

Ohne Rechenzentren kein Wachstum

Von Dr. Sören Grabowski und Dr. Tobias Bopp

Die Debatte über Künstliche Intelligenz (KI), Digitalisierung und digitale Souveränität blendet häufig eine zentrale Voraussetzung aus: Ohne ausreichende Energie und Rechenkapazität bleiben diese Anwendungen nur eingeschränkt nutzbar. Energie und Rechenkapazität sind die Grundvoraussetzungen, damit sich die digitale Wertschöpfung entfalten kann. Erst wenn diese Infrastruktur zuverlässig bereitsteht, kann ein Wirtschaftsstandort seine digitale Leistungsfähigkeit wirklich entfalten.

Rechenzentrumskapazität als Ausgangspunkt zukünftigen Wirtschaftswachstums

Vor 150 Jahren waren es Energie, Rohstoffe und Verkehrswege, die darüber entschieden, wo Unternehmen investierten und wirtschaftlicher Wohlstand entstand. Diese Infrastruktur machte Deutschland zu einer der führenden Industrienationen der Welt. Heute sind zunehmend die Datenauswertung, Rechenleistung und digitale Vernetzung die Grundlage wirtschaftlicher Wertschöpfung. KI, Cloud Computing und datengetriebene Geschäftsmodelle treiben Innovationen voran, steigern die Produktivität und schaffen neue Märkte. Wie einst Eisenbahnnetze und Kraftwerke bilden heute digitale Infrastrukturen die Voraussetzung für Wachstum und Wettbewerbsfähigkeit.

Die Infrastruktur des Wohlstands verändert sich

Damit wird die digitale Infrastruktur neben Straßen, Schienen und Stromnetzen zu einem weiteren entscheidenden Faktor für die Wettbewerbsfähigkeit von Volkswirtschaften. Glasfasernetze übernehmen den Datentransport, während Daten in Rechenzentren gespeichert und verarbeitet werden. So entwickelt sich diese Infrastruktur von einer technischen Grundlage zu einem strategischen Produktionsfaktor der Datenökonomie und digitalen Wertschöpfung. Ohne ausreichende Rechenkapazitäten lassen sich weder KI-Modelle trainieren, noch digitale Plattformen betreiben oder industrielle Prozesse intelligent steuern. Rechenzentren folgen daher nicht mehr nur wirtschaftlichem Wachstum, sondern schaffen zunehmend dessen Grundlage.

Rechenleistung wird zum neuen Produktionsfaktor

Diese Entwicklung ist bereits deutlich sichtbar: Einerseits an den steigenden Investitionen, andererseits am wachsenden Bedarf an Rechenleistung. Laut der Studie „Rechenzentren in Deutschland: Aktuelle Marktentwicklungen

2025“ vom Bitcom investierten Unternehmen allein in 2025 rund 12 Milliarden Euro in deutsche Rechenzentren. Gleichzeitig wird prognostiziert, dass die installierte IT-Anschlussleistung von rund drei Gigawatt im Jahr 2025 bis 2030 auf mehr als fünf Gigawatt anwachsen wird. Besonders stark wächst der Bedarf durch KI. Bereits in wenigen Jahren könnte sie rund 40 Prozent der gesamten Rechenzentrumskapazität beanspruchen.

Diese Zahlen zeigen mehr als nur das Wachstum einer einzelnen Branche. Sie zeigen einen tiefgreifenden Strukturwandel der Wirtschaft. Rechenleistung entwickelt sich zu einer Ressource, deren strategische Bedeutung zunehmend mit der von Energie vergleichbar sein wird. Unternehmen benötigen sie, um Produktionsprozesse zu automatisieren, Lieferketten zu optimieren, große Datenmengen auszuwerten oder neue, KI-gestützte Produkte und Dienstleistungen zu entwickeln und damit ihre Wertschöpfung zu erhöhen. Je stärker Geschäftsmodelle digitalisiert werden, desto stärker wächst die Nachfrage nach Rechenkapazität. Der Zugang zu Rechenkapazität entwickelt sich damit zu einer strategischen Voraussetzung für Innovation, Produktivität und wirtschaftliches Wachstum.

Der neue Standortwettbewerb entscheidet sich an der digitalen Infrastruktur

Deutschland verfügt derzeit noch über den größten Rechenzentrumsmarkt Europas. Aktuelle Marktanalysen zeigen aber, dass der internationale Wettbewerb erheblich an Dynamik gewinnt. Die laut Bitcom bis 2030 in Deutschland erwarteten 5 GW zusätzlicher Rechenzentrumskapazität wirken im internationalen Kontext vergleichsweise gering. In den USA und Asien entstehen derzeit zahlreiche Hyperscale-Rechenzentren mit Leistungen von mehreren hundert Megawatt pro Standort. Die USA verfügen bereits heute über knapp das Zehnfache der in Deutschland installier-

Wo jetzt gehandelt werden muss

- » Energie wird zum limitierenden Faktor des digitalen Wachstums. Der Ausbau von Stromnetzen, intelligente Energiekonzepte und eine stärkere Integration von Rechenzentren in lokale Energiesysteme entscheiden darüber, ob neue Kapazitäten entstehen können. Seite 3
- » Digitale Souveränität braucht leistungsfähige, europäische Cloud- und Dateninfrastrukturen. Offene Standards, interoperable Plattformen und europäische Lösungen stärken die Unabhängigkeit von außereuropäischen Anbietern und schaffen die Grundlage für eine resiliente digitale Wirtschaft. Seiten 4 – 5
- » Innovation und Datensouveränität müssen gemeinsam gedacht werden. Moderne Cloud-Architekturen und neue Sicherheitskonzepte ermöglichen es, das Potenzial von KI und Cloud zu nutzen, ohne die Kontrolle über sensible Daten aufzugeben. Seite 6
- » Ein starker europäischer Rechenzentrumsmarkt erhöht Wettbewerbsfähigkeit und Resilienz. Leistungsfähige europäische Anbieter schaffen Wahlfreiheit, stärken die digitale Souveränität und reduzieren strategische Abhängigkeiten. Seite 7
- » Planungs- und Genehmigungsverfahren müssen deutlich schneller werden. Bürokratische Hürden und langwierige Prozesse verzögern Investitionen und gefährden Deutschlands Wettbewerbsfähigkeit im internationalen Standortwettbewerb. Seite 8

ten Rechenleistung und bauen ihre Kapazitäten mit hoher Geschwindigkeit weiter aus.

Mit dieser Entwicklung verändern sich auch die Kriterien für Investitionsentscheidungen. Jahrzehntlang konkurrierten Standorte vor allem über Faktoren wie Lohnkosten, Steuern oder Verkehrsanbindung. Im KI-Zeitalter wird die verlässliche Verfügbarkeit digitaler Infrastruktur

Impressum

Verlag: Reif Verlag GmbH · Alfred-Jost-Straße 11 · 69124 Heidelberg
Peter Reif · peter.reif@reifverlag.de · www.manager-wissen.com

Redaktion: Christian Deutsch · info@deutsch-werkstatt.de
Regina Gödde, E-Mail: regina.goedde@reifverlag.de
Layout: metropolmedia · 69245 Bammental
Druck: ColorDruck Solutions · 69181 Leimen



zu einem zentralen Wettbewerbsfaktor. Unternehmen investieren bevorzugt dort, wo die notwendige Infrastruktur schnell verfügbar ist oder innerhalb eines verlässlichen Zeit- und Kostenrahmens verfügbar sein wird. Wenn ein neuer Produktionsstandort innerhalb weniger Monate an ausreichend Rechenleistung angebunden werden kann, hat dies unmittelbar Einfluss auf Investitionsentscheidungen. Denn Investitionen folgen dorthin, wo Infrastruktur rechtzeitig bereitsteht.

Nachhaltigkeit und Tempo werden zu Standortfaktoren

Der Ausbau der Rechenzentrumskapazitäten für die digitale Infrastruktur steht in Deutschland und Europa vor einer doppelten Herausforderung. Einerseits steigt der Energiebedarf datenintensiver Anwendungen und KI-gestützter Prozesse kontinuierlich an, andererseits wachsen die Anforderungen an Energieeffizienz, Nachhaltigkeit und Klimaschutz. Moderne Rechenzentren zeigen jedoch, dass sich wirtschaftliches Wachstum und nachhaltiger Betrieb miteinander verbinden lassen, etwa durch den Einsatz erneuerbarer Energien, intelligente Energiesteuerung und die Nutzung von Abwärme.

Neben Nachhaltigkeit und Energieeffizienz wird auch die Geschwindigkeit des Rechenzentrumsbaus zunehmend zu einem entscheidenden Wettbewerbsfaktor. Schnelle Genehmigungsverfahren, planbare Netzanschlüsse und der rechtzeitige Ausbau von Strom- und Glasfasernetzen werden damit zu wesentlichen Standortvorteilen bei der Ansiedlung neuer Rechenzentren.

Internationale Investoren bewerten den deutschen Markt weiterhin als attraktiv und sind bereit, Geld in neue Rechenzentrumsprojekte zu investieren. Der eigentliche Engpass liegt jedoch häufig nicht im Zugang zu Kapital, sondern in fehlender Infrastruktur und komplexen bürokratischen Anforderungen. Dazu gehören auch leistungsfähige Stromnetze, Glasfaseranbindungen, geeignete Flächen und vor allem verbindlich zugesagte Netzanschlüsse. Diese Faktoren entscheiden darüber, ob neue Bauprojekte realisiert oder in andere Regionen verlagert werden. Diese Entwicklung führt dazu, dass der Ausbau neuer Rechenzentrumskapazitäten in einigen Regionen langsamer vorankommt, obwohl die Nachfrage nach Rechenleistung durch KI und andere datenintensive Anwendungen deutlich steigt. Hintergrund ist, dass die dafür notwendige Energie- und Netzinfrastruktur nicht im gleichen Tempo ausgebaut wird. In der Folge entstehen Kapazitäten zunehmend dort, wo Infrastrukturmaßnahmen schneller umgesetzt werden können, sodass sich auch Teile der digitalen Wertschöpfung in diese Regionen der Welt verlagern. Gerade hierin liegt eine der größten Herausforderungen – und zugleich ein Risiko für Deutschland. Denn die Folgen betreffen nicht nur die Rechenzentrumsbranche, sondern wirken weit in andere Bereiche der digitalen Wirtschaft und darüber hinaus.

Digitale Souveränität beginnt bei der Infrastruktur

Die Debatte über Rechenzentren ist längst keine rein technische Diskussion mehr. Im Kern geht es um die Leistungsfähigkeit des Wirtschaftsstandorts. Defizite bei Energieversorgung, Netzinfrastruktur und Rechenleistung begrenzen Innovation, digitale Geschäftsmodelle und Wertschöpfung sowohl in Industrie als auch in Verwaltung, Gesundheitswesen und Finanzsektor gleichermaßen. Unternehmen und Investoren fragen zunehmend, ob auch zukünftig ausreichend digitale Infrastruktur verfügbar sein wird, um wettbewerbsfähig zu bleiben. Vor diesem Hintergrund erhält auch die Diskussion über digitale Souveränität eine neue Bedeutung.

Die Diskussion über digitale Souveränität konzentriert sich häufig auf Datenschutz, europäische Cloud-Lösungen oder regulatorische Anforderungen. Diese Aspekte bleiben wichtig, greifen aber zu kurz. Denn jede Form digitaler Souveränität setzt zunächst voraus, dass ausreichend eigene Rechenkapazitäten vorhanden sind, um Daten im eigenen Rechtsraum zu verarbeiten.

Wer kritische digitale Infrastruktur nicht selbst bereitstellen kann, bleibt dauerhaft auf Kapazitäten anderer Staaten oder Anbieter angewiesen. Damit entstehen nicht nur technologische, sondern auch wirtschaftliche und geopolitische Abhängigkeiten. Gerade vor dem Hintergrund zunehmender internationaler Spannungen gewinnt die Fähigkeit, kritische digitale Dienste sicher und resilient in Deutschland und Europa betreiben zu können, erheblich an Bedeutung. Digitale Souveränität beginnt deshalb nicht erst in der Cloud, sondern sie beginnt dort, wo Rechenleistung entsteht – im Rechenzentrum.

Der Ausbau wird zur Gemeinschaftsaufgabe

Der Ausbau digitaler Infrastruktur kann deshalb nicht isoliert betrachtet werden. Betreiber, Energieversorger, Netzbetreiber, Kommunen, Investoren und Politik müssen Kapazitätsaufbau, Energieversorgung und Flächenentwicklung wesentlich enger aufeinander abstimmen als bisher.

Infrastruktur-, Energie- und Digitalpolitik dürfen künftig nicht länger getrennt gedacht werden. Erst ihr Zusammenspiel entscheidet darüber, ob Deutschland die Voraussetzungen schafft, um die nächste Welle digitaler Wertschöpfung im eigenen Land zu ermöglichen.

Fazit

Deutschland verfügt über hervorragende Voraussetzungen: den größten Rechenzentrumsmarkt Europas, eine starke Industrie, exzellente Forschung und eine hohe Nachfrage nach digitalen Lösungen. Gleichzeitig investieren andere Regionen der Welt mit hoher Geschwindigkeit in neue Kapazitäten und schaffen damit attraktive Bedingungen für Rechenzentrumsbetreiber und für Unternehmen mit datenintensiven Anwendungen.

Ohne Rechenzentren kein Wachstum – Key Takeaways

- › Rechenzentren bilden die Produktionsbasis der digitalen Wirtschaft. Sie schaffen die Rechenkapazitäten, auf denen KI, Cloud-Anwendungen und datengetriebene Geschäftsmodelle aufbauen und werden damit zur Voraussetzung für zukünftiges Wirtschaftswachstum.
- › Verfügbare Rechenleistung wird zum strategischen Standortfaktor. Investitionen fließen zunehmend dorthin, wo Energie, Netzinfrastruktur und digitale Kapazitäten schnell und zuverlässig verfügbar sind.
- › Deutschlands Wettbewerbsfähigkeit wird künftig maßgeblich von der Verfügbarkeit digitaler Infrastruktur abhängen. Der rechtzeitige Ausbau von Rechenzentrumskapazitäten schafft die Basis für Innovation, wirtschaftliches Wachstum und digitale Souveränität.

Die entscheidende Frage ist deshalb nicht mehr, ob Deutschland zusätzliche Rechenzentren benötigt. Sie lautet: Wie schnell können die dafür erforderlichen Kapazitäten geschaffen werden?

Die Geschichte der deutschen Wirtschaft zeigt: Wohlstand ist immer dort entstanden, wo rechtzeitig in die notwendige Infrastruktur investiert wurde. Im Industriezeitalter waren es Kraftwerke, Verkehrswege und Produktionsanlagen. Im digitalen Zeitalter übernehmen Rechenzentren eine vergleichbare Rolle. Sie sind längst nicht mehr nur technische Infrastruktur, sie werden zur Grundlage von Produktivität, Innovation und wirtschaftlicher Souveränität.

Eine Investition in Rechenzentren ist nicht nur eine Investition in Server oder Gebäude. Es ist eine Investition in die Wachstumsfähigkeit des Wirtschaftsstandorts Deutschland.

Die Autoren



Dr. Sören Grabowski ist Partner bei EY-Parthenon und berät Unternehmen im Technologie-, Medien- und Telekommunikationssektor zu Strategie- und Transformation, mit Fokus auf digitaler Infrastruktur.



Dr. Tobias Bopp ist Manager bei EY-Parthenon und wissenschaftlicher Mitarbeiter an der TU Braunschweig mit dem Forschungsschwerpunkt strategische Bedeutung digitaler Infrastruktur und Souveränität.

Der entscheidende Erfolgsfaktor der Datenökonomie: Energie zur richtigen Zeit

Von Marten Bunnemann

In Deutschland wird viel über digitale Wertschöpfung als Grundlage künftiger Wettbewerbsfähigkeit gesprochen – jedoch selten über die physische Infrastruktur, die sie ermöglicht. Rechenzentren sind die Fabriken des digitalen Zeitalters. Sie entstehen nicht „in der Cloud“, sondern dort, wo Energie- und Netzinfrastruktur, digitale Anbindung, verfügbare Flächen, Genehmigungen und lokale Akzeptanz zusammenkommen.

Der globale Wettbewerb um digitale Wertschöpfung ist damit auch ein Wettbewerb um Infrastruktur. Entscheidend ist nicht nur der Zugang zu Energie, sondern ihre Verfügbarkeit zum richtigen Zeitpunkt.

Für Deutschland ist das eine industriepolitische Weichenstellung: Die Fähigkeit, Rechenleistung bereitzustellen, bestimmt künftig Wettbewerbsfähigkeit, Innovationskraft und Wohlstand.

Der Weg von der Energie zur Intelligenz

Rechenzentren übersetzen elektrische Energie in Rechenleistung: Die Grundlage für KI, Cloud und Digitalisierung. Damit wird Energieverfügbarkeit zum zentralen Standortfaktor. Entscheidend ist nicht nur, ob genügend Strom vorhanden ist, sondern wie schnell die benötigte Leistung am Standort bereitgestellt werden kann. Diese „Time-to-Power“ bestimmt, ob Rechenzentren entstehen, wie rasch Investitionen wirksam werden und wo digitale Wertschöpfung künftig stattfindet.

„Die zentrale Herausforderung der Datenökonomie ist nicht der stark wachsende Bedarf an Rechenleistung. Entscheidend ist, ob daraus schnell genug realisierbare, wirtschaftlich tragfähige und lokal integrierte Infrastruktur entsteht. Time-to-Power wird damit vom technischen Detail zum entscheidenden Standort- und Wirtschaftsfaktor der Datenökonomie.“

Marten Bunnemann

Time-to-Power wird zum Standortfaktor

Frankfurt zeigt die Herausforderung deutlich: Mit dem DE CIX verfügt die Region über einen der weltweit wichtigsten digitalen Knotenpunkte. Bestehende Infrastruktur und kurze Latenzen machen den Standort attraktiv. Doch während Rechenzentren oft schnell geplant und gebaut werden, benötigen Energieinfrastruktur und Genehmigungen deutlich mehr Vorlauf.

So entsteht eine Lücke zwischen digitaler Ambition und infrastruktureller Realität, die zunehmend darüber entscheidet, wo und wann Investitionen tatsächlich umgesetzt werden. Fehlen Energie und Netzkapazitäten, wandern Projekte und digitale Wertschöpfung an andere Standorte.

Hybrid statt „Entweder-oder“ als neues Versorgungsmodell

Die Lösung liegt nicht im „Entweder-oder“ zwischen Netz und lokaler Erzeugung, sondern in einer neuen Infrastruktur-Logik. Hybride Energiekonzepte verbinden Netzanschluss, lokale Erzeugung, Speicher, intelligente Steuerung und Wärmenutzung zu einem integrierten Energiesystem. Statt auf kostenintensive Autarkie zu setzen, nutzen sie die Stärken aller verfügbaren Energiequellen. Das Netz bleibt das Rückgrat der Versorgung. Hybride Modelle können jedoch die Abhängigkeit vom sofortigen Vollanschluss reduzieren, zusätzliche Standortoptionen eröffnen und Projekte früher realisierbar machen.

Vom passiven Energieverbraucher zum aktiven Teil des Energiesystems

Hybride Konzepte verändern die Rolle von Rechenzentren im Energiesystem. Ihr Energiebedarf bleibt erheblich. Richtig geplant und gesteuert, können sie jedoch vom passiven Energieverbraucher zum aktiven Teil des Energiesystems werden. Intelligentes Energiemanagement macht Flexibilitätspotenziale nutzbar, hilft Netzbezug und Lasten besser zu steuern und Netzengpässe zu reduzieren. Die Kombination aus Netz und lokalen Versorgungslösungen stärkt die operative Resilienz und erhöht die Versorgungssicherheit. So können Rechenzentren das Energiesystem nicht nur belasten, sondern aktiv mitgestalten.

Akzeptanz durch lokalen Nutzen

Neben Energie entscheidet die lokale Akzeptanz über die Realisierbarkeit neuer Projekte. Rechenzentren werden dauerhaft nur dort erfolgreich sein, wo sie als Teil der lokalen Infrastruktur wahrgenommen werden. Der größte Hebel liegt in der Nutzung von Abwärme: Sie kann einen wertvollen Beitrag zur lokalen Wärmeversorgung leisten. Wird sie in Wärmenetze, Quartiere oder Gewerbegebiete integriert, entsteht konkreter Mehrwert für Kommunen und ein Beitrag zur Dekarbonisierung.

Internationale Wettbewerbsfähigkeit

Die wirtschaftspolitische Frage lautet: Schafft Deutschland die infrastrukturellen Voraussetzungen für die digitale Wertschöpfung?

Energie- und digitale Infrastruktur müssen gemeinsam gedacht werden – mit schnelleren Verfahren, flexiblen Anschlussmodellen und einem regulatorischen Rahmen für integrierte Energiekonzepte.

Andere Regionen handeln bereits entsprechend. Investitionen folgen realisierbaren Projekten, nicht politischen Ambitionen. Wer digitale Souveränität erreichen will, muss die dafür notwendige Energieinfrastruktur rechtzeitig bereitstellen.

„Unser Ziel ist es, Rechenzentren von Anfang an als Teil lokaler Energiesysteme zu entwickeln – von der Energieversorgung über Kühlung bis zur Nutzung von Abwärme. So schaffen wir digitale Infrastruktur und gleichzeitig einen messbaren Mehrwert für den Standort.“

Jannis Lange,
Global Lead
Data Center Solutions



Energieinfrastruktur als Schlüssel für digitale Wertschöpfung

Rechenzentren funktionieren nicht mehr isoliert. Energie, Datennetze, Wärmenutzung, Fläche und kommunale Planung müssen zusammengedacht werden.

E.ON Energy Infrastructure Solutions überträgt jahrzehntelange Erfahrung aus energieintensiven Industrien auf die Anforderungen moderner Rechenzentren. Die Entwicklung integrierter Energielösungen, die Netzanschlüsse, lokale Erzeugung, Speicher und Wärmenutzung optimal miteinander verbinden, gehört seit vielen Jahren zu unserem Kerngeschäft. Heute unterstützen wir damit Betreiber, Kommunen und Investoren dabei, digitale Infrastruktur zu ermöglichen und lokale Energiesysteme zukunftsfähig zu gestalten.

Am Ende entscheidet sich daran, ob Deutschland die Voraussetzungen für digitale Wertschöpfung schafft oder ob Investitionen, Innovation und Wachstum in andere Regionen abwandern.

Der Autor

Marten Bunnemann ist CEO von E.ON Energy Infrastructure Solutions und seit 2002 in verschiedenen Fach- und Führungsfunktionen innerhalb des E.ON-Konzerns tätig.

Unter seiner Leitung realisiert das Unternehmen als



Wachstumssegment des Konzerns in 14 europäischen Ländern zukunftssichere Energiesysteme für Städte und Industrien.

Mit der Cloud-Blaupause zur Souveränität: Wie NeoNephos das Ende der Abhängigkeit einläutet

Von Stephan Ilaender

Digitale Souveränität minimiert geschäftliche Risiken, sichert Handlungsfreiheit und ermöglicht freieres Wirtschaften. Statt skeptischer Passivität braucht es jetzt den gemeinsamen Willen, Lösungsansätze zu etablieren, die Souveränität fördern. Die Open-Source-Stiftung NeoNephos zeigt als Paradebeispiel, wie der Abbau europäischer Marktfragmentierung gelingt. Sie setzt das um, was die EU-Kommission in Initiativen fordert, indem sie dem heterogenen Cloud-Markt ein Kontinuum beiseite stellt: für echte Interoperabilität, Datenhoheit und maximale Wahlfreiheit.

Was ist digitale Souveränität und welche wirtschaftlichen Vorteile birgt sie?

Wie frei sind wir in unserem Handeln? Die alte philosophische Frage nach der Handlungsfreiheit hat momentan Konjunktur, bildet sie doch eines der vielen Kernkonstrukte digitaler Souveränität. Ein Begriff, der im Alltag lange Zeit wenig sichtbar war und heute zu einem der zentralen Hebel für wirtschaftliche Resilienz avanciert. Denn bei proprietären Software- und Cloud-Lösungen können Systeme, Datenstrukturen und Prozesse zunehmend eng mit den Technologien einzelner Anbieter verknüpft werden. Dadurch können Abhängigkeiten entstehen, die die strategische Handlungsfreiheit einschränken.

Was bedeutet diese Entwicklung konkret für industrielle Entscheider, ihre Prozesse und die langfristige Unternehmensstrategie? Wer heute bei der Ausgestaltung seiner Digital- und KI-Strategie die Weichen falsch stellt, riskiert, auf Jahre in einen technologischen Lock-in zu geraten. Marktdynamiken bei proprietären Softwarelösungen zeigen, wie schnell Unternehmen einseitig diktierten Preiserhöhungen oder abrupten Änderungen der Lizenzmodelle ausgeliefert sind, wenn ihre Architektur fest an einen einzigen Anbieter gebunden ist. Auch die Integration von branchen- oder unternehmensspezifisch entwickelten Applikationen von Drittanbietern gestaltet sich dann oft schwierig.

Besonders im ressourcenintensiven Feld der Künstlichen Intelligenz (KI) wird diese Vorfestlegung zum kritischen Faktor für die künftige Wertschöpfung. Es greift strategisch zu kurz, aus reiner Gewohnheit oder getrieben von kurzfristigen Technologie-Hypes, den vermeintlich einfachen Weg auf geschlossene Plattformen zu wählen. Diese etablierten Anbieter sind zwar historisch weit verbreitet,

doch im Kontext heutiger Ansprüche an Flexibilität, Interoperabilität und Offenheit erweisen sich ihre Angebote als unnötig einschränkend. Stattdessen bedarf es einer wohlüberlegten Architektur, die ein zukunftsfähiges und skalierbares Fundament für kommende Innovationen bildet.

Genau hier positioniert sich NeoNephos als architektonische Blaupause. Die Stiftung validiert das Konzept praxisnah, indem sie konsequent auf offene Kollaboration setzt, statt Einzellösungen zu bewerben. Für Stakeholder aus der Industrie bietet dieser Ansatz einen wegweisenden Kompass: Er befähigt Unternehmen, leistungsstarke IT-Infrastrukturen aufzubauen, ohne die Kontrolle über Kosten und Handlungsfreiheit abzugeben.

Europäische Rahmenwerke für digitale Souveränität

Der technologische Lock-in birgt jedoch nicht nur wirtschaftliche Fallstricke. Diese Abhängigkeiten zeigen sich beispielsweise darin, dass der Betrieb eigener Infrastrukturen erschwert wird und Daten an Drittstaaten abfließen können.

Das Cloud Sovereignty Framework der Europäischen Union (EU) definiert hierfür ein Fundament aus acht Dimensionen, die ein Cloud-Anbieter erfüllen muss, um als digital souverän zu gelten. Während europäische Rahmenwerke die strategische Richtung vorgeben, benötigen Unternehmen konkrete Kriterien, um digitale Souveränität messbar und im IT-Betrieb umsetzbar zu machen.

Genau hier setzt der ES³-Standard (European Sovereign Stack Standard) von Schwarz Digits an. Als praktisches Umsetzungsmodell übersetzt er abstrakte Compliance-Ziele in messbare Reifegrade, die im IT-Betrieb funktionieren und die Souveränitätsfrage gezielt um die Dimension KI erweitern.

Mit diesem praxisnahen Ansatz unterstützt das Modell die übergeordnete Digitalstrategie

der EU. Diese soll aufzeigen, wie Europa der Sprung in die digitale Unabhängigkeit gelingen kann. Schließlich handelt es sich dabei um eine der drängendsten wirtschaftlichen und gesellschaftlichen Herausforderungen unserer Zeit.

Damit aus dieser politischen Vision wirtschaftliche Realität wird, braucht es neben klaren Richtlinien auch ein solides Fundament für die praktische Umsetzung. Als Beispiel sei der Aufbau einer ersten einheitlichen Cloud-Referenzarchitektur für Europa herangezogen, welcher durch die Umsetzung von technologischen Projekten der Industrie entwickelt wurde.

Um mögliche wirtschaftliche Risiken im Zusammenhang mit der Realisierung solcher Projekte zu minimieren, gibt es zahlreiche Unterstützungsformate, wie beispielsweise die sogenannten Important Projects of Common European Interest (IPCEI). Hinter diesem Begriff steckt ein Mix aus strategischer Vision und Finanzierungs-Kickstarter für innovative Technologien. So wurde Ende 2023 das IPCEI Next Generation Cloud Infrastructure and Services (IPCEI-CIS) ins Leben gerufen. Es soll den technologischen Grundstein für die angestrebte europäische Referenzarchitektur legen. Und genau dieses Ziel in industrielle Praxis umzusetzen, hat sich die NeoNephos-Foundation auf die Fahne geschrieben.

Wie funktioniert NeoNephos und wie treibt es die digitale Souveränität Europas voran?

Seit der Mitbegründung von NeoNephos unter der Ägide der Linux Foundation Europe steht vor allem eines im Zentrum: die Erschaffung eines europäischen Cloud-Edge-Kontinuums. Zu diesem Zweck werden Cloud-native Module etabliert, die die wesentlichen Technologien für den Aufbau und Betrieb von Clouds jedweder Größe umfassen. Diese Komponenten sind so flexibel skaliert, dass sie sowohl auf einem einzelnen Minicomputer in einer Fabrik laufen als auch das Fundament für das Rechenzentrum eines großen Cloud-Anbieters bilden können.

Ein Cloud-Edge-Kontinuum erweitert das Konzept der klassischen, zentralisierten Cloud um entscheidende Vorteile: Es ermöglicht das flexible Verschieben von Anwendungen und Daten aus Rechenzentren an den Rand des eigenen Unternehmens-Netzwerks, der Edge, und umgekehrt. Das Kontinuum erlaubt somit eine Kombination aus zentralem und dezentralem Anwendungsbetrieb, der Speicherung und Verarbeitung von Daten. Je nach Bedarf und Anforderung lässt sich die eigene IT-Architektur dabei flexibel anpassen.

Neben geringeren Latenzen und höherer Resilienz stärkt diese Architektur vor allem die digitale Souveränität: Unternehmen kön-

nen Anwendungen flexibler betreiben, Cloud-Anbieter leichter wechseln und neue Technologien schneller integrieren. Technologisch gelingt dieser Spagat, wenn man die IT-Architektur in drei eigenständige Bereiche unterteilt. Erst durch diese Entkopplung entsteht die nötige Flexibilität, Wechselfähigkeit und somit Unabhängigkeit. Diese technologische Offenheit spiegelt sich auch im Organisationsmodell von NeoNephos wider.

Offene Plattformen als Schlüssel zur digitalen Unabhängigkeit

Die Gründungsmitglieder – europäische Technologiegrößen wie SAP, Schwarz Digits oder T-Systems – wählten von Beginn an einen anderen Ansatz als die Anbieter aus Übersee. Statt in Konkurrenz zueinander zu agieren, entwickeln sie gemeinschaftlich. Dabei starten sie nicht bei Null, sondern greifen gezielt auf bestehende, praxiserprobte Lösungen aus ihren eigenen Unternehmen zurück.

Sowohl bewährte als auch neue Lösungen werden ausschließlich als Open Source entwickelt und fortgeführt. Dabei bleibt der Quellcode öffentlich einsehbar und für Unternehmen eigenständig wartbar. Open Source gilt als eines der effektivsten Modelle zur Softwareentwicklung, da an den Projekten Fachleute verschiedenster Expertisen als kollaborativ entwickelnde Community zusammenarbeiten. Diese Arbeitsweise ähnelt dem aus der Wissenschaft bekannten Peer-Review-Verfahren. Der Code einer Software wird so stetig weiterentwickelt. Die kontinuierliche Überprüfung durch eine breite Entwicklergemeinschaft erhöht Transparenz und trägt dazu bei, Schwachstellen frühzeitig zu erkennen und zu beheben.

Die gemeinschaftliche Zusammenarbeit in der Foundation ist keine leere Absichtserklärung, sondern fest in der DNA von NeoNephos verwurzelt. Sie versteht sich zugleich als eine konkrete Einladung an die Tech-Gemeinschaft, aktiv an der digitalen Unabhängigkeit des europäischen Wirtschaftsraums mitzuwirken.

Wie NeoNephos Pionierleistungen im Bereich Cloud-Infrastruktur liefert

Die zweite große Stärke von NeoNephos ist die Interoperabilität des Kontinuums, die von Stunde eins an mitgedacht wurde. Die entwickelten Bausteine sind nicht an einzelne Anbieter gebunden, von denen es Hunderte in der EU gibt. Damit setzt die Initiative eine zentrale Vorgabe von IPCEI-CIS um, die ein solches, anbieterunabhängiges Multi-Provider-System fokussiert. Auf diese Weise wird die Fragmentierung des europäischen Marktes reduziert und Raum für

Die NeoNephos-Vision: Der modulare Stack

Um KI-Anwendungen unabhängig und flexibel zu betreiben, bricht dieses Schichtenmodell die klassische, starre Kopplung von Hard- und Software auf:

› Einsatzbereite Souveränität – KI-Applikationen:

Hochentwickelte KI-Anwendungen werden über einfache Benutzeroberflächen gesteuert. Dank des offenen Unterbaus lassen sie sich flexibel bei einem Cloud-Anbieter nach Wahl betreiben.

› Open Source für die Industrie – Middleware und Orchestrierung:

Die offene Softwareschicht sitzt als modularer Baukasten direkt zwischen Hardware und Anwendung. Entwickler und Dienstleister können einzelne Bausteine über offene Schnittstellen frei kombinieren und austauschen, ohne das Gesamtsystem neu aufbauen zu müssen. Da der Code komplett öffentlich zugänglich ist, bleibt jeder Datenstrom transparent und nachvollziehbar.

› Silicon Diversity – Infrastruktur und Hardware:

Die physische Basis liefert die reine Rechenleistung. Durch die technologische Offenheit auf Chiplevel bleibt die Hardware flexibel austauschbar und frei kombinierbar. Das schützt Unternehmen vor der Abhängigkeit von einzelnen, dominierenden Chipherstellern.

eine neue Konnektivität über nationale Grenzen hinweg geschaffen.

Für Anwender bedeutet das vor allem maximale Flexibilität. Damit wird ein zentrales Ziel digitaler Souveränität Realität: mehr Handlungsfreiheit, weniger technologische Abhängigkeiten und eine umsetzbare, zukunftsfähige Multi-Cloud-Strategie.

Wie NeoNephos europäische KI umsetzbar machen kann

Mit der Umsetzung des Cloud-Edge-Kontinuums ist ein großer Schritt in Richtung digitaler Souveränität gemacht. Da digitale Souveränität ein vielschichtiges Thema ist, das ganzheitlich gedacht werden muss, sind die von NeoNephos etablierten Kompatibilitäts- und Governance-Richtlinien bewusst flexibel gestaltet. Auf diese Weise stünde die Architektur perspektivisch auch jenen Komponenten offen, die künftig im Rahmen des Ende 2025 initiierten IPCEI-AI zu erwarten sind. Das IPCEI-AI konzentriert sich auf Künstliche Intelligenz und ist darauf ausgelegt, auf den Fundamenten des IPCEI-CIS aufzubauen. Die Schlüsseltechnologie KI wird bereits

heute maßgeblich über Cloud-Infrastrukturen genutzt. Damit unterliegt sie im Zweifelsfall ähnlichen Einschränkungen der Handlungsfreiheit wie proprietäre Clouds und Software. Das Open-Source-Modell von NeoNephos bietet hier das technologische Fundament, um die Prinzipien der Interoperabilität langfristig auch auf den Bereich der Künstlichen Intelligenz zu übertragen.

Fazit: Digitale Souveränität entsteht nicht durch Abschottung, sondern durch offene Zusammenarbeit – und die Fähigkeit, digitale Infrastrukturen selbst zu gestalten.

NeoNephos überträgt den europäischen Gedanken der gemeinsamen Entwicklung auf die digitale Infrastruktur und adressiert damit eine der aktuell größten wirtschaftlichen Herausforderungen: Wie können Europa und seine Unternehmen in Zeiten geopolitischer Unsicherheiten digital souverän handeln und ihre strategische Handlungsfreiheit bewahren?

Der Fahrplan der Initiative ist durch EU-Rahmenwerke klar strukturiert und denkt Cloud-Lösungen konsequent zu Ende: vom Rechenzentrum über das Netzwerk-Edge bis hin zur Künstlichen Intelligenz. Das Ziel ist ein groß angelegter Fragmentierungsabbau durch das erste europäische Cloud-Edge-Kontinuum. Mittels interoperabler Cloud-nativer Module wird der Wechsel zwischen Cloud-Anbietern sowie deren Kombination erheblich vereinfacht.

Als Open-Source-Stiftung geht NeoNephos bewusst einen radikal anderen Weg als die dominierenden Hyperscaler. Statt proprietärer Codes und künstlicher Abhängigkeiten stehen Kollaboration, Transparenz, Handlungsfreiheit und echte technologische Unabhängigkeit im Mittelpunkt. Damit schafft die Initiative eine wichtige Grundlage für digitale Souveränität und die langfristige Wettbewerbsfähigkeit europäischer Unternehmen.

Der Autor



Stephan Ilaender ist Field CTO bei STACKIT, dem souveränen europäischen Hyperscaler von Schwarz Digits. In dieser Funktion berät Ilaender Kunden bei der Transformation ihrer IT-Infrastruktur und unterstützt sie dabei, digital souverän zu werden und zu agieren.

Telefónica: Innovationskraft und Datensouveränität im Einklang

Von Lasse Jenzen

Unternehmen bewegen sich aktuell in einem heiklen Spannungsfeld: Auf der einen Seite herrscht ein massiver Druck, Innovationsprozesse mit Cloud-Technologien, Daten und Künstlicher Intelligenz (KI) voranzutreiben. Auf der anderen Seite verlangen regulatorische Anforderungen und geopolitische Risiken nach souveränen, lokal betriebenen Lösungen, die genau diese Innovationskraft hemmen können. Ein Beispiel der Telefónica Deutschland zeigt, wie sich auch beim Einsatz hochsensibler Daten ein gesundes Gleichgewicht zwischen geschäftlichem Nutzen sowie der erforderlichen Kontrolle und Sicherheit herstellen lässt.

Die Telefónica Deutschland verarbeitet vertrauliche Telekommunikationsdaten – sogenannte Call Detail Records – von über 35 Millionen Kunden. Infolgedessen fällt das Unternehmen unter das Dachgesetz für den Schutz und die Resilienz von kritischen Infrastrukturen (KRITIS). Das bedeutet, dass die Anforderungen an die Datensouveränität und -sicherheit besonders hoch sind. Im Gegenzug hängt der wirtschaftliche Erfolg in hohem Maße von einem unternehmensweiten Einsatz der Datenbestände ab. Die Verantwortlichen meistern diesen Balanceakt durch eine spezielle Kombination technologischer Komponenten.

„At Telefónica Germany, we are committed to maintain the highest standards of data privacy and IT security for our customers.“

*Dr. Jens Johannesson,
Head of Data Intelligence,
Telefónica Deutschland*

Komponente 1: Sovereign Public Cloud

Die Datenlandschaft von Telefónica basiert auf Azure-Cloud-Technologien von Microsoft. Im Rahmen der sogenannten Sovereign Cloud stellt der Anbieter drei Varianten zur Verfügung: eine Public Cloud, eine Private Cloud sowie die National Partner Cloud.

Das höchste Schutzniveau bieten dabei die Sovereign Private Cloud sowie die Sovereign National Partner Cloud. Der erste Ansatz basiert auf einer lokalen, isolierten Cloud-Plattform, die der Kunde selbst betreibt. Im zweiten Fall wird die Cloud-Umgebung sogar von staatlich genehmigten lokalen Betreibern bereitgestellt, die vollständig unabhängig von Microsoft sind. Der Nachteil: Beide Konzepte schränken aufgrund dieser Vorkehrungen eine dynamische Nutzung von KI und datengetriebenen Geschäftsmodellen sehr stark ein.

Die Telefónica setzt daher bei ihrer Lösung auf die Sovereign Public Cloud. Dieser Ansatz verbindet die Nutzung europäischer Azure-Regionen mit zusätzlichen Kontrollfunktionen für den Datenspeicherort, die Betriebsaufsicht

und die kundenseitig verwaltete Verschlüsselung. Die Kundendaten verbleiben in Europa und unterliegen dem europäischen Recht. Gleichzeitig müssen die Workloads nicht in eine separate Cloud-Umgebung migriert werden.

Allerdings ist die Public Cloud für sich genommen problematisch hinsichtlich der Erfüllung der regulatorischen Anforderungen. Als US-amerikanisches Unternehmen unterliegt Microsoft dem US Cloud Act. Das heißt, dass US-Behörden unter bestimmten Voraussetzungen einen Zugriff auf die Daten verlangen können – unabhängig davon, wo diese physisch gespeichert sind. Ein relevanter Unsicherheitsfaktor besteht somit weiterhin.

Komponente 2: Azure Databricks Confidential Computing

Um diese Sicherheitslücken zu schließen, kommt bei Telefónica ein spezieller Lösungsaufbau zum Einsatz. Das Unternehmen nutzt eine Azure-Databricks-Plattform in der Public Cloud, die mit Confidential Computing als zusätzlichem Sicherheitslayer ausgestattet ist. Das Besondere an Confidential Computing: Die Daten sind nicht nur bei der Speicherung und Übertragung vor unautorisierten Zugriffen geschützt, sondern auch während der Verarbeitung.

Ermöglicht wird dies durch hardwarebasierte, isolierte Ausführungsumgebungen, sogenannte Trusted Execution Environments. Hier lassen sich Analysen sensibler Daten nur mit eigens bereitgestellten Sicherheitscodes durchführen. Zusammen mit den gängigen Schutzmaßnahmen für die Datenspeicherung und -übertragung wird letztlich eine Ende-zu-Ende-Verschlüsselung ermöglicht, die selbst privilegierte Systemzugriffe – etwa durch Administratoren oder den Cloud-Betreiber – technisch einschränkt und kontrollierbar macht.

Auf diese Weise entsteht schließlich ein praktikabler Mittelweg. Telefónica kann die Innovationspotenziale der Public Cloud erschließen und gleichzeitig das erforderliche Maß an Sicherheit und Datensouveränität gewährleisten.

Fazit: Datensouveränität hängt nicht nur vom Provider ab

Datensouveränität muss also kein Hindernis bei der digitalen Transformation des Geschäfts sein. Sie entsteht auch nicht allein durch den Cloud-Anbieter. Vielmehr kommt es auf ein ausgewogenes Zusammenspiel von Governance, Architektur und technischer Absicherung an. Die zentrale Herausforderung besteht darin, Innovation und Kontrolle miteinander zu verbinden, statt sie gegeneinander auszuspielen.

Das Beispiel zeigt: Datensouveränität ist kein Entweder-oder. Unternehmen müssen Kontrolle und Innovationsgeschwindigkeit ausbalancieren – nicht nur im KRITIS-Umfeld. Daraus ergeben sich fünf zentrale Managementfragen:

1. **Datenklassifizierung:** Welche Daten und Anwendungen sind kritisch?
2. **Architekturstrategie:** Welche Workloads gehören in welche Cloud?
3. **Governance:** Wie werden Verantwortlichkeiten, Compliance und Audits organisiert?
4. **Souveränität und Regulierung:** Welche Anforderungen ergeben sich aus CLOUD Act, NIS2, KRITIS und weiteren Vorgaben?
5. **Innovationsfähigkeit:** Wo ist Geschwindigkeit ein entscheidender Wettbewerbsfaktor?

Gleichzeitig etablieren sich alternative Cloud-Angebote. Neben Sovereign-Cloud-Ansätzen gewinnen auch nationale Provider an Bedeutung, die mit einer stärkeren lokalen Kontrolle werben, ohne die Innovationskraft außer Acht zu lassen. Zwar zeigt sich, dass entsprechende Lösungen gegenwärtig noch nicht vollkommen ausgereift sind. Gerade bei den Services für den Aufbau moderner Cloud-Plattformen besteht ein gewisser Nachholbedarf. Doch die stetig wachsende Nachfrage wird die Entwicklung sichtbar vorantreiben, sodass auch hier bald relevante Ansätze zu erwarten sind.

Der Autor



Lasse Jenzen ist Associate Partner bei dem Daten- und KI-Experten ORAYLIS. Er konzipiert in führender Funktion moderne Cloud-Plattformen für den gehobenen Mittelstand und Konzerne auf Basis von Microsoft- und Databricks-Technologien. Mit

seiner langjährigen Erfahrung im Bereich Datenarchitektur ist er darauf spezialisiert, Prozesse zur Datenintegration und -transformation vollständig zu automatisieren und dabei maximale Effizienz und Datensicherheit zu gewährleisten.

Wachstum braucht kontrollierbare Infrastruktur

Von Sebastian Cler

Der nächste Engpass der KI-Wirtschaft ist nicht der Algorithmus. Entscheidend ist, ob Unternehmen über Rechenleistung, Sicherheit, Datenkontrolle und tragfähige Betriebsmodelle verfügen, um digitale Geschäftsmodelle tatsächlich zu skalieren. Für den Mittelstand bedeutet das: Souveränität entsteht nicht durch Abschottung, sondern durch bewusst getroffene Architekturentscheidungen.

Rechenleistung wird zur strategischen Engpassressource

Viele Vorstände diskutieren über KI-Strategien, ohne die Infrastrukturfrage beantwortet zu haben. Doch wer über Künstliche Intelligenz, Automatisierung, Cloud oder datengetriebene Geschäftsmodelle spricht, spricht immer auch über verfügbare, sichere und skalierbare IT-Kapazität.

Der Markt zeigt, wie schnell sich diese Frage zuspitzt. Laut Bitkom wird sich die installierte Rechenzentrumsleistung in Deutschland von rund 2.980 Megawatt im Jahr 2025 auf mehr als 5.000 Megawatt bis 2030 erhöhen. Gleichzeitig wird der Anteil von KI- und hochrechenintensiven Anwendungen von rund 15 auf 40 Prozent wachsen. Rechenzentren werden somit zu einem entscheidenden Faktor für Produktivität, Innovationsfähigkeit und digitale Souveränität.

Der Mittelstand steht vor einer neuen Make-or-Buy-Frage

Viele mittelständische IT-Organisationen arbeiten bereits am Limit. Betrieb, Security, Cloud, Compliance und Notfallmanagement binden Ressourcen, während gleichzeitig Fachkräfte fehlen. Für viele Unternehmen ist es daher kaum realistisch, Rechenzentrumsbetrieb, Cloud-Architektur, 24/7-Security, Compliance und Wiederherstellung vollständig intern aufzubauen.

Die Frage lautet deshalb nicht mehr: Eigenbetrieb oder Outsourcing? Sie lautet: Welche Verantwortung bleibt im Unternehmen – und wo erhöhen externe Partner Stabilität, Sicherheit und Skalierbarkeit?

Souveränität heißt Entscheidungsfähigkeit

Digitale Souveränität wird häufig mit Datenlokation verwechselt. Natürlich ist es relevant, ob Daten in Deutschland, Europa oder einem anderen Rechtsraum verarbeitet werden. Entscheidend ist aber nicht allein, wo Server stehen. Entscheidend ist, ob Unternehmen ihre Abhängigkeiten kennen und steuern können: Wo liegen welche Daten? Wer hat Zugriff? Welche Subdienstleister sind beteiligt? Welche Exit-Optionen gibt es? Wie schnell lassen sich kritische Systeme wiederherstellen?

Richtig gestaltete externe Infrastruktur kann Kontrolle sogar erhöhen: durch geprüfte Prozesse, klare Verantwortlichkeiten, doku-

mentierte Sicherheitsmechanismen, transparente Nachweise und belastbare Service Level. Souverän ist nicht das Unternehmen, das alles besitzt. Souverän ist das Unternehmen, das seine Architektur bewusst steuert.

Colocation als kontrollierbarer Mittelweg

Viele mittelständische Unternehmen suchen ein Modell, das Kontrolle und Professionalität verbindet. Colocation bietet genau das: Unternehmen betreiben ihre eigene Hardware in einem externen, hochverfügbaren Rechenzentrum – mit professioneller Energieversorgung, physischer Sicherheit, redundanter Netzanbindung und 24/7-Monitoring.

Der Nutzen liegt in der Kombination: hohe Ausfallsicherheit, Entlastung der internen IT, bessere Skalierbarkeit und geringere Investitionen in eigene Infrastruktur. Zugleich behalten Unternehmen die Kontrolle über Server, Anwendungen und Daten. Colocation ist damit weder klassischer Eigenbetrieb noch vollständige Cloud-Nutzung, sondern ein pragmatischer Mittelweg. Moderne Architekturen verbinden Colocation mit Private Cloud, Hybrid-Cloud, Managed Services und IT-Security – je nach Schutzbedarf und Workload.

Praxisbeispiel: Wenn Verfügbarkeit über Umsatz entscheidet

Für viele Mittelständler sind digitale Vertriebskanäle längst kein Zusatzgeschäft mehr, sondern zentraler Umsatzbringer. Ein anonymisiertes Beispiel aus dem B2B-Handel zeigt, wie schnell daraus eine strategische Infrastrukturfrage wird: Über die digitale Plattform eines mittelständisch geprägten Handelsunternehmens werden täglich Waren im siebenstelligen Eurobereich bestellt; ein Teil der Kunden wird Just-in-Time beliefert.

Die Herausforderung lag nicht allein in zusätzlicher Rechenleistung. Entscheidend waren maximale Verfügbarkeit, sichere Anbindung an das Warenwirtschaftssystem und stabile Performance bei Lastspitzen. Die Lösung: eine hybride IT-Architektur aus virtuellen und dedizierten Systemen, kombiniert mit Datenbankbetrieb, Loadbalancing, Firewall-Schutz, Backup, Monitoring und 24/7-Betriebsverantwortung.

So konnte das Unternehmen sein digitales Geschäftsmodell weiter skalieren. Die interne

IT blieb steuernd eingebunden, wurde aber bei Betrieb, Verfügbarkeit und Sicherheit entlastet. Genau darin liegt moderne Souveränität: Kontrolle behalten, ohne jede Fähigkeit selbst vorhalten zu müssen.

Europäische Infrastruktur bewusst nutzen

Europäische und deutsche Infrastrukturanbieter spielen dabei eine wichtige Rolle. Nicht aus Protektionismus, sondern aus Gründen des Risikomanagements. Wer kritische Daten und Anwendungen betreibt, braucht Alternativen zu einseitigen Plattformabhängigkeiten. Europäische Anbieter können Rechtsraum, Nähe, Nachvollziehbarkeit und ein besseres Verständnis regulatorischer Anforderungen verbinden.

Gleichzeitig dürfen europäische Lösungen nicht verklart werden. Sie müssen leistungsfähig, wirtschaftlich und integrationsfähig sein. Der Anspruch muss deshalb sein, souveräne Infrastrukturen als professionell anschlussfähige Alternative zu verstehen: sicher, flexibel, auditierbar und praxistauglich. Risiken sind nicht per se schlecht. Aber sie müssen bewusst eingegangen werden.

Was Entscheider jetzt tun müssen

Digitale Geschäftsmodelle, KI und Skalierung scheitern selten an Ideen, sondern häufig an fehlender oder nicht ausreichend kontrollierbarer Infrastruktur. Für die Geschäftsführung gilt daher: Infrastrukturstrategie ist Unternehmensstrategie.

Der erste Schritt muss keine große Migration sein. Oft genügt ein strukturierter Infrastruktur-Check: Welche Anwendungen und Daten sind geschäftskritisch? Wissen wir, wo sie liegen, wer Zugriff hat und wie ein Exit möglich wäre? Können wir Verfügbarkeit, Security und Wiederherstellung intern dauerhaft leisten – oder brauchen wir gezielt externe Expertise?

Darauf aufbauend lässt sich das passende Betriebsmodell wählen: Eigenbetrieb für strategische Systeme, Colocation für Kontrolle ohne eigene Rechenzentrumsinvestitionen, Private oder Hybrid-Cloud für Skalierung, Managed Security für zusätzlichen Schutz. Die nächste Welle der Digitalisierung entscheidet sich nicht allein an Algorithmen, sondern an der Infrastruktur, auf der sie laufen.

Der Autor



Sebastian Cler ist operativer Vorstand der SpaceNet AG. Das Münchner Unternehmen betreibt eigene Rechenzentren und unterstützt mittelständische Kunden mit Colocation, Cloud-, Managed-Services- und IT-Security-Lösungen beim sicheren Betrieb geschäftskritischer IT.

Time-to-Capacity

Die neue Standortwährung der digitalen Wirtschaft

Von Günter Eggers

Deutschland braucht neue Wachstumspfade: durch KI, durch eine produktive digitale Verwaltung und durch Industrieunternehmen, die aus Daten endlich mehr Wertschöpfung generieren. Doch eine wichtige Voraussetzung wird dabei noch zu oft übersehen: Rechenleistung.

Rechenzentren sind die physische Basis der digitalen Wirtschaft. Ohne sie bleibt KI ein Versprechen, Cloud-Souveränität ein unerfüllter Anspruch und Digitalisierung ein Projektplan. Jede digitale Anwendung in Unternehmen, Behörden, Kliniken oder Forschung braucht sichere, hochverfügbare und effizient betriebene Infrastruktur. Die Standortfrage der nächsten Jahre lautet deshalb auch: Wo entsteht Rechenleistung, die Wachstum ermöglicht?

Deutschlands Ausgangslage

Deutschland startet nicht bei null. Mit über 2.000 Rechenzentren und rund 3.000 Megawatt installierter IT-Anschlussleistung, davon erst etwa 500 Megawatt für KI und Hochleistungsrechnen, ist das Land bereits einer der führenden Standorte Europas. Die industrielle Nachfrage ist vorhanden, zentrale Internetknoten, Know-how und Investoren ebenfalls. Auch politisch ist die Bedeutung angekommen: So wurde im März 2026 die Nationale Rechenzentrumsstrategie beschlossen, die das Ziel benennt, die IT-Anschlussleistung bis 2030 gegenüber 2025 zu verdoppeln und jene für KI und Hochleistungsrechnen mindestens zu vervierfachen. Die Richtung stimmt. Doch der Kern liegt in der Umsetzung. Der Engpass ist nicht fehlende Nachfrage oder fehlendes Kapital.

Fünf Standortaufgaben für die KI-Ökonomie

- 1. Rechenzentren als Wachstumsinfrastruktur begreifen.** Ohne verfügbare Kapazität keine skalierbare KI, keine souveräne Cloud, keine digitale Industrie.
- 2. Time-to-Capacity zur Standortkennzahl machen.** Entscheidend ist nicht nur, ob Projekte gewollt sind, sondern auch, wann sie tatsächlich ans Netz gehen.
- 3. Energie, Genehmigung und Flächen zusammen planen.** Digitale Infrastruktur braucht leistungsfähige Stromnetze, Glasfaser, Bauleit- und Wärmeplanung.
- 4. Ambition europäisch anschlussfähig halten.** Effizienz und Nachhaltigkeit sind Standortvorteile. Nationale Sonderwege sind es nicht.
- 5. Kommunen zu Partnern machen.** Akzeptanz entsteht durch lokale Wertschöpfung, Abwärmeperspektiven, Infrastruktur und frühzeitige Einbindung.

Nach Berechnungen der German Datacenter Association erfordert allein die Verdopplung Investitionen von 30 bis 40 Milliarden Euro. Der Engpass liegt vielmehr darin, ob diese Projekte rechtzeitig realisiert werden: mit Flächen, Anschlussleistung, Genehmigungen, realistischen Effizianzforderungen und Akzeptanz vor Ort.

Time-to-Capacity als Standortfaktor

Die neue Standortwährung heißt Time-to-Capacity. Früher fragte man: Wann läuft die Fabrik? Heute kommt hinzu: Wann ist die Rechenkapazität verfügbar? Für Unternehmen, Investoren und öffentliche Auftraggeber entscheidet diese Frage über den Standort. Wer KI-Modelle trainieren, Daten sicher verarbeiten oder digitale Dienste skalieren will, braucht planbar zusätzliche Kapazität.

Damit Kapazität entsteht: Drei Hebel für schnellere Realisierung

Drei Hebel sind jetzt wichtig:

1. Integrierte Infrastrukturplanung

Der erste Schritt ist eine integrierte Infrastrukturplanung. Rechenzentren entstehen nicht isoliert. Sie brauchen Stromnetze, Flächen, Bauleitplanung, Konnektivität und Fachkräfte. Heute werden diese Fragen zu oft getrennt behandelt. Der globale Wettbewerb entscheidet aber parallel. Ob ein Standort geeignet ist, hängt heute primär davon ab, welche elektrische Anschlussleistung zeitnah verfügbar ist, welche Genehmigungen nötig sind und wie eng Kommunen, Netzbetreiber und Betreiber zusammenarbeiten.

2. Planbare Netzanschlüsse

Zweitens muss der Netzanschluss planbarer werden. Es ist richtig, knappe Kapazitäten nicht einfach nach dem Prinzip „Wer zuerst kommt, mahlt zuerst“ zu vergeben. Realisierungsreife muss zählen. Gleichzeitig darf daraus kein „Henne-Ei-Problem“ entstehen: Investoren brauchen eine belastbare Anschlusszusage, um Finanzierung und Fläche final zu sichern. Eine Anschlusszusage setzt aber oft genau diese Punkte voraus. Eine frühe, bedingte Reservierung kann beide Seiten absichern: verbindlich genug für Investoren, aber an klare Meilensteine geknüpft. Das ersetzt den Netzausbau jedoch nicht. Deutschland muss seine Netze schneller ausbauen.

3. Verlässliche und europäisch anschlussfähige Regulierung

Drittens braucht Regulierung Verlässlichkeit und europäische Anschlussfähigkeit. Effizienz, erneuerbare Energien und Abwärmenutzung sind richtige Ziele. Daran hat die Branche selbst ein Interesse. Regeln müssen jedoch in der Praxis funktionieren und zu europäischen Standards passen. Nationale Sonderwege erhöhen den Aufwand, ohne automatisch mehr Nachhaltigkeit zu schaffen. Sie können im Gegenteil dazu führen, dass Kapazität außerhalb Deutschlands entsteht.

Abwärme und Akzeptanz vor Ort: Rechenzentren als Teil der lokalen Infrastruktur

Ein gutes Beispiel ist Abwärme. Das Potenzial ist real. Die Umsetzung ist häufig sehr langwierig. Wo Standort, Wärmenetz und Abnehmer zusammenpassen, kann die Abwärme von Rechenzentren einen Beitrag zur lokalen Wärmenetze leisten. Aber Wärme lässt sich nicht per Gesetz nutzbar machen. Wärme wird erst nutzbar, wenn vor Ort ein Abnehmer existiert, sich die Investition trägt und alle früh genug miteinander planen.

Das gilt auch für die Akzeptanz vor Ort. Rechenzentren müssen gute Nachbarn sein. Anliegen von Bürgerinnen und Bürgern, Kommunen und der lokalen Wirtschaft sind ernst zu nehmen. Wer eine schnellere Umsetzung digitaler Infrastruktur ermöglichen will, muss aufzeigen, welchen Nutzen sie vor Ort bringt: Einnahmen für die Gemeinde, Perspektiven für die Wärmewende und Verlässlichkeit im Dialog.

Fazit: Kapazität entsteht durch Umsetzung

Noch ist es nicht zu spät für Deutschland. Aber: Strategien allein schaffen noch keine Kapazität. Am Ende zählen angeschlossene Megawatt, genehmigte Standorte, verlässliche Zeitpläne und Rechenzentren, in denen die Server tatsächlich laufen.

Als Stimme der Rechenzentrumsbranche bringt die GDA die Beteiligten dafür an einen Tisch: Politik, Netzbetreiber, Kommunen und Betreiber. Die Frage ist deshalb nicht, ob Deutschland neue Rechenzentren braucht. Die Frage ist, ob wir sie rechtzeitig ermöglichen. Wer KI, digitale Souveränität und neues Wachstum möchte, muss Rechenleistung als das betrachten, was sie ist: eine Schlüsselressource der kommenden Wirtschaftsordnung.

Der Autor

Günter Eggers ist Vorstandsvorsitzender der German Datacenter Association (GDA).

