, Arbeitsabläufe neu zu denken. /// von Michael Bochmann

DER AUTOR
Michael Bochmann
ist Chief Product & Technology Officer bei Docuware.
Bild: Docuware

FÜR KMUS SIND KI-GESTÜTZTE TECHNOLOGIEN wie Intelligent Document Processing (IDP) und Workflow-Automatisierung längst zum Kern effizienter Geschäftsabläufe geworden. Sie ersetzen manuelle Dateneingaben, beschleunigen Genehmigungsprozesse und minimieren Fehlerquellen. Was früher Stunden beanspruchte, ist heute oft in Sekunden erledigt. Mitarbeiter verbringen dadurch weniger Zeit mit Routineaufgaben und können sich als Resultat wertschöpfenderen Tätigkeiten widmen.

Transformation mit System

Doch die reine Digitalisierung, wie etwa das bloße Scannen von Dokumenten, reicht nicht aus, um langfristig wettbewerbsfähig zu bleiben. Eine echte Transformation entsteht erst, wenn Unternehmen KI systematisch einsetzen, um Entscheidungen datenbasiert zu treffen. Fortschrittliche KMUs nutzen dafür cloudbasierte Plattformen, die keine umfangreiche IT-Infrastruktur erfordern. Mit No-Code-Werkzeugen, KI-Assistenten und Echtzeit-Analysen können Fachabteilungen Automatisierungen eigenständig konfigurieren, ohne lange auf Entwicklerressourcen warten zu müssen.

Das senkt die Einstiegshürde erheblich und stellt sicher, dass die gewählten Lösungen sowohl budget- als auch wachstumsfreundlich bleiben. Transformation ist dabei kein punktuelles Projekt, sondern eine fortlaufende Reise. Rahmenbedingungen, Märkte und Kundenerwartungen ändern sich ständig – und mit ihnen die technologische Agenda. Erfolgreiche KMUs hinterfragen daher regelmäßig ihre Systeme und Prozesse: Werden Datenquellen optimal genutzt? Entspricht der Workflow den heutigen Compliance-Vorgaben? Auf Grundlage solcher Fragen lassen sich Lücken identifizieren und priorisieren. Ein iterativer Ansatz schafft Raum für Experimente, liefert aber zugleich belastbare Kennzahlen, mit denen sich Fortschritte belegen lassen.

KI-basierte Lösungen sorgfältig integrieren

Entscheidend ist eine Unternehmenskultur, die Veränderungen nicht nur zulässt, sondern aktiv fördert. Klare Ziele schaffen Orientierung. Werden diese Ziele messbar definiert, kann das Team die passende Technologie gezielt auswählen und ihren Beitrag zum Ergebnis eindeutig nachweisen. Schulungen, interdisziplinäre Projektteams und ein offener Austausch über Erfolge wie auch Misserfolge stärken das gemeinsame Lernen: ein Schlüsselfaktor, wenn Innovation Teil der täglichen Arbeit werden soll.

Sorgfältig integrierte KI übertrifft dabei den Nutzen isolierter Einzellösungen: Wenn IDP beispielsweise direkt mit dem ERP-System kommuniziert, sind Datensätze sofort konsistent. Solche End-to-End-Automatisierungen senken Kosten, erhöhen die Transparenz und machen Unternehmen resilienter gegenüber Marktvolatilität. Damit wächst nicht nur die Effizienz, sondern auch die Fähigkeit, Chancen schneller zu erkennen.

Kurzum:

KI ist für KMUs kein Zukunftsversprechen, sondern ein pragmatischer Hebel, um mit begrenzten Ressourcen mehr Wirkung zu erzielen. Wer kontinuierlich evaluiert, kleine Pilotprojekte skaliert und die Mitarbeiter mitnimmt, verwandelt technologische Möglichkeiten in nachhaltigen Geschäftserfolg. •

Keine Medienbrüche mehr im Steinbruch

Eine von Medienbrüchen geprägte Software-Infrastruktur war bei dem Rottweiler Maschinenbauer AMR GmbH lange der Grund dafür, dass aktuelle Geschäftskennzahlen fehlten und viele Prozesse manuell erfolgten. Dies änderte sich mit der Einführung eines durchgängigen ERP-Systems, das auf die speziellen Anforderungen der Einzelfertigung zugeschnitten ist. /// von Axel Schmidhäuser

DIE AMR GMBH IST SPEZIALISIERT AUF DIE HERSTELLUNG KUNDENINDIVIDUELLER MASCHINEN, Anlagen und Komplettlösungen, die beim Abbau und der Aufbereitung mineralischer Rohstoffe wie Schotter, Kalkstein, Zement oder Gips zum Einsatz kommen. Das Leistungsspektrum des weltweit agierenden Unternehmens reicht von der Beratung, Planung und Projektierung über die Konstruktion, Fertigung und Montage bis hin zur Wartung und zum Ersatzteil- und Service-Geschäft der teilweise tonnenschweren Vorbrechanlagen.

Die Internationalisierung des schwäbischen Familienunternehmens nahm spätestens mit dem Eintritt von Berit Müller (4. Generation) in die Geschäftsführung im Jahr 2001 richtig an Fahrt auf. Zugleich konnte der jährliche Umsatz kontinuierlich auf heute bis zu 18 Millionen Euro gesteigert werden. Infolge des sich dadurch ausweitenden Projektgeschäfts wurde jedoch irgendwann das Fehlen automatisch ineinandergreifender Abläufe immer offensichtlicher.

Dies lag vor allem an der damaligen Geschäftssoftware, die funktional zu sehr auf den kaufmännischen Bereich ausgerichtet war und zudem nicht an die benachbarten Systeme für CAD (Autodesk Vault) oder das Finanzwesen (Datev) angebunden war. Relevante Kennzahlen zur aktuellen Kostenentwicklung konnte sie nicht bereitstellen.

DER AUTOR
Axel Schmidhäuser
ist Leading Expert bei ams.Solution.
Bild: ams.solution

Alte Software-Landschaft zu limitiert

Berit Müller berichtet, dass ihre Angebots- und Projektkalkulation zu weiten Teilen auf Schätzungen beruhte, was sie angesichts der mehrmonatigen Durchlaufzeiten und der hohen Investitionsvolumina als nicht mehr tragbar ansah. Dass AMR mit der früheren Arbeitsweise an deutliche Grenzen gestoßen war, bestätigt der Einkaufsleiter Tobias Reisbeck: „Unsere Software war nicht in der Lage, vielschichtige Stücklistenebenen darzustellen. Noch gravierender war, dass es wegen der begrenzten Prozessabdeckung und der fehlenden Schnittstellen keinen abteilungsübergreifenden Datenfluss gab. Deshalb musste etwa unsere Arbeitsvorbereitung die CAD-Stücklisten immer händisch übertragen." Für ihn stand damit ebenso wie für Berit Müller fest, dass der Umstieg auf ein integriertes System mit stärkerem Branchenfokus unumgänglich war.

Eine konkrete Vorstellung davon, wie das neue System beschaffen sein sollte, erhielt Tobias Reisbeck während des Besuchs einer Praxisveranstaltung, auf der das ERP-System der ams.Solution AG ausführlich vorgestellt wurde. Die Präsentation des Leistungsumfangs überzeugte ihn, speziell mit Blick auf das Buchungsverhalten, die Materialdisposition und die Stücklistenverwaltung. Dabei war der Zuschnitt der Software auf die besonderen Belange eines Einzelfertigers wie AMR immer sichtbar. Schnell waren sich die Verantwortlichen darüber einig, die bisherigen Defizite in der Projektabwicklung mit ams.erp beheben zu können. Die Entscheidung für die Implementierung fiel im Herbst 2020.

Dass es bis zum Echtstart danach noch ca. anderthalb Jahre dauerte, lag daran, dass der kurzfristig mögliche Umzug an einen neuen Firmenstandort Vorrang hatte. Der positive Nebeneffekt des nachgelagerten ERP-Projekts bestand jedoch darin, dass an dem neuen Standort von Beginn an ein logistisch sauberer Durchlauf etabliert

> „ Die Bestandsführung gestaltetet sich **viel strukturierter**, auch die Inventur wurde deutlich erleichtert.
>
> *Axel Schmidhäuser*

Seit 2022 konstruiert und fertigt die AMR GmbH ihre kundenindividuellen Maschinen, Anlagen und Komplettlösungen für die Bergbauindustrie an ihrem neuen Standort außerhalb Rottweils.
Bild: AMR

Gefertigt werden unter anderem Kettenförderer, Schubaufgeber, Plattenbänder, Backenbrecher, Rollenroste sowie sogenannte Fingerrollenroste zur Aufbereitung von stark verunreinigtem Siebschutt.
Bild: AMR

wurde, den die ams-Berater ebenso sauber im System abbilden konnten. Dies zeigt sich u.a. bei der Lagerverwaltung, wo seit der ERP-Implementierung Barcode-Scanner zum Einsatz kommen. Neben dem Blechlager wird auch das Kleinteilelager mit seinen Kardex-Regalen über ams.erp verwaltet und mittels der Handscanner ein- und ausgebucht. Dadurch gestaltetet sich die Bestandsführung viel strukturierter, auch die Inventur wurde deutlich erleichtert.

Datendurchgängigkeit sorgt für Transparenz

Für Einkaufsleiter Tobias Reisbeck liegt der entscheidende Vorteil der neuen Software in der Durchgängigkeit der Daten, die erstmals einen Überblick über den gegenwärtigen Stand der Auftragsabwicklung verschafft. Die Logik der durchgehenden Datenhaltung erforderte allerdings die Abkehr von einigen gewohnten Arbeitsweisen. Während es früher beispielsweise gängige Praxis war, Rechnungen im Nachhinein anpassen zu können oder einen Auftrag nach dem Schreiben der Rechnung noch einmal komplett umzustellen, lassen sich Rechnungen heute immer erst nach Auftragsabschluss anfertigen. Darüber hinaus ist erstmals für jede Auslieferung ein Lieferschein obligatorisch. Dadurch erhöht sich die übergreifende Prozesssicherheit immens.

Als spürbare Erleichterung erachtet der Einkaufsleiter die automatisierte Schnittstelle zum CAD-System, die die kompletten Stücklisten direkt in ams.erp überträgt. Ebenso wichtig ist für ihn die systemgestützte Materialdisposition. Die Vorgänger-Software besaß keinerlei Materialwirtschaft, sodass am Jahresende rückwirkend ausgebucht werden musste – mit der entsprechenden Fehleranfälligkeit. Aus Sicht von Geschäftsführerin Berit Müller stechen die vielfältigen Kalkulationsmöglichkeiten heraus. Die Angebotskalkulation läuft heute komplett über das System, wodurch die Angebote viel genauer sind als zuvor, als die einzelnen Positionen zur Maschinenauslegung oder zum Material in langen Excel-Listen verglichen wurden. „Früher haben wir Pi mal Daumen gerechnet, wohingegen wir nun mit Kostenstellen, Kostenarten sowie Zuschlagsätzen arbeiten“, so die Firmenchefin.

Exakte Kalkulation statt Schätzungen

Dank der exakten mitlaufenden Kalkulation verfügt sie im späteren Projektverlauf jederzeit über tagesaktuelle Kennzahlen, während sie die Wirtschaftlichkeit von Aufträgen zuvor immer erst nach deren Abschluss nachvollziehen konnte. Dies war vor allem in langlaufenden Projekten im Drei- oder Vier-Millionen-Euro-Bereich risikoreich. „Wenn ich demgegenüber heute im Projektverlauf abzusehende Mehrkosten erkenne, kann ich beispielsweise das Gespräch mit den Auftraggebern zu suchen, wenn für nachträgliche Änderungen zusätzliche Kosten anfallen“, führt Berit Müller aus.

Derlei kundenbedingte Änderungen im laufenden Fertigungsprozess kommen regelmäßig vor und werden über die Funktionalität der wachsenden Stückliste aufgefangen, die die neue ERP-Software von Hause aus mitbringt. Das Arbeiten mit mehreren Stücklistenebenen und die Möglichkeit des konstruktionsbegleitenden Anpassens der Stücklisten bringen laut der Firmenchefin immense Vorteile mit sich. •

Cloud-ERP auf dem Prüfstand:

Argumente für die Transformation

Die Transformationsstudie 2025 von NTT DATA Business Solutions zeigt: Mehr als die Hälfte der Unternehmen verlagert ihre Anwendungen inzwischen in die Cloud. Gerade ERP-Systeme geraten bei dieser Entwicklung ins Visier der Entscheider. Aber ist der IT-Trend die beste Lösung? Diese Kriterien sind entscheidend. /// von Jens Claes

UNTERNEHMEN STEHEN VOR DER HERAUSFORDERUNG, IHRE GESCHÄFTSMODELLE in einer komplizierten Gemengelage zukunftssicher aufzustellen. Fachkräftemangel, Preisdruck, technologische Quantensprünge und dynamische Marktentwicklungen prägen den Wunsch, Strukturen flexibler und effizienter zu gestalten. Gleichzeitig wird der Zugang zu Innovationen wichtiger. Die Cloud gilt als Wegbereiter und Voraussetzung – der Migrationsdruck wächst, auch bei ERP-Systemen.

Doch nicht für jede Organisation ist der Wechsel ins Public-Cloud-ERP gleich sinnvoll. Wer schnell skalieren möchte, rasch neue Märkte oder Geschäftsmodelle erschließt oder auf aktuelle Technologien wie KI und Automatisierung angewiesen ist, findet in der Public Cloud die nötige Agilität und den Zugang zu Innovationen. Ebenso eignen sich Public-Cloud-Lösungen für Unternehmen, die auf standardisierte Best-Practice-Prozesse setzen, wenig Individualentwicklungen benötigen und Wert auf eine schnelle Einführung legen.

Dem gegenüber stehen Unternehmen, für die maximale Kontrolle, tiefgreifende Individualisierung und spezifische Compliance-Anforderungen im Vordergrund stehen. Wer auf komplexe, historisch gewachsene Prozesse zwingend angewiesen ist oder regelmäßig individuelle Anpassungen am ERP-System vornehmen muss, kann mit einem Public-Cloud-ERP an Grenzen stoßen. Auch wenn Datenschutz oder regulatorische Vorgaben ein Höchstmaß an Datensouveränität verlangen – etwa in hochregulierten Branchen –, kann eine Private Cloud die bessere Wahl sein.

Prozesse, Kosten und Skalierung – was wirklich zählt

Im Detail zeigt sich: Unternehmen mit dynamischen Geschäftsmodellen und sich schnell ändernden Anforderungen profitieren besonders von Public-Cloud-ERP-Lösungen. Sie können neue Funktionen und Prozesse zügig ausrollen, profitieren von regelmäßigen Updates und zahlen nur für die tatsächlich genutzten Leistungen.

DER AUTOR
Jens Claes
ist Head of Division New Business bei NTT DATA Business Solutions

Gerade für wachsende Mittelständler oder international aufgestellte Firmen ist diese Flexibilität ein echter Wettbewerbsvorteil.

Wer hingegen auf komplexe Eigenentwicklungen oder eine hohe Integrationstiefe in bestehende IT-Landschaften angewiesen ist, sollte genau prüfen, ob die Standardprozesse der Public Cloud genügen. Denn individuelle Anpassungen sind im Public-Cloud-Modell eingeschränkt möglich – und können zu erhöhtem Aufwand, höheren Folgekosten und Kompromissen führen.

Auch beim Kostenfaktor gilt: Die Public Cloud liefert Transparenz und Planbarkeit durch abonnementbasierte Preismodelle. Für Unternehmen mit klar umrissenen, eher standardisierten Prozessen ist das die bessere Wahl – insbesondere dann, wenn man die IT-Investitionen in wirtschaftlichen Mehrwert umwandeln kann. Wer das jedoch nicht kann und noch dazu regelmäßig Anpassungen oder Zusatzleistungen benötigt, sollte die Gesamtkosten sorgfältig kalkulieren.

Compliance & Innovation – Chancen und Grenzen

Ein weiterer Schlüsselfaktor ist die Compliance. Public-Cloud-ERP-Anbieter bieten umfassende Sicherheits- und Compliance-Frameworks, regelmäßige Audits und automatisierte Updates, die den gesetzlichen Anforderungen in vielen Branchen gerecht werden. Wer jedoch hohe Datenschutzanforderungen oder lokalen Vorgaben erfüllen muss, wie z. B. Player im Pharma- oder Finanzsektor, sollte genau prüfen, ob die Cloud-Option alle regulatorischen Vorgaben erfüllt. Für diese Unternehmen können hybride oder private Cloud-Modelle die notwendige Sicherheit bieten.

Auf der Innovationsseite hingegen punkten Public-Cloud-ERPs mit der schnellen Verfügbarkeit neuer Features, etwa im Bereich KI, prädiktive Analytik oder Automatisierung. Unternehmen, die von diesen Technologien profitieren möchten, erhalten über die Cloud einen direkten Zugang zu Innovationen – ohne lange Implementierungs- oder Updatezyklen. Ein E-Commerce-Unternehmen beispielsweise kann mit Cloud-ERP binnen weniger Wochen neue Märkte anbinden und direkt KI-gestützte Prognosen einsetzen.

Branchenkompetenz und Support – ein unterschätztes Kriterium

Nicht zuletzt spielt die Branchenkompetenz des Anbieters eine zentrale Rolle. Public-Cloud-ERPs wie GROW with SAP bieten heute bereits zahlreiche branchenspezifische Best Practices und Support-Services. Unternehmen, die auf standardisierte Prozesse setzen und internationale Unterstützung benötigen, profitieren davon besonders. Wer jedoch sehr spezifische Branchenanforderungen hat, sollte die verfügbaren Funktionen und Services genau prüfen, um keine Überraschungen zu erleben.

Fazit

Cloud-ERP ist ein mächtiger Hebel für Innovation und Wettbewerbsfähigkeit. Vor der Entscheidung müssen die Prozesse, Anforderungen und Ziele bewertet werden. Wer maximale Individualisierung, besondere regulatorische Anforderungen oder komplexe Eigenentwicklungen benötigt, sollte Alternativen prüfen. In jedem Fall gilt: Wer den Wandel aktiv gestaltet und die Transformation strategisch angeht, sichert sich nachhaltige Vorteile im digitalen Wettbewerb. •

WIE GELINGT DER UMSTIEG?

PRAXISTIPPS FÜR DIE CLOUD-TRANSFORMATION

Ob die Entscheidung für ein Public-Cloud-ERP fällt oder nicht: Der Umstieg ist immer ein tiefgreifender Veränderungsprozess. Aus der Praxis lassen sich einige Erfolgsfaktoren ableiten:

Zunächst empfiehlt es sich, ein klares Zielbild und IT-Strategie für die Rolle des ERP-Systems im Unternehmen zu entwickeln. Nur so lassen sich technologische Möglichkeiten und strategische Anforderungen in Einklang bringen.

Eine gute Datenhygiene ist essenziell: Die Transformationsstudie 2025 von NTT Data Business Solutions zeigt, dass rund ein Viertel der Unternehmen beim Wechsel in die Cloud von der Qualität ihrer Daten negativ überrascht wurde. Wer vor dem Umstieg seine Daten bereinigt und konsolidiert, kann Budgetüberschreitungen und Verzögerungen vermeiden.

Erfolgreiches Change-Management ist der Schlüssel: Mitarbeitende müssen frühzeitig einbezogen, geschult und durch den Wandel begleitet werden. Insbesondere Führungskräfte müssen den Transformationsprozess aktiv unterstützen.

Die Wahl eines erfahrenen Umsetzungspartners mit Branchenkenntnis erleichtert die Migration und sorgt dafür, dass sowohl technische als auch organisatorische Herausforderungen gemeistert werden.

Schließlich sollten Sicherheit und Compliance nicht erst am Ende bedacht werden. Wer hier frühzeitig mit Experten zusammenarbeitet, schafft die Basis für nachhaltigen Erfolg.

„ **Unternehmen mit dynamischen Geschäftsmodellen** und sich schnell ändernden Anforderungen profitieren besonders von Public-Cloud-ERP-Lösungen. Sie können neue Funktionen und Prozesse zügig ausrollen, profitieren von regelmäßigen Updates und zahlen nur für die tatsächlich genutzten Leistungen.

Jens Claes

Warum Unternehmen Workloads aus der Cloud zurückholen

Die Public Cloud gilt wegen ihrer Energieeffizienz und globalen Skalierbarkeit als besonders nachhaltig. Einerseits ist sie das auch. Andererseits haben die Hyperscaler Microsoft, Google und Amazon einen Energiebedarf auf dem Niveau mittlerer Staaten. Viele Unternehmen holen daher ihre Daten wieder zurück aus der Cloud. /// von Björn Orth

UM IHRE RECHENZENTREN DAUERHAFT MIT STROM ZU VERSORGEN und CO2-Neutralität zu signalisieren, investieren Hyperscaler seit geraumer Zeit in nukleare Energieinfrastrukturen. Ein Zielkonflikt. Denn was als „grüne" Lösung dasteht, wird energiepolitisch zunehmend heikel. Und nicht nur energiepolitisch.

Cloud-only: bequem, aber mit Risiko

Im Sinne einer nachhaltigen Geschäftsentwicklung, die wohl jedes Unternehmen anstrebt, ist es bedenklich, in welche Abhängigkeiten Cloud-only-Strategien führen können. Microsoft nutzte dies in den letzten Jahren für drastische Preiserhöhungen – und machte Cloud-Abos

> „ Im Sinne einer nachhaltigen Geschäftsentwicklung, die wohl jedes Unternehmen anstrebt, **ist es bedenklich, in welche Abhängigkeiten Cloud-only-Strategien führen können**.
>
> *Björn Orth*

zu einem betriebswirtschaftlichen Risikofaktor. Nicht weniger heikel ist der US Cloud Act: Er birgt die theoretische Gefahr, dass US-Behörden die Herausgabe europäischer Daten von US-basierten Dienstanbietern verlangen können. Das wirft regulatorische Fragen auf, weil es die Datenschutzvorgaben der DSGVO unterläuft – und nicht im Interesse europäischer Unternehmen sein dürfte. Immer mehr Organisationen prüfen daher, welche ihrer Anwendungen tatsächlich in die Cloud gehören – und welche lokal effizienter, sicherer und nachhaltiger betrieben werden können. In dem Zuge erlebt die sogenannte Repatriierung einen Aufschwung – sie macht die Vorteile der Microsoft Cloud nutzbar, ohne vollständig von ihr abhängig zu sein.

Hybrid schafft Nachhaltigkeit in der IT

Ein mögliches Szenario einer solchen hybriden Infrastruktur könnte sein: Kollaboration und Kommunikation laufen weiter über M365, geschäfts- und DSGVO-kritische sowie

DER AUTOR

Björn Orth ist CEO bei Vendosoft.

Bild: Vendosoft

kostenintensive Systeme werden (wieder) lokal installiert. Bezieht ein Unternehmen die On-Premises-Programme gebraucht, wie es etwa bei Vendosoft auditsicher möglich ist, so ist hybrid eine der nachhaltigsten Lösungen. Wiederverwendete Software verlängert Nutzungszyklen und spart Ressourcen.

Vor allem aber bei den Kosten ist ihr Effekt enorm: Ein Unternehmen mit rund 300 Mitarbeitern spart über einen Zeitraum von drei Jahren etwa 30.000 Euro, wenn es gebrauchte Office-2024-Lizenzen nutzt statt M365 Apps for Enterprise. Ältere Versionen können die Lizenzkosten sogar um bis zu 70 Prozent senken. Diese ökonomische Komponente ist kein Nebenaspekt, sondern Teil nachhaltigen Handelns, das auch die Resilienz eines Unternehmens und die Einhaltung von Compliance-Vorgaben im Blick hat.

Handlungsspielräume kennen – und nutzen

Hybride Modelle schaffen Spielräume – technisch, organisatorisch und finanziell. Sie senken die Abhängigkeit von Preisanpassungen und schützen vor Datenverlust, Cyberrisiken und Industriespionage. Die Kunst, tragfähige, zukunftsgewandte hybride IT-Strukturen zu schaffen, liegt allerdings in der Wahl der Lizenzierungen.

Die Herausforderung für Unternehmen ist meist nicht, zu definieren, welche User und Systeme in die Cloud gehören und welche nicht. Die Herausforderung liegt in den Microsoft-Lizenzbestimmungen. Läuft Office beispielsweise auf Terminal-Servern, kann es zu Einschränkungen kommen. Die Details muss man kennen. Auch dass Microsoft 365 ab 2026 zwingend Windows Server 2025 voraussetzt.

Diese und weitere Kompatibilitätsfragen bei Mischszenarien nicht zu beachten, kann zu Migrationsverzögerungen führen – und damit zu unnötigen Kosten!

Partielle Repatriierung als Weg zur Stabilität

Die Rückführung von Workloads aus der Cloud ist kein Rückschritt, sondern ein Schritt zu mehr Stabilität. Eine partielle Cloud-Repatriierung schafft Datensouveränität – und eine wirtschaftlich und organisatorisch nachhaltig ausgerichtete IT. •

> „ Die **Rückführung von Workloads aus der Cloud ist kein Rückschritt,** sondern ein Schritt zu mehr Stabilität.
>
> *Björn Orth*

MEHR NACHHALTIGKEIT MIT GEBRAUCHT-SOFTWARE

Wiederverwendung statt Neukauf

Gebraucht-Software ist ein oft übersehener Hebel für nachhaltige IT. Indem Unternehmen ungenutzte, zeitlich unbefristete Lizenzen weiterverkaufen und andere sie erwerben, werden digitale Produkte mehrfach genutzt – das reduziert Ressourceneinsatz, vermeidet Neuanschaffungen und verlängert die Lebensdauer bestehender Hardware. Ältere Versionen mit moderaten Anforderungen laufen häufig stabil auf vorhandenen Systemen und sparen so energieintensive Hardware-Refreshs.

Wirtschaftlich locken Einsparungen von 30 bis 70 Prozent, ökologisch zählt die Vermeidung versteckter Emissionen aus Entwicklung, Distribution und Infrastruktur.

Die Nachhaltigkeit von Secondhand-Lizenzen hängt von einigen Faktoren ab, ergänzt jedoch auf sinnvolle Weise bestehende IT-Maßnahmen zur Reduktion von Treibhausgasen.

So funktionieren elektronische Rechnungen im internationalen Geschäftsverkehr

Die E-Rechnung soll Geschäftsprozesse vereinfachen und dem Umsatzsteuerbetrug vorbeugen. Technisch gehen die EU-Länder das Thema jedoch zum Teil sehr unterschiedlich an. Was Unternehmen jetzt beachten sollten. /// von Dina Ziems

EUROPAWEIT HÄLT E-INVOICING SCHRITT FÜR SCHRITT EINZUG. In Belgien, Frankreich und Polen gilt ab 2026 eine Versandpflicht für elektronische Rechnungen im B2B, Deutschland ist ein Jahr später an der Reihe.

Die E-Rechnungspflicht bedeutet, eine Rechnung muss in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen werden. Technische Grundlage für die elektronische Rechnungsstellung ist die europäische Norm EN 16931, auf welche die einzelnen nationalen Regelungen grundsätzlich referenzieren.

In Deutschland kennt man die XRechnung bereits aus dem B2G-Umfeld. In der freien Wirtschaft wird außerdem das ZUGFeRD-Format eingesetzt. Beide entsprechen in ihren aktuellen Versionen der EN 16931, sind damit also zulässig. In mehreren EU-Ländern ist daneben BIS Billing 3.0 die technische Basis der E-Rechnung. Wer mit elektronischen Rechnungen zu tun hat, sollte alle drei Formate kennen.

EU-Standard hebelt Komplexität nicht aus

Unter dem Etikett des europäischen Standards verbergen sich deutlich mehr länderspezifische Ausprägungen und technische Anforderungen, als man nun annehmen könnte. Die EN 16931 dient lediglich als Orientierung, innerhalb derer die Staaten jeweils eigene Formate und Anhänge (die ebenfalls verpflichtend sein können) entwickeln, verwenden und auch wieder ändern dürfen. Formate, die der EN 16931 entsprechen, sind zum Beispiel OIOUBL (Dänemark) oder FatturaPA (Italien). Jedes von ihnen ist von den jeweiligen nationalen Gesetzgebungen abhängig und muss beachtet werden.

Wer also innerhalb von Deutschland eine FatturaPA-Rechnung erhält, ist verpflichtet, sie zu verarbeiten, da es sich um eine offizielle E-Rechnung handelt. Neben den obligatorischen Feldern enthalten die meisten Formate eine Vielzahl optionaler Felder, deren Nutzung von individuellen Vereinbarungen abhängig ist. Im Zusammenspiel mit dem ERP-System muss dies beachtet werden und erfordert ein anspruchsvolles Feldmapping.

Herausforderung bei länderübergreifenden Geschäftsaktivitäten

Eine Standardisierung wird mit E-Rechnungen bislang also vor allem auf nationaler Ebene erreicht. Auf europäischer Ebene steht sie – trotz Bestrebungen wie auf Landesebene – noch aus. Zu unterscheiden ist auch zwischen B2B- und B2G-Rechnungen, die hinsichtlich Übertragungskanälen, Pflichtfeldern und Formaten voneinander abweichen können. In bestimmten Ländern sind zudem Portale für den Rechnungsversand vorgeschrieben.

Für Unternehmen mit grenzüberschreitenden, internationalen Absatz- und Bezugsmärkten reicht die nationale Standardisierung allein nicht aus. Der Aufwand, Eingang und Versand von E-Rechnungen adäquat abzubilden und mit dem eigenen ERP-System in Einklang zu bringen, potenziert sich schnell. International agierende Unternehmen sollten daher die E-Rechnung als ein Querschnittsprojekt betrachten, das IT und Fachabteilungen (für Steuern, Finanzen und Recht) gleichermaßen angeht. Um die typischen Stolpersteine bei der Umsetzung der E-Rechnungspflicht im internationalen Kontext zu umgehen, empfiehlt sich die Einhaltung einiger Grundregeln:

Jetzt handeln – ohne individuelle Lösungen

Selbst wenn derzeit nur wenige elektronische Rechnungen in Unternehmen eintreffen oder die direkte Nachfrage von Geschäftspartnern dazu ausbleibt, ist eines klar: Die gesetzlichen Vorgaben greifen Schritt für Schritt und sind unumkehrbar. Wer jetzt untätig bleibt und sich nicht mit passenden Lösungen beschäftigt, verspielt wertvolle Vorbereitungszeit und läuft Gefahr, den Anschluss zu verlieren.

Auch das oft übliche Vorgehen, auf Individuallösungen zu setzen, macht die Sache nicht leichter. Angesichts sich schnell ändernder technologischer Gegebenheiten und regulatorischer Anforderungen bedeutet eine Eigenentwicklung immer einen enorm hohen Wartungsaufwand. Kaum ist eine Anpassung umgesetzt, steht schon die nächste bevor. Sinnvoller ist es deshalb, auf erprobte – im besten Fall flexible und cloudbasierte – Standardlösungen zu setzen. xSuite hat dafür im Vorfeld der E-Rechnungspflicht bereits Mitte 2024 mit xSuite eDNA

eine Cloud-Plattform veröffentlicht, mit der sowohl die Annahme unterschiedlichster E-Rechnungsformate und ihre Umwandlung in ein einfach zu verarbeitendes, standardisiertes Format möglich ist als auch die Erstellung und der Versand von Debitorenrechnungen aus SAP SD in XML-Formaten.

Verantwortlichkeiten, Prozesse, Steuerungsinstrumente

Für eine erfolgreiche Projektumsetzung gibt es unterstützend einige klare Handlungsempfehlungen. Wichtig ist vor allem der Aufbau eines nachhaltigen Compliance-Prozesses, in dem Verantwortlichkeiten und Abläufe so festgelegt werden, dass gesetzliche Änderungen weltweit kontinuierlich beobachtet, Fristen eingehalten und alle Anpassungen transparent dokumentiert werden können.

Ebenso entscheidend ist es, die bestehenden E-Invoicing-Fähigkeiten innerhalb der Organisation zu identifizieren. Oft sind bereits Tools, Systeme oder Prozesse im Einsatz, mit denen Rechnungen erstellt, empfangen, gemeldet oder verarbeitet werden – Potenziale, die sich möglicherweise erweitern und skalieren lassen.

Schließlich empfiehlt es sich, eine strategische Roadmap für die E-Invoicing-Compliance zu entwickeln. Wer den aktuellen Stand im Unternehmen mit bekannten und absehbaren gesetzlichen Anforderungen vergleicht, erkennt Lücken, Prioritäten und kann konkrete Maßnahmen einleiten. Diese Roadmap ist nicht als starres Dokument zu verstehen, sondern sie ist ein dynamisches Steuerungsinstrument, das sich an ein hochdynamisches regulatorisches Umfeld anpassen muss.

Fazit

Die Umsetzung der E-Rechnungspflicht ist nicht nur ein technisches Update – und weit mehr als der Sprung von Papier- und PDF-Formaten zur rein digitalen (XML-) Rechnung. Es handelt sich vielmehr um ein unternehmensweites Transformationsprojekt mit erheblicher Compliance-Relevanz. Wer frühzeitig systematisch plant und skalierbare Strukturen aufbaut, stellt nicht nur sicher, dass die gesetzlichen Vorgaben erfüllt werden, sondern schafft gleichzeitig die Basis für noch transparentere sowie effizientere Rechnungsverarbeitungs-prozesse – und das auf globaler Ebene. •

DIE AUTORIN
Dina Ziems
ist Senior Lead Marketing bei Xsuite. Bild: Xsuite

> „Die Umsetzung der E-Rechnungspflicht ist **nicht nur ein technisches Update** – und weit mehr als der Sprung von Papier- und PDF-Formaten zur rein digitalen (XML-) Rechnung."
>
> *Dina Ziems*

Schwachstelle MFP:

NIS-2 im Fokus

Multifunktionssysteme (MFP) fliegen als Schwachstellen bei IT-Sicherheitskonzepten gerne mal unter dem Radar. Das kann kritisch werden, denn sie verarbeiten sensible Daten und durch die Cyberschutz-Verpflichtung NIS-2 steigt für Firmen auch der Druck, IT-Sicherheit ganzheitlich sicherzustellen. So meistern Unternehmen die NIS-2-Richtlinie auch im Büro. /// von Philipp Wanner

DIE ZWEITE EU-RICHTLINIE ZUR NETZWERK- UND INFORMATIONSSICHERHEIT (NIS-2-Richtlinie) für den verpflichtenden Schutz wichtiger Anlagen und Unternehmen vor Cyberangriffen nimmt, anders als ihre Vorgängerregelung von 2016, nicht nur kritische Infrastrukturen (KRITIS) in die Pflicht – wie das Finanzwesen, Gesundheitsdienstleister oder Energieversorger – sondern erweitert den Kreis der Betroffenen erheblich. Unter den schätzungsweise rund 29.000 Firmen befinden sich auch mittelständische Unternehmen aus den verschiedensten Branchen. Betroffene Firmen sind gefragt, organisatorische und technische Schutzmaßnahmen zu implementieren. Anfang 2023 trat die Richtlinie in Kraft, die EU-Mitgliedstaaten müssen sie in nationales Recht umsetzen. Voraussichtlich bis Anfang 2026 will die Bundesregierung die EU-Richtlinie in Deutschland gesetzlich verankern.

Unternehmen sollten sich besser früher als später darauf vorbereiten, denn bei Verstößen drohen empfindliche Bußgelder. Nachfolgend fünf Bereiche, die für einen sicheren Betrieb von MFP und Druckern im smarten Office beachtet werden sollten, damit diese der NIS-2-Richtlinie entsprechen.

Fünf Features für NIS-2-konforme MFP und Drucker

1. Geräte-Verwaltung:
   Jedes Multifunktionssystem muss erfasst, überwacht und regelmäßig aktualisiert werden. Moderne Lösungen ermöglichen das Management der gesamten Druckerflotte über Fernwartung inklusive automatischer Firmware-Updates. Veraltete Software zählt zu den häufigsten Schwachstellen und ist ein Einfallstor für Cyberattacken.
2. Zugangs- und Rechteverwaltung:
   Wer darf was drucken, scannen oder kopieren? Die Nutzeranmeldung am Gerät begrenzt Zugriffe und dokumentiert alle Aktivitäten. Das verhindert unbefugten Zugang und schafft Transparenz auch bei Sicherheitsvorfällen.
3. Dokumentenschutz:
   Vertrauliche Ausdrucke dürfen nicht unbeaufsichtigt im offenen Ausgabefach liegen. Eine sichere Druckfreigabe durch Authentifizierung per PIN oder Chip sorgt dafür, dass Aufträge erst nach Anmeldung am Gerät ausgegeben werden. So gelangen sensible Dokumente, wie Gehaltsabrechnungen oder Verträge, nicht in falsche Hände.
4. Angriffserkennung:
   Moderne MFP erkennen und melden Manipulationsversuche automatisch. Sichere Startvorgänge (Secure Boot), kontinuierliche Systemprüfungen (Run Time Integrity Check) und Sicherheits-Monitoring (Security Information and Event Management/SIEM) protokollieren verdächtige Aktivitäten und benachrichtigen IT-Administratoren sofort.
5. Technologie-Standards:
   Als gute Leitplanken dienen der BSI IT-Grundschutz und die ISO 27001:2022 Zertifizierung, die auch IT-Sicherheitsanforderungen für MFP definieren. Funktionen wie die Festplattenverschlüsselung, sichere Boot-Prozesse, Authentifizierung und fortlaufende Integritätschecks gehören zum Mindeststandard.

Unternehmen sollten jetzt aktiv werden

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Unternehmen, sich auf die NIS-2-Regulierung vorzubereiten, indem sie konkrete technisch-organisatorische Maßnahmen umsetzen. Für höchste Sicherheit muss dabei auch die Druckumgebung in die Sicherheitsstrategie einbezogen werden. In Zeiten stetig steigender Cyberangriffe sollten Unternehmen die Richtlinie nicht nur als Pflicht begreifen, sondern auch als eine große Chance, um die eigene Wettbewerbsfähigkeit nachhaltig zu stärken. •

DER AUTOR

Philipp Wanner ist Produktmanager bei der Fachhandelsmarke UTAX.

Dell GmbH
Unterschweinstiege 10
60549 Frankfurt am Main

www.delltechnologies.com

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

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

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

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

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

Esker Software Entwicklungs- und Vertriebs-GmbH
Dornacher Straße 3a
85622 Feldkirchen
info@esker.de
www.esker.de

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

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

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

Sybit GmbH
Sankt-Johannis-Straße 1-5
78315 Radolfzell
+49 7732 9508-2000
sales@sybit.de
www.sybit.de

We Create Customer Experience Champions!
Vom KI-gestützten CRM bis zum umfassenden Kundenportal: Die Sybit GmbH ist darauf spezialisiert, Customer Journeys End-to-End zu gestalten.
Ob Lösungen für Vertrieb, eCommerce, Service oder Marketing: Sybit ist der Partner für ganzheitliches Customer Experience Management. Als Europas führende Beratung für CX vertrauen uns über 500 Konzerne und weltweit agierende mittelständische Unternehmen.

MARKETPLACE
06

DIGITAL BUSINESS

01 2026

/// QUANTENCOMPUTING
Enterprise Ready
Wo die Technologie heute schon im Einsatz ist – von der Theorie in die Praxis

/// SECURITY INSIGHT
Expertentalk
Bedrohungslandschaft neu gedacht

/// CRM
Modernisierung mit KI
Wie künstliche Intelligenz die Kundenanalyse perfektioniert

/// HR
Mehr Analyse bitte
Datengetriebene Personalentscheidungen unterstützen das Personalmanagement

Die nächste Ausgabe erscheint am 12.02.2026

Redaktionell erwähnte Firmen dieser Ausgabe

Alugha, Amazon Web Services, ams.solution, Auerswald, Averbis, Bain &Company, BVDW, Cosmo-Consult, DC Datacenter, Docuware, Doctolib, Fieldfisher, Fortinet, Gaia-X, Google Cloud, Keepit, KPMG, Kumavision, Matrix42, Micorfin, NinjaOne, noris network, NTTData Solutions, Okta, Software Business Alliance, Splunk, TrendMicro, Utax, Vendosoft, Versa Networks, Watchguard, Xsuite

IMPRESSUM

DIGITAL BUSINESS Magazin
www.digitalbusiness-magazin.de

HERAUSGEBER UND GESCHÄFTSFÜHRER
Matthias Bauer, Dennis Hirthammer, Günter Schürger

So erreichen Sie die Redaktion
Chefredaktion:
Heiner Sieger (v. i. S. d. P.), heiner.sieger@win-verlag.de
Tel.: +49 (89) 3866617-14
Redaktion:
Konstantin Pfliegl, konstantin.pfliegl@win-verlag.de
Tel. +49 (89) 3866617-18
Stefan Girschner, stefan.girschner@win-verlag.de
Tel.: +49 (89) 3866617-16

Mitarbeiter dieser Ausgabe:
Ulrich Ahle, Joachim Astel, Pantelis Astenburg, Christian Auerswald, Philipp Behre, Michael Bochmann, Jens Claes, Andreas Dangl, Susanne Dubuisson, Kai Ebert, Peter H. Ganten, Thorsten Henning, Michael Heuer, Russel Howe, Mustafa Isik, Marianne Janik, Christian Jensen, Santeri Jussila, Andreas Kadler, Sven Kniest, Melanie Ludolph, Tom Molden, Paul Moll, Dr. Florian Müller, Björn Orth, Patrick Östringer, Dr. Julia Pergrande, Sonja Philipp, Patrick Roth, Axel Schmidhäuser, Ralf Siefen, Philipp Wanner, Richard Werner, Dina Ziems

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

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

Abonnentenservice und Vertrieb
Tel: +49 89 3866617 46
www.digitalbusiness-magazin.de/hilfe
oder eMail an
abovertrieb@win-verlag.de mit Betreff „www.digitalbusiness“
Gerne mit Angabe Ihrer Kundennummer vom Adressetikett

Artdirection/Titelgestaltung: DesignConcept Dagmar Friedrich-Heidbrink
Bildnachweis/Fotos: stock.adobe.com, Werkfotos

Druck:
Vogel Druck und Medienservice GmbH
Leibnizstraße 5
97204 Höchberg

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

Anschrift Anzeigen, Vertrieb und alle Verantwortlichen
WIN-Verlag GmbH & Co. KG
Chiemgaustr. 148, 81549 München
Telefon +49 (89) 3866617-0

Verlags- und Objektleitung
Martina Summer, martina.summer@win-verlag.de,
Tel.: +49 (89) 3866617-31, (anzeigenverantwortlich)

Zentrale Anlaufstelle für Fragen zur Produktsicherheit
Martina Summer (martina.summer@win-verlag.de, Tel.:089/3866617-31)

Bezugspreise
Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement (6 Ausgaben): 69,00 Euro in D, A, CH und 82,20 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler, Auszubildende und Wehrdienstleistende gegen Vorlage eines Nachweises auf Anfrage. Bezugspreise außerhalb der EU auf Anfrage.

29. Jahrgang; Erscheinungsweise: 6-mal jährlich

Ausgabe: 06/2025
ISSN 2510-344X
Unsere Papiere sind PEFC zertifiziert
Wir drucken mit mineralölfreien Druckfarben

Außerdem erscheinen beim Verlag:
AUTOCAD Magazin, BAUEN AKTUELL, r.energy, DIGITAL ENGINEERING Magazin, DIGITAL MANUFACTURING, e-commerce Magazin, KGK Rubberpoint, PLASTVERARBEITER, PlastXnow

UNSER TEAM SUCHT VERSTÄRKUNG

Unser Verlagshaus ist einer der Pioniere und einer der führenden Fachzeitschriftenverlage im Bereich der Digitalen Transformation. Unsere B2B-Zeitschriften sind innovativ und gehören in ihren Bereichen jeweils zur Spitzengruppe.

Sie möchten mit Ihrer Kreativität den Erfolg unserer Fachmagazine mitgestalten?
Dann sind Sie bei uns richtig. Derzeit suchen wir engagierte Mediaberater (m/w/d) in Voll- oder Teilzeit.

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

WIN VERLAG

Abonnieren Sie den WIN-verlagsübergreifenden

KI NEWSLETTER!

Bleiben Sie auf dem Laufenden mit den neuesten Entwicklungen und Trends aus der Welt der Künstlichen Intelligenz. Unser kostenfreier Newsletter vom WIN-Verlag wird monatlich versendet und bietet Ihnen spannende Einblicke, exklusive Inhalte und Expertenmeinungen der verschiedenen Branchen.

Melden Sie sich jetzt an und verpassen Sie keine Ausgabe!

Bild: Ben/AdobeStock

win-verlag.de

WIN VERLAG