

L Ü N E N D O N K „

Lünendonk®-Studie

Digitale Souveränität – Vom Risiko zur Resilienz

Balanceakt zwischen technischem Fortschritt und geopolitischer Realität

Eine Studie von Lünendonk & Hossenfelder in Zusammenarbeit mit

adesso

exeta



MAIBORNWOLFF

MATERNA

msg

TECHNI
DATA
it-gruppe

Inhaltsverzeichnis

Vorwort	3
Management Summary	4
Rückblick: Wichtige Ereignisse im Überblick	5
Methodik	6
Standortbestimmung: was, wo, wie & warum?	
Digitale Souveränität in der Praxis	8
Status quo: Wo Unternehmen und Organisationen heute stehen	17
Souveräne Cloud: Neue Marktchancen für Hyperscaler und europäische Superscaler	21
Investitionen, Verantwortlichkeiten & Rolle externer Partner	28
Fazit & Ausblick	31
Nachwort	33
Beiträge der Studienpartner	
Fachbeitrag von adesso	35
Lünendonk im Interview mit	
Exxeta	40
MaibornWolff und dem FWU	43
Materna	47
msg	50
TechniData	53
Unternehmensprofile	56
Lizenz- und Studieninformation	62
Über Lünendonk & Hossenfelder	63





Vorwort

Tobias Ganowski
Senior Consultant



Liebe Leserinnen, liebe Leser,

Digitale Souveränität ist kein abstraktes Leitbild mehr – sie hat sich zu einem zentralen Wettbewerbsfaktor mit klar messbarem Business Impact entwickelt. 2026 steht Europa an einem digitalen Wendepunkt: Globale Spannungen, extraterritoriale Gesetzgebung und die wachsende Dominanz internationaler Technologieanbieter werfen grundlegende Fragen auf. Wer kontrolliert unsere Daten? Wie abhängig sind wir innerhalb unserer IT Wertschöpfungsketten von einzelnen Technologielieferanten? Und wie sichern Unternehmen ihre digitale Handlungsfähigkeit in einer Welt, in der Innovationen immer schneller, Risiken aber immer komplexer werden?

Dabei ist digitale Souveränität nicht mit Autarkie oder einer Abkehr von US-amerikanischen Technologieanbietern gleichzusetzen. Entscheidend ist die bewusste Steuerung von Abhängigkeiten: Hyperscaler bleiben aufgrund ihrer Innovationskraft und Skalierbarkeit essenzielle Bausteine moderner IT-Architekturen. Gleichzeitig gewinnen souveräne Alternativen überall dort an Bedeutung, wo Kontrolle, Compliance oder besondere Schutzanforderungen strategisch relevant sind.

Unternehmen, die ihre digitale Souveränität stärken, gewinnen weit mehr als Risikominimierung. Sie schaffen Vertrauen bei Kunden und Partnern, erhöhen Effizienz durch klare und flexible IT-Architekturen, stärken ihre Verhandlungsposition gegenüber Technologieanbietern und schaffen Freiräume für zukunftsweisende Innovation. Kurz: Sie gestalten digital – statt lediglich auf äußere Impulse zu reagieren.

Der Weg dorthin ist jedoch anspruchsvoll. Historisch gewachsene Systemlandschaften, begrenzte Transparenz über Datenbestände und ganzheitliche Prozessketten, komplexe Multi-Cloud-Strukturen und steigende regulatorische Anforderungen machen digitale Souveränität zu einem komplexen, strategischen Transformationsvorhaben. Genau hier setzt diese Studie an: Sie gibt Orientierung, schafft Klarheit und zeigt, welche Weichen Unternehmen jetzt stellen müssen, um ihre digitale Zukunft aktiv und souverän zu gestalten.

Die vorliegende Studie bietet einen umfassenden Überblick über den aktuellen Stand und die zentralen Prioritäten digitaler Souveränität. Sie entstand in Kooperation und fachlicher Zusammenarbeit mit adesso, Exxeta, MaibornWolff, Materna, msg und TechniData.

Wir wünschen Ihnen eine informative Lektüre und freuen uns auf Ihr Feedback.

Tobias Ganowski

Management Summary

TREIBER FÜR DIGITALE SOUVERÄNITÄT

95 %

Reduktion von zu hohen Abhängigkeiten in der IT-Lieferkette

94 %

Stärkung der Resilienz in Krisensituationen

93 %

Schutz vor unkontrolliertem Datenabfluss & extraterritorialen Zugriffen

93 %

Umsetzung regulatorischer Anforderungen

96 Prozent

ERWARTEN, DASS DIGITALE SOUVERÄNITÄT AUCH BEI EINER ENTSPANNUNG DER GEOPOLITISCHEN LAGE EIN ZENTRALES THEMA BLEIBT.



86 Prozent

halten höhere Investitionen in souveräne Angebote für sinnvoll, da die Opportunitätskosten von nicht-souveränen Angeboten höher sind.

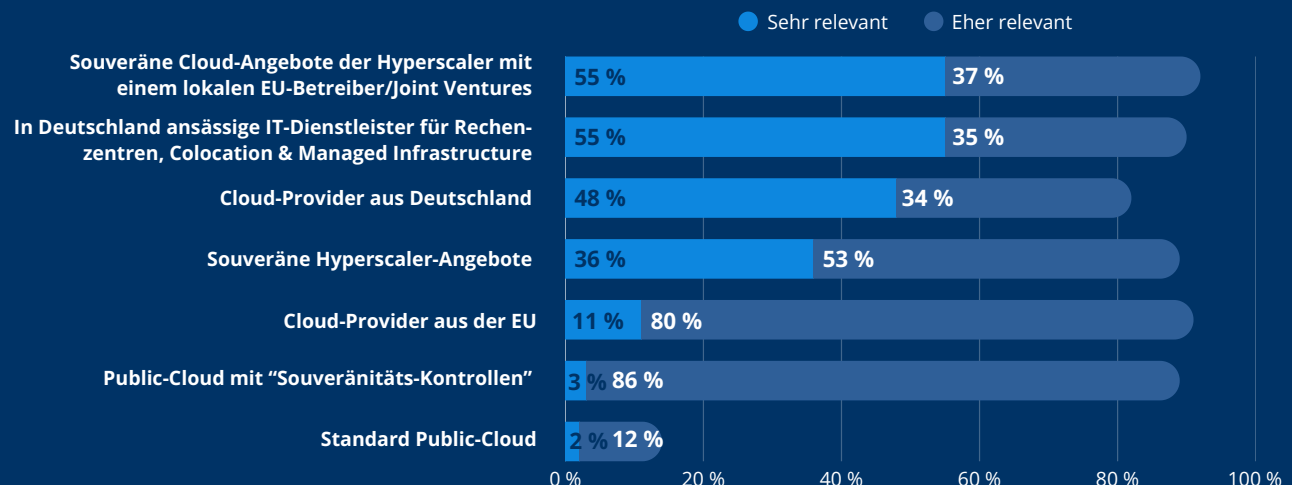
80 Prozent

erhöhen ihr IT-Budget, da Anschaffungs- und Betriebskosten von souveränen Angeboten höher sind.

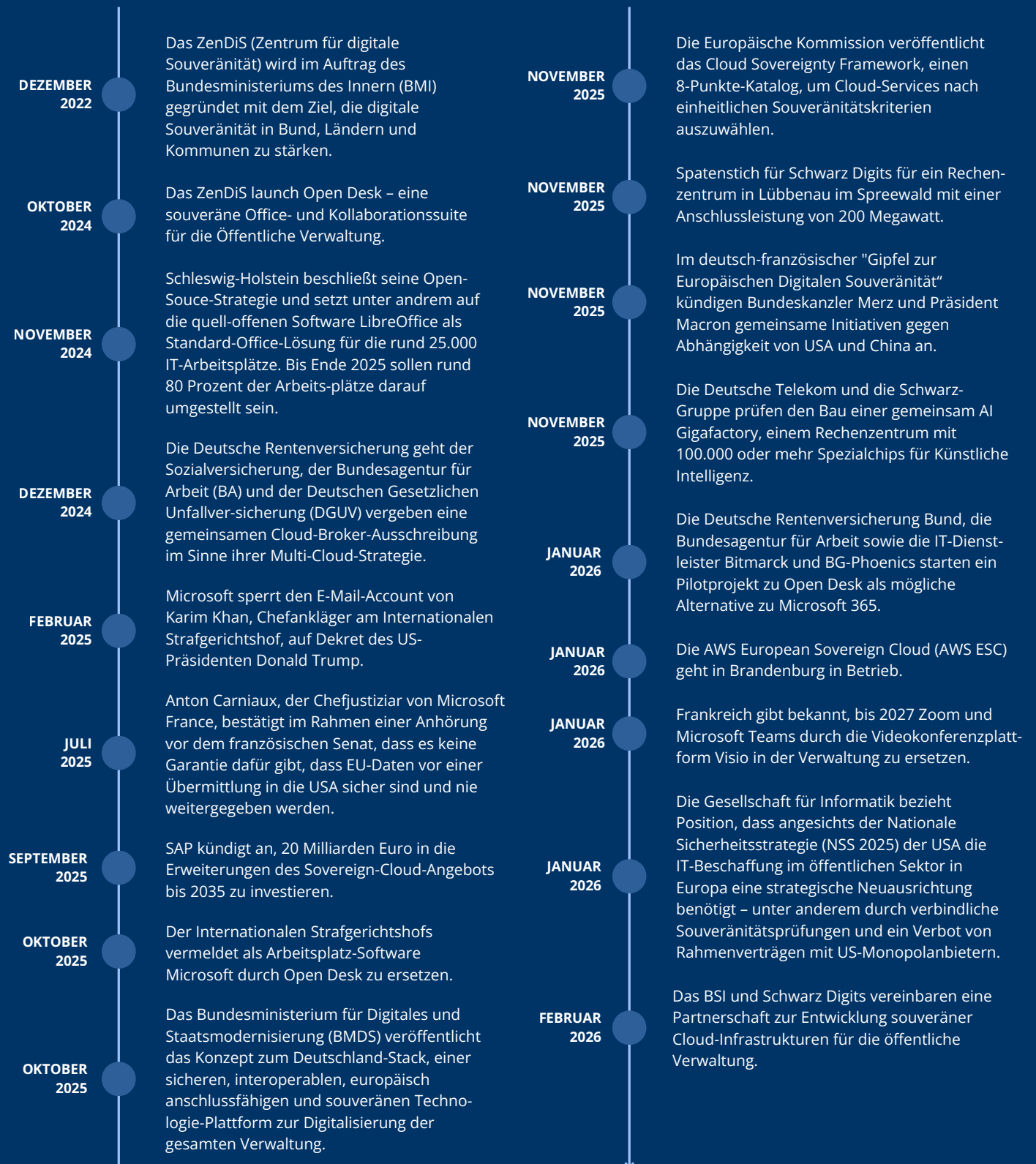
74 Prozent

berücksichtigen digitale Souveränität umfassend in ihrer IT- und Sourcing-Strategie.

Welche Rolle spielen die folgenden Anbietermodelle mit Blick auf die kommenden drei Jahre bei geschäftskritischen Prozessen / sensiblen Daten?



Rückblick: Wichtige Ereignisse im Überblick



Methodik



Für die Studie wurden zwischen Dezember 2025 und Januar 2026 insgesamt 155 Telefoninterviews geführt. Fast die Hälfte der Befragten sind IT-Bereichsleiter, unter anderem aus den Bereichen Enterprise Architecture Management, IT Operations und Anwendungsentwicklung. Rund 20 Prozent bekleiden eine leitende Position im GRC- oder Cyber-Security-Umfeld; ebenfalls knapp jeder Fünfte stammt aus dem IT-Einkauf. CIOs und weitere C-Level-Verantwortliche aus dem Business bilden 16 Prozent der Zielgruppe.

Neben dem in Deutschland traditionell starken Industriesektor lag bei der Branchenverteilung ein besonderer Fokus auf Unternehmen mit kritischen Infrastrukturen (KRITIS).

15 Prozent der Teilnehmenden arbeiten in den Bereichen Gesundheit, Transport/Verkehr, Energie/Utilities oder im öffentlichen Sektor. Zudem ist jeder zehnte Befragte dem Banken- und Versicherungssektor zuzuordnen.

Jeweils die Hälfte der Unternehmen gehört zum gehobenen Mittelstand oder zu den Konzernen. 61 Prozent verfügen über ein stark international ausgerichtetes Geschäft; 39 Prozent sind überwiegend innerhalb der EU oder ausschließlich in Deutschland tätig.

Übersicht der Studienteilnehmer – 155 telefonische Interviews in der DACH-Region

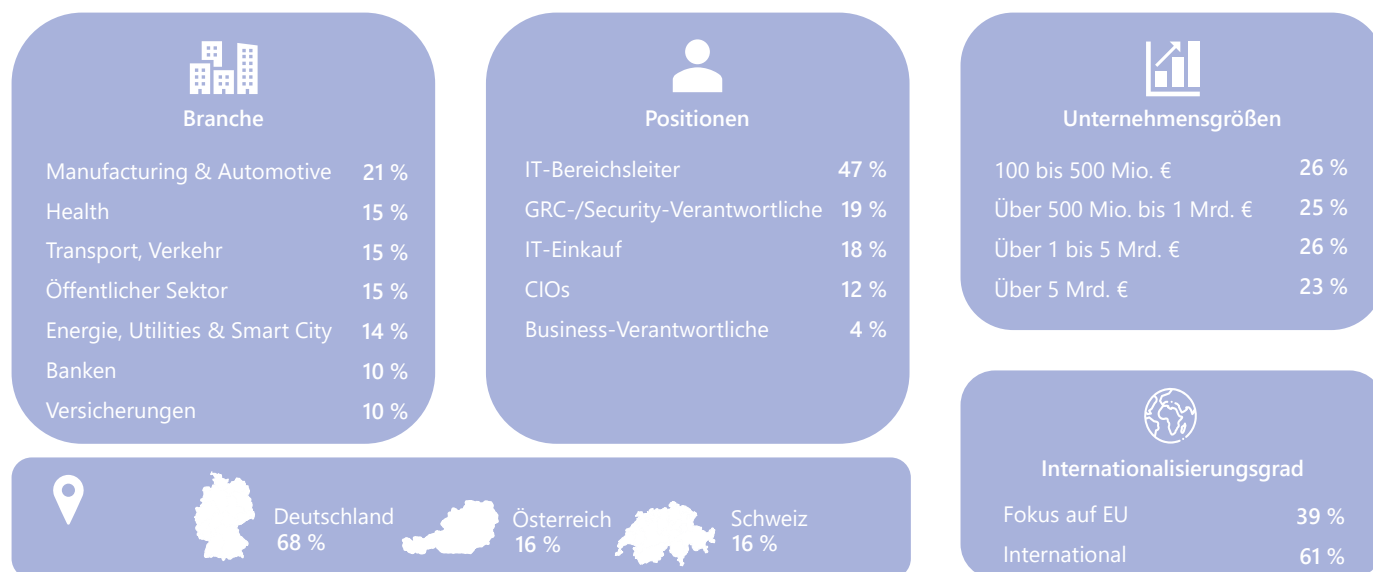


Abb. 1: Branche; Funktion; Unternehmensgröße; Geografische Verteilung; Fokus; relative Häufigkeitsverteilung; n = 155

Ebenso wurde der Cloud-Reifegrad abgefragt, sodass eine differenzierte Betrachtung der Ergebnisse je nach Reifegrad genommen werden kann. Neun von zehn Studienteilnehmern geben an, dass sie Kunde mindestens eines Hyper-scalers sind. 42 Prozent verfügen über eine Multi-Cloud-Architektur, in der mehrere Cloud Services parallel eingesetzt und orchestriert werden. Weitere 46 Prozent planen den Aufbau einer solchen Multi Cloud Struktur – sei es, um Abhängigkeiten im Sinne eines Best-of-Breed-Ansatzes zu einzelnen Anbietern zu reduzieren oder um für kritische Geschäftsprozesse Backup-Services zu einem zweiten Cloud-Provider vorzuhalten (zumindest bei IT-Infrastrukturthemen). Gleichzeitig steigt dadurch jedoch der Management und Integrationsaufwand deutlich.

12 Prozent der Unternehmen – vor allem große Konzerne – schätzen ihren Cloud Reifegrad als hoch ein und zählen sich damit zu den Cloud Leaders. Die große Mehrheit, 77 Prozent, verortet sich im Mittelfeld: Sie nutzen Cloud- Technologien produktiv, verfügen jedoch noch nicht über durchgängig standardisierte Architekturen, Betriebsmodelle oder Governance Strukturen. 11 Prozent der Unternehmen haben einen geringen Cloud-Reifegrad.

Cloud-Reifegrad wird überwiegend mittelmäßig eingeschätzt – Multi-Cloud wird deutlich wichtiger

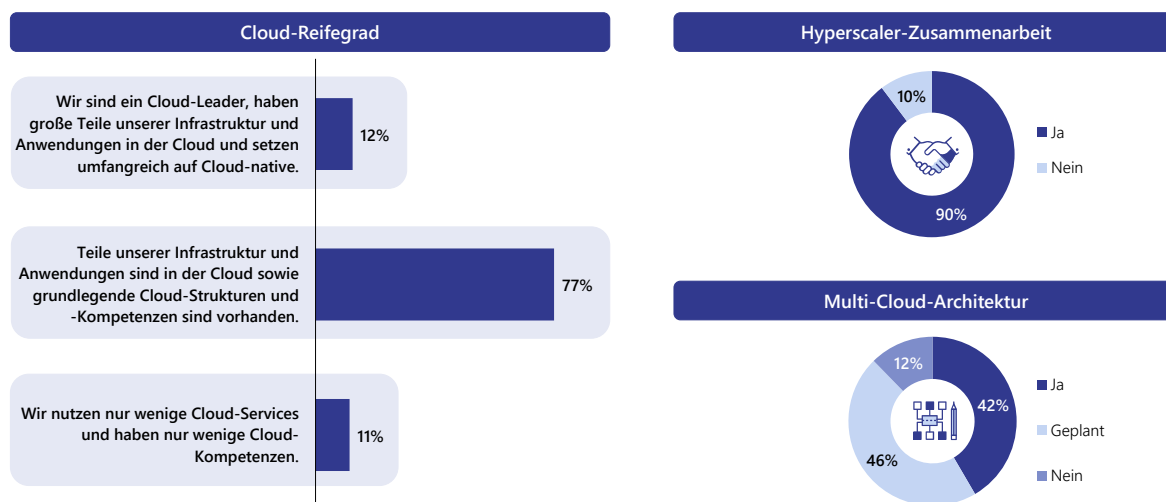


Abb. 2: Wie schätzen Sie den Cloud-Reifegrad Ihrer Organisation ein?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Ist Ihr Unternehmen Kunde von einem Hyperscaler?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Nutzt Ihre Organisation eine Multi-Cloud-Architektur und setzt somit mehrere Cloud-Plattformen ein?; relative Häufigkeitsverteilung; alle Unternehmen; n = 154



Standortbestimmung: was, wo, wie & warum? Digitale Souveränität in der Praxis

”

Das Jahr 2026 markiert für Europa einen Wendepunkt in der digitalen Souveränität: Geopolitische Spannungen, das kritische Hinterfragen extraterritorialer Gesetzgebung sowie wachsende Abhängigkeiten von nicht-europäischen Cloud-, Plattform- und KI-Anbietern rücken für Unternehmen und Organisationen zentrale Fragen in den Fokus – darunter, wem Daten gehören, wer sie verarbeitet, wie stark Unternehmen einzelnen Cloud- und IT-Anbietern vertrauen können, wie sich entsprechende Risiken steuern lassen und welche Alternativen verfügbar sind. Zugleich wird deutlich, dass digitale Fähigkeiten wie die Kontrolle über Daten, Infrastruktur, Lieferketten und KI zu entscheidenden Voraussetzungen für Wettbewerbsfähigkeit und Resilienz geworden sind.

Definition: Souveränität ist vielschichtig

Digitale Souveränität besitzt keine eindeutige Definition und kein allgemein anerkanntes Verständnis. Im Mittelpunkt steht jedoch die Fähigkeit, digitale Technologien, Daten und Infrastrukturen selbstbestimmt zu gestalten, Abhängigkeiten transparent zu steuern und jederzeit handlungsfähig zu bleiben. Sie beschreibt keine vollständige Abschottung oder Autarkie, sondern die bewusste Kontrolle über kritische digitale Abhängigkeiten, sodass Wahlfreiheit und Handlungsspielräume erhalten bleiben. Im Kern geht es darum, externe Risiken – etwa politische Einflussnahmen, Lock-in-Effekte oder regulatorische Konflikte – zu reduzieren und zugleich Innovationsfähigkeit, Wettbewerbsfähigkeit und Resilienz langfristig zu sichern.

Digitale Souveränität umfasst verschiedene Aspekte und verfolgt mehrere Ziele. Im Kern lässt sie sich in vier Dimensionen gliedern:

- **Betriebliche Souveränität** bezeichnet die Fähigkeit, digitale Systeme, Prozesse und Anbieterbeziehungen so zu steuern, dass Organisationen jederzeit arbeits- und handlungsfähig bleiben und in zentralen Entscheidungen unabhängig agieren können. Dazu gehört die Vermeidung kritischer Lock-in-Effekte und die Sicherstellung der eigenen Betriebsfähigkeit auch bei externen Störungen oder geopolitischen Risiken wie etwa einem Kill Switch. Stabilität und Agilität stehen dabei in einem ausgewogenen Verhältnis.
- **Technische Souveränität** bezieht sich auf die Verfügbarkeit und Kontrolle über Schlüsseltechnologien wie Cloud-Infrastrukturen, KI oder Sicherheitslösungen. Ziel ist dabei nicht die vollständige Eigenentwicklung, sondern die Fähigkeit, Technologien bewusst auszuwählen, zu kombinieren und eigenständig weiterzuentwickeln, um Abhängigkeiten zu reduzieren und die Innovationsfähigkeit zu stärken. Konkret bedeutet dies, dass IT Systeme interoperabel, portierbar und auditierbar sind, wodurch Vendor-Lock-ins minimiert werden. Beispielsweise findet unter diesen Gesichtspunkten aktuell eine immer stärker geführte Diskussion um Best-of-Breed-Architekturen statt, um in zentralen Applikationslandschaften wie ERP oder CRM an Flexibilität zu gewinnen und zu hohe Abhängigkeiten kritischer Geschäftsprozesse zu einem einzigen Provider zu reduzieren.

- **Datensouveränität** bezeichnet die Fähigkeit, eigene Daten zu besitzen, zu kontrollieren, zu schützen und ihre Nutzung selbst zu bestimmen. Dazu gehören der Ort der Datenspeicherung und -verarbeitung (Datenresidenz), klare Zugriffsrechte, Verschlüsselungshoheit, Transparenz über Datenflüsse sowie die Möglichkeit, Daten sicher mit Partnern auszutauschen oder zurückzuführen. Da Daten und datenbasierte Geschäftsmodelle für Unternehmen stark an Bedeutung gewonnen haben und weiter gewinnen werden, ist Datensouveränität ein zentrales Element digitaler Souveränität.
- **Juristische Souveränität** bedeutet, digitale Systeme so zu betreiben, dass Organisationen rechtskonform nach lokalen Vorgaben handeln können – ohne durch extraterritoriale Gesetze anderer Staaten (wie den CLOUD Act oder FISA) in Konflikte zu geraten. Dies ist entscheidend, um Datenschutz, Informationskontrolle und Compliance sicherzustellen.

Die vier Dimensionen von digitaler Souveränität

Betriebliche Souveränität

- Fähigkeit, digitale Systeme und Prozesse stabil und unabhängig zu betreiben
- Vermeidung kritischer Lock-ins und Sicherstellung der Betriebsfähigkeit
- Kontrolle über Anbieterbeziehungen und Ausfallszenarien
- Resilienz gegenüber geopolitischen oder marktseitigen Störungen



Technologische Souveränität

- Zugriff auf und Kontrolle über Schlüsseltechnologien (Cloud, KI, Security)
- Fähigkeit, Technologien bewusst auszuwählen, zu kombinieren und weiterzuentwickeln
- Nutzung vertrauenswürdiger technologischer Ökosysteme & Open Source
- Reduktion strategischer Abhängigkeiten



Datensouveränität

- Kontrolle darüber, wer auf Daten zugreifen, sie nutzen und verarbeiten darf
- Festlegung von Datenlokalisierung und sicheren Austauschmechanismen
- Sicherstellung von Interoperabilität und Portabilität
- Schutz vor unbefugtem Zugriff, Verlust oder externer Einflussnahme



Juristische Souveränität

- Sicherstellung der Compliance mit europäischen und nationalen Vorgaben
- Minimierung von Konflikten mit extraterritorialen Gesetzen anderer Staaten
- Transparenz über Datenflüsse und Verantwortlichkeiten
- Rechtskonformer Betrieb selbst in internationalen Systemlandschaften



Abb. 3: Überblick über die vier Dimensionen der digitalen Souveränität; Darstellung Lünendonk

Diese vier Dimensionen bilden gemeinsam das Fundament, das Organisationen benötigen, um in einer digitalisierten Welt handlungsfähig, rechtskonform und wettbewerbsfähig zu bleiben. Entsprechend stuften nahezu alle Studienteilnehmer diese Elemente als wichtig für ihre Organisation ein – mit besonderem Fokus auf Datensouveränität und betriebliche Souveränität. Daten und datenbasierte Geschäftsmodelle gewinnen im Zuge der Digitalisierung stark an Bedeutung und entwickeln sich zunehmend zu einem zentralen Wertschöpfungs- und Differenzierungsfaktor. Betriebliche Souveränität wiederum zielt auf Resilienz und Stabilität ab und stellt sicher, dass digitale Handlungsfähigkeit jederzeit gewährleistet ist.

Technische Souveränität ist ebenfalls erstrebenswert, doch die Befragten betrachten Abhängigkeiten von einzelnen IT- oder Cloud-Providern nicht grundsätzlich als nachteilig. Deshalb stuften sie diese Dimension als etwas weniger relevant ein. Ebenso existieren für bestimmte Use Cases keine souveränen oder europäischen Alternativen mit ähnlichen Eigenschaften, sodass aufgrund fehlender Alternativen kein Wechsel möglich oder praktikabel ist. Ähnlich verhält es sich mit der juristischen Souveränität: Je nach Use Case bestehen vereinzelte Möglichkeiten, Rechtskonformität sicherzustellen und zu steuern – auch wenn dies mit Kompromissen bei der Innovationsfähigkeit verbunden sein kann.

Betriebliche Souveränität und Datensouveränität sind unverhandelbar

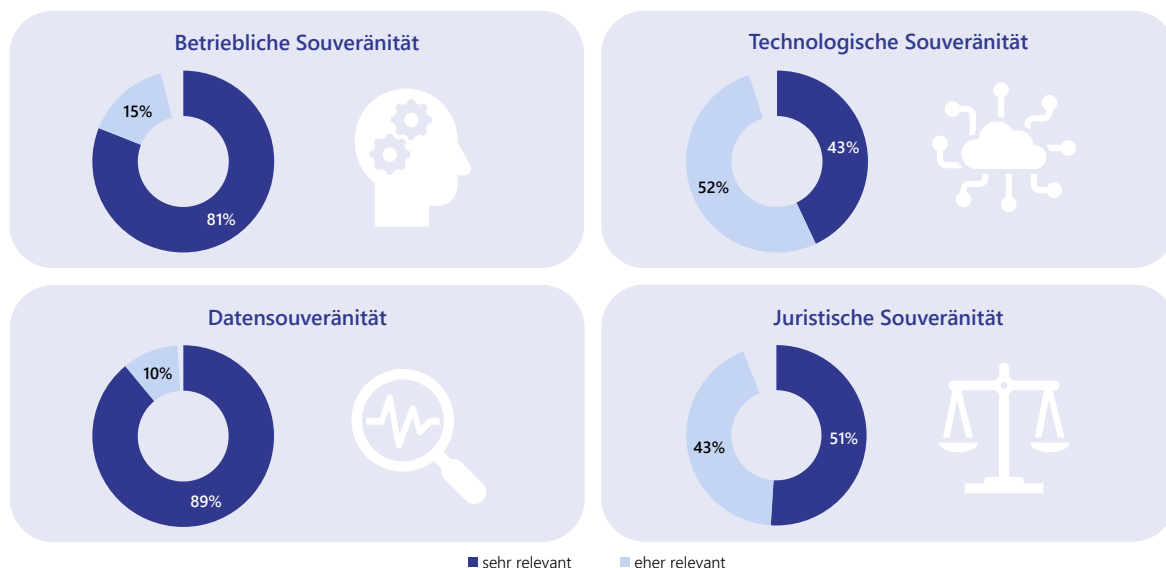


Abb. 4: Wie wichtig sind die folgenden Souveränitätsprinzipien für Ihre Organisation?; Skala von 1 = „nicht relevant“ bis 4 = „sehr relevant“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Souveränität, Autarkie und Fremdbestimmung im Vergleich

Wichtig ist, Souveränität nicht mit Autarkie zu verwechseln. Der [bitkom](#) stellte bereits 2015 klar, dass Souveränität im Kern die Fähigkeit beschreibt, selbstbestimmt entscheiden und handlungsfähig bleiben zu können – sei es als Land, Unternehmen oder Individuum. Autarkie hingegen bedeutet, sich vollständig von externen Einflüssen abzuschotten –

ein sowohl unrealistisches als auch unerwünschtes Szenario, das mit erheblichen Nachteilen verbunden wäre. Ebenso ist Fremdbestimmung ein unerwünschtes Extrem, bei dem externe Akteure maßgeblich über das eigene Handeln entscheiden. Entscheidend ist daher, für jedes Anwendungsszenario den angemessenen Grad an Souveränität zu bestimmen.

Souveränität, Autarkie und Fremdbestimmung im Vergleich

Fremdbestimmung	Souveränität	Autarkie
<i>“Andere Entscheiden, was wir tun.”</i> Wir verfügen in digitalin Schlüsseltechnologien über keine eigenen Kompetenzen. Uns fehlt die Fähigkeit, Technologie in puncto Sicherheit zuverlässig zu bewerten und sie im Bedarfsfall zu härten.	<i>“Wir sind handlungsfähig und entscheiden selbst, was wir tun.”</i> Wir verfügen in zentralen Technologiefeldern, Diensten und Plattformen über eigene Fähigkeiten auf weltweitem Spitzenniveau. Wir sind in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden.	<i>“Wir machen alles selbst.”</i> Wir entwickeln und fertigen Schlüsseltechnologien mit eigenen Ressourcen. Wir ziehen Technologien aus eigener Fertigung Dritten auch dann vor, wenn sie weniger leistungsfähig sind.

Abb. 5: Darstellung Lünendonk, in Anlehnung an bitkom: "Digitale Souveränität - Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa."

Digitale Souveränität ist mehr als nur ein kurzzeitiger

Trend

Doch was bedeutet das im unternehmerischen Alltag? Für 93 Prozent der Unternehmen besitzt digitale Souveränität bereits heute eine hohe Relevanz. Zudem stimmen 96 Prozent der Teilnehmenden der Aussage zu, dass sie in den kommenden drei Jahren deutlich an Bedeutung gewinnen wird. Diese Einschätzung wird dadurch gestützt, dass ebenfalls 96 Prozent der Meinung sind, das Thema werde auch dann auf der Agenda bleiben, wenn sich das Verhältnis zwischen den USA und Europa sowie die geopolitischen Spannungen wieder entspannen sollten. Der Konflikt mag zwar ein Auslöser gewesen sein, doch die grundlegende Relevanz und strategische Notwendigkeit werden erkannt.

Treiber: warum Unternehmen digitale Souveränität anstreben

Die Diskussion um digitale Souveränität wird häufig emotional geführt. Schließlich prägen digitale Technologien und die digitale Transformation maßgeblich die Zukunft. Nicht nur die Wettbewerbsfähigkeit einzelner, sondern nahezu aller Unternehmen in der EU hängt davon ab. Die Studie soll einen rationalen und praxisnahen Einblick in die Gründe für die Relevanz der digitalen Souveränität vermitteln und zugleich aufzeigen, welche Maßnahmen zur Bewältigung der damit verbundenen Herausforderungen notwendig sind. Vier Themen stehen dabei im Fokus:

- **Reduktion übermäßiger Abhängigkeiten in der IT-Lieferkette (Vendor Lock-in):** Übermäßige Abhängigkeiten untergraben die Fähigkeit von Unternehmen, technologische Entscheidungen unabhängig zu treffen, und machen sie erpressbar oder politisch beeinflussbar durch einzelne Anbieter, Staaten oder Rechtsräume. Die Sperrung des E-Mail-Kontos des Chefanklägers des Internationalen Strafgerichtshofs durch Microsoft im Kontext US-amerikanischer Sanktionen wirkte in diesem Zusammenhang als deutlicher Weckruf: Sie hat vielen Organisationen vor Augen geführt, wie unmittelbar geopolitische Entscheidungen die betriebliche Handlungsfähigkeit beeinflussen können. Entsprechend rückt die Notwendigkeit in den Fokus, die eigene digitale

Digitale Souveränität wird in Zukunft deutlich wichtiger

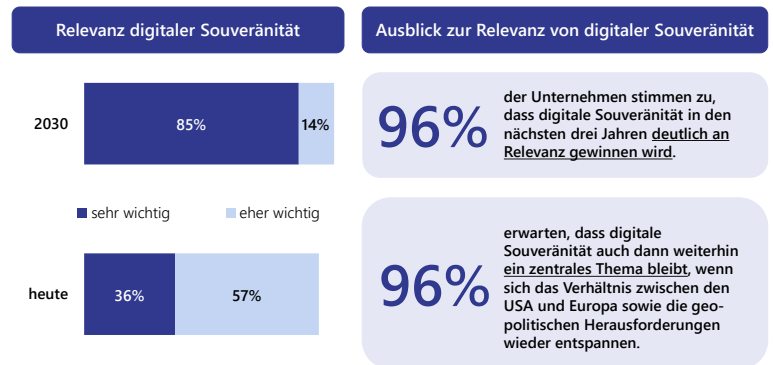


Abb. 6: Digitale Souveränität ist aktuell ein sehr zentrales Thema in der öffentlichen Diskussion. Wie wichtig ist digitale Souveränität für Ihre Organisation?; Skala von 1 = „unwichtig“ bis 4 = „sehr wichtig“; heute und 2030; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Angenommen, das Verhältnis zwischen den USA und Europa sowie die geopolitischen Herausforderungen entspannen sich wieder. Für wie wahrscheinlich halten Sie es, dass digitale Souveränität auch dann weiterhin ein zentrales Thema sein wird?; Skala von 1 = „unwahrscheinlich“ bis 4 = „sehr wahrscheinlich“ dargestellte Antworten beziehen sich auf „eher wahrscheinlich“ und „sehr wahrscheinlich“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Souveränität zu stärken, Abhängigkeiten von einzelnen, insbesondere ausländischen IT-Anbietern kritisch zu bewerten und gezielt zu verringern. Denn ohne realistische Alternativen und belastbare Exit-Szenarien werden Unternehmen von Gestaltern zu Getriebenen ihrer eigenen IT-Strategie. Ebenso haben empfindliche Preissteigerungen – etwa bei Microsoft M365 oder bei VMware im Zuge der Broadcom-Übernahme – bei vielen CIOs ein Umdenken ausgelöst. Ohne Alternativen und Exit-Pläne entstehen kritische Abhängigkeiten, die dazu führen, dass Unternehmen vom Gestalter zum Getriebenen ihrer eigenen IT-Strategie werden.

- **Stärkung der Resilienz in Krisensituationen:** Geopolitische Spannungen, eine zunehmende Zahl komplexer Cyberangriffe, gestörte Lieferketten, Fachkräftemangel und die hohe Vernetzung von Systemen und Partnern führen dazu, dass Unternehmen in einem immer fragileren Umfeld agieren. In vielen IT-Strategien werden diese Risiken jedoch noch unzureichend berücksichtigt, sodass im Ernstfall belastbare Fallback-Szenarien, durchdachte Notfallpläne oder regelmäßig getestete Recovery-Konzepte fehlen.

Hinzu kommen politisch motivierte Eskalations-szenarien, die bis hin zu Zugriffsblockaden oder einem faktischen „Kill Switch“ für einzelne Cloud- oder Softwaredienste reichen. Sie machen deutlich, dass Resilienz heute nicht nur technische Redundanz, sondern auch regulatorische, vertragliche und architektonische Vorsorge erfordert.

- **Schutz vor unkontrolliertem Datenabfluss und extraterritorialen Zugriffen:** Im Zentrum stehen dabei der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) sowie Abschnitt 702 des FISA (Foreign Intelligence Surveillance Act). US-Hyperscaler unterliegen diesen Gesetzen und müssen US-Behörden weitreichende, auch extraterritoriale Zugriffsmöglichkeiten auf Daten einräumen – selbst dann, wenn diese physisch in europäischen Rechenzentren gespeichert sind. Dadurch entsteht für europäische Unternehmen ein strukturelles Spannungsfeld zwischen der Nutzung globaler Cloud-Plattformen und der Einhaltung von Datenschutz-, Compliance- und Geheimhaltungsanforderungen. Technische Maßnahmen wie Verschlüsselung oder reine Datenlokalisierung reichen je nach Anwendungsfall ohne ergänzende juristische und organisatorische Kontrollen nicht aus, um Zugriffe ausländischer Behörden verlässlich auszuschließen.

Hinzu kommt, dass der US-Präsident durch eine Executive Order amerikanische IT-Provider – und somit auch die Hyperscaler – verpflichten kann, Daten an US-Behörden weiterzugeben. Zwar bewerten viele Unternehmen dieses Risiko aktuell noch als abstrakt, dennoch hat es Einfluss auf IT- und Sourcing-Strategien – insbesondere bei jenen Unternehmen, die bereits in größerem Umfang Cloud-Technologien einsetzen.

- **Umsetzung regulatorischer Anforderungen:** Ob DSGVO, NIS-2, EU AI Act, DORA oder CRA: In den vergangenen Jahren haben regulatorische Vorgaben deutlich zugenommen und dieser Trend wird sich voraussichtlich fortsetzen. Zwar ist ihre Umsetzung zwingend erforderlich, um Strafzahlungen zu vermeiden und Compliance sicherzustellen, doch ihre tatsächliche Implementierung in der IT ist äußerst ressourcenintensiv und entwickelt sich schnell zu einem komplexen, dauerhaften Organisations- und Technologieprojekt.

Souveränität als Antwort auf zunehmende Abhängigkeiten und der Notwendigkeit nach mehr Resilienz

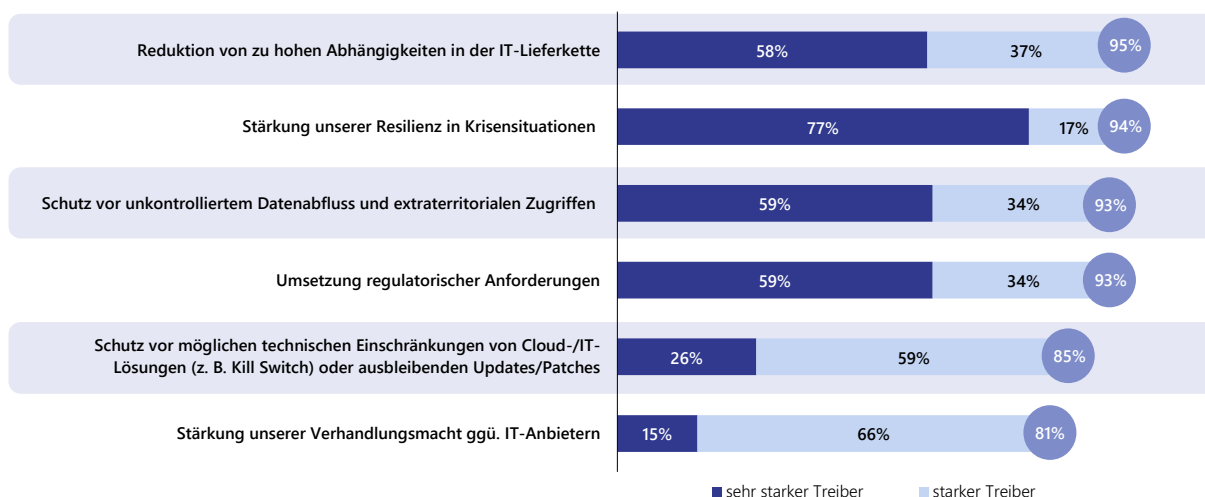


Abb. 7: Digitale Souveränität hat viele Facetten. Wie stark sind die folgenden Aspekte ein Treiber für Ihre Organisation, digitaler Souveränität auszubauen?; Skala von 1 = „kein Treiber“ bis 4 = „sehr starker Treiber“; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

Für 81 Prozent der Unternehmen ist die Stärkung der Verhandlungsmacht gegenüber IT-Providern zwar ebenfalls ein Treiber, jedoch geht es ihnen nicht primär darum, ihre Position gegenüber Anbietern auszubauen. Vielmehr steht für sie im Vordergrund, in kritischen Situationen handlungsfähig zu bleiben und Risiken gezielt steuern zu können. Auch das Risiko technischer Einschränkungen – ein Kill Switch wäre hierbei ein Extrembeispiel – wird als relevant eingestuft. Allerdings sehen nur 26 Prozent darin einen sehr starken Treiber für den Ausbau digitaler Souveränität.

Kill Switch: Lizenz zum Abschalten?

In der öffentlichen Diskussion ist der „Kill Switch“, also die Einschränkung oder Abschaltung digitaler Dienste für einzelne Personen, Organisationen oder sogar ganze Staaten, ein viel beachtetes Thema. Eine zentrale Rolle spielt dabei US-Präsident Donald Trump, der öffentlich damit gedroht hat, den Zugang zu US-Digitaldiensten, wie denen der Hyper-scaler, einzuschränken oder vollständig zu sperren. Zwar handelt es sich bislang lediglich um politische Statements ohne unmittelbare Auswirkungen, dennoch verdeutlichen sie, dass ein solches Szenario als theoretisches Druckmittel existiert.

Knapp die Hälfte der Befragten (47 %) hält einen politisch motivierten Kill Switch einzelner Cloud- oder Software-Lösungen mit weitreichenden Folgen in den kommenden zwei Jahren für realistisch. Entsprechend sehen 83 Prozent der Unternehmen den Kill Switch als relevantes Risikoszenario, das ihre IT- und IT-Sourcing-Strategie beeinflusst – etwa durch die Prüfung von Exit-Playbooks, Architekturabhängigkeiten oder Alternativenanbietern. Besonders intensiv beschäftigen sich damit jene Unternehmen, die bereits einen hohen Cloud-Reifegrad aufweisen und entsprechend mit US-amerikanischen Cloud-Providern vernetzt sind. Auch große Unternehmen berücksichtigen dieses Szenario überdurchschnittlich häufig, da sie oftmals auf umfangreiche Software-Suites setzen und die USA in diesem Bereich eine dominierende Stellung einnehmen.

Lizenz zum Abschalten? Trotz unklarer Eintrittswahrscheinlichkeit haben Kill-Switch-Szenarien einen Impact auf IT- und Sourcing-Strategien

Eintrittswahrscheinlich und Auswirkungen des Kill Switch

83%

Ein Kill Switch ist für uns ein relevantes Risikoszenario, welches die IT- und Sourcing-Strategie stark beeinflusst.



47%

Ein politisch motivierter Kill Switch einzelner Cloud- oder Software-Lösungen mit umfangreichen Auswirkungen ist in den nächsten zwei Jahren realistisch.



16%

Die Möglichkeit eines Kill Switch ist zwar gegeben, wir sehen darin aber kein wesentliches Risiko.



Abb. 8: Der Kill Switch, also die Einschränkung oder Abschaltung von digitalen Diensten für einzelne Personen, Organisationen oder ganze Staaten, ist ein viel diskutiertes Thema. Wie bewerten Sie die folgenden Aussagen in Bezug auf Ihre Organisation?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; dargestellte Antworten beziehen sich auf „stimme eher zu“ und „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Mehr als nur Risikominimierung:

Digitale Souveränität schafft Wertschöpfung,

Transparenz und Wettbewerbsvorteile

Auf Basis der bisherigen Ergebnisse könnte der Eindruck entstehen, digitale Souveränität werde nur mit der Minimierung von Risiken in Verbindung gebracht. Die Studienergebnisse zeigen jedoch ebenso deutlich, dass das Thema auch mit positiven Aspekten verbunden ist, die echte Wertschöpfung ermöglichen und klare Vorteile schaffen.

So geben 94 Prozent der Studienteilnehmer an, dass ein hohes Maß an digitaler Souveränität sich positiv auf ihre Kundenbeziehungen auswirkt. Digitale Systeme und Anwendungen sind das Rückgrat moderner Unternehmen. Wenn sie stabil und zuverlässig laufen und Datenschutz sowie Datensicherheit ernst genommen werden, entsteht auf Kundenseite Vertrauen und Sicherheit.

Digitale Souveränität wirkt sich darüber hinaus positiv auf Kosten- und Effizienzpotenziale aus: 93 Prozent der Unternehmen berichten, dass sich durch das kritische Hinterfragen bestehender Strukturen, IT-Architekturen und Prozesse sowie durch mehr Transparenz Einsparungen und eine höhere operative Effizienz realisieren lassen – etwa durch optimierte Lizenz- und Betriebsmodelle. Souveränität erfordert somit Transparenz – und Transparenz spart Geld.

Neben monetären Faktoren bestätigen 85 Prozent der Befragten, dass digitale Souveränität ihr Unternehmen besser befähigt, Risiken bewusst einzugehen und aktiv zu steuern. Durch mehr Transparenz bei Abhängigkeiten, Datenflüssen und rechtlichen Rahmenbedingungen sowie durch die Etablierung robuster Governance-Strukturen lassen sich technologische, regulatorische und geopolitische Risiken gezielter bewerten, dosiert eingehen und im Zeitverlauf aktiv managen, anstatt ihnen passiv ausgeliefert zu sein.

Nachweise zur eigenen Souveränität werden für externe Stakeholder wichtiger

Die zunehmende Bedeutung der digitalen Souveränität zeigt sich auch darin, dass 7 von 10 Studienteilnehmern angeben, bereits externe Anfragen erhalten zu haben, wie ihr Unternehmen in puncto digitale Souveränität aufgestellt ist, oder entsprechende Nachweise erbringen mussten. Dies betrifft nicht nur Kunden, sondern auch externe Stakeholder wie Banken oder Versicherungen, etwa im Rahmen von Risikobewertungen für Kredite oder Versicherungsabschlüsse. Zudem gehen 92 Prozent der befragten Unternehmen davon aus, dass es künftig noch wichtiger wird, belastbare Nachweise darüber vorlegen zu können, wie es um ihre digitale Souveränität bestellt ist.

Digitale Souveränität hat nicht nur interne Implikationen, sondern auch auf die Kundenzusammenarbeit

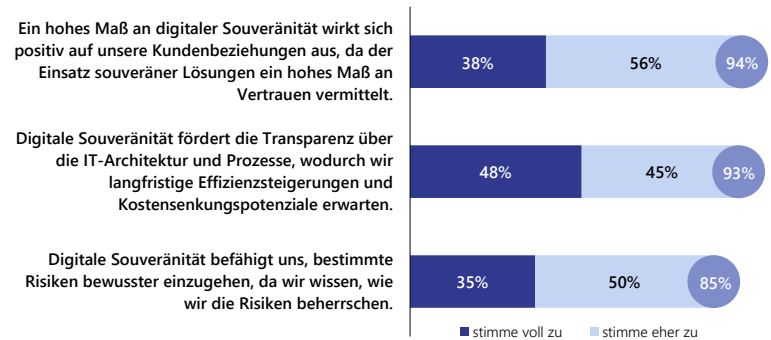


Abb. 9: Wie stehen Sie zu den folgenden Aussagen, wie digitale Souveränität in Ihrer Organisation aufgefasst wird?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

Vom internen Anspruch zur externen Anforderung: Nachweise nach digitaler Souveränität werden häufiger von Stakeholdern eingefordert

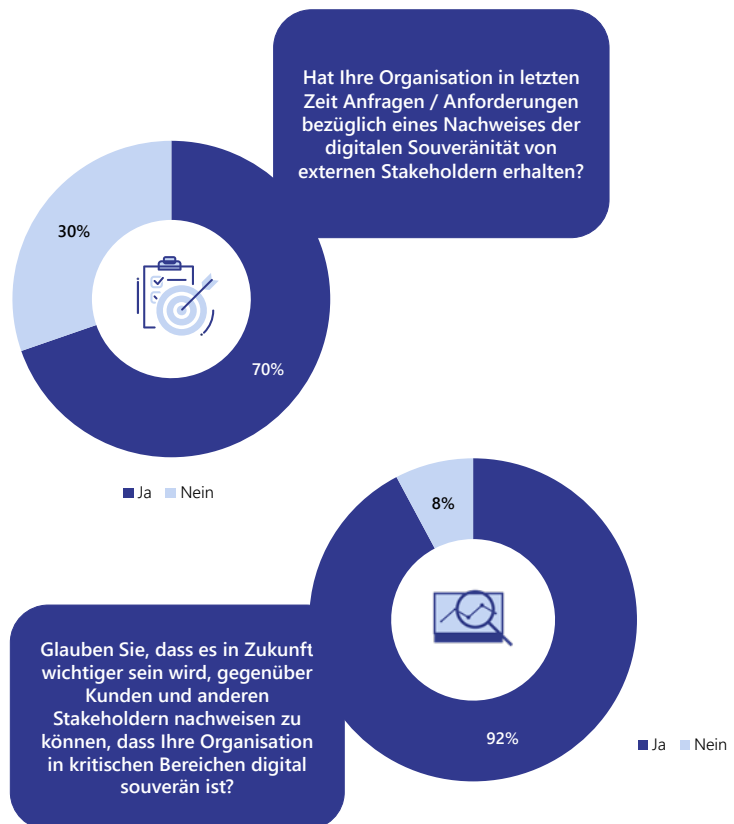


Abb. 10: Hat Ihre Organisation in letzten Zeit Anfragen / Anforderungen bezüglich eines Nachweises der digitalen Souveränität von externen Stakeholdern erhalten (z. B. Kunden, Banken, Versicherungen)?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155
Glauben Sie, dass es in Zukunft wichtiger sein wird, gegenüber Kunden und anderen Stakeholdern nachweisen zu können, dass Ihre Organisation in kritischen Bereichen digital souverän ist?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Herausforderungen: komplexe IT-Landschaften, hohe Wechselbarrieren, fehlende Alternativen und hohe Investitionen

Die Vorteile digitaler Souveränität liegen auf der Hand, doch die damit verbundenen Herausforderungen dürfen nicht unterschätzt werden. 65 Prozent der IT- und Business-Verantwortlichen geben an, dass ihre aktuelle IT-Landschaft sehr komplex ist und Veränderungen daher mit erheblichem Aufwand verbunden sind. Historisch gewachsene Systeme, unübersichtliche Schnittstellenlandschaften, individuelle Einzellösungen und ein hoher Anteil technischer Schulden führen dazu, dass jede Anpassung an neue Souveränitätsanforderungen tief in laufende Betriebsprozesse eingreift. Für viele Unternehmen bedeutet der Weg zu mehr digitaler Souveränität daher nicht nur eine strategische Entscheidung, sondern ein mehrjähriges Transformationsprogramm, das Architektur, Organisation und Sourcing gleichermaßen betrifft – insbesondere bei Unternehmen mit mehr als 500 Millionen Euro Umsatz.

Zudem nennen 44 Prozent der Studienteilnehmer hohe Wechselbarrieren von IT-Providern als große Herausforderung, während weitere 47 Prozent sie als eher große Herausforderung bewerten. Langjährige (Outsourcing-)

Partnerschaften, proprietäre Best-of-Suite-Plattformen und tief integrierte Managed-Services-Verträge haben in vielen Fällen zu einem ausgeprägten Lock-in geführt. Dabei erschweren nicht nur technologische, sondern auch vertragliche und organisatorische Abhängigkeiten einen Anbieterwechsel oder den Aufbau alternativer Szenarien erheblich. Exit-Strategien wurden zudem lange vernachlässigt und oft als theoretische Notfallpläne ohne operative Relevanz betrachtet.

Hinzu kommt, dass digitale Souveränität ihren Preis hat. Ob durch die Migration auf alternative Angebote oder durch den Bezug neuer souveräner Komponenten von bestehenden IT Providern: Unternehmen müssen investieren – teils massiv, abhängig von Ausgangslage und Zielbild. Vor dem Hintergrund der aktuellen konjunkturellen Situation – mit einem leicht rückläufigen deutschen BIP in den Jahren 2024 und 2025 und lediglich moderaten Wachstumsaussichten für 2026 – stehen Befürworter digitaler Souveränität vor der Herausforderung, dass Budgets knapp sind und Investitionen streng unter Business Value Gesichtspunkten geprüft werden.

Hoher Anspruch trifft auf herausfordernde Umsetzungsrealität: Hürden bei der souveränen Journey

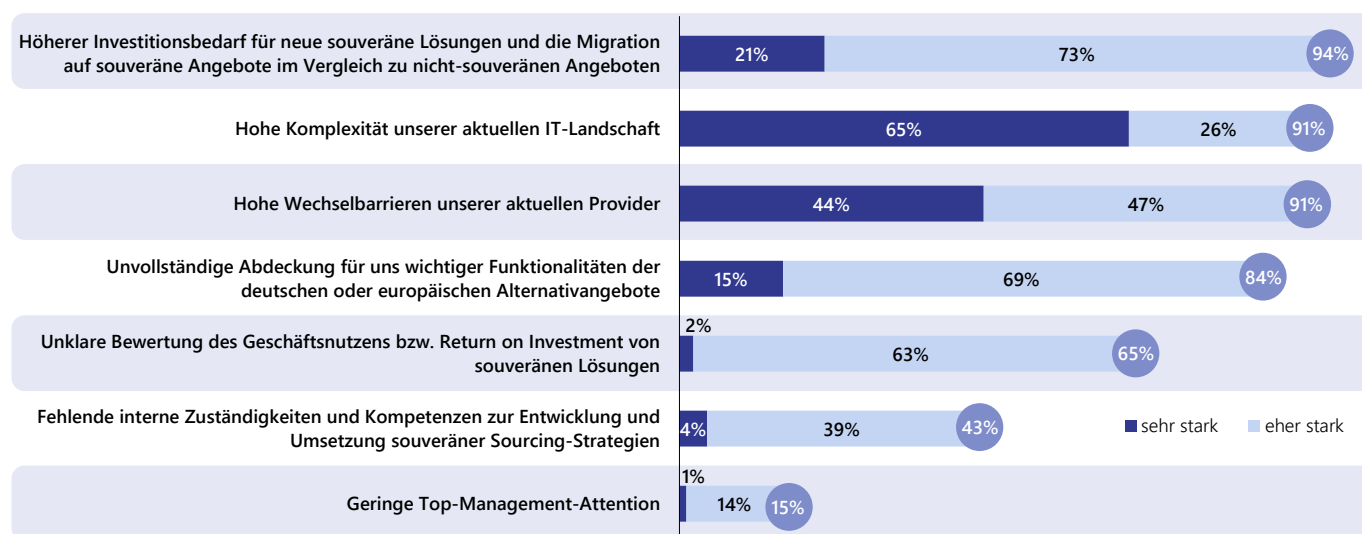


Abb. 11: Wie stark fordern Ihre Organisation die folgenden Aspekte beim Aufbau von mehr digitaler Souveränität heraus?; Skala von 1 = „gar nicht“ bis 4 = „sehr stark“; relative Häufigkeitsverteilung; alle Unternehmen; n = 152

Europäischen Angeboten fehlt es oft noch an Wettbewerbsfähigkeit

Ebenso stellen fehlende Funktionalitäten europäischer Anbieter für 84 Prozent der Unternehmen eine sehr große oder große Hürde dar. Wie im Kapitel „Souveräne Cloud: Neue Marktchancen für Hyperscaler und europäische Superscaler“ deutlich wird, setzen Unternehmen zwar große Hoffnungen in deutsche oder europäische Cloud-Anbieter, doch deren Leistungsportfolio ist derzeit nicht mit dem der Hyperscaler vergleichbar. Auch mittelfristig gehen nur wenige Studienteilnehmer davon aus, dass lokale Anbieter diesen Rückstand vollständig aufholen können.

Der funktionale Rückstand europäischer Anbieter ist vor allem auf strukturelle Faktoren zurückzuführen. Hyperscaler verfügen über deutlich größere Investitionsvolumina, profitieren von massiven Skaleneffekten und können Innovationen durch global verfügbare Ökosysteme wesentlich schneller ausrollen. Europäische Anbieter agieren hingegen in einem stärker fragmentierten Markt, haben kleinere F&E-Budgets und müssen ihre Angebote häufig an strengere regulatorische Rahmenbedingungen anpassen. Dies hat zur Folge, dass der Funktionsumfang, die Innovationsgeschwindigkeit und die globale Reichweite europäischer Lösungen derzeit nicht mit denen der Hyperscaler konkurrieren können.

Hohe C-Level-Präsenz, offene Strategief Frage: Der nächste Schritt entscheidet

Positiv ist, dass nur 15 Prozent eine geringe Aufmerksamkeit des Top-Managements als Herausforderung sehen. Digitale Souveränität besitzt somit eine klare C-Level-Relevanz und wird dort auch berücksichtigt – wenngleich dies nicht automatisch bedeutet, dass bereits die richtige strategische Ausrichtung gewählt wurde oder der Weg zu mehr digitaler Souveränität gesichert ist. Vielmehr ist entscheidend, wie Unternehmen diese Aufmerksamkeit konkret nutzen und in substantielle Maßnahmen übersetzen.



Status quo: Wo Unternehmen und Organisationen heute stehen

”

Digitale Souveränität steht weit oben auf der Agenda vieler Unternehmen – doch zwischen strategischem Anspruch und operativer Realität besteht noch eine deutliche Lücke. Bevor Unternehmen gezielt in Maßnahmen und Technologien investieren können, müssen Unternehmen zunächst klären, wie souverän sie heute tatsächlich sind und an welchen Stellen sie souveräner werden möchten.

Souveränität wird teilweise bereits gelebt, jedoch selten als strategische Entscheidung mit einem integrierten Ansatz

Die Cloud spielt heute in den meisten Unternehmen eine zentrale Rolle. Beim Cloud Sourcing stellt sich somit die Frage, in welchem Maße die Services gesteuert und kontrolliert werden können. Zwar stimmen 30 Prozent der Studienteilnehmer voll zu, dass sie die technische und organisatorische Kontrolle über ihre Cloud-Infrastrukturen besitzen, und weitere 66 Prozent stimmen dem eher zu. In vielen Organisationen sind Zugriffsrechte sowie Identitäts- und Berechtigungskonzepte zwar grundsätzlich etabliert, jedoch häufig noch nicht durchgängig und plattformübergreifend konsistent umgesetzt. Zwar stehen Verschlüsselungsmechanismen über große Plattformen bereit, entscheidend ist jedoch, wer die Hoheit über die Schlüssel verfügt (Key Management). Zudem ist kritisch zu hinterfragen, ob diese Einschätzung auch durch einen neutralen Auditor bestätigt würde oder ob das subjektive Empfinden der Unternehmen (unwissentlich) zu positiv ist.

51 Prozent der Unternehmen sehen sich bei der frühzeitigen Integration von Datenschutzanforderungen in die IT-Architektur (Privacy by Design) sehr gut aufgestellt. Dadurch können Datenschutzanforderungen systematisch in Requirements, Solution Design und DevOps-Prozesse eingebunden werden. Dabei sollte berücksichtigt werden, dass Organisationen bei regulatorischen Themen dazu neigen, bereits das Vorhandensein von Richtlinien, Checklisten oder Prozessvorlagen als hohen Reifegrad zu interpretieren. Eine systematische Einbindung des Datenschutzes bedeutet jedoch, dass Datenflüsse konsequent analysiert, Prinzipien wie Datenminimierung und Pseudonymisierung stringent angewendet oder Datenschutzkontrollen automatisiert in Build- und Deployment-Prozesse integriert sind. Ein derart industrialisierter Ansatz ist eher die Ausnahme als die Regel. Insbesondere kleinere Organisationen weisen hier noch ein deutliches Nachholpotenzial auf.

87 Prozent der Studienteilnehmer stimmen voll oder eher zu, dass ihre IT-Landschaft überwiegend aus proprietären Anwendungen besteht, deren Quellcode nicht einsehbar ist. Im Vergleich zu Open-Source-Lösungen, die Souveränitätsgewinne wie Quellcode-Transparenz, unabhängige Audits, flexible Anpassbarkeit und geringere Lock-in-Effekte bieten können, liegen bei proprietärer Software die zentralen Steuerungshebel für Sicherheit, Interoperabilität und Exit-Szenarien maßgeblich bei den Herstellern – und somit außerhalb des direkten Einflussbereichs der IT-Organisation.

Souveränität wird noch zu selten als strategische Entscheidung mit einem integrierten Ansatz gelebt

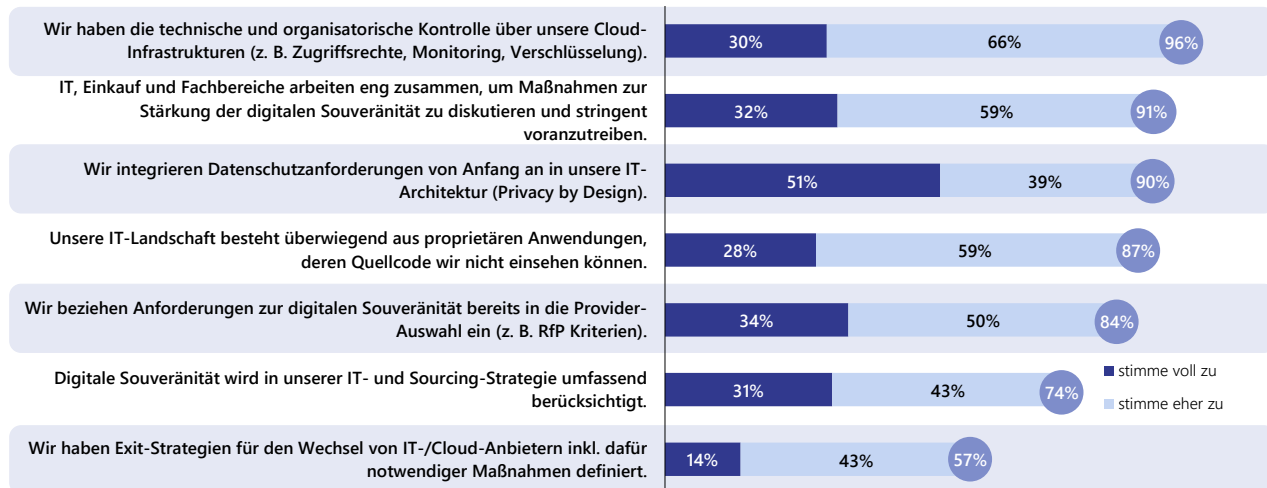


Abb. 12: Wie stehen Sie zu den folgenden Aussagen bezüglich Ihrer Sourcing-Strategie und IT-Landschaft?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

34 Prozent der befragten Unternehmen berücksichtigen Souveränitätsanforderungen bereits umfassend als Kriterium in Ausschreibungen, weitere 50 Prozent tun dies zumindest teilweise. Dazu zählen beispielsweise Anforderungen zur Datenlokation, zu Sicherheitsprozessen, zur Schnittstellen-offenheit oder zu Transparenzberichten. Obwohl diese Kriterien in die Anbieterbewertung einfließen, bedeutet dies nicht zwangsläufig, dass Provider mit einem niedrigen Souveränitäts-Scoring ausgeschlossen werden, da auch weitere Kriterien wie Funktionalität, Reifegrad und Preis berücksichtigt werden müssen.

Den größten Schwachpunkt sehen die Studienteilnehmer bei Exit-Strategien. Nur 14 Prozent von ihnen schätzen sich in diesem Bereich als sehr fortgeschritten ein. Da Wechsel-szenarien in der Vergangenheit vielfach als theoretisch betrachtet wurden und Exit-Strategien entsprechend keine operative Relevanz besaßen, sind viele Unternehmen auf die heute real mögliche Notwendigkeit eines Anbieterwechsels nicht vorbereitet. Datenmodelle, Schnittstellen und Export-formate sind häufig nicht systematisch auf Portabilität ausgelegt. Migrationsaufwand, -dauer, -kosten und Verantwortlichkeiten wurden nur selten realistisch bewertet. Dies schränkt die Handlungs- und Reaktionsfähigkeit erheblich ein. Überdurchschnittlich betroffen sind kleinere Unternehmen mit einem Umsatz unter 500 Millionen Euro.

Ein zusammenfassendes Bild ergibt sich daraus, dass 31 Prozent der Unternehmen angeben, digitale Souveränität bereits umfassend in ihre IT- und Sourcing-Strategie integriert zu haben. Diese Unternehmen verfolgen das Thema strategisch und steuern entsprechende Maßnahmen strukturiert. Die Mehrheit (43 %) agiert jedoch vorwiegend über Einzelmaßnahmen, ohne ein durchgängiges Gesamtkonzept zu verfolgen. Digitale Souveränität ist in vielen Organisationen somit bereits sichtbar, jedoch vielfach eher als Sammlung isolierter Initiativen und weniger als integrierte Steuerungsgröße für IT- und Sourcing-Entscheidungen.

Fortschritte und Rückstände: Verschlüsselung und Datenklassifizierung sind vorhanden, vollständige Transparenz und KPIs aber nur selten

Auch bei Verschlüsselungsmechanismen und der Datenklassifizierung sieht sich die Mehrheit der Unternehmen gut aufgestellt. Viele Organisationen haben ihre Daten nach Kritikalität und Sensitivität klassifiziert und diese Klassen mit technischen Maßnahmen wie Verschlüsselung, Zugriffsregeln oder Backup Vorgaben hinterlegt – ein zentraler Bestandteil von Datensouveränität. Dies bedeutet jedoch nicht automatisch, dass die Datenhoheit vollständig bei den Unternehmen liegt.

Gerade im Kontext von Vendor Lock-in wird deutlich: Echte Datenhoheit ist erst dann erreicht, wenn geschäftskritische Daten unabhängig von einzelnen Anbietern portierbar sind, in alternativen Umgebungen weiter nutzbar sind und nicht durch proprietäre Formate, Plattformabhängigkeiten oder beim Provider liegende Schlüssel faktisch „eingesperrt“ sind.

Bei regelmäßigen Risikoanalysen oder Audits zur Abhängigkeit von IT- und Cloud-Anbietern sehen sich 35 Prozent der Unternehmen als sehr fortgeschritten. Dies erreichen sie beispielsweise durch definierte, wiederkehrende Verfahren, die prüfen, wie kritisch einzelne Provider sind, welche Auswirkungen Vertrags-, Preis- oder Rechtsänderungen hätten und welche realistischen Alternativen verfügbar sind. Weitere 47 Prozent schätzen sich als eher fortschrittlich ein. Die Abhängigkeiten von Hyperscalern, SaaS-Anbietern oder Outsourcing-Partnern werden zwar wahrgenommen, jedoch nicht durchgängig systematisch überwacht oder getestet.

Während Zuständigkeiten für das Thema digitale Souveränität in vielen Unternehmen bereits definiert und operativ verankert sind, zeigen sich größere Lücken bei der Nutzung von Tools zur Analyse geschäftskritischer Hardware- und Software-Komponenten. Ohne geeignete Analysewerkzeuge fehlt häufig der klare Blick darauf, welche Komponenten potenzielle „Single Points of Failure“ darstellen – und diese Risiken treten oft erst in akuten Situationen zutage.

Die Entwicklung und Nutzung von Messsystemen und KPIs zur digitalen Souveränität, um den Reifegrad kontinuierlich und transparent nachzuverfolgen, steht bei den Unternehmen noch am Anfang. Wo keine klaren KPIs, Reifegradmodelle oder Dashboards existieren, basiert die Einschätzung des eigenen Souveränitätsniveaus weitgehend auf Bauchgefühl und Einzelbeobachtungen statt auf belastbaren Kennzahlen. Dadurch lässt sich digitale Souveränität nur schwer aktiv steuern, priorisieren oder gegenüber Management und Aufsichtsrat nachvollziehbar erläutern.

Reifegrad: Technische Schutzmaßnahmen und Risikoanalysen sind vorhanden, vollständige Transparenz und KPIs dahingegen die Ausnahme

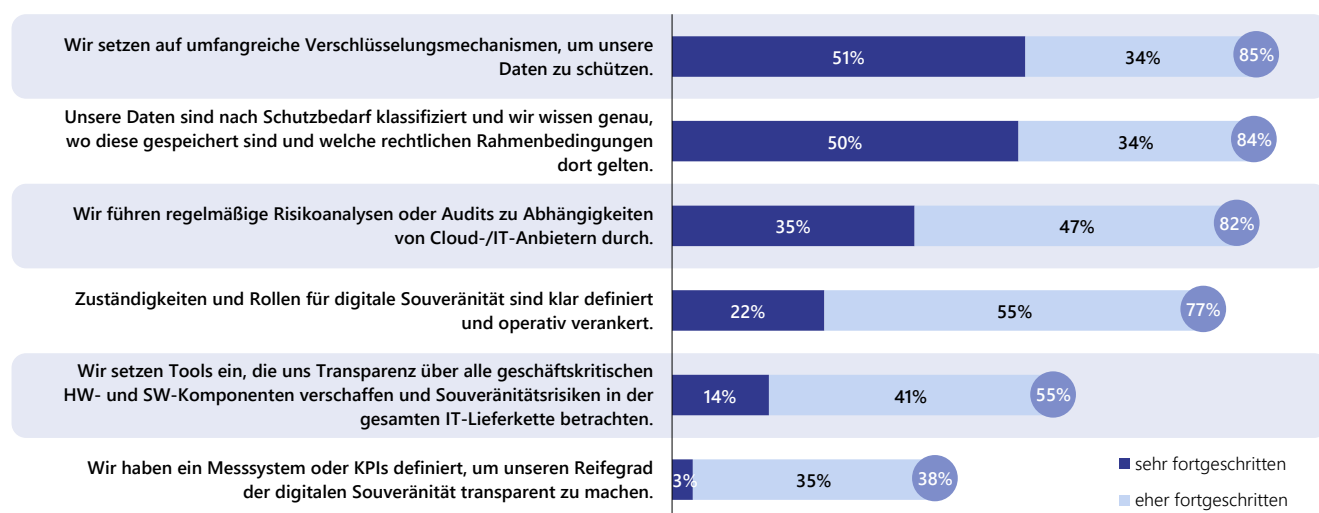


Abb. 13: Wie fortgeschritten ist Ihre Organisation bei den folgenden Maßnahmen?; Skala von 1 = „stehen am Anfang“ bis 4 = „sehr fortgeschritten“; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

Showtime für Open Source?

Einige der beschriebenen Risiken lassen sich durch Open Source reduzieren oder sogar vollständig eliminieren. Dies setzt allerdings andere Voraussetzungen voraus und bringt neue Herausforderungen mit sich, sodass Unternehmen zwangsläufig Kompromisse eingehen müssen. Offener Quellcode schafft Transparenz, ermöglicht Prüfbarkeit und erhöht die Kontrolle über eingesetzte Technologien. Dadurch wird nachvollziehbar, wie Systeme funktionieren und wie sie mit Daten umgehen. Das reduziert wiederum das Risiko eines Vendor Lock-ins.

18 Prozent der Unternehmen stimmen voll zu, künftig in deutlich größerem Umfang auf Open Source zu setzen. Weitere 72 Prozent stimmen dem zumindest teilweise zu. Tendenziell sind es größere Organisationen, die sich in diesen Antwortkategorien wiederfinden. Sie betrachten Open Source auch als strategischen Hebel zur Stärkung ihrer digitalen Souveränität. Dass zwar jedes zweite Unternehmen dieser Aussage zumindest teilweise zustimmt, aber nur 15 Prozent voll zustimmen, zeigt jedoch: Zwar erkennen viele das Potenzial von Open Source und halten punktuelle Umstellungen für realistisch, doch eine vollständige Ablösung proprietärer Anwendungen wird nicht angestrebt – oder gilt als realitätsfern. Beispiele wie das des Landes Schleswig-Holstein, das Microsoft Office durch das quelloffene LibreOffice ersetzt hat, verdeutlichen jedoch, dass es Alternativen zu Standardsoftware großer Tech-Anbieter gibt.

Voraussetzung hierfür ist jedoch der Aufbau entsprechender Kompetenzen. Nur 8 Prozent der Unternehmen stimmen voll zu, dass sie über ausreichende Fähigkeiten für den nachhaltigen Einsatz von Open Source verfügen. Weitere 49 Prozent stimmen zumindest teilweise zu. In der Praxis bedeutet das: Ohne gezielten Kompetenzaufbau in den Bereichen Entwicklung, Betrieb, Governance und Security droht Open Source zwar strategisch gewollt zu sein, de facto aber weiterhin zu Abhängigkeiten von Dienstleistern, Communities oder Herstellern zu führen – und damit nur bedingt als wirklicher Hebel digitaler Souveränität zu wirken.

Erschwerend kommt hinzu, dass lediglich jedes zweite Unternehmen eine klare Open Source Strategie formuliert hat oder zumindest vereinzelte Policies zum Einsatz von Open Source vorliegen. Dies erschwert nicht nur den systematischen Kompetenzaufbau und die Etablierung standardisierter Betriebsmodelle, sondern birgt auch Risiken – etwa hinsichtlich Lizenz-Compliance, Security, Supportfähigkeit und langfristiger Wartbarkeit.

Open Source: steigende Relevanz trifft auf geringen Reifegrad

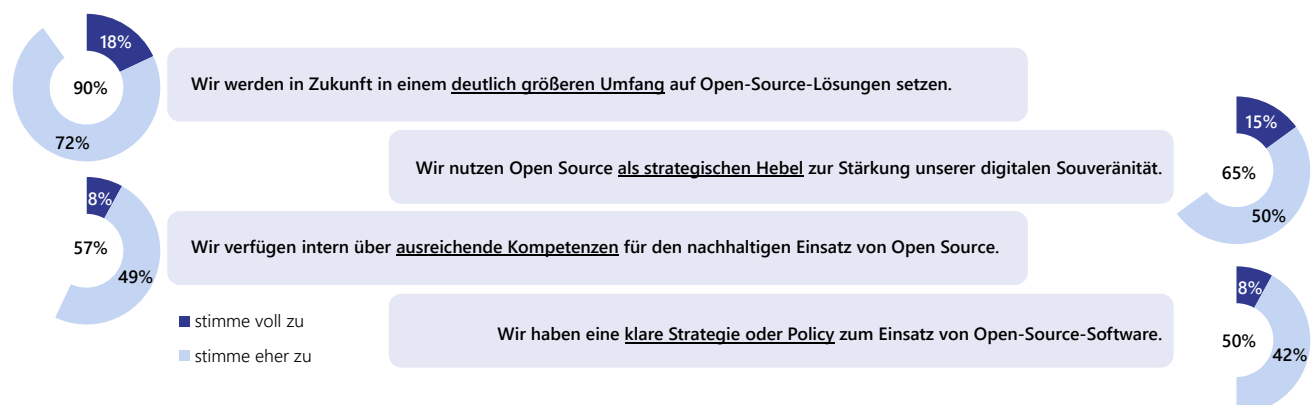


Abb. 14: Open Source ist ein weiteres Instrument zur Stärkung der digitalen Souveränität. Wie stehen Sie zu den folgenden Aussagen hinsichtlich Ihrer Organisation?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155



Souveräne Cloud: Neue Marktchancen für Hyperscaler und europäische Superscaler



Deutsche Unternehmen sind auf ausländische Produkte und Services angewiesen

Deutschland und die EU nehmen bei vielen digitalen Schlüsseltechnologien keine führende Marktposition ein. Entlang der digitalen Wertschöpfungskette spielen nur wenige europäische Unternehmen eine zentrale Rolle. Maßgeblich dominieren Anbieter aus den USA und Asien, insbesondere aus China, Taiwan, Südkorea und Singapur. Laut [bitkom](#) sind 90 Prozent der Unternehmen sehr stark oder eher stark vom Bezug digitaler Technologien oder Dienstleistungen aus dem Ausland abhängig.

Diese Abhängigkeit ist besonders kritisch im Bereich der Cloud-Technologien. Im europäischen Cloud-Markt dominieren US-Hyperscaler wie AWS, Microsoft Azure und Google Cloud mit einem Marktanteil von rund 70 Prozent. Da zentrale Geschäftsprozesse, Datenplattformen und zunehmend auch KI-Services auf diesen Infrastrukturen betrieben werden, verlagert sich ein wesentlicher Teil der digitalen Wertschöpfung in außereuropäische Rechtsräume und Ökosysteme.

Souveränität zwischen Fremdbestimmung, Kontrolle und Autarkie: Cloud-Anbietermodelle im Vergleich

Da die Anforderungen an Kontrolle, Verfügbarkeit, Skalierbarkeit, Jurisdiktion, Innovationsgeschwindigkeit und Kosten von Cloud Services je nach Anwendungsfall und Branche unterschiedlich sind, lassen sich keine pauschalen Einschätzungen oder allgemeingültigen Schlussfolgerungen treffen. Pauschale Einschätzungen oder allgemeingültige Schlussfolgerungen sind daher nur bedingt möglich.

Um dennoch ein strukturiertes Stimmungsbild zu erhalten, wurden die Studienteilnehmer gebeten, die Relevanz verschiedener Cloud-Anbietermodelle einzuordnen – getrennt nach geschäftskritischen Anwendungen, auf denen sehr wichtige Prozesse und sensible Daten laufen, sowie unkritischen Prozessen beziehungsweise unsensiblen Daten.

Die größte Relevanz bei geschäftskritischen Anwendungen haben:

- **Souveräne Hyperscaler-Angebote mit lokalem EU-Betreiber:**

Die technologische Basis stammt zwar von einem Hyperscaler, der operative Betrieb wird jedoch durch einen lokalen IT-Service-Provider übernommen. Dadurch lassen sich die Innovations- und Skalierungsvorteile der Hyperscaler nutzen, während zugleich die juristische und organisatorische Kontrolle bei einem europäischen Betreiber liegt. Abhängigkeiten von außereuropäischen Cloud-Providern bestehen weiterhin, fallen jedoch je nach Ausgestaltung geringer aus, als wenn kein lokaler Betreiber eingeschaltet ist. Risiken werden somit reduziert, aber nicht vollständig eliminiert. Ein Beispiel hierfür ist die Delos Cloud: Als Tochterunternehmen von SAP ist sie ein deutsches Unternehmen. Technologisch basiert das Angebot jedoch auf Microsoft Azure und Microsoft 365 und der operative Betrieb wird durch Arvato Systems gewährleistet. Dadurch bietet Delos deutliche Vorteile in Bezug auf Datensouveränität, jedoch keine vollständige technische Souveränität. Auch die Bereitstellung von Sicherheits- und Funktionsupdates bleibt im Extremfall vom Hyperscaler abhängig und kann somit potenziell gefährdet sein.

- IT-Service-Provider aus Deutschland:** IT-Dienstleister, die Managed-Infrastructure-Leistungen oder den Betrieb von Rechenzentren oder Colocation-Ressourcen anbieten, nehmen in Deutschland eine zentrale Rolle ein. Sie verbinden technische Leistungsfähigkeit mit einem Vertrauens- und Rechtsrahmen im eigenen Land und können Betriebsmodelle, Supportstrukturen und Sicherheitsprozesse so ausrichten, dass sie revisionssicher, prüfbar und eng in die Governance der Kundenorganisation eingebettet sind. Im Vergleich zu großen Hyperscalern verfügen sie allerdings über deutlich geringere Skalierungsmöglichkeiten, eine geringere Innovationsgeschwindigkeit und eine weniger breite Servicepalette.
- Cloud Provider aus Deutschland:** Insbesondere IONOS, STACKIT und die T Cloud Public der Deutschen Telekom entwickeln sich zu deutschen Superscalern, also zu Cloud-Providern mit signifikanten (IaaS-) Kapazitäten und Enterprise-Fähigkeiten, die jedoch nicht die globale Tiefe und technologische Breite der Hyperscaler erreichen. SaaS-Lösungen werden teilweise über Cloud-Marktplätze angeboten oder mittels Partnerschaften, wie etwa zwischen STACKIT und Google Workspace, zur Verfügung gestellt.
- Souveräne Hyperscaler-Angebote:** Auch die Hyperscaler selbst bringen zunehmend eigene Angebote mit erweiterten Souveränitäts-Features auf den Markt. Große Aufmerksamkeit erhielt beispielsweise die im Januar 2026 in Brandenburg in Betrieb gegangene AWS European Sovereign Cloud. Die Plattform wird über eine neue europäische Muttergesellschaft sowie lokale Gesellschaften in Deutschland geführt und ausschließlich durch in der EU ansässige Mitarbeitende betrieben. Infrastruktur, Daten, Metadaten und Betriebszugriffe sollen demnach vollständig innerhalb der EU verbleiben. Kritisch diskutiert wird jedoch, inwieweit damit tatsächlich juristische Souveränität erreicht wird. Denn US-Rechtszugriffe – etwa über den CLOUD Act oder FISA – lassen sich allein durch technische oder organisatorische Abtrennung nicht vollständig ausschließen. Auch hierzu folgen im weiteren Verlauf des Kapitels vertiefende Einschätzungen.

Unternehmen setzen große Hoffnungen auf neue souveräne Cloud-Modelle und deutsche Provider – gerade in kritischen Bereichen

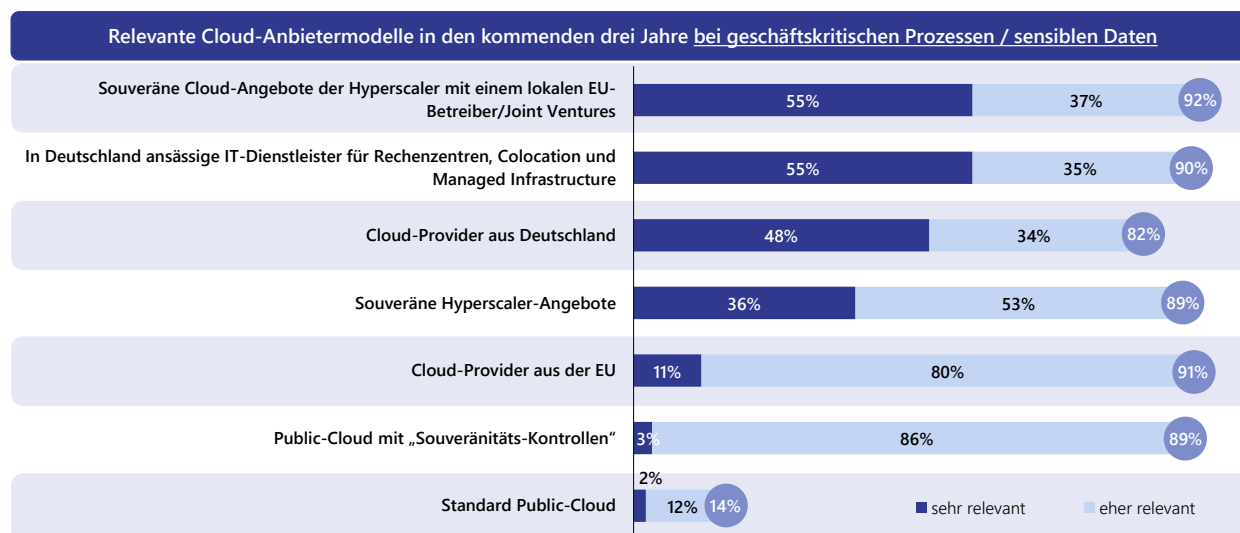


Abb. 15: Welche Rolle spielen folgende Anbietermodelle für Ihre Organisation mit Blick auf die kommenden drei Jahre; bei geschäftskritischen Prozessen / sensiblen Daten?; Skala von 1 = „nicht relevant“ bis 4 = „sehr relevant“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

8 von 10 Unternehmen (82 %) stufen Cloud Provider aus der EU als eher relevant ein, jedoch sehen lediglich 11 Prozent sie als sehr relevant an. Dies könnte damit zusammenhängen, dass deutsche Cloud Provider bevorzugt werden – Stichwort „Local Bias“ – oder damit, dass deutsche Anbieter im europäischen Vergleich als fortschrittlicher wahrgenommen werden. Europäische Lösungen aus anderen Ländern sind zwar ebenfalls relevant, jedoch weniger sichtbar oder weniger stark vertreten. Auch Public-Cloud-Angebote mit zusätzlichen Souveränitätskontrollen – also reguläre Public-Cloud-Services, die jedoch um erweiterte Datenkontroll- und Schutzmechanismen ergänzt werden – werden grundsätzlich als relevant bewertet. Im Vergleich zu souveränen Hyperscaler-Angeboten messen die Studienteilnehmer dieser Option jedoch eine geringere Bedeutung bei, da das erreichte Souveränitätsniveau als niedriger eingeschätzt wird.

Hybride Realität statt ideologischer Debatten

Während in der öffentlichen Diskussion zu Cloud-Themen oft ein Schwarz-Weiß-Narrativ verfolgt wird, zeigt die Studie, dass die Realität deutlich vielschichtiger ist. Anstelle von Entweder-oder-Szenarien dominieren hybride IT-Landschaften im Sinne einer Multi-Cloud-Architektur, die je nach Anwendungsfall die jeweils besten Lösungen miteinander

der vereinen – dies bestätigt auch die [Lünendonk-Studie „IT-Sourcing-Trends 2025/2026“](#). Ebenso geht es CIOs nicht nur um die Frage „US-amerikanische Cloud-Provider versus europäische Cloud-Provider“, sondern generell um die Frage: „Wie hoch ist der Lock-in eines bestimmten Providers und wie schnell kann ich wechseln?“

Die „normale“ Public Cloud bleibt bei unkritischen Daten und Anwendungen klar führend

Ein nahezu umgekehrtes Bild zeigt sich bei unkritischen Prozessen und unsensiblen Daten: Hier liegen klar die Standardangebote der Hyperscaler sowie Angebote mit zusätzlichen Souveränitäts-Kontrollen vorn. Das verdeutlicht, dass Souveränitätsanforderungen je nach Anwendung unterschiedlich ausfallen und stets im Einklang mit weiteren Faktoren wie Wirtschaftlichkeit, Verfügbarkeit und Innovationszugang stehen müssen.

Standard-Clouds dominieren weiterhin bei unkritischen Workloads

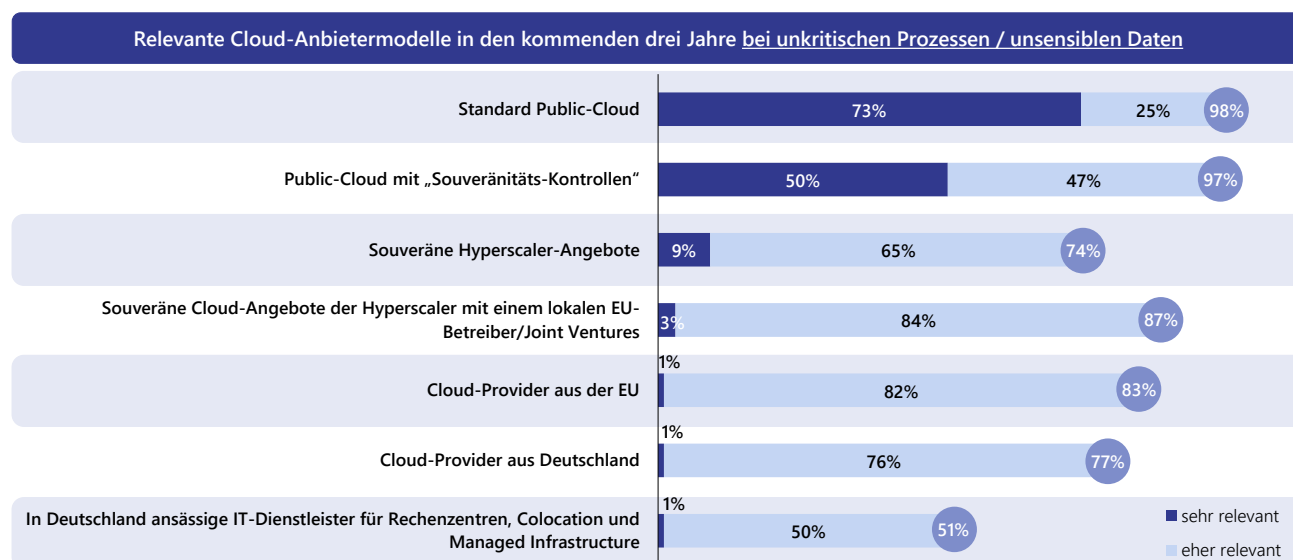


Abb. 16: Welche Rolle spielen folgende Anbietermodelle für Ihre Organisation mit Blick auf die kommenden drei Jahre; bei unkritischen Prozessen / unsensiblen Daten?; Skala von 1 = „nicht relevant“ bis 4 = „sehr relevant“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Hyperscaler & Souveränität: Match oder Widerspruch?

Neben der vorangegangenen ersten Einordnung wurde vertieft betrachtet, wie die souveränen Hyperscaler-Angebote wahrgenommen werden. Positiv ist zunächst hervorzuheben, dass sich eine große Mehrheit der Studienteilnehmer bewusst ist, dass auch bei Nutzung dieser neuen Angebote mit erweiterten Souveränitätsmechanismen weiterhin strukturelle Abhängigkeiten zu den jeweiligen Anbietern bestehen bleiben. Zwar können Compliance-Anforderungen – je nach Branche – besser erfüllt werden, doch die Natur der Zusammenarbeit verändert sich dadurch nicht grundlegend. Dies gilt zwar grundsätzlich für jede Kooperation mit externen IT- und Cloud-Anbietern, aufgrund der Marktmacht der Hyperscaler, der unterschiedlichen Rechtsrahmen sowie des angespannten Vertrauensverhältnisses zu den USA hat dieser Aspekt in der Zusammenarbeit mit Hyperscalern jedoch eine besondere Relevanz.

Ebenso ist den allermeisten Unternehmen bewusst, dass der CLOUD Act auch dann wirksam bleibt, wenn sich Rechenzentren in Europa befinden oder Cloud Services über europäische Tochtergesellschaften erbracht werden. Lokale Datenresidenz schützt somit nicht vor einer potenziellen Datenübermittlung.

So beschreibt AWS die European Sovereign Cloud als umfassend geschützt: Die Lösung wird ausschließlich von EU-Bürgern betrieben, ist technisch vollständig von der regulären AWS-Infrastruktur getrennt und nutzt Verschlüsselung sowie den AWS-Nitro-Hypervisor als Schutzmaßnahmen. Auch AWS-eigene Operatoren sollen keinen Zugriff auf die Daten haben. Zusätzlich soll die juristische Konstruktion inklusive Gesellschafterstruktur unberechtigte Zugriffe verhindern.

Gleichzeitig sorgen Aussagen wie die des Chefjustizars von Microsoft France, der betont, dass keine hundertprozentige Garantie gegeben werden könne, dass Daten niemals übermittelt würden, sowie politische Äußerungen und Handlungen des US-Präsidenten Donald Trump dafür, dass bei vielen Unternehmen eine gewisse „Restskepsis“ bestehen bleibt. Vertrauen wird damit zu einem zentralen Faktor.

Vor diesem Hintergrund passt es ins Bild, dass 89 Prozent der Unternehmen den neuen Angeboten zwar zutrauen, den digitalen Souveränitätsgrad ihrer Organisation zu erhöhen, gleichzeitig jedoch 66 Prozent diesen Angeboten gegenüber misstrauisch sind. Der Markt befindet sich somit in einer Orientierungsphase und Unternehmen sind auf der Suche nach belastbarem Vertrauen.

Ambivalentes Bild: Souveräne Hyperscaler-Angebote fördern Souveränität, werden gleichzeitig aber auch kritisch betrachtet

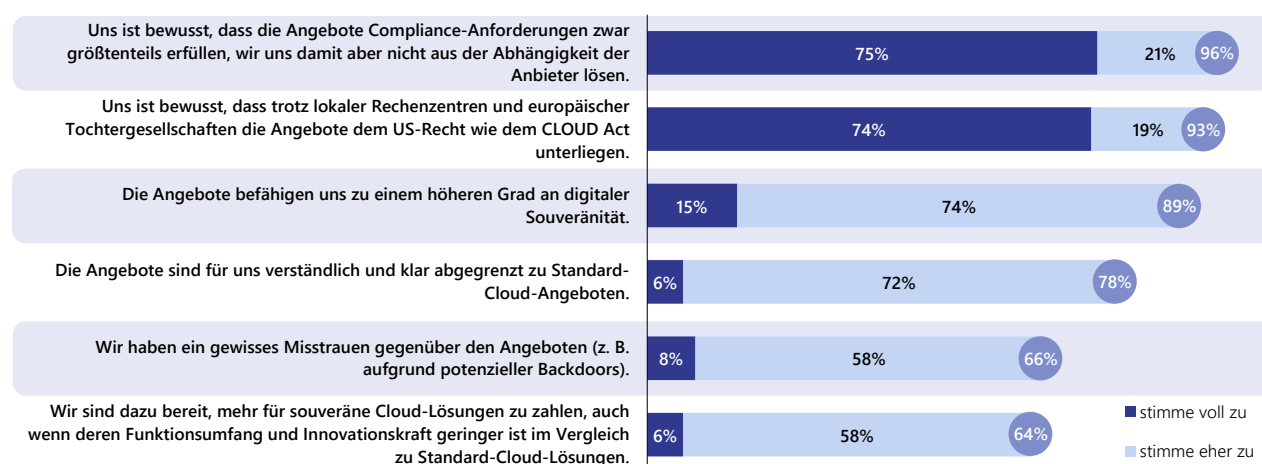


Abb. 17: Wie stehen Sie zu den folgenden Aussagen hinsichtlich der von den Hyperscalern angebotenen souveränen Cloud-Lösungen?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

78 Prozent der befragten IT- und Business-Verantwortlichen geben an, dass die souveränen Cloud-Angebote verständlich sind und sich klar von den Standardangeboten abgrenzen lassen. Dem stimmen jedoch nur 6 Prozent voll zu. Damit zeigt sich: Bei den Studienteilnehmern ist zwar ein grundsätzliches Verständnis der neuen Angebote vorhanden, die Detailkenntnisse sind jedoch oft noch begrenzt.

Ebenfalls 6 Prozent stimmen voll zu, dass sie bereit wären, für souveräne Cloud-Lösungen mehr zu bezahlen, um einen höheren Grad an Souveränität zu erreichen – selbst wenn der Funktionsumfang und die Innovationsgeschwindigkeit im Vergleich zu Standardangeboten geringer ausfallen sollten. Weitere 58 Prozent stimmen dem zumindest teilweise zu. Aus betriebswirtschaftlicher Sicht wägen Unternehmen somit je nach Use Case ab, in welchen Szenarien teurere souveräne Lösungen angemessen sind und in welchen nicht.

Europäische Cloud-Anbieter gewinnen Akzeptanz – bleiben aber funktional im Rückstand

Der Wunsch nach einem europäischen Gegengewicht zu den US-amerikanischen Hyperscalern ist groß. Jahrzehntelange Investitionen in digitale Technologien und die hohe Innovationskraft der US-Cloud-Provider haben jedoch zu einer enormen Marktmacht geführt. Allein AWS plant im Zeitraum von 2024 bis 2040 Investitionen von 7,8 Milliarden Euro in die European Sovereign Cloud. Zwischen 2014 und 2023 beliefen sich die Investitionen in Europa bereits auf 9,6 Milliarden Euro. Auf globaler Ebene zeigt sich die finanzielle Stärke besonders deutlich: Microsoft investierte allein im ersten Quartal des Geschäftsjahres 2026 rund 35 Milliarden US-Dollar – maßgeblich getrieben durch den Ausbau von KI-Rechenzentren.

Vor diesem Hintergrund überrascht es nicht, dass nur 31 Prozent der befragten Unternehmen europäische Cloud-Anbieter derzeit als wettbewerbsfähig gegenüber den Hyperscalern einschätzen. Lediglich 3 Prozent stimmen dieser Aussage voll zu. Mit Blick auf das Jahr 2030 fallen die Erwartungen verhalten optimistisch aus. 51 Prozent rechnen damit, dass europäische Anbieter zumindest teilweise funktional aufholen werden. Nur 2 Prozent glauben fest an einen spürbaren Gleichstand.

Aus Sicht der CIOs bleiben die Hyperscaler mittelfristig der klare Taktgeber in puncto Innovationskraft und Servicebreite. Europäische Cloud-Angebote werden dagegen vor allem als komplementäre Option für regulierte, sensible oder souveränitätskritische Workloads gesehen – nicht als vollwertiger Ersatz. Laut [IT-Agenda 2026 von Metrics und dem VOICE e.V.](#) stimmen zudem 84 Prozent der Unternehmen zu, dass die Innovationsgeschwindigkeit europäischer Cloud Provider zu langsam sei und die US-Hyperscaler hier einen deutlichen Wettbewerbsvorteil hätten.

Die Einschätzungen zu wichtigen Zukunftstechnologien wie KI und Quantencomputing fallen leicht optimistischer aus: 67 Prozent der Unternehmen stimmen voll oder teilweise zu, dass europäische Cloud-Provider in den kommenden Jahren passende Lösungen anbieten werden. Erwartet wird jedoch eher die Entwicklung domänenspezifischer, compliancefähiger Lösungen als ein vollständiger Gleichstand bei Skalierung, Modellvielfalt oder globaler Ökosystemstärke.

In der Gesamtschau geben 93 Prozent der Unternehmen an, dass europäische Cloud-Provider auf der Infrastrukturebene in einzelnen Aspekten durchaus mithalten können, ihr Angebot an höherwertigen Services und Ökosystemleistungen jedoch bei weitem nicht so ausgereift ist wie das der Hyperscaler. Entsprechend stimmen nur 12 Prozent der Befragten voll zu, dass sie deutlich stärker auf europäische Cloud-Provider setzen würden, um digitale Souveränität zu gewinnen, wenn dies gleichzeitig Abstriche bei Innovation und Skalierung bedeutet. Dass jedoch 67 Prozent dieser Aussage zumindest teilweise zustimmen, zeigt, dass dieser Trade-off je nach Use Case durchaus in Betracht gezogen wird. Insbesondere Unternehmen mit einem hohen Cloud-Reifegrad können sich einen solchen Ansatz vorstellen.

Europäische Cloud-Anbieter gewinnen Akzeptanz – bleiben aber funktional im Rückstand

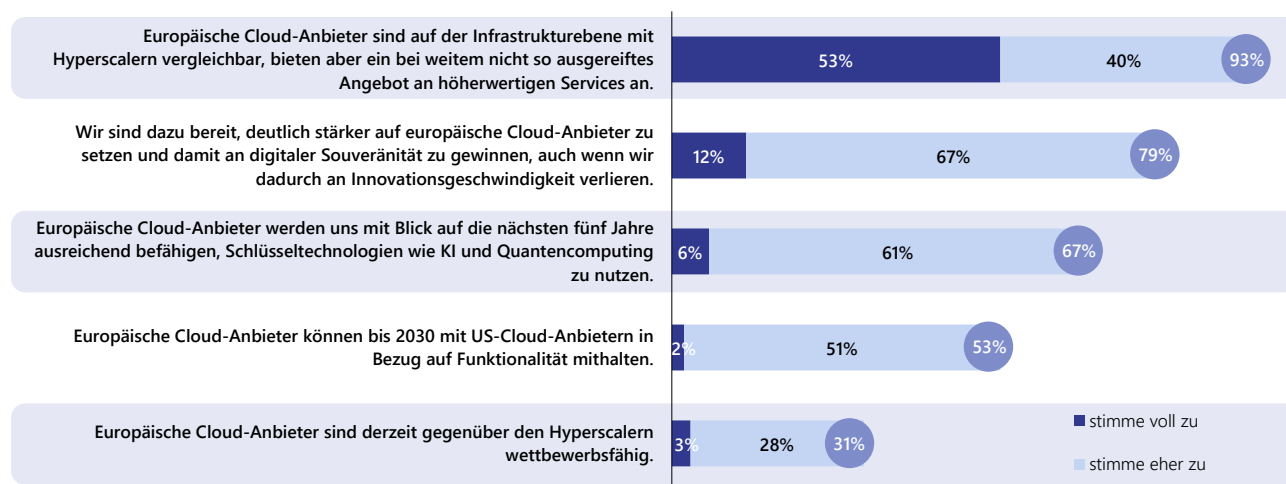


Abb. 18: Deutsche oder europäische Cloud-Provider sind eine Alternative zu den Hyperscalern. Wie stehen Sie zu den folgenden Aussagen?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

Aktuelle Hyperscaler-Workloads bleiben auch weiterhin auf Cloud-Infrastrukturen

Was bedeuten die vorangegangenen Ergebnisse konkret für die Workloads, die heute bereits auf Hyperscalern laufen? Je nach Anforderungen ergreifen Unternehmen unterschiedliche Maßnahmen – jedoch zeigt sich ein eindeutiges Bild: Nahezu alle befragten Organisationen wollen ihre bestehenden Hyperscaler Umgebungen um zusätzliche Sicherheitsmechanismen ergänzen, etwa durch erweiterte Verschlüsselung, strengere Identity und Zugriffsmodelle oder ein ausgebautes Monitoring.

Es handelt sich also nicht um eine Abkehr von den Hyperscalern, sondern um eine Absicherung des laufenden Betriebs.

Zudem können sich 87 Prozent der Unternehmen vorstellen, zu souveränen Hyperscalern zu migrieren. 89 Prozent ziehen außerdem eine Verlagerung bestimmter Workloads zu europäischen Cloud-Providern in Betracht.

Hyperscaler-Workloads sollen zusätzliche Sicherheitsmechanismen erhalten oder zu souveränen Alternativen migriert werden

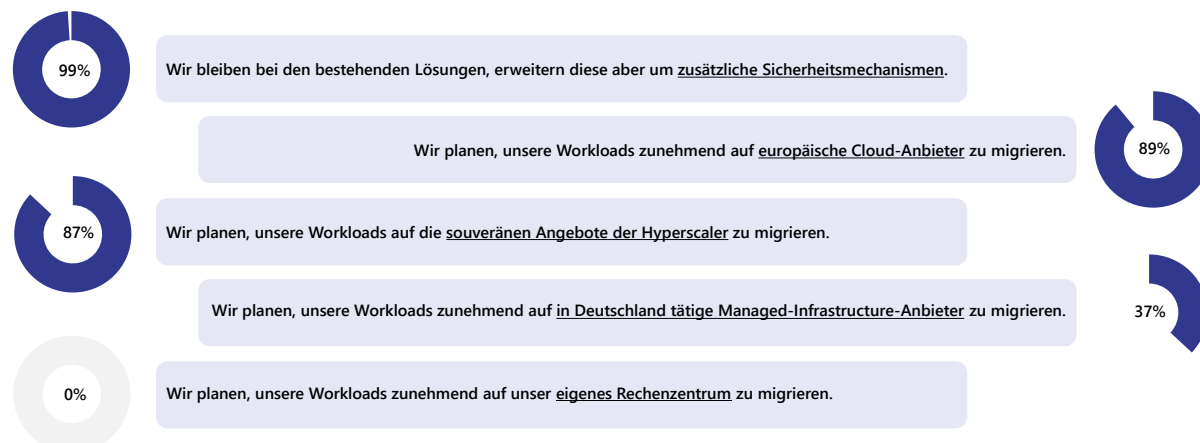


Abb. 19: Wie stehen Sie zu den folgenden Aussagen bezüglich der Workloads, die aktuell auf den Hyperscalern laufen?; Mehrfachauswahl; nur Hyperscaler-Kunden; n = 139

Eine Abkehr von der Cloud – gleich welcher Art – bleibt hingegen die Ausnahme. Für 37 Prozent der Hyperscaler-Nutzer kommt eine Migration zu Managed-Infrastructure-Anbietern infrage, eine Rückverlagerung in ein eigenes Rechenzentrum ist für keines der befragten Unternehmen eine Option. Für Unternehmen lautet die zentrale Frage daher nicht mehr „Cloud oder nicht Cloud?“, sondern: „Welches Cloud-Modell bietet den passenden Grad an Kontrolle und Souveränität?“

Auswahlkriterien von souveränen Cloud-Angeboten

Ergänzend wurde untersucht, welche Kriterien bei der Auswahl souveräner Cloud Angebote für Unternehmen ausschlaggebend sind. Zwar können diese Anforderungen in der Praxis mit wirtschaftlichen Zielen kollidieren, für die Studie wurden jedoch bewusst die „Wunschvorstellungen“ abgefragt. Zudem stehen einige der genannten Kriterien naturgemäß im Wettbewerb zueinander.

Für nahezu alle Unternehmen (87 %) ist der Schutz vor extraterritorialen Gesetzen und unberechtigten Datenzugriffen von zentraler Bedeutung. Ebenso entscheidend ist die Exit-Fähigkeit (83 %), also die Möglichkeit, bei Bedarf mit vertretbarem Aufwand den Anbieter wechseln zu können.

Damit wollen sich Unternehmen strategische Handlungsfähigkeit bewahren – etwa im Falle geopolitischer Konflikte, unerwarteter Preisschocks oder veränderter Provider-Strategien. Beide Kriterien sind Kernelemente digitaler Souveränität: juristische Kontrolle und echte Wahlfreiheit.

Etwas nachgelagert, aber weiterhin klar relevant, sind klassische Qualitäts-, Sicherheits- und Vertrauensmerkmale. Dazu zählen Zertifizierungen, die souveräne und sichere Betriebsmodelle nachweisen, Skalierungsoptionen sowie Transparenz über Prozesse und interne Abläufe der Cloud-Anbieter.

Deutschsprachiger Support oder die Bereitstellung umfassender Self-Services werden hingegen als wünschenswert, aber nicht als zwingend betrachtet. Die vergleichsweise geringe Relevanz integrierter KI-Ressourcen zeigt zudem, dass souveräne Clouds derzeit vor allem für schutzbedürftige, regulatorisch sensible Workloads genutzt werden. Anspruchsvolle KI-Anwendungen werden dagegen eher in spezialisierten KI-Cloud-Umgebungen erwartet – funktionale Bequemlichkeit wird dem Prinzip „Souveränität first“ bewusst untergeordnet.

Auswahlkriterien: Rechtssicherheit, Exit-Fähigkeit und Transparenz sind entscheidend – bei gleichzeitiger Skalierungsfähigkeit

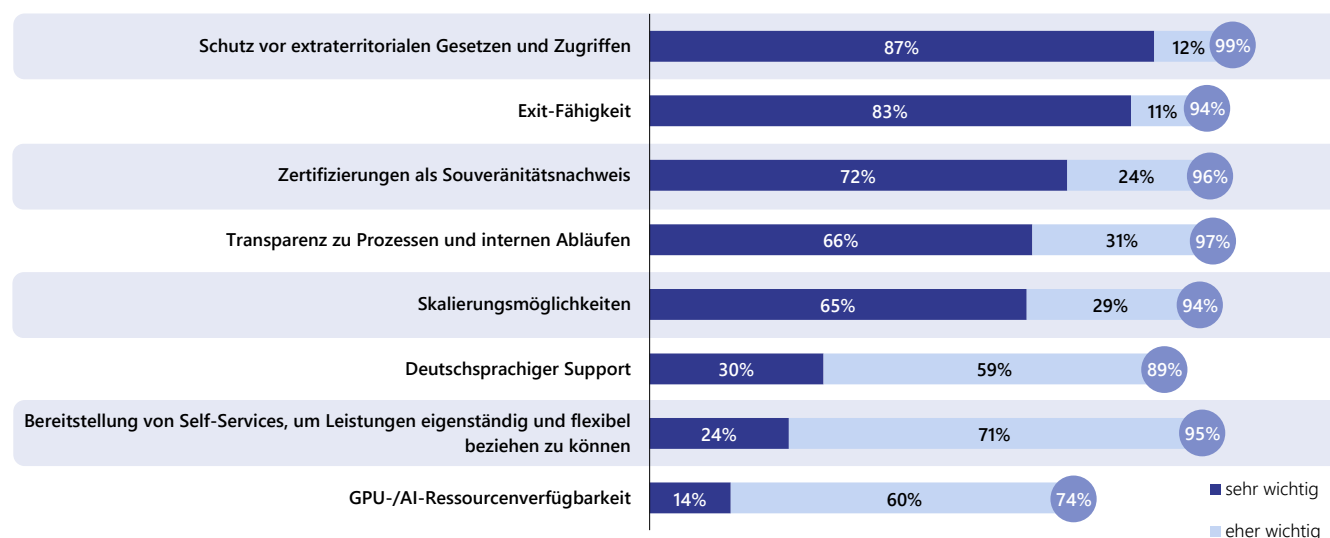


Abb. 20: Wie wichtig sind die folgenden Kriterien bei der Auswahl eines souveränen Cloud-Anbieters?; Skala von 1 = „unwichtig“ bis 4 = „sehr wichtig“; relative Häufigkeitsverteilung; alle Unternehmen; n = 152

Investitionen, Verantwortlichkeiten & Rolle externer Partner



Zu Beginn der Studie wurde bereits deutlich, dass eine fehlende Top Management Attention kein wesentliches Hindernis für digitale Souveränität darstellt. Noch wichtiger als reine Aufmerksamkeit ist jedoch, wer das Thema verantwortet, vorantreibt und über die notwendigen Kompetenzen verfügt. Zwar sehen nur 4 Prozent der Unternehmen hierin eine große Herausforderung, für weitere 39 Prozent stellt die fehlende Verantwortungszuordnung jedoch zumindest teilweise eine Hürde dar.

Geteilte Verantwortung, gemeinsames Ziel:

Digitale Souveränität als Teamaufgabe

Die Ergebnisse zeigen, dass das Thema zwar klar beim CIO verankert ist, sich aber zunehmend zu einer gemeinsamen Aufgabe von IT und Fachbereichen entwickelt. In 93 Prozent der Unternehmen liegt die führende Rolle beim CIO, da nur er Architektur, Cloud-Modelle, Security, Datenflüsse und die technische Machbarkeit souveränitätsrelevanter Maßnahmen so gut beurteilen und steuern kann.

Gleichzeitig befassen sich in 83 Prozent der Unternehmen auch Fachbereiche aktiv mit digitaler Souveränität. Das zeigt einerseits, dass Themen wie Datenhoheit, Plattformabhängigkeiten, KI-Nutzung oder Compliance direkt in Produkte, Prozesse und Geschäftsmodelle hineinwirken. Andererseits wird digitale Souveränität zunehmend als strategischer Steuerungsfaktor verstanden, der nur wirksam adressiert werden kann, wenn IT und Fachbereiche gemeinsame Prioritäten, Anforderungen und Trade-offs definieren.

Eine wichtige Rolle nehmen zudem die Verantwortlichen für GRC und IT-Security ein. Sie übersetzen regulatorische und Risikovorgaben in konkrete Richtlinien, Kontrollen und Prüfmechanismen. So stellen sie sicher, dass die Souveränitätsziele nicht nur technisch, sondern auch aus Sicht von Compliance, Risiko und Auditierbarkeit erreicht werden. Auch die Geschäftsführung treibt das Thema in einigen Unternehmen aktiv voran. Dies verdeutlicht, dass digitale Souveränität zunehmend als strategisches Top-Management-Thema wahrgenommen wird, selbst wenn die operative Verantwortung an anderer Stelle liegt.

CIOs sind Haupttreiber für digitale Souveränität – aber auch Fachbereiche haben einen starken Einfluss



Abb. 21: Welche Funktionen treiben in Ihrer Organisation das Thema digitale Souveränität voran?; Mehrfachantwort; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Digitale Souveränität ist zwar strategisch gesetzt, wird aber evolutionär und unter Budgetrestriktionen umgesetzt

Zudem stellt sich die Frage, wie es um das Investitionsverhalten bezüglich digitaler Souveränität steht. 86 Prozent der Unternehmen bestätigen, dass sich souveräne Lösungen auch dann lohnen, wenn der Umstieg erhebliche Investitionen erfordert oder die Angebote teurer sind. Die dahinterliegende Logik ist folgende: Die potenziellen Folgekosten – etwa durch Lock-in-Effekte, regulatorische Verstöße, Reputationsschäden oder eine eingeschränkte Verhandlungs- und Exit-Fähigkeit – werden höher bewertet als die Mehrkosten souveräner Infrastrukturen und Plattformen. Digitale Souveränität wird somit zu einem wirtschaftlich rationalen Risikoschutz und zu einer strategischen Investition in Zukunfts- und Handlungsfähigkeit – selbst wenn sie kurzfristig teurer erscheint.

Gleichzeitig müssen die finanzielle Realität und das aktuelle Marktumfeld berücksichtigt werden. Zwar signalisiert eine große Mehrheit der Unternehmen grundsätzlich die Bereitschaft, die IT-Budgets für souveräne Lösungen zu erhöhen, doch nur 14 Prozent tun dies mit voller Überzeugung. Ein ähnliches Bild zeigt sich bei der generellen Zahlungsbereitschaft für souveräne Cloud-Angebote.

Digitale Souveränität wird zwar als wichtig und ökonomisch sinnvoll erachtet, dennoch gibt es eine deutliche Zurückhaltung, wenn es um konkrete, spürbare Mehrkosten im laufenden Budget geht. In der Praxis dürfte dies dazu führen, dass souveräne Lösungen selektiv und risikobasiert eingesetzt werden. Viele Unternehmen werden zunächst mit Pilotprojekten, einzelnen Workloads oder spezifischen Domänen – etwa in sensiblen Datenräumen oder KRITIS-nahen Anwendungen – starten, anstatt ihre gesamte IT-Landschaft kurzfristig auf souveräne Angebote umzustellen.

Bei der Frage, ob digitale Souveränität zu einer verstärkten Investition in eigenentwickelte Anwendungen führt und die Nutzung externer Standardsoftware entsprechend reduziert, fällt das Bild ambivalent aus. Einerseits legt digitale Souveränität die Verwendung kontrollierbarer, eigenentwickelter Lösungen nahe und reduziert die Abhängigkeit von proprietären Systemen. Andererseits stehen dem jedoch hohe Entwicklungs- und Betriebskosten, Fachkräftemangel, Time-to-Market-Druck und die Innovationsgeschwindigkeit externer Plattformen entgegen. Tendenziell befürworten vor allem jene Unternehmen diese Strategie, die bereits einen hohen Grad an Souveränität aufweisen.

Digitale Souveränität wird als strategische Investition bewertet – wird aber evolutionär und unter Budgetrestriktionen umgesetzt

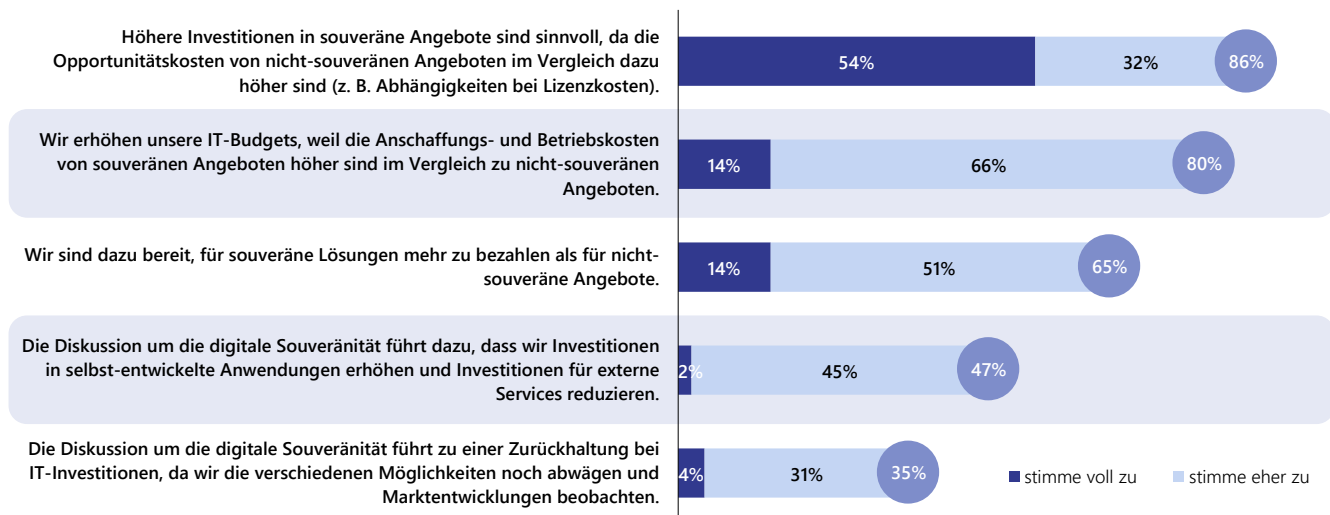


Abb. 22: Wie stehen Sie zu den folgenden Aussagen in Bezug auf Ihre Organisation?; Skala von 1 = „stimme nicht zu“ bis 4 = „stimme voll zu“; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

Einsatzbereiche von externen Partnern

Unternehmen investieren auch in externe Partner, die sie dabei unterstützen, ihre digitale Souveränität zu bewerten, entsprechende Strategien zu entwickeln und diese umzusetzen. Am häufigsten planen Unternehmen eine Zusammenarbeit für Weiterbildungen und Trainings (95 %) sowie für Cloud-Migrationen und -Modernisierungen (94 %). Einerseits fehlen in vielen Organisationen noch ausgereifte Kompetenzen in den Bereichen Cloud, Security, Open Source und Governance, andererseits laufen geschäftskritische Workloads bereits heute auf Hyperscalern und müssen nun hinsichtlich der digitalen Souveränität optimiert, segmentiert oder migriert werden.

Am häufigsten soll die Zusammenarbeit bei Weiterbildungen und Trainings (95 %) sowie bei Cloud-Migrationen und -Modernisierungen (94 %) in Anspruch genommen werden. Einerseits fehlen in vielen Organisationen noch ausgereifte Skills rund um Cloud, Security, Open Source und Governance, andererseits sitzen die geschäftskritischen Workloads heute bereits auf Hyperscalern und müssen nun souveränitätsfähig gemacht, segmentiert oder migriert werden.

Der Bedarf an technischer Beratung und Strategieentwicklung ist mit 88 Prozent ebenfalls sehr hoch, dicht gefolgt vom Aufbau von Governance-Strukturen mit 86 Prozent. Unternehmen suchen somit Unterstützung beim Erstellen eines konsistenten Zielbilds und eines belastbaren Ordnungsrahmens aus Richtlinien, Rollen und Prozessen.

Mit Sourcing Advisory (80 %) und Unterstützung bei der Open-Source-Nutzung (72 %) rückt zudem die externe Perspektive auf Anbieterstrategien, Lock-in-Risiken sowie Lizenz- und Governance-Fragen stärker in den Fokus. Die Studie zeigt deutlich, dass viele Unternehmen zwar vermehrt auf Open-Source-Lösungen und souveräne Anbieter setzen möchten, jedoch weder über eine ausgereifte Sourcing-Strategie noch über ausreichende interne Open-Source-Kompetenzen verfügen. Die strategische Auswahl, Kombination und Steuerung von Anbietern im Spannungsfeld zwischen Hyperscalern, souveränen Clouds, IT-Service-Providern und Open-Source-Ökosystemen gewinnt damit weiter an Bedeutung.

Der IT-Betrieb wird hingegen vergleichsweise selten als Bereich für externe Unterstützung im Kontext digitaler Souveränität genannt (47 %). Dies dürfte vor allem daran liegen, dass häufig bereits etablierte Souveränitätslösungen von Anbietern – insbesondere im Cloud-Umfeld – genutzt werden. Zudem stehen weniger operative Betriebsfragen als vielmehr Themen rund um Architektur, Governance, Sicherheitsmechanismen und die strategische Ausrichtung der Anbieterlandschaft im Vordergrund. Unternehmen mit einem geringeren Cloud-Reifegrad sehen hier allerdings einen höheren Unterstützungsbedarf als die Cloud-Leader.

Externe Partner sollen an diversen Stellen unterstützen – Wachstumspotenzial für IT-Dienstleister und Berater

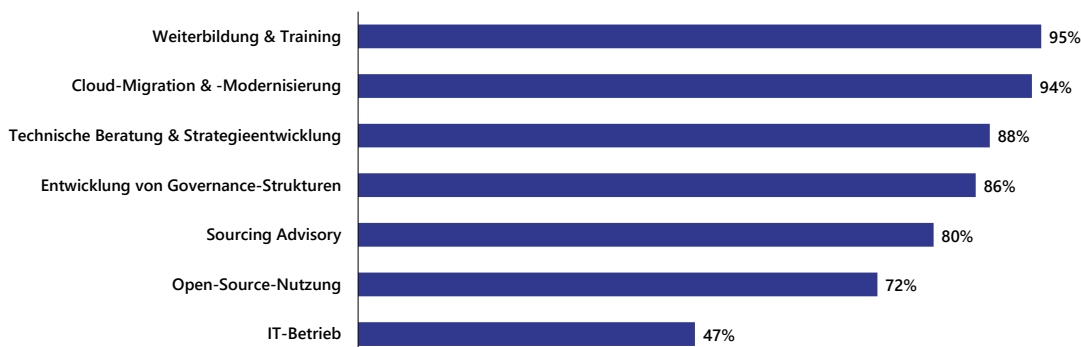


Abb. 23: In welchen Bereichen werden Sie künftig mit externen Partnern zusammenarbeiten, um Ihre digitale Souveränität zu stärken?; Mehrfachantwort; relative Häufigkeitsverteilung; alle Unternehmen; n = 154



Fazit & Ausblick



Digitale Souveränität ist in Deutschland längst kein Nischenthema mehr, sondern entwickelt sich zu einer strategischen Kernfrage von Wettbewerbsfähigkeit, Innovationsgeschwindigkeit, Resilienz und Compliance. Dabei geht es ausdrücklich nicht um Autarkie, sondern um die Fähigkeit, kritische Abhängigkeiten bewusst zu gestalten, Risiken zu steuern und Handlungsfähigkeit zu sichern – entlang der Dimensionen betriebliche, technische, datenbezogene und juristische Souveränität. So erwarten 96 Prozent der Unternehmen, dass digitale Souveränität in den kommenden drei Jahren weiter an Bedeutung gewinnt.

Politisches Wunschdenken trifft auf die Realität des Marktes

Unternehmen und Organisationen sehen sich einem doppelten Spannungsfeld ausgesetzt: Einerseits nehmen Druck und Relevanz zu, beispielsweise durch Vendor-Lock-ins, hohe Preissteigerungen, fragile Lieferketten, geopolitische Risiken bis hin zum Kill-Switch-Szenario, extraterritoriale Zugriffsrechte wie der CLOUD Act und FISA sowie eine wachsende Dichte an Regulierungen. Dem stehen erhebliche Hürden gegenüber: komplexe, historisch gewachsene IT-Landschaften, ausgeprägte Vendor Lock-ins mit entsprechend hohen Wechselkosten, Budgetrestriktionen sowie ein funktionaler Rückstand europäischer Anbieter gegenüber Hyperscalern. Diesen Rückstand halten viele für kurz- und mittelfristig nicht vollständig aufholbar, sodass digitale Souveränität nicht von jetzt auf gleich realisierbar ist. „Made in Europe“ mag aus politischer EU-Sicht somit ein Ziel sein, die Marktgegebenheiten sprechen jedoch eine andere Sprache.

Der Status quo ist ebenfalls ambivalent: Digitale Souveränität ist auf der Führungsebene präsent und wird in vielen Organisationen bereits in Teilaspekten umgesetzt – etwa durch Cloud-Governance, Identity- und Berechtigungskonzepte, Verschlüsselung und Privacy by Design. Gleichzeitig dominieren aktuell proprietäre Best-of-Suite-Anwendungen. Exit-Strategien sind häufig schwach ausgeprägt oder gar nicht vorhanden. Nur etwa ein Drittel der befragten Unternehmen hat digitale Souveränität systematisch in IT- und Sourcing-Strategien integriert. Oft bleibt es bei isolierten Einzelinitiativen ohne konsistentes Zielbild, belastbare KPIs und Reifegradmodelle.

Vernetzt statt Entweder-oder: Hyperscaler und europäische Cloud-Anbieter werden miteinander kombiniert

In Puncto Cloud bleibt die Abhängigkeit von außer-europäischen Anbietern hoch: US-amerikanische Hyperscaler dominieren den europäischen Cloud-Markt. 9 von 10 Unternehmen nutzen mindestens einen Hyperscaler. Multi-Cloud-Architekturen werden vor allem genutzt, um Abhängigkeiten zu reduzieren oder Best-of-Breed-Szenarien zu ermöglichen. Eine vollständige Abkehr von den Hyperscalern ist somit nicht zu beobachten. Dafür werden Cloud-Architekturen differenzierter und abhängig von den jeweiligen Anforderungen entsprechende Cloud-Modelle genutzt. Spannend bleibt, wie die souveränen Angebote der Hyperscaler in den nächsten Monaten aufgenommen werden. 89 Prozent der Unternehmen stimmen zu, dass diese ihnen zu mehr digitaler Souveränität verhelfen. Gleichzeitig äußern 66 Prozent Misstrauen, da die Angebote weiterhin von US-Unternehmen stammen und nicht vollständig überprüfbar sind.

Gleichzeitig geben knapp 8 von 10 Unternehmen an, deutlich stärker auf europäische Cloud-Anbieter setzen zu wollen, auch wenn dadurch an Innovationsgeschwindigkeit verloren geht. Knapp jedes dritte Unternehmen ist zwar der Ansicht, dass europäische Cloud-Anbieter mit den Hyperscalern heute nicht mithalten können. Immerhin 53 Prozent erwarten aber, dass sie bis 2030 mit den Hyperscalern in Sachen Funktionalität mithalten können.

In Summe zeigt sich: Digitale Souveränität wird als strategisches Zielbild breit geteilt – die operative Umsetzung erfolgt jedoch oft fragmentiert, reaktiv und unter Rahmenbedingungen, die nicht kurzfristig aufzulösen sind. So schaffen viele Unternehmen erst schrittweise die strukturellen, technologischen und organisatorischen Voraussetzungen, um digitale Souveränität systematisch und langfristig zu verankern.



Nachwort



Eine solch umfassende Erhebung wäre ohne externe Unterstützung nicht denkbar und kann auch nicht kostenfrei zur Verfügung gestellt werden. Aus diesem Grund danken wir folgenden Beratungen und IT-Dienstleistern für ihre freundliche Unterstützung bei der Studiumsetzung:

- adesso
- Exxeta
- MaibornWolff
- Materna
- msg
- TechniData

An dieser Stelle gilt unser besonderer Dank auch allen Studienteilnehmern, die sich Zeit für die telefonischen Interviews genommen haben, sowie dem Auswertungsteam der Lünendonk & Hossenfelder GmbH. Vielen Dank für die umfassende Unterstützung bei der Erarbeitung dieser Lünendonk-Studie.

Die Lünendonk & Hossenfelder GmbH ist auch nach nunmehr 40 Jahren intensiver Marktanalysen und einem ständigen Dialog mit Expertinnen und Experten aus Wissenschaft, Unternehmen und Verbänden bestrebt und sicher, solide Ergebnisse und Interpretationen zu liefern.

Gleichwohl glauben wir, dass sich immer neue Aspekte, Ideen und Verbesserungsvorschläge ergeben. Für derartige Hinweise sind wir stets dankbar und rufen hiermit auch unsere Leserinnen und Leser dieser Studie dazu auf.

Herzlichen Dank im Voraus!



Beiträge der Studienpartner



adesso	35
Damian Kirtz, Managing Consultant, Digitale Souveränität	
Exxeta	40
Markus Fischer, Cloud Fellow	
MaibornWolff	43
Christian Leinweber, Technical Director Cloud Sovereignty & Compliance	
Dr. Jan Renz, Co-Leitung Mediendienste, FWU Institut für Film und Bild	
Materna	47
Timon Schmotz, Business Development Manager	
msg	50
Karl Lassak, Principal Consultant	
TechniData	53
Peter Jung, CEO	

Digitale Souveränität als Chance: Unternehmenserfolg aktiv gestalten

Digitale Souveränität wird für Unternehmen zunehmend zum entscheidenden Faktor, um in einem komplexen digitalen Umfeld selbstbestimmt und zukunftsfähig zu handeln. Sie eröffnet nicht nur Schutz vor Risiken, sondern schafft die Basis für Innovationskraft und strategische Weiterentwicklung. Im Fachbeitrag zeigt Damian Kirtz von adesso, wie Unternehmen mit dem adesso-Souveränitätsbaukasten technologische, organisatorische und datenbezogene Abhängigkeiten transparent machen und daraus klare Prioritäten ableiten können. Durch strategisches Cloud-Management, eine transparente Applikationslandschaft und gezielten Kompetenzaufbau entsteht echte Handlungsfähigkeit.



Damian Kirtz
Managing Consultant,
Digitale Souveränität
adesso

Die vorliegende Studie zeigt deutlich: Digitale Souveränität wird häufig primär als Instrument zur Risikominderung verstanden. Im Fokus stehen die Reduktion kritischer Abhängigkeiten in der IT-Lieferkette, die Stärkung der Resilienz in Krisensituationen sowie der Schutz vor unkontrolliertem Datenabfluss und extraterritorialen Zugriffen.

Dabei ist die Auseinandersetzung mit digitaler Souveränität weit mehr als reine Risikoabsicherung. Sie eröffnet konkrete Chancen zur Steigerung des Unternehmenserfolgs und schafft die Grundlage für nachhaltige Wettbewerbsfähigkeit.

Vom Risiko zur Chance: Der Souveränitätsbaukasten

Auf Basis unserer langjährigen Projekterfahrung haben wir bei adesso einen Souveränitätsbaukasten entwickelt, der als strukturiertes Arbeitsinstrument einsetzbar ist. Er orientiert sich an den in der Studie definierten Dimensionen und ergänzt diese um die Dimension „Kompetenzen“ (Abbildung 1). Die juristische Souveränität verorten wir innerhalb des Geschäftsbetriebs. Insgesamt umfasst der Baukasten damit die vier Dimensionen Technologie, Daten, Geschäftsbetrieb und Kompetenzen. Ihnen zugeordnet sind 18 Themenfelder und 105 Einzelthemen.



Souveränitätsbaukasten

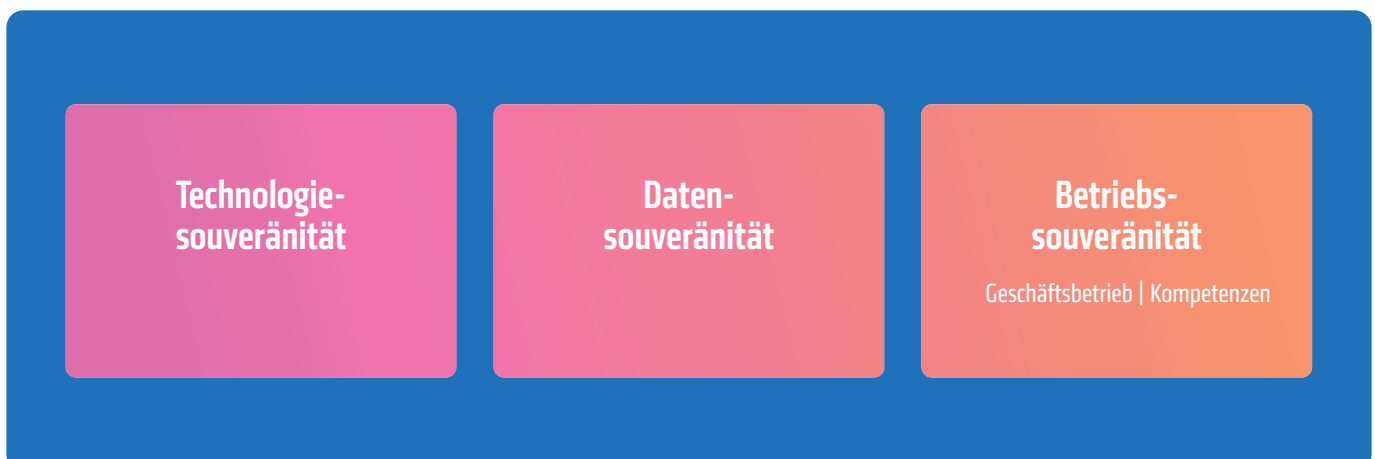


Abb. 24: Die Dimensionen des Souveränitätsbaukasten – ergänzt um „Kompetenzen“. (Quelle: adesso SE)

In der praktischen Anwendung des Baukastens analysieren wir gemeinsam mit unseren Kunden alle relevanten Themenfelder. Für jedes Thema definieren wir den konkreten Handlungsbedarf und bewerten die Auswirkungen auf Leistungsfähigkeit, Kostenstruktur und operative Handlungsfreiheit. So entsteht mit überschaubarem Aufwand ein transparenter Überblick über Prioritäten und Wertbeiträge. Unternehmen erhalten eine belastbare Entscheidungsgrundlage, statt isolierte Einzelmaßnahmen umzusetzen.

Strategisches Cloud Management statt Autarkie-Zwang

Ein aktuelles Beispiel aus der Dimension Technologie ist das Themenfeld Cloud. Um hier digitale Souveränität zu erreichen, sind weder Autarkie um jeden Preis noch der pauschale Verzicht auf Hyperscaler das Ziel. Entscheidend ist vielmehr eine differenzierte Betrachtung: Welche Workloads enthalten welche Daten? Wie sind Daten und Geschäftsprozesse zu klassifizieren?

Auf dieser Basis lassen sich Workloads strategisch auf unterschiedliche Infrastrukturen verteilen. So entsteht ein ausgewogenes Verhältnis aus Innovationsfähigkeit, Wirtschaftlichkeit und Kontrolle. Entscheidungen beruhen auf klaren Kriterien, nicht auf geopolitischer Unsicherheit oder kurzfristigem Druck.

Durch diese Herangehensweise entstehen strategische Leitplanken, die operativ greifbar sind. Sie lassen sich in sechs zentrale Handlungsfelder zusammenfassen, die den gesamten Zyklus des strategischen Cloud Managements abdecken. Den Ausgangspunkt bildet das Handlungsfeld „Cloud-Strategie & Governance“. Hier wird grundlegend festgelegt, ob ein Cloud-first-, Hybrid- oder Multi-Cloud-Ansatz verfolgt wird. Darauf aufbauend ermöglicht ein dediziertes „Cloud Portfolio- & Architektur-Management“ die gezielte Auswahl zwischen Public Cloud, EU Sovereign Cloud oder Private Cloud unter Berücksichtigung des jeweils optimalen Providers (Handlungsfeld 2).

Für die technische Umsetzung ist das Handlungsfeld „Cloud Engineering & Migration“ verantwortlich, welches den Aufbau, die Migration sowie die Automatisierung der Prozesse steuert. Parallel dazu stellt das Handlungsfeld „Cloud Operation Management“ den laufenden Betrieb sicher, indem es Aspekte wie Incident und Performance Management, Maintenance sowie den Support ganzheitlich handhabt.

Um eine optimale Balance aus Kontrolle und Wirtschaftlichkeit zu wahren, sind zwei zentrale, flankierende Handlungsfelder Teil des Zyklus. Das Handlungsfeld Cloud Security, Risk & Compliance stellt die regulatorische Leitplanke dar, indem es die konsequente Umsetzung von Access-, Security- und Compliance-Vorgaben sowie ein ganzheitliches Risikomanagement sicherstellt. Ergänzend dazu sichert das Handlungsfeld „Financial Operations und Innovation Management“ die ökonomische Nachhaltigkeit der Cloud-Lösung ab: Durch präzise Kostenkontrolle sowie Showback- und Chargeback-Modelle wird eine vollständige finanzielle Transparenz geschaffen, während parallel dazu das Innovations- Management und gezielte Initiativen, beispielsweise für eine Green IT, aktiv vorangetrieben werden.

„Um digitale Souveränität zu erreichen, sind weder Autarkie um jeden Preis noch der pauschale Verzicht auf Hyperscaler das Ziel.“



Damian Kirtz
adesso

Transparente Applikationslandschaft als Schlüssel zu Effizienz und Sicherheit

Ähnlich verhält es sich beim Themenfeld Applikationslandschaft. Eine umfassende Transparenz über bestehende Anwendungen, deren konkreten Beitrag zu den Business-Fähigkeiten sowie zukünftige Bedarfe bildet die essenzielle Grundlage für ein aktives Architektur- und Lizenz-Management. Dieser Ansatz erhöht die Effizienz, verbessert die Sicherheit sowie die Interoperabilität und unterstützt maßgeblich die Einhaltung regulatorischer Anforderungen.

Der Mehrwert zeigt sich unter anderem in konkreten, operativen Entlastungen: So führt die Identifikation von „Schatten-IT“ und redundanter Software zu spürbaren Kostensenkungen durch Lizenz-Bereinigungen. Wenn beispielsweise drei Abteilungen unterschiedliche Projektmanagement-Tools nutzen, spart die Konsolidierung auf eine einzige Lösung nicht nur Lizenzgebühren, sondern reduziert auch den Schulungsaufwand erheblich. Gleichzeitig minimiert dies Risiken im Bereich Security und Compliance, da veraltete Legacy-Systeme ohne Sicherheitsupdates rechtzeitig erkannt und ersetzt werden können.

Kompetenzaufbau als Antwort auf den Fachkräftemangel

Neben dieser technologischen Dimension digitaler Souveränität sind die Dimensionen Kompetenz und Geschäftsbetrieb weitere entscheidende Faktoren. Eigene digitale Kompetenzen und die organisatorische Verankerung sind in diesem Kontext unabdingbar. Nur Unternehmen, die digitale Fähigkeiten systematisch aufbauen, sichern langfristig ihre Betriebsouveränität als Basis für Automatisierung, Skalierung und den produktiven Einsatz von Technologien wie KI.

Gerade für mittelständische Unternehmen bedeutet dieser Kompetenzaufbau einen direkten Wettbewerbsvorteil, da internes Know-how das Management von Partnern und den Aufbau eines erfolgreichen Ökosystems ermöglicht. Schlüsseltechnologien wie Cloud-Orchestrierung oder Datenanalyse können dann auch von spezialisierten IT-Dienstleistern durchgeführt werden. Das Unternehmen bleibt „Herr der Lage“ und kann seine Strategien selbstbestimmt umsetzen.

Zudem ermöglicht das eigene digitale Know-how eine tiefergehende Automatisierung, da geschulte Mitarbeitende – etwa im Lager eines herstellenden Betriebs oder Händlers – eigenständig Potenziale für Software-Bots (RPA) erkennen, die wiederum Fachkräfte von Routineaufgaben entlasten können. Diese „KI-Readiness“ verwandelt Künstliche Intelligenz von einem theoretischen Hype in ein praktisches Werkzeug. Nicht zuletzt steigert ein solch modernes, digital souveränes Umfeld die Attraktivität als Arbeitgeber im „War for Talents“. Es zeigt, dass IT im Unternehmen als Enabler verstanden und behandelt wird.

Die Arbeit mit dem Souveränitätsbaukasten schafft somit Transparenz über Reifegrad, Prioritäten und Wechselwirkungen. Im Ergebnis entsteht eine priorisierte Themenlandkarte als Grundlage für Roadmap und Maßnahmenplanung. Priorisiert wird nach Business-Kritikalität, strategischer Leistungsfähigkeit und wirtschaftlichem Nutzen. Unterm Strich wirkt sich das methodische Vorgehen positiv auf das Geschäft aus. Der zu erzielende Mehrwert wird idealerweise bereits während der Arbeit mit dem Souveränitätsbaukasten definiert und kann kurzfristig oder langfristig entstehen.

„Nur Unternehmen, die digitale Fähigkeiten systematisch aufbauen, sichern langfristig ihre Betriebsouveränität als Basis für Automatisierung, Skalierung und den produktiven Einsatz von Technologien wie KI.“



Damian Kirtz
adesso

Mehrwerte in drei Kategorien: Sicherheit, Kosten, Wachstum

Neben der zeitlichen Komponente lässt sich dieser Mehrwert in drei Kategorien einteilen: „Steigerung der Sicherheit, Resilienz und Compliance“, „Kosteneinsparungen“ sowie „Größeres Wachstum, Innovationsfähigkeit und Profitabilität“. In der Kategorie Steigerung der Sicherheit, Resilienz und Compliance geht es unter anderem darum, geistiges Eigentum besser zu schützen und das Unternehmen vor Cyber-Angriffen zu bewahren. Dies führt automatisch zu einer gesicherten Wettbewerbsfähigkeit als Grundlage des betriebswirtschaftlichen Erfolgs. Des Weiteren ist es wichtig, Notfallpläne für eine schnellere Wiederherstellung von Daten sowie die Aufrechterhaltung des Geschäftsbetriebs zu entwickeln – entscheidende Punkte für die eigene digitale Souveränität. Ebenso sind die vorbeugende Vermeidung möglicher Bußgelder und eines Reputationsschadens ein Resultat steigender Souveränität. Risiken sowie Regularien sind im Unternehmen bekannt und werden entsprechend beachtet.

Nutzenpotenziale des Souveränitätsbaukastens

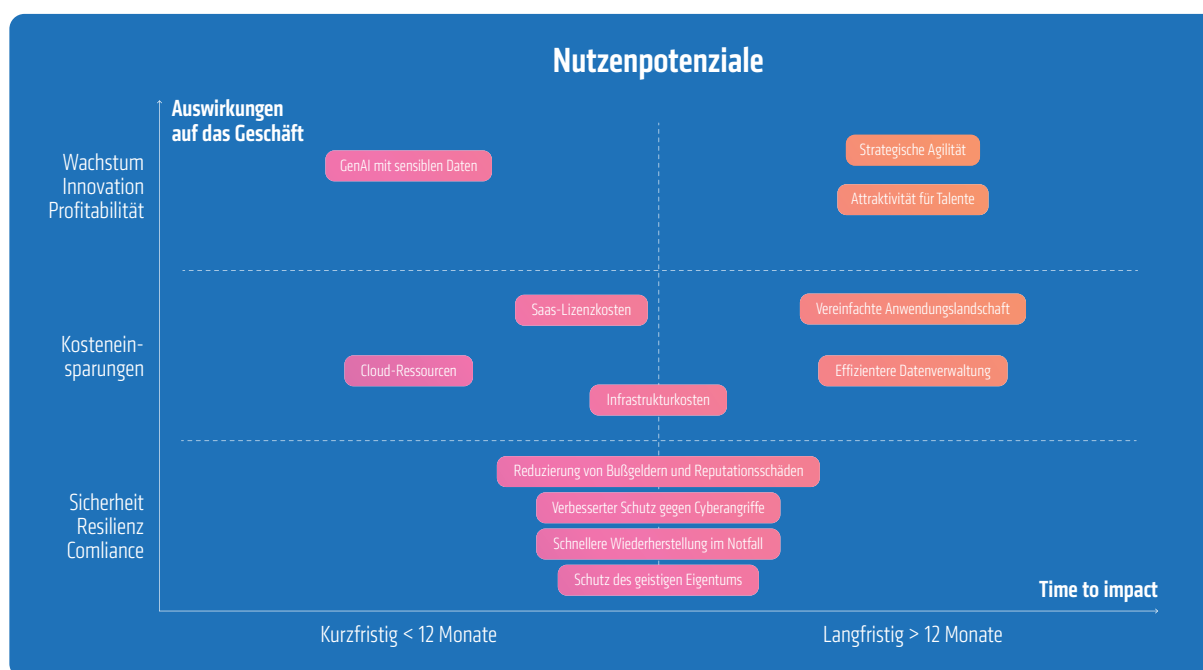


Abb. 25: Die Mehrwerte der Arbeit mit dem Souveränitätsbaukasten lassen sich unterschiedlich schnell in den Kategorien Wachstum, Kosten und Sicherheit erreichen. (Quelle: adesso SE)

Ein Nutzen, der sehr schnell zum Tragen kommt und sich langfristig positiv auf den Unternehmenserfolg auswirkt, ist die Transparenz und Kontrolle über die Infrastrukturkosten. Dies verordnen wir in der Kategorie Kosteneinsparungen. Die meisten Unternehmen bekommen nicht auf Knopfdruck einen Überblick über ihre Software im Unternehmen – geschweige denn über eine echte Kosten-Nutzen-Betrachtung. Dies kann im Rahmen der digitalen Souveränität nachgeholt werden und bewirkt, dass nur Kosten für Software entstehen, die einen wirklichen Beitrag zur Produktivität oder Innovationskraft leisten. Dabei wird erfahrungsgemäß auch die eigene Infrastruktur-Landkarte – von Hardware bis Software – zielgerichtet vereinfacht. Neben einer steigenden Kosteneffizienz führt dies auch zu langfristigen Mehrwerten im IT-Management. Durch die smarte Nutzung von Cloud-Lösungen können sowohl bei der Hardware als auch im Betrieb weitere Kosteneinsparungen erfolgen, ohne dabei die eigene Souveränität zu mindern.

Die größte langfristige Auswirkung auf den Geschäftserfolg hat die Steigerung der strategischen Agilität und Attraktivität für Talente. Unternehmen schaffen eine attraktive Grundlage für Arbeitnehmende, wenn sie die eigene Handlungsfähigkeit steigern und beherrschen. Dazu wächst die Fähigkeit, schnell und dynamisch auf Veränderungen zu reagieren. Diese Agilität ist für Unternehmen zunehmend wettbewerbsentscheidend, um in einer sich schnell verändernden Welt selbstbestimmt agieren zu können.

Ein weiterer, kurz- wie auch langfristiger Hebel, ist die souveräne Handhabung der eigenen Unternehmensdaten. Sobald die eigenen Daten richtig klassifiziert sind, können sie, je nach Sensibilität aufbewahrt und für GenAI-Anwendungen genutzt werden. Dies führt zu größerem Wachstum, mehr Innovationsfähigkeit und besserer Profitabilität.

Fazit: Digitale Souveränität ist ein echter Faktor für Wachstum

Unsere Erfahrung zeigt: Die systematische Entwicklung digitaler Souveränität stärkt die Handlungsfähigkeit eines Unternehmens nachhaltig. Sie verbindet Risikoreduktion mit strategischer Positionierung. So wird aus einem vermeintlichen Defensivthema ein aktiver Hebel für Wachstum und Transformation.

Von der Buzzword-Falle zur belastbaren IT-Strategie: Digitale Souveränität in der Praxis

Digitale Souveränität entwickelt sich für viele Unternehmen zunehmend zum geschäftskritischen Faktor – getrieben durch geopolitische Risiken, strengere Regulierung und neue Datenflüsse im KI-Zeitalter. Markus Fischer erläutert im Interview, dass Organisationen heute vor allem Kontrolle über Daten, Betriebsmodelle und Rechtsrahmen einfordern und Entscheidungen dabei workloadspezifisch statt binär treffen. Zugleich wächst die Bedeutung von offenen Standards, Exit-Fähigkeiten und souveränen Cloud-Architekturen, die pragmatisch mit Hyperscaler-Services kombiniert werden. Echte Souveränität entsteht laut Fischer jedoch nur durch eine ganzheitliche Strategie, klare Governance und realistische Migrationspfade.



Markus Fischer

Fellow Cloud
Exxeta

Wie bewerten Sie aktuell die Relevanz digitaler Souveränität für Ihre Kunden – eher politisches Schlagwort oder echter geschäftskritischer Faktor?

Markus Fischer: Digitale Souveränität ist längst kein Buzzword mehr, sondern für viele Unternehmen ein geschäftskritischer Faktor. Durch geopolitische Spannungen und regulatorische Anforderungen ist das Thema bei vielen unserer Kunden hoch priorisiert, weil es unmittelbar um Risiko, Resilienz und Handlungsfähigkeit geht. Der Druck ist bei kritischer Infrastruktur natürlich am größten: Regulierung, hohe Schutzbedarfe und Ausfallszenarien sind dort Alltag. Dort haben wir gerade bei einem großen deutschen Netzbetreiber den Auftrag, souveräne Cloud-Betriebsmodelle gegen Hyperscaler-Optionen zu bewerten. Der Fokus liegt dabei auf Datenhoheit, Exit-Fähigkeit, Governance und realistischen Migrationspfaden. Aber wir sehen das Thema genauso bei Industrie, Finanzdienstleistern oder Unternehmen mit sensiblen Daten und geschäftskritischen Plattformen. Da geht es nicht um politische Symbolik, sondern um eine klare, workloadspezifische Entscheidung: Was muss souveräner werden – und was darf pragmatisch bleiben?

Welche konkreten Anforderungen stellen Unternehmen heute an digitale Souveränität, und wie hat sich diese Erwartungshaltung in den vergangenen Jahren verändert?

Markus Fischer: Im Kern geht es meist um drei Dinge: Kontrolle über Daten, Kontrolle über Betriebsmodell und rechtliche Klarheit. Also ganz konkret: Wer kommt an die Daten? Wo liegen sie? Und unter welchem Rechtsrahmen werden sie verarbeitet? Früher war Cloud vor allem eine Effizienz- und Time-to-Market-Frage. Heute kommt eine zweite Achse hinzu: Resilienz. Unternehmen wollen Transparenz, verlässliche Governance und eine Exit-Fähigkeit. Also

exxeta

die realistische Option, Anbieter zu wechseln oder Workloads zu verlagern, ohne geschäftskritische Systeme zu destabilisieren. Gleichzeitig ist der Wille gestiegen, stärker auf offene Standards und Open Source zu setzen. Nicht als Selbstzweck, sondern als Werkzeug, um Portabilität, Transparenz und Unabhängigkeit zu verbessern. Und viele Kunden kommen inzwischen mit der Frage „Wie weise ich Souveränität nach?“. Denn das Thema wird nicht nur intern diskutiert, sondern zunehmend von Aufsicht, Partnern und Stakeholdern explizit eingefordert. Oft wird in der Debatte Souveränität zu binär gedacht.

Wie meinen Sie das mit der Aussage, Souveränität sei kein binäres Ja oder Nein?

Markus Fischer: Oft wird nur in „souverän“ oder „nicht souverän“ gedacht. In der Praxis ist das deutlich differenzierter. Digitale Souveränität hat mehrere Dimensionen und je nach Use Case braucht es mehr oder weniger davon. Ich unterscheide vor allem drei Ebenen: technologisch, betrieblich und juristisch. Technologische Souveränität betrifft die Architektur: Wie stark bin ich an proprietäre Services gebunden? Wie portabel sind meine Workloads? Betriebliche Souveränität beschreibt die Kontrolle über den laufenden Betrieb: Wer administriert Systeme? Wie transparent sind Prozesse, Logging und Zugriff? Und juristische Souveränität stellt die Frage nach dem Rechtsrahmen und Zugriffsrechten.

Je nach Kritikalität eines Systems kann eine Organisation in einer Dimension sehr souverän sein und in einer anderen bewusst Abhängigkeiten akzeptieren. Souveränität ist kein Label, das man einmal kauft und dann „hat“. Sondern ein Reifegrad, den ich aktiv steuere.

Inwieweit beeinflusst die Debatte um Souveränität die strategische IT-Planung Ihrer Kunden – insbesondere im Hinblick auf Architekturentscheidungen und Cloud-Strategien?

Markus Fischer: Die Debatte schlägt inzwischen direkt in Architekturentscheidungen durch, insbesondere bei kritischen Systemen. In Ausschreibungen sehen wir zunehmend Anforderungen, die Hyperscaler entweder explizit ausschließen oder zumindest eine souveräne Betriebsvariante verlangen. Technisch führt das oft zu stärkerer Containerisierung, mehr Plattform-Standards wie Kubernetes und eine bewusste Entkopplung von proprietären Services. Vor allem für unsere Kunden im öffentlichen Sektor spielt Open Source eine zentrale Rolle und reicht vom Backend bis hin zum digitalen Arbeitsplatz. Aber auch Unternehmen außerhalb stark regulierter Branchen reagieren. Viele Kunden, die heute sehr auf einen Hyperscaler setzen, entwickeln ihre Landschaft weiter Richtung Multi-Cloud. Und das bedeutet inzwischen mehr als AWS, Azure und Google.

Welche Alternativen zu den bekannten Hyperscalern gibt es und welche Vor- und Nachteile bringen diese mit?

Markus Fischer: Die bekannten Hyperscaler AWS und Microsoft Azure sind nach wie vor der Goldstandard in Sachen Cloud-Migration – und das auch zurecht. In Bezug auf Funktionalitäten, Skalierbarkeit und Innovation sind sie unschlagbar. Nur das allein reicht vielen nicht mehr aus, es soll digital souverän werden. AWS hat mit seiner European Sovereign Cloud ein stärker abgeschottetes EU-Modell eingeführt. Strukturell bleibt es jedoch das Angebot eines US-Hyperscalers.

Ein anderes Modell ist die Delos Cloud. Hier wird Microsoft-Azure-Technologie in einer eigenständigen, in Deutschland verankerten Struktur bereitgestellt und durch SAP betrieben. Das erhöht die operative und rechtliche Kontrolle im deutschen Kontext deutlich. Allerdings basiert auch hier dieses

Modell auf der Technologie eines US-Hyperscalers. Rein europäische Anbieter wie STACKIT, IONOS oder OVHcloud gehen noch einen Schritt weiter. Sie operieren sowohl eigentümerseitig als auch technologisch unter europäischer Jurisdiktion. In der Praxis zeigt sich jedoch ein Trade-off: Je höher die Souveränitätsanforderung, desto stärker muss ich funktionale Lücken, geringere Innovationsgeschwindigkeit oder mehr Integrationsaufwand einkalkulieren. Darum entscheiden sich viele für ein pragmatisches Modell: kritische Komponenten souverän aufstellen – und dort, wo es sinnvoll ist, weiterhin Hyperscaler-Services nutzen. Allerdings mit klaren Kontrollmechanismen und Exit-Szenarien.

„Ohne ein belastbares Zielbild wird digitale Souveränität schnell zur Sammlung gut gemeinter Einzelmaßnahmen. Deshalb braucht es zuerst eine Strategie, die fachliche Kritikalität, Regulierung und technische Realität zusammenbringt.“

„

Markus Fischer
Exxeta

Viele Organisationen kämpfen mit Fragmentierung, Legacy und komplexen Betriebsmodellen. Welche technologischen oder organisatorischen Weichen müssen gestellt werden, um souveräne Architekturen überhaupt realisierbar zu machen?

Markus Fischer: Ohne ein belastbares Zielbild wird digitale Souveränität schnell zur Sammlung gut gemeinter Einzelmaßnahmen. Deshalb braucht es zuerst eine Strategie, die fachliche Kritikalität, Regulierung und technische Realität zusammenbringt. Am besten ist diese mit der höchsten Management-Ebene abgestimmt. Unsere Erfahrung zeigt: Souveränitätsprojekte sind mit einem klaren Go „von oben“ oft schneller und effizienter am Ziel. Ein sehr wirksamer Hebel ist aus meiner Sicht ein Architektur-Board mit echtem Mandat. Dieses Board schaut einmal ganzheitlich auf die IT-Landschaft, definiert verbindliche Standards und sorgt dafür, dass Fragmentierung nicht weiter wächst. Und das vielleicht Wichtigste: Legacy darf nicht umschifft werden. Wer Souveränität ernst meint, braucht zumindest einen klar priorisierten Modernisierungs- und Migrationsplan. Sonst baut man Souveränität auf einem Fundament, das nicht trägt.

Generative KI verändert Wertschöpfungsketten fundamental. Gleichzeitig entstehen neue Datenflüsse in Richtung externer Modelle und Plattformen. Welche Auswirkungen hat das auf die Datensouveränität von Unternehmen – und lässt sich digitale Souveränität unter diesen Bedingungen überhaupt aufrechterhalten?

Markus Fischer: Generative KI macht digitale Souveränität nicht unmöglich, aber auf jeden Fall anspruchsvoller, weil neue Datenflüsse entstehen. Prompts, Kontextdaten, Logs – je nach Use Case sind da hochkritische Informationen dabei. Beherrschbar bleibt das nur, wenn sich Unternehmen ernsthaft mit ihrer Governance und technischen Leitplanken auseinandersetzen. Also klare Provider- und Modellstrategie, Datenklassifizierung, Freigabeprozesse, Rollen und Auditierbarkeit. Technisch heißt das: saubere Mandantentrennung, Verschlüsselung, Zugriffskontrollen, Logging, DLP-Mechanismen – und oft auch eine Architektur, in der sensible Daten nicht „frei“ in externe Modelle laufen, sondern über kontrollierte RAG-/Gateway-Konzepte. Digitale Souveränität ist im KI-Zeitalter weniger ein Verbotsschild, sondern ein Regelwerk plus Architektur.

Welche Schritte sind aus Ihrer Sicht unverzichtbar, um eine belastbare Souveränitäts-Roadmap zu entwickeln?

Markus Fischer: Zunächst sollte man sich über drei Dinge klar werden: Welche Daten, Prozesse und Plattformen sind kritisch und warum? Digitale Souveränität muss aus unterschiedlichen Perspektiven betrachtet werden – was heißt „souverän genug“ pro Bereich? Und wie kann ich das transparent messen und nachweisen? Es braucht also eine ganzheitliche Strategie, sonst bleibt digitale Souveränität nur ein Schlagwort. Darauf aufbauend wird es operativ: Standards definieren etwa für Exit-Patterns, Portabilität oder Identitäts- und Zugriffsmodelle. Provider-Modelle bewerten und Migrationspfade priorisieren. Und vor allem Skills aufbauen und regelmäßige Risiko-Reviews etablieren.

Wie unterstützt Exxeta Unternehmen konkret dabei, Souveränität und Skalierbarkeit in Einklang zu bringen?

Markus Fischer: Viele Unternehmen wollen digitale Souveränität entschlossen angehen und merken schnell, wie komplex das Thema in der Umsetzung wird. Genau hier setzen wir an. Wir beginnen mit einer strukturierten Architektur-, Risiko- und Kostenanalyse der bestehenden IT-Landschaft und bewerten Workloads nach Kritikalität, Abhängigkeiten, Austauschbarkeit und regulatorischen Anforderungen. Daraus entsteht eine priorisierte Exit-Strategie mit klarer Roadmap und transparenter Zeit- und Kostenstruktur.

Souveränität ist dabei nicht nur eine Architekturfrage, sondern auch eine Frage der Governance. Deshalb entwickeln wir Entscheidungs- und Freigabemodelle, die Verantwortlichkeiten und Kontrollmechanismen klar regeln. Die Umsetzung erfolgt risikobasiert entlang der definierten Strategie – ohne Big Bang. Wir migrieren priorisierte Workloads schrittweise und stellen sicher, dass Mandantentrennung, Verschlüsselung, Zugriffskontrollen, Logging und klare Betriebsmodelle von Anfang an etabliert sind. Wo sinnvoll, ergänzen wir das durch Managed Services.

Entscheidend für uns ist ein pragmatischer Ansatz. Wir streben nicht maximale Souveränität um jeden Preis an, sondern ein angemessenes, wirtschaftlich tragfähiges Souveränitätsniveau je Anwendungsfall.

„Digitale Souveränität ist im KI-Zeitalter weniger ein Verbotsschild, sondern ein Regelwerk plus Architektur.“

”

Markus Fischer
Exxeta

KI im Bildungsbereich souverän gestalten

KI-gestützte Lernumgebung zwischen Datenschutz, Föderalismus und Cloud: Im Projekt AIS (Adaptives Intelligentes System) verantwortet das FWU Institut für Film und Bild in Wissenschaft und Unterricht im Auftrag der Länder eine Lehr- und Lernumgebung für allgemeinbildende Schulen in Deutschland, die individuelles Lernen revolutioniert: Ein KI-Tutor begleitet Schülerinnen und Schüler durch adaptive Lernpfade, die sich kontinuierlich an Lernstand und -fortschritt anpassen. Im Interview geben Dr. Jan Renz und Christian Leinweber Einblicke in die technische Umsetzung und erläutern, warum europäische Cloud-Provider und Open Source zentrale Bausteine sind.



Christian Leinweber
Technical Director Cloud
Sovereignty & Compliance
MaibornWolff



Dr. Jan Renz
Co-Leitung Mediendienste
FWU Institut für Film und Bild

Herr Renz, was ist das Adaptive Intelligente System (AIS) und was macht es so komplex?

Dr. Jan Renz: Das innovative Adaptive Intelligente System (AIS) ist ein in vielen Dimensionen ambitioniertes System. Anders als klassische Lern-Management-Systeme will es nicht nur Inhalte verwalten, sondern stellt konsequent den einzelnen individuellen Lernenden in den Mittelpunkt. Dieser lernt dann, begleitet durch die Lehrkraft, entlang seinen Bedarfen nicht nur durch optimierte Lernpfade, sondern bekommt auf ihn angepasste Inhalte und bedarfsgerechte Unterstützung durch einen KI-Tutor. Um dies zu ermöglichen, brauchen wir nicht nur entsprechende Rechnerkapazitäten, das System muss auch eine erhebliche Menge an personenbeziehbaren Informationen speichern und verarbeiten. Datenschutz und Informationssicherheit sind daher zentraler Bausteine bei allen Aspekten der Umsetzung und des Betriebes.

Hier sind auch die Länder gefordert die rechtlichen Grundlagen herzustellen, und das in einem Umfeld, in dem sich Regelungen und Anforderungen stetig weiterentwickeln. Je mehr AIS im schulischen Alltag ankommt, um so wichtiger ist es zudem, dass das System verlässlich verfügbar ist, auch wenn ein Land mal im Schneesturm versinkt und großflächig digitales Lernen notwendig wird.

Gleichzeitig wollen wir ein Ökosystem bereitstellen, welches es für die Bildungsmedienanbieter attraktiv macht, Inhalte über das AIS bereitzustellen. Neben der Gewährleistung digitaler Souveränität ist es für uns auch wichtig, die Software nachnutzbar als Open Source zur Verfügung zu stellen. Dadurch gewährleisten wir zudem maximale Transparenz.



MAIBORNWOLFF



Herr Leinweber, als Teil des Konsortiums Assecor und KI macht Schule verantwortet MaibornWolff die Cloud- und Plattform-Infrastruktur für das AIS. Die Lünendonk-Studie attestiert europäischen Cloud-Providern noch einen mittelmäßigen Reifegrad. Auf welchen Cloud-Provider setzt Ihr Konzept? Wie bewerten Sie souveräne Angebote der großen Hyperscaler in Bezug auf AIS?

Christian Leinweber: Wir setzen bei AIS auf STACKIT als Cloud-Provider. Diese Partnerschaft hat sich für uns als wertvoll erwiesen. Natürlich bewegen wir uns in einem dynamischen Marktumfeld, in dem europäische Cloud-Provider ihre Leistungsfähigkeit kontinuierlich ausbauen. Wir haben uns aber bewusst für diesen Weg entschieden, weil er mehrere wichtige Aspekte vereint: Die Entscheidung für einen deutschen, souveränen Provider findet bei den Ländern eine sehr hohe Akzeptanz. Es gibt bereits länderübergreifende Initiativen wie PCI.SCHULE, die eine einheitliche Bildungsinfrastruktur anstrebt und bereits erste Projekte mit STACKIT aufgesetzt hat. Darüber hinaus schätzen wir die konstruktive und engagierte Zusammenarbeit mit STACKIT – wir haben ein gemeinsames Interesse daran, innovative Projekte wie AIS erfolgreich zu gestalten.

Zu den souveränen Cloud-Angeboten der großen Hyperscaler: Wir halten uns verschiedene Optionen offen. Multi-Cloud-Fähigkeit wird zunehmend wichtiger, und es kann Szenarien geben, in denen wir spezifische Service-Leistungen nutzen. Vor allem, weil wir in erster Linie, wo immer mög-

lich auf PaaS-Services setzen. Unser Grundansatz bleibt jedoch auf europäische, regionale Strukturen ausgerichtet. Das entspricht den Erwartungen unserer Auftraggeber – von den Datenschutzbehörden über die Länder bis zu den Schulträgern – und schafft eine Vertrauensbasis für technische Innovationen.

Open Source gewinnt auch im öffentlichen Sektor zunehmend an Bedeutung. Welche Rolle spielt Open Source bei AIS aus technischer Perspektive?

Christian Leinweber: Das AIS wird vollständig auf Basis von Open Source entwickelt. Aber Open Source spielt im Projekt auf mehreren Ebenen eine zentrale Rolle. Wir setzen auf etablierte Open-Source-Technologien wie Kubernetes und eine Vielzahl anderer Tools aus dem CNCF-Umfeld, weil sie uns breite Unterstützung und eine lebendige Community bieten. Diese Communities treiben technologische Innovationen oft mit bemerkenswerter Geschwindigkeit voran. Interessanterweise haben auch die großen Cloud Provider dies erkannt und tragen aktiv zu diesen Open-Source-Projekten bei – ein offensichtliches Signal für die Bedeutung und Qualität dieser Technologien.

Ich bin überzeugt davon, dass Open Source ein wesentlicher Baustein digitaler Unabhängigkeit ist. Wir vermeiden damit strukturelle Abhängigkeiten von einzelnen Anbietern, ohne dabei auf professionelle Platform-as-a-Service-Angebote verzichten zu müssen. Diese Kombination – technologische Offenheit bei gleichzeitig professionellem Betrieb – ist für uns der optimale Weg.

Eine KI-gestützte Lernumgebung bringt besondere Anforderungen mit sich. Welche Herausforderungen ergeben sich daraus, wenn man eine KI-gestützte Lernumgebung für den Schulkontext konzipiert, in dem sensible Daten von Kindern und Jugendlichen verarbeitet werden?

Dr. Jan Renz: Zunächst ist es wichtig, dass wir an AIS technologieneutral herangegangen sind. Bei der Konzeption war uns klar, welche pädagogisch-didaktischen Ziele wir erreichen wollen. Es hat sich gezeigt, dass KI ein gutes Werkzeug im digitalen Werkzeugkoffer ist. Während es bei der Cloud-Infrastruktur durch den Einsatz von Open-Source-Technologien wie Kubernetes gut möglich ist, eine herstel-

lerunabhängige Betriebsinfrastruktur mit vergleichbarer Qualität zu betreiben, stellen sich beim KI-Einsatz wichtige Herausforderungen: Zum einen muss gewährleistet sein, dass auch beim Einsatz von KI und LLMs die Daten nicht an andere Anbieter abfließen. Auch muss ausgeschlossen sein, dass die Daten durch die Anbieter zum Training verwendet werden. Im Idealfall werden Sprachmodelle verwendet, bei denen nicht nur das eigentliche Modell und die Gewichte offen sind, sondern auch die verwendeten Trainingsdaten. Noch führen solche Anforderungen zu schlechteren Ergebnissen – dieses Spannungsverhältnis müssen wir genau im Blick behalten.

"Ich bin überzeugt davon, dass Open Source ein wesentlicher Baustein digitaler Unabhängigkeit ist."



**Christian Leinweber
MaibornWolff**

Welche technischen Datenschutzmaßnahmen haben Sie für minderjährige Nutzer implementiert?

Christian Leinweber: Datenschutz ist bei AIS von Anfang an integraler Bestandteil der Architektur. Das beginnt bereits beim Zugang – hier setzen wir auf VIDIS. Dabei handelt es sich um ein föderales Identitätsmanagement für Schulen, das von der FWU entwickelt wurde und eine datenschutzkonforme Authentifizierung ermöglicht, ohne dass personenbezogene Daten unnötig erhoben oder verarbeitet werden müssen.

Auf technischer Ebene arbeiten wir mit mehreren komplementären Ansätzen: Zunächst nutzen wir konsequent Pseudonymisierung und Anonymisierung von Daten. Personenbeziehbare Informationen, werden in speziellen, PII-Vaults getrennt von den Anwendungsdaten gespeichert. Datenschutzrelevante Anfragen werden in Form von Audit-Logs in einem WORM-Storage (Write Once, Read Many) gespeichert, und jede Art von Interaktion mit personenbezogenen Daten wird über Role-Based Access Control gesteuert. Natürlich sind das auch technische Anforderungen an den Cloud Provider, wenn man in der Cloud eine souveräne Umgebung schaffen möchte.

Herr Renz, Sie sind über Ausschüsse in Aktivitäten der Länder eingebunden, unter anderem im Projekt PCI-Schule zum Aufbau von Cloud-Infrastrukturen für den Bildungssektor. Wie fügt sich AIS in diese übergreifenden Initiativen ein? Wo sehen Sie Synergien und wo möglicherweise auch Spannungsfelder zwischen föderalen Landeslösungen und einem bundesweiten Projekt?

Dr. Jan Renz: Als Informatiker und Ingenieur ist es für mich naheliegend, Redundanzen zu vermeiden und Komplexität zu reduzieren oder zu verteilen. Das Projekt PCI hat sich zum Ziel gesetzt, pädagogische Anwendungen einen sicheren und skalierbaren Betrieb in der Cloud zu ermöglichen. Obwohl wir in der FWU schon länger unsere Anwendungen „cloud native“ umsetzen und betreiben, begrüße ich daher Projekte wie PCI.

Neben der Vereinfachung der Beschaffung von Cloud-Ressourcen und begleitenden betriebsunterstützenden Tätigkeiten wird hier erstmalig landesübergreifend diskutiert und definiert, welche Mindestkriterien für Hyperscaler gelten. Außerdem werden Betriebsumgebungen standardisiert und gehärtet sowie in Abstimmung mit den Landesdatenschützern dokumentiert. So kann man sich, so die Idee, bei der Bereitstellung von digitalen Lern- und Lehranwendungen zukünftig auf die anwendungsspezifischen Aspekte konzentrieren und erleichtert den Aufsichtsbehörden die Arbeit. Gleichzeitig wird eine Interoperabilität der angebotenen Dienste angestrebt, so dass Multi-Cloud-Szenarien, mindestens aber eine Vermeidung von Vendor-Lock-in ermöglicht werden.

Ich beobachte, dass die Länder – unter anderem durch die länderübergreifenden Vorhaben im Rahmen des Digitalpakts Schule – gelernt haben, dass sich die Umsetzung landesspezifischer Zielbilder und die Nutzung technisch-infrastruktureller Synergien nicht gegenseitig ausschließen. Anders als beim Einer-für-Alle-Ansatz des Onlinezugangsgesetz wird hier eher auf ein gemeinsames Vorgehen gesetzt, das unter anderem durch ländereigene Institute wie das FWU ermöglicht wird.

Bei unseren bundesweiten Projekten – oder ländergemeinsamen Projekten wie ich sie lieber nenne – bleiben die Länder übrigens stets im Fahrersitz und entschieden über konkrete landesspezifische Ausgestaltungen. Das kann man gut am Beispiel der im AIS-Projekt angebotenen KI-Chatbot-Lösung sehen: Hier bieten wir eine Vielzahl von LLMs an. Manche Länder aktivieren dann OpenAI-Modelle aus einem europäischen Azure-Rechenzentrum, andere setzen ausschließlich auf offene Modelle.

Deutschland ist im Bildungsbereich föderal organisiert. Wie lässt sich eine Cloud-Infrastruktur gestalten, die wiederverwendbar und skalierbar ist, ohne die Autonomie der Länder zu beschneiden?

Christian Leinweber: Der Föderalismus ist aus technischer Sicht eine Anforderung an intelligentes Design. Unser System ermöglicht Flexibilität: Mandanten-Instanzen können in verteilten Rechenzentren betrieben werden, wenn ein Land dies benötigt. Unser Ziel ist es aber, eine gemeinsame Basis zu schaffen, bei der die Vorteile so deutlich überwiegen, dass es für die einzelnen Länder attraktiv ist, gemeinsam voranzugehen. Dabei orientieren wir uns eng an Initiativen wie PCI. Wir verstehen AIS als Beitrag zu einer gemeinsamen Cloud-Plattform für den Bildungssektor, auf der weitere Projekte aufsetzen können.

„Ich beobachte, dass die Länder gelernt haben, dass sich die Umsetzung landesspezifischer Zielbilder und die Nutzung technisch-infrastruktureller Synergien nicht gegenseitig ausschließen.“

”

**Dr. Jan Renz
FWU**

Technisch bedeutet das: offene APIs, etablierte Standards, keine Silos. AIS wird eine Plattform für Bildungsinhalte und Medienanbieter, wo Querschnittsthemen wie Authentifizierung oder Datenschutz zentral bereitgestellt werden – so können sich Länder und Entwickler auf pädagogische Innovationen konzentrieren.

Wenn Sie den Blick über die technische Umsetzung hinaus weiten: Auf welchen Ebenen kann AIS konkret zum Thema digitale Souveränität im Bildungssektor beitragen? Welches Signal sendet ein solches Projekt – an Schulen, an Länder, an andere Bildungsakteure?

Dr. Jan Renz: AIS passt sich gut in das Zielbild der ländergemeinsamen Bildungsmedieninfrastruktur (BMI) ein. Die BMI soll Schulen einen einfachen, effizienten und rechtssicheren Einsatz von digitalen Bildungsmedien ermöglichen und allen Anbietern von Bildungsmedien in unserem föderalen System offenstehen: von Lehrkräften, die offene Bildungsinhalte erstellen, über junge EdTech-Unternehmen bis hin zu großen Verlagen. Dabei sind wir fest überzeugt, dass die rechtlichen und strategischen Anforderungen ohne Kompromisse erfüllt werden können und trotzdem gute Produkte im Klassenzimmer ankommen.

AIS geht nun einen Schritt weiter, indem es nicht nur einen datensparsamen Zugang ermöglicht (wie bei VIDIS) oder Transparenz über die rechtssichere Ausgestaltung eines Angebots schafft (wie bei eduCheck Digital), sondern auch eine Infrastruktur bereitstellt, in der verschiedene Inhalteanbieter nutzerzentriert zusammenkommen. Diese müssen nun keinen großen Aufwand für die Infrastruktur betreiben, sondern können mithilfe der in AIS bereitgestellten Funktionen ihren Fokus auf die Erstellung und Bereitstellung innovativer und wirksamer Inhalte legen.

Von der Abhängigkeit zur Handlungsfähigkeit: Der Weg zur digitalen Souveränität

Digitale Souveränität ist längst kein politisches Schlagwort mehr, sondern entwickelt sich für Unternehmen und Behörden zur strategischen Überlebensfrage. Timon Schmotz von Materna zeigt im Interview, wie geopolitische Unsicherheiten, strenge Regulierung und der Wunsch nach technologischer Unabhängigkeit neue Maßstäbe für Cloud-Architekturen, KI-Einsatz und Sicherheitsstrategien setzen. Er macht deutlich, wo heute die größten blinden Flecken liegen – von intransparenten Service-Ketten bis hin zu proprietären Lock-ins – und warum echte Souveränität nur durch klare Kontrolle über Daten, Betreiberstrukturen und Prozesse entsteht.



Timon Schmotz
Business Development Manager
Materna

Viele Unternehmen sehen digitale Souveränität zunehmend als geschäftskritische Fähigkeit. Was ist aus Ihrer Sicht der wichtigste Treiber: geopolitische Unsicherheiten, regulatorischer Druck oder der Wunsch nach mehr technologischer Gestaltungsfreiheit?

Timon Schmotz: Aus unserer Arbeit mit Kunden sehen wir, dass sich alle drei Treiber gegenseitig verstärken. Im öffentlichen Sektor ist der regulatorische Druck zweifellos der dominierende Faktor, denn hier müssen Vorgaben zu Datenschutz, Datenlokalisierung, IT-Sicherheit und Compliance zwingend eingehalten werden. Gleichzeitig wirken geopolitische Unsicherheiten als Katalysator, weil extraterritoriale Gesetze oder politische Spannungen Abhängigkeiten von globalen IT-Anbietern plötzlich zu strategischen Risiken machen können. In Industrien wie Automotive, Manufacturing oder Finance erleben wir häufiger, dass der Wunsch nach technologischer Gestaltungsfreiheit im Vordergrund steht – etwa um Innovation selbstbestimmt zu steuern oder proprietäre Lock-ins zu vermeiden. Übergreifend zeigt sich jedoch: Digitale Souveränität ist heute ein strategisches Thema der Resilienz und Zukunftsfähigkeit, nicht nur ein technisches oder politisches.

Digitale Souveränität bedeutet im ersten Schritt, bestehende Abhängigkeiten sichtbar zu machen. Wo erleben Sie heute die größten „Blind Spots“ in IT-Architekturen und Service-Beziehungen?

Timon Schmotz: Die größten blinden Flecken entstehen dort, wo Transparenz über Herkunft, Kontrolle und Betriebswege digitaler Dienste fehlt. Viele Organisationen verfügen nicht über eine vollständige Sicht darauf, welche Unterauftragnehmer in ihren Service-Ketten beteiligt sind, welche Softwarekomponenten tatsächlich eingesetzt werden

MATERNA

oder wie Daten zwischen Systemen fließen. Besonders im Public Sector stoßen wir häufig auf unklare Betreiberstrukturen bei Cloud-Diensten, in denen Verantwortlichkeiten schwer zuzuordnen sind. Hinzu kommt, dass ein großer Teil der bestehenden IT-Landschaften auf proprietären Anwendungen basiert, deren Funktionsweise und Risiken mangels Quellcode-Transparenz nur eingeschränkt nachvollziehbar sind. Diese Kombination aus technischer Komplexität und fehlender Einsicht ist einer der zentralen Gründe, warum viele Organisationen ihren Abhängigkeitsgrad unterschätzen.

"Digitale Souveränität ist heute ein strategisches Thema der Resilienz und Zukunftsfähigkeit, nicht nur ein technisches oder politisches."



Timon Schmotz
Materna

Die Cloud bleibt der zentrale Baustein moderner IT-Landschaften. Wie verändern souveräne Cloud-Modelle Ihrer Beobachtung nach die Architektur- und Sourcing-Entscheidungen von Unternehmen und Behörden?

Timon Schmotz: Wir beobachten eine deutliche Verschiebung hin zu differenzierten, mehrstufigen Cloud-Strategien. Statt einer generischen Cloud-First-Logik entscheiden Kunden heute viel stärker anhand der Kritikalität ihrer Daten, wo und wie Workloads betrieben werden sollen. Sensible oder besonders schützenswerte Informationen werden zunehmend in souveräne Betriebsmodelle überführt,

die entweder von europäischen beziehungsweise deutschen Anbietern stammen oder in speziellen Hyperscaler-Modellen mit EU-Betreiberstrukturen realisiert werden. Gleichzeitig behalten Standard-Public-Clouds eine wichtige Rolle, jedoch meist ergänzt durch zusätzliche Sicherheits- und Kontrollmechanismen. Multi-Cloud-Architekturen werden zur Normalität, und Exit-Fähigkeit entwickelt sich zu einer Grundanforderung im Sourcing. Dadurch entstehen hybride, hochsegmentierte Architekturen, die regulatorische Sicherheit und technologische Innovationsfähigkeit miteinander verbinden sollen.

Viele Anbieter positionieren sich mit „souveränen“ Lösungen. Wie unterscheiden Sie echte Souveränitätsmerkmale von Marketingversprechen, und welche Kriterien sollten Unternehmen dafür heranziehen?

Timon Schmotz: Der zentrale Maßstab ist immer die tatsächliche Kontrolle über Daten, Prozesse und Betreiberstrukturen. Eine souveräne Lösung zeichnet sich dadurch aus, dass klar erkennbar ist, welchem Rechtsraum sie unterliegt, welche Organisation letztlich Betreiber ist und welche technischen Mechanismen dem Kunden die tatsächliche Hoheit über seine Daten geben. Dazu gehören eigene Schlüsselhoheit, transparente Rollen- und Berechtigungskonzepte, Auditierbarkeit aller Betriebsprozesse und eine nachvollziehbare Exit-Strategie. Wenn Anbieter hingegen vor allem mit geografischen Hosting-Standorten argumentieren oder Souveränität als reine „Label-Eigenschaft“ verwenden, ohne diese Kontrollpunkte abzubilden, handelt es sich eher um Marketing. Unternehmen sollten daher konsequent nachweisen lassen, wie sich Betreiberstrukturen, Verantwortlichkeiten und technische Kontrollen tatsächlich darstellen.

Mit Blick auf AI-Plattformen, generative Modelle und Datenräume entstehen völlig neue Abhängigkeiten. Wie müssen Unternehmen ihre Souveränitätsstrategie anpassen, wenn KI künftig tief in Kernprozesse eingreift?

Timon Schmotz: Sobald KI ein integraler Bestandteil der Wertschöpfung wird, verschiebt sich auch die Diskussion über Souveränität. Die eigentlichen Abhängigkeiten entstehen dann weniger bei Infrastruktur-Themen, sondern bei Modellen, Trainingsdaten, Update-Mechanismen und dem

Zugriff auf spezialisierte Hardware. Unternehmen sollten ihre Strategien daher um den Aspekt der KI-Souveränität erweitern. Dazu gehört, Modelle und Datenflüsse klar zu kontrollieren, Trainingsprozesse transparent zu gestalten, europäische oder offene Modelle als Alternative zu prüfen und Governance-Strukturen zu etablieren, die den Umgang mit KI-Risiken nachvollziehbar regeln. Besonders Behörden verlangen zunehmend KI-Lösungen, die auditierbar, rechtskonform und sicher betreibbar sind – und zwar auch dann, wenn die Technologie selbst hochdynamisch ist. Wer diese Perspektive früh berücksichtigt, reduziert langfristige Abhängigkeiten und sichert seine Handlungsfähigkeit.

Wenn Sie auf Ihre Kunden blicken: Woran erkennt man, dass ein Unternehmen tatsächlich souveräner werden möchte – und nicht nur das Vokabular der politischen Debatte übernimmt?

Timon Schmotz: Man erkennt es daran, dass aus der Diskussion echte Maßnahmen werden. Organisationen, die souveräner werden wollen, definieren Verantwortlichkeiten, schaffen Governance-Strukturen, klassifizieren ihre Daten systematisch und führen Risikoanalysen für ihre Cloud- und Softwarelieferketten durch. Sie investieren in Transparenz über ihre Architekturen, schärfen ihre Sicherheitsmechanismen und etablieren Prozesse, die einen Anbieterwechsel tatsächlich möglich machen.

Unternehmen, die hingegen nur den Begriff in strategische Dokumente aufnehmen, jedoch weder Architekturen anpassen noch Budgets bereitstellen, sind meist eher im diskursiven als im operativen Modus. Souveränität zeigt sich daher nicht im Wording, sondern in der Konsequenz technischer und organisatorischer Entscheidungen.

„Organisationen, die souveräner werden wollen, definieren Verantwortlichkeiten, schaffen Governance-Strukturen, klassifizieren ihre Daten systematisch und führen Risikoanalysen für ihre Cloud- und Softwarelieferketten durch.“

”

Timon Schmotz
Materna

Was bedeuten all diese Entwicklungen für Materna? Was erwarten Ihre Kunden von Ihnen, um souveräne IT-Ökosysteme erfolgreich aufzubauen und zu betreiben?

Timon Schmotz: Für Materna bedeutet dies eine deutliche Erweiterung unserer Rolle. Wir werden zunehmend als vertrauenswürdiger Partner gesucht, der technologische Expertise, regulatorisches Verständnis und architektonische Weitsicht miteinander verbindet. Unsere Kunden erwarten, dass wir sie ganzheitlich begleiten – von der Entwicklung einer souveränen Cloud- und Datenarchitektur über die Umsetzung von Governance-Modellen bis hin zu Sicherheit, Data-Management, KI-Strategien und Open-Source-Integration. Dabei geht es nicht nur um technische Implementierung, sondern immer häufiger auch um die Befähigung der Organisation selbst. Viele Kundinnen und Kunden möchten langfristig unabhängiger werden und benötigen Partner, die ihnen helfen, diese Eigenständigkeit strukturiert aufzubauen. Genau hier sehen wir unseren Auftrag: Souveränität nicht nur technisch, sondern auch organisatorisch zu ermöglichen.

Wenn wir drei Jahre vorspulen: Wie wird sich digitale Souveränität aus Ihrer Sicht weiterentwickeln? Welche Fortschritte erwarten Sie – und welche Herausforderungen werden Unternehmen und Behörden weiterhin begleiten?

Timon Schmotz: Digitale Souveränität wird deutlich stärker verankert sein – sowohl in Vergaben und regulatorischen Anforderungen als auch in Architekturentscheidungen. Souveräne Cloud-Modelle werden gereifter und funktional umfassender sein. Europäische Anbieter werden an Bedeutung gewinnen, auch wenn die Hyperscaler in vielen technologischen Segmenten weiterhin führend bleiben. Gleichzeitig wird der Bedarf an Nachweisen und Zertifizierungen steigen: Stakeholder möchten zunehmend sehen, wie Organisationen Souveränität tatsächlich umsetzen. Die größte Herausforderung wird allerdings in der Komplexität hybrider Architekturen liegen. Unternehmen und Behörden müssen lernen, regulatorische Sicherheit, Innovationsgeschwindigkeit und wirtschaftliche Effizienz miteinander auszubalancieren. Wer hier früh auf transparente und robuste Architekturen setzt, wird langfristig klar im Vorteil sein – und genau das ist die Entwicklung, die wir in den kommenden Jahren erwarten.

Lünendonk im Interview mit msg

Zwischen Wunsch und Wirklichkeit: Wie Unternehmen souveräne Cloud-Angebote bewerten

Kaum ein IT Thema sorgt aktuell für so viel Bewegung wie die Frage, wie digital souverän Unternehmen wirklich sind. Karl Lassak ist Principal Consultant bei msg und Experte für das Thema digitale Souveränität. Im Interview mit Lünendonk ordnet er ein, wie Unternehmen die neuen souveränen Hyperscaler-Angebote bewerten, warum die Nutzungsbereitschaft trotz hoher Erwartungen differenziert ausfällt und welche Rolle kombinierte Ansätze künftig spielen werden.



Karl Lassak
Principal Consultant
msg

Das Thema digitale Souveränität wird in Politik und Wirtschaft seit einigen Monaten intensiv diskutiert. Wie blicken Sie auf diese Gemengelage und wo stehen deutsche Unternehmen?

Karl Lassak: Wir beobachten aktuell eine starke Dynamik rund um das Thema digitale Souveränität. Während politisch häufig die Frage im Vordergrund steht, wie Europa technologische Unabhängigkeit erreicht, suchen CIOs ganz pragmatisch nach Maßnahmen, die sie kurz- bis mittelfristig umsetzen können.

Die zentrale Frage dabei ist, ob Unternehmen ihre kritischen Prozesse, Datenflüsse und Kernsysteme auch in Krisensituationen kontrollieren können. Viele IT-Verantwortliche sehen dabei sehr klar die Notwendigkeit, Abhängigkeiten in der IT-Lieferkette zu reduzieren, ohne gleich vollständige technologische Autarkie anzustreben. Es geht also primär darum, Risiken bewusst zu managen, Alternativen zu schaffen und die eigenen Kernkompetenzen gezielt auszubauen.

Deutsche Unternehmen sind wach, sensibilisiert und auf dem Weg, Souveränität nicht als politischen Leitsatz, sondern als konkreten Gestaltungsauftrag für die eigene IT zu verstehen.

Im Zuge der Souveränitätsdebatte werden die Hyperscaler, also AWS, Microsoft Azure und Google Cloud Platform, die mit ausgereiften und fortschrittlichen Cloud-Services sowie globaler Präsenz punkten, kritischer betrachtet. Nehmen Sie wahr, dass Unternehmen ihre Zusammenarbeit mit den Hyperscalern auf den Prüfstand stellen?



Karl Lassak: Die Zahlen sprechen hier eine deutliche Sprache: Laut der Studie arbeiten rund 90 Prozent der befragten Unternehmen bereits heute mit mindestens einem Hyperscaler zusammen. Die Hyperscaler sind technisch überlegen, bieten globale Skalierbarkeit und ermöglichen Innovationsgeschwindigkeit, die On-Premises-Modelle allein kaum liefern könnten. Dieses Fundament stellt niemand ernsthaft infrage.

"Hyperscaler bleiben ein zentraler Bestandteil der Strategie, doch ihre Rolle wird stärker in ein Gesamtkonzept eingebettet, das Kontrolle, Flexibilität und Risikoreduktion verbindet."



Karl Lassak
msg

Was sich jedoch verändert, ist die strategische Perspektive auf Abhängigkeiten. Wir nehmen hier keine generelle Abkehr von Hyperscalern wahr, sondern eher eine neue Form der reflektierten Nutzung. Hyperscaler bleiben also ein zentraler Bestandteil der Strategie, doch ihre Rolle wird stärker in ein Gesamtkonzept eingebettet, das Kontrolle, Flexibilität und Risikoreduktion verbindet.

Wir beobachten daher, dass auch Multi-Cloud-Strategien massiv an Bedeutung gewinnen. Das zeigt auch die Studie: Bereits 42 Prozent der Unternehmen haben Multi-Cloud-Architekturen umgesetzt, weitere 46 Prozent planen diese aktiv. Das ist ein sehr deutliches Signal dafür, dass Abhängigkeiten gezielt reduziert werden sollen – nicht aus reinem Misstrauen, sondern vielmehr mit der Absicht eines professionellen Risikomanagements.

Als eine Antwort auf die Debatte reagieren die Hyperscaler mit neuen souveränen Angeboten. Im Januar 2026 hat die AWS European Sovereign Cloud (AWS ESC) den Betrieb aufgenommen – msg ist Launch Partner. Auch Microsoft und Google treiben Initiativen voran. Wie bli- cken Sie auf diese Entwicklung – welche Relevanz haben die neuen Hyperscaler-Angebote?

Karl Lassak: Die souveränen Angebote der Hyperscaler, wie die neue AWS European Sovereign Cloud oder die Initiativen von Microsoft und Google, sind ein wichtiger Schritt, weil sie Compliance Anforderungen, Datenlokalität und operative Kontrolle besser adressieren. Gleichzeitig zeigen die Studienergebnisse sehr klar ihre Grenzen. 96 Prozent der Unternehmen wissen, dass diese Angebote zwar Compliance unterstützen, aber keine Unabhängigkeit vom Anbieter schaffen. Und 93 Prozent sind sich bewusst, dass trotz europäischer Rechenzentren weiterhin US Recht wie der CLOUD Act gilt.

Das heißt, die souveränen Hyperscaler Clouds sind relevant und werden stark nachgefragt. Sie lösen jedoch das Grundproblem der Abhängigkeit nicht. Unternehmen sehen sie deshalb als wertvollen Baustein, der immer im Rahmen einer breiteren Souveränitätsstrategie kombiniert wird, zum Beispiel durch Multi-Cloud-Strategien, lokale Provider und eigene Kompetenzen.

Es ist immer wieder zu hören, dass es sich dabei um „Souveränitäts-Washing“ handelt. Wie ordnen Sie das ein?

Karl Lassak: Der Begriff „Souveränitäts Washing“ adressiert einen Punkt, der für einige Anbieter durchaus zutreffen kann. In bestimmten Fällen wird von souveräner IT gesprochen, obwohl zentrale Abhängigkeiten, wie etwa von speziellen Technologien, proprietären Plattformen oder außer-

europäischen Rechtsräumen, weiter bestehen. In solchen Konstellationen wird Souveränität eher als kommunikatives Label genutzt, denn als tragfähiges, klar definiertes Zielbild. Entscheidend ist deshalb, genau hinzuschauen, welche Anbieter echte strukturelle Veränderungen vornehmen und wo Souveränität primär als Marketingbotschaft eingesetzt wird.

Viele Unternehmen gehen aber bereits sehr bewusst mit dem Thema um und wissen, dass vollständige digitale Souveränität kurzfristig kaum erreichbar ist. Stattdessen werden pragmatische Zwischenlösungen gewählt, die Risiken reduzieren, ohne bestehende Plattformen komplett aufzugeben.

Entscheidend ist daher weniger das Label „souverän“, sondern die Transparenz: Welche Abhängigkeiten bestehen weiterhin, welche Kontroll- und Ausweichmöglichkeiten gibt es und in welchen Bereichen wird Souveränität tatsächlich erhöht? Dort, wo diese Fragen ehrlich beantwortet werden, ist es kein „Washing“, sondern ein realistischer Umgang mit Zielkonflikten.

„Viele Unternehmen suchen Alternativen, die stärker auf Souveränität, lokale Kontrolle und europäische Rechtsrahmen ausgerichtet sind.“



Karl Lassak
msg

Der Gegenpol zu den Hyperscalern sind deutsche und europäische Cloud-Provider. Wie die Studie zeigt, setzen Unternehmen auf die Anbieter große Hoffnungen, wenn- gleich Wunsch und Realität noch weit auseinanderklaffen. Wie bewerten Sie die Initiativen der hiesigen Cloud-Provider? Und werden diese zunehmend nachgefragt?

Karl Lassak: Die Erwartungen an deutsche und europäische Cloud-Provider sind hoch und das völlig zu Recht. Viele Unternehmen suchen Alternativen, die stärker auf Souveränität, lokale Kontrolle und europäische Rechtsrahmen ausgerichtet sind. Die Studie zeigt jedoch ein sehr differenziertes Bild zwischen Wunsch und tatsächlicher Realität. Am stärksten nachgefragt werden derzeit souveräne Cloud-Angebote der Hyperscaler in Kombination mit lokalen EU-Betreibern sowie deutsch ansässige IT-Dienstleister

für Rechenzentren, Colocation und Managed Infrastructure. Das zeigt: Unternehmen vertrauen auf etablierte Betriebsmodelle, klare Verantwortlichkeiten und die Kombination aus globaler Technologie und lokaler Kontrolle. Deutsche Cloud-Provider liegen mit 48 Prozent ebenfalls weit vorn und können zukünftig eine zunehmend wichtige Rolle spielen. Fest steht, dass europäische Clouds sich in einer aktiven Weiterentwicklungsphase befinden. Prozesse, Self Service Funktionen oder Plattform Ökosysteme sind noch nicht durchgängig auf demselben Niveau wie bei Hyperscalern. Unternehmen bewerten dies pragmatisch: Für kritische Datenströme akzeptieren sie dies teilweise, für skalierende Anwendungen jedoch weniger.

Zum Abschluss: Was raten Sie IT-Verantwortlichen, welche eine Standortbestimmung vornehmen möchten, wie ihr Reifegrad an digitaler Souveränität ist und an welchen Stellen sie ansetzen können?

Karl Lassak: Für IT-Verantwortliche, die ihren Reifegrad an digitaler Souveränität bestimmen möchten, empfehlen wir einen strukturierten, aber pragmatischen Ansatz. Viele Unternehmen wissen genau, dass sie Handlungsbedarf haben.

Der erste Schritt ist eine Standortbestimmung entlang der zentralen Souveränitätsdimensionen: Betriebliche Souveränität, Datensouveränität, technologische Souveränität und vertragliche beziehungsweise juristische Souveränität. Es gilt Fragen zu klären, die zeigen, wie abhängig kritische Prozesse, Systeme und Lieferketten von einzelnen Anbietern sind, wo sensible Daten liegen und ob das eigene Team die Schlüsseltechnologien noch selbst beherrscht. Auf dieser Basis lassen sich dann konkrete Maßnahmen identifizieren.

Zudem können etablierte Standards hilfreiche Orientierung bieten: ISO 27001 schafft beispielsweise einen klaren Rahmen für Informationssicherheitsmanagement und unterstützt Unternehmen dabei, Governance Strukturen, Kontrollmechanismen und Verantwortlichkeiten systematisch aufzubauen. Der Digital Operational Resilience Act – kurz DORA – adressiert wiederum speziell die digitale Betriebsstabilität im Finanzsektor, bietet aber auch für andere Branchen wertvolle Leitplanken, um Abhängigkeiten von Drittanbietern, Auslagerungsrisiken und Resilienzanforderungen strukturiert zu bewerten.

Letztlich ist digitale Souveränität kein „Alles oder Nichts“-Projekt. Unternehmen sollten sich auf die Bereiche konzentrieren, in denen Souveränität unmittelbar geschäftskritisch ist und dort zuerst handeln.

Wer die Daten kontrolliert, gewinnt – Souveränität als Zukunftswährung

Digitale Souveränität ist längst zur strategischen Überlebensfrage geworden und erfordert klare Entscheidungen darüber, wer die Kontrolle über Daten, Systeme und KI-Modelle behält. Peter Jung, CEO der TechniData IT AG, erläutert, wie Unternehmen sich aus Abhängigkeiten lösen, ohne Innovationskraft einzubüßen, und warum hybride IT-Modelle zum neuen Standard werden. Er macht deutlich: Souveränität bedeutet heute nicht Abschottung, sondern professionelle Governance, transparente Partner und die konsequente Sicherung von Wechsel- und Handlungsfähigkeit.



Peter Jung
CEO
TechniData

Herr Jung, die TechniData IT-Gruppe ist ein deutscher IT-Service- und -Solution-Provider. Was bedeutet digitale Souveränität für Sie und welche Rolle nimmt TechniData dabei ein?

Peter Jung: Digitale Souveränität heißt für mich, bewusst zu entscheiden, welche Technologien wir einsetzen, wo unsere Daten liegen, wer im Ernstfall darauf zugreifen darf und unter welchen rechtlichen Rahmenbedingungen das geschieht. Es geht um Wettbewerbsfähigkeit, um Resilienz und Regulierung. Wer die Hoheit über Daten und Systeme verliert, verliert langfristig seinen Handlungsspielraum.

Wir sehen TechniData in der Rolle des Architekten und Sparringspartners. Wir bauen und betreiben IT-Infrastrukturen, organisatorisch, prozess- und sicherheitstechnisch. Ob in unserem, mit Blauem Engel und ISO 27000 zertifizierten Rechenzentrum am deutschen Standort, im lokalen Rechenzentrum des Kunden oder in der Cloud. Entscheidend ist, dass die Lösungen für den Kunden passend sind und nachhaltig seine digitale Souveränität stärken. Am Ende sollen unsere Kunden sagen können: Wir wissen was wir tun und wir behalten die Kontrolle..

Zu Ihren Kunden zählen Konzerne wie auch der Mittelstand. Welche Besonderheiten zeigt aus ihrer Sicht der Mittelstand im Vergleich zu Konzernen in Sachen Souveränität?

Peter Jung: In Bezug auf die Anforderungen sehen wir kaum Unterschiede zwischen Konzernen, Mittelstand oder öffentlicher Verwaltung. Die Ziele sind weitgehend identisch: unabhängig werden, Risiken beherrschen, Innovation ermöglichen.

Oft sind die Wege dorthin aber unterschiedlich. Je internationaler ein Unternehmen agiert, umso komplexer sind die technischen, juristischen und regulatorischen Anforderungen. Für viele global tätige Unternehmen führt deshalb Stand heute kein Weg an den großen amerikanisch dominierten Hyperscalern vorbei. An diesem Zustand wird sich auch kurzfristig kaum etwas ändern.

Was sich aber generell verändert hat: das Bewusstsein für Abhängigkeiten wächst spürbar. Wer kontrolliert die Plattform? In welchem Rechtsraum bewegen wir uns? Der Mittelstand denkt heute strategischer als noch vor einigen Jahren.

Wir haben davon gesprochen, dass der Mittelstand auch weiterhin IT-Services in eigenen Rechenzentren betreibt. Einerseits sind externe Abhängigkeiten somit eher gering, gleichzeitig kämpft der Mittelstand mit der digitalen Transformation, dem Fachkräftemangel und einer globalen Wettbewerbssituation. Sind die zunehmenden Souveränitätsanforderungen nun ein Treiber dafür, die IT-Strategie zu überdenken und neue Wege zu gehen?

Peter Jung: Ganz klar: ja. Wir erleben gerade so etwas wie eine strategische Standortbestimmung. Viele Unternehmen fragen sich sehr nüchtern: Was können und wollen wir selbst betreiben? Wo überfordern wir uns personell oder technologisch?



Das eigene Rechenzentrum galt lange als Inbegriff von Kontrolle. Heute sehen wir: Security, Compliance und ein 24/7-Betrieb sind in Zeiten des Fachkräftemangels nur schwer wirtschaftlich abzubilden. Für viele Mittelständler ist es sinnvoller, auf zertifizierte Rechenzentren von lokalen Dienstleistern oder Managed Services zu setzen. Nicht als Kontrollverlust, sondern als bewusste Arbeitsteilung. Souveränität entsteht durch professionelle Sicherheits- und Betriebsstandards, nicht allein durch den Standort.

Hybride Modelle spielen dabei eine große Rolle. Kritische Systeme bleiben in einer souveränen Umgebung, andere Workloads laufen flexibel in der Cloud. Digitale Souveränität wird so zum Kompass: Was gehört strategisch ins eigene Haus? Was in ein Datacenter „Made in Germany“? Wo nutze ich bewusst internationale Plattformen? Diese Differenzierung schafft Stabilität und Machbarkeit, ohne Innovationskraft einzubüßen.

89 Prozent der Studienteilnehmer geben an, dass Datensouveränität eine sehr hohe Relevanz für Ihr Unternehmen hat. Hinterfragen Kunden heute stärker, wo ihre Daten liegen und wie sicher sie sind?

Peter Jung: Absolut! Die Frage nach dem Datenstandort ist kein reines IT-Thema mehr. Auch endet sie nicht bei der Geografie. Es geht um Zugriffsmöglichkeiten, um Rechtsräume, um Transparenz. Gesetze wie die DSGVO oder internationale Regelwerke wie der Cloud Act haben das Bewusstsein geschärft. Auch wenn viele Unternehmen über die europäischen Datenschutzregeln schimpfen, so wollen doch die allermeisten von diesen Regeln profitieren.

Unternehmen wollen wissen: Wer kann im Zweifel auf Daten zugreifen? Wie sind Zugriffe dokumentiert? Wie sehen Backup- und Recovery-Konzepte aus? Insbesondere im Gesundheitswesen, in der Industrie oder bei kritischen Infrastrukturen ist das existenziell. Dort geht es um Patientendaten, um geistiges Eigentum oder um Versorgungs- und Produktionsfähigkeit.

Datensouveränität bedeutet deshalb nicht Abschottung oder komplette Rückkehr zu On-Premises-Lösungen, sondern Professionalität und Lösungswillen.

Unternehmen suchen Partner, die transparent, zertifiziert und nachvollziehbar arbeiten. Datensouveränität ist kein Hemmschuh für Innovation, sie ist ihre Voraussetzung und schafft Mut für weitere Digitalisierungsschritte.

Ebenso zeigt die Studie auf, dass komplexe IT-Landschaften die Förderung von digitaler Souveränität stark beeinträchtigen, da historisch gewachsene Systeme nur mit großem Aufwand anpassbar sind und die Betriebsfähigkeit dadurch gefährdet wird. An welchen Stellen ist digitale Souveränität überhaupt sinnvoll und realisierbar?

Peter Jung: Tatsächlich ist die Ablösung von gewachsenen IT-Systemen, unabhängig vom Betriebsmodell, für alle Unternehmen eine riesige Herausforderung. Digitale Souveränität kann auch verloren gehen, wenn wir zu lange an Systemen oder Technologien festhalten, deren Support und Wartung immer schwieriger wird. Dies trifft besonders stark auf eigenentwickelte Systeme zu.

„Datensouveränität ist kein Hemmschuh für Innovation, sie ist ihre Voraussetzung.“



Peter Jung
TechniData

Solche Systeme bremsen nicht nur Transformation, sondern schaffen zudem Abhängigkeiten von Einzelpersonen oder spezialisiertem Know-how und gefährden damit langfristige Souveränität. Gleichzeitig haben sich Cloud-Lösungen vor allem im Bereich Collaboration und Arbeitsplatzsysteme in den vergangenen Jahren stärker durchgesetzt, weil sie skalierbar und effizient sind. Es muss daher immer eine bewusste Entscheidung sein, welche Systeme in die Cloud migriert werden und welche Systeme unbedingt lokal betrieben werden müssen. Die Zukunft liegt hier ganz klar in hybriden Systemlandschaften, die je nach Anforderung die Vorteile von Cloud und On-Premises sinnvoll kombinieren.

Kritische Workloads können im eigenen Rechenzentrum oder in einer souveränen Cloud betrieben werden, während weniger sensible Anwendungen in flexiblen, skalierbaren Public-Cloud-Umgebungen laufen.

Mit dem Vormarsch generativer KI verschieben sich Datenflüsse und Abhängigkeiten erneut. Wie verändert der Einsatz von KI aus Ihrer Sicht die Anforderungen an digitale Souveränität. Welche Leitplanken empfehlen Sie Unternehmen konkret, bevor sie sensible Prozesse oder Daten an KI-Plattformen koppeln?

Peter Jung: KI ist keine Entscheidung für oder gegen ein Toolset, sondern ein Technologiesprung, dessen Anfänge wir gerade erst erleben. Aber hier gelten im Grund die gleichen Fragen wie bei der Auslagerung von Daten an dritte Anbieter. Welche Daten dürfen das eigene Haus verlassen und welche nicht?

Generative KI schafft eine neue Qualität der Abhängigkeit. Dabei werden nicht nur Daten verarbeitet. Modelle, die mit Unternehmenswissen angereichert sind, erzeugen neue Inhalte und Entscheidungsgrundlagen. Damit entsteht eine zusätzliche Ebene der Souveränität: die Kontrolle über Wissensableitung und Modellverhalten.

In sensiblen Bereichen kann eine generative KI-Lösung in einer On-Premises-Architektur sinnvoll sein. In anderen Szenarien bieten Plattformlösungen enorme Innovationsgeschwindigkeit. Entscheidend ist, dass Architektur, Governance und Compliance sauber definiert sind. Dazu gehören eine verbindliche Prompt-Governance, die Protokollierung von Interaktionen sowie gezielte Schulungen für Mitarbeitende, um unbeabsichtigte Datenabflüsse zu vermeiden.

Letztendlich geht es auch bei KI darum, dass ein Unternehmen die Kontrolle über die genutzten Modelle, Datenquellen und Zugriffsrechte behält. Souveränität setzt voraus, Modelle oder Plattformen bei Bedarf wechseln zu können. Architekturentscheidungen sollten daher konsequent auf Portabilität und Exit-Fähigkeit ausgelegt sein.

Wenn ein Unternehmen digitale Souveränität ernsthaft angehen will: Wie sieht aus Ihrer Sicht ein professioneller Einstieg aus – von der Risikoanalyse bis zu einer tragfähigen Souveränitätsstrategie?

Peter Jung: Ein professioneller Einstieg beginnt immer mit einem Perspektivwechsel. Digitale Souveränität ist weit mehr als nur die Frage, wo Daten gespeichert werden. Es geht zuallererst um den aktiven Schutz der digitalen Identität eines Unternehmens, seiner Systeme und seiner gesamten Geschäftsprozesse.

Wir starten deshalb immer mit einer strukturierten Vorgehensweise. Wo werden sensible Daten verarbeitet? Welche Abhängigkeiten bestehen? Welche rechtlichen und technischen Risiken ergeben sich? Darauf aufbauend erfolgt eine Bestandsaufnahme der kompletten IT-Landschaft.

Auf dieser Basis entwickeln wir eine Sicherheitsarchitektur und bewerten den Reifegrad entlang von Infrastruktur, Applikationen, Daten und internem Know-how. Regulatorische Anforderungen wie DSGVO oder NIS-2 werden integriert. Die Datenhaltung und -verarbeitung sollte idealerweise im rechtssicheren EU-Raum erfolgen, vorzugsweise in einem zertifizierten deutschen Rechenzentrum.

"Digitale Souveränität ist weit mehr als nur die Frage, wo Daten gespeichert werden. Es geht zuallererst um den aktiven Schutz der digitalen Identität eines Unternehmens, seiner Systeme und seiner gesamten Geschäftsprozesse."



Peter Jung
TechniData

Daraus entsteht eine tragfähige Souveränitätsstrategie, mit definierten Zielen, priorisierten Handlungsfeldern und konkreten Projekten. Entscheidend ist jedoch: Digitale Souveränität ist kein einmaliges Projekt, sondern ein laufender Steuerungsprozess mit regelmäßigen Reviews. Genau deshalb gehört sie ins Board und nicht isoliert in die IT. Die Verantwortung sollte organisatorisch klar auf C-Level organisiert sein, denn sie beeinflusst unmittelbar Geschäftsmodell, Risikoprofil und Wettbewerbsfähigkeit. Wird sie so verstanden, wachsen unternehmerische Handlungsfähigkeit, Resilienz und Wettbewerbsvorteile.

adesso ist einer der führenden IT-Dienstleister im deutschsprachigen Raum und spezialisiert auf Beratung sowie individuelle Softwareentwicklung. Seit der Gründung 1997 in Dortmund verfolgt adesso das Ziel, Unternehmen und öffentliche Verwaltungen mit passgenauen IT-Lösungen zu unterstützen und die Wettbewerbsfähigkeit von Unternehmen zu stärken. Die Strategie des Unternehmens basiert auf drei Säulen: umfassendes Branchen-Know-how der Mitarbeitenden, herstellerneutrale Technologiekompetenz und erprobte Methoden bei der Umsetzung von Softwareprojekten. Mit über 11.000 Mitarbeitenden (FTE), was mehr als 11.800 Mitarbeitenden nach Köpfen entspricht und einem Jahresumsatz von rund 1,5 Milliarden Euro (2025) zählt adesso zu den größten deutschen IT-Dienstleistern. Die adesso-Aktie ist im Prime Standard/SDAX notiert.

adesso bedient eine Vielzahl von Branchen, darunter Versicherungen, Banken, Gesundheitswesen, Energieversorgung, Automotive, Handel, Verkehrsbetriebe, Lotterie und Sport. Zu den Kunden zählen namhafte Unternehmen wie die Commerzbank, Münchener Rück, E.ON, Mercedes-Benz, Bosch und Borussia Dortmund. International arbeitet adesso mit Partnern wie Swisscom, AXA Schweiz und der Schweizer Bundesbahn zusammen.

UNTERNEHMENSPROFIL

adesso

KONTAKT

Alexander Busam

CIO Advisory

E-Mail: alexander.busam@adesso.de

Damian Kirtz

Managing Consultant

E-Mail: damian.kirtz@adesso.de

adesso SE

Adessoplatz 1, 44269 Dortmund

Website: www.adesso.de/

Exxeta ist ein unabhängiger IT- und Technologieanbieter, der strategische Beratung mit der Entwicklung und dem Betrieb innovativer Lösungen verbindet. Seit der Gründung 2005 in Karlsruhe unterstützt das Unternehmen Organisationen dabei, Geschäftsmodelle, Prozesse und IT-Strukturen nachhaltig weiterzuentwickeln.

Das Leistungsspektrum reicht von Architektur- und Strategiefragen über Software- und Plattformentwicklung bis hin zum stabilen Betrieb individueller, komplexer Systeme. Exxeta ist in mehreren Branchen tätig, darunter Automotive, Energie, Finanzdienstleistungen und der öffentliche Sektor.

Mit über 1.200 Mitarbeitenden in fünf Ländern verfügt Exxeta über umfassende Expertise in Künstlicher Intelligenz, Daten- und Cloud-Architekturen sowie der Modernisierung gewachsener IT-Landschaften – mit dem Ziel, technologische Handlungsfähigkeit und digitale Souveränität langfristig zu sichern.

Im Bereich der digitalen Souveränität unterstützt Exxeta Organisationen dabei, technologische Abhängigkeiten bewusst zu steuern und ihre Handlungsfähigkeit im digitalen Raum langfristig zu sichern. Das Leistungsspektrum reicht von der Entwicklung souveräner Cloud- und Plattformstrategien über Architekturentscheidungen zur Vermeidung von Vendor Lock-in bis hin zum Aufbau kontrollierbarer Daten- und KI-Lösungen in regulierten Umfeldern.

UNTERNEHMENSPROFIL

exxeta

KONTAKT

Markus Fischer
Fellow Cloud
Exxeta AG

Victor-Gollancz-Straße 5, 76137 Karlsruhe
E-Mail: markus.fischer@exxeta.com
Website: www.exxeta.com

MaibornWolff ist ein deutsches IT-Dienstleistungsunternehmen mit Hauptsitz in München, das rund 800 Mitarbeitende an 10 Standorten in Deutschland, Spanien und Afrika beschäftigt. Das Unternehmen wurde 1989 von Volker Maiborn und Holger Wolff mit der Vision gegründet, zukunftsweisende Technologielösungen mit einem menschenzentrierten Ansatz zu verbinden.

MaibornWolff betreut Kunden aus unterschiedlichen Branchen, darunter öffentliche Verwaltungen wie die Bundesagentur für Arbeit, Automobilhersteller wie BMW, Mercedes Benz, MAN und Volkswagen, Mobilitätsdienstleister wie die Deutsche Bahn sowie Industrieunternehmen wie Dräger, ifm, Miele und TK Elevator. Darüber hinaus zählen Handels- und Versicherungskonzerne wie IKEA Deutschland und R+V zum Kundenportfolio.

Das Leistungsspektrum umfasst den Aufbau souveräner Cloud-Plattformen sowie die Implementierung von Hybrid- und Multicloud-Infrastrukturen. Weitere Schwerpunkte bilden die Entwicklung und der Betrieb von Datenplattformen, IoT- und Smart-Factory-Lösungen sowie die Entwicklung von Anwendungen für Mobile, Web, Mixed Reality und die KI-getriebene Modernisierung legacy-basierter Softwaresysteme. MaibornWolff arbeitet strategisch mit führenden Cloud-Anbietern wie AWS, Microsoft Azure und auch europäischen Lösungen wie STACKIT zusammen, um entwickelte Lösungen in hochskalierbare und regulatorisch konforme Betriebsumgebungen zu integrieren. Das Unternehmen verfügt über Erfahrungen aus mehr als 1.000 realisierten Großprojekten im Enterprise-Umfeld.

UNTERNEHMENSPROFIL



MAIBORNWOLFF

KONTAKT

Christian Leinweber
Technical Director Cloud Sovereignty &
Compliance
MaibornWolff GmbH

Theresienhöhe 13, 80339 München
E-Mail: christian.leinweber@maibornwolff.de
Website: www.maibornwolff.de

Die Materna-Gruppe realisiert komplexe und geschäftskritische Digitalisierungsprojekte für Konzerne, Mittelstand und öffentliche Verwaltung. Das Unternehmen erzielte im Jahr 2025 einen vorläufigen Gruppenumsatz von 795 Millionen Euro und beschäftigt weltweit rund 4.500 Mitarbeitende.

Mit dem Strategieprogramm Elevate richtet Materna ihre Weiterentwicklung auf nachhaltiges und profitables Wachstum aus. Im Fokus steht die verlässliche Umsetzung anspruchsvoller Vorhaben – auch in sensiblen und regulierten Umfeldern. Die Kompetenzen der Gruppe bündeln sich in vier strategischen Dimensionen: Platform-based Transformation, Human x Digital, Artificial Intelligence und Business Resilience. Als Familienunternehmen steht Materna für verantwortungsbewusstes Handeln und wirtschaftlich tragfähige Umsetzungskraft.

UNTERNEHMENSPROFIL

MATERNA

KONTAKT

Timon Schmotz

Business Development Manager

Public Sector und KRITIS

Materna Information & Communications SE

Robert-Schuman-Straße 20, 44263 Dortmund

E-Mail: marketing@materna.group

Website: <https://www.materna.de/>

msg ist eine unabhängige, international agierende Unternehmensgruppe mit weltweit über 10.000 Mitarbeitenden. Wir sind in 34 Ländern vertreten und unterstützen unsere Kunden mit einem umfassenden End-to-End-Leistungsspektrum bei der digitalen Transformation – von der strategischen Beratung über maßgeschneiderte Lösungen bis hin zur erfolgreichen Implementierung und laufenden Optimierung. Zu unserem Leistungsspektrum zählen Business- und IT-Consulting sowie die Entwicklung von Standardsoftware und Individuallösungen, einschließlich innovativer Cloud- und KI-Lösungen zur Optimierung von Geschäftsprozessen und der Digitalisierung von Unternehmen.

Als europäischer Partner begleiten wir unsere Kunden auf ihrem Weg zur selbstbestimmten digitalen Souveränität – mit der Entwicklung souveräner Cloud-Strategien, dem Aufbau hybrider Architekturen oder dem Betrieb kritischer Systeme auf europäischen Infrastrukturen – stets mit Blick auf Compliance, Datensicherheit und Zukunftsfähigkeit. Wir setzen auf Partnerschaften mit Hyperscalern, bieten unseren Kunden aber ebenso deutsche und europäische Alternativen. So unterstützen wir Unternehmen dabei, digitale Souveränität strategisch zu verankern und operativ umzusetzen.

UNTERNEHMENSPROFIL



KONTAKT

Karl Lassak
Principal Consultant
msg

Robert-Bürkle-Straße 1, 85737 Ismaning
E-Mail: info@msg.group
Website: <https://www.msg.group>

Digitale Souveränität erfordert eine sichere und verlässliche IT. Die TechniData IT-Gruppe entwickelt und betreibt IT-Infrastrukturen für Mittelstand, Konzerne und öffentliche Einrichtungen und schafft damit eine stabile, zukunftsfähige Basis für Geschäftsprozesse. Unser Anspruch ist es, IT so zu gestalten, dass Transparenz, Kontrolle und langfristige Handlungsfähigkeit gewährleistet sind.

Wir begleiten unsere Kunden ganzheitlich, von der Beratung über die Konzeption moderner IT-Architekturen bis zu Implementierung, Betrieb und kontinuierlicher Weiterentwicklung. Unser Service Desk gewährleistet stabile IT-Prozesse im Tagesgeschäft.

IT verstehen wir als integralen Bestandteil des Geschäftsmodells. Technologien entfalten ihren Wert erst dann, wenn sie sicher, wirtschaftlich und nachhaltig eingesetzt werden. Ein zentraler Pfeiler digitaler Souveränität ist unsere eigene Datacenter-Infrastruktur: Im Raum Stuttgart betreiben wir ein hochsicheres, hochverfügbares Rechenzentrum, ergänzt durch zwei georedundante Standorte im Raum Frankfurt. Dort stellen wir mit der „Flex Cloud“ eine souveräne Cloud bereit, die volle Transparenz über Speicherung und Verarbeitung der Daten bietet. Unser eigenes Security Operations Center (SOC) sorgt durch kontinuierliches Monitoring, strukturierte Prozesse und klare Verantwortlichkeiten für hohe Sicherheit und digitale Resilienz.

Mit unseren spezialisierten und eigenständigen Gesellschaften decken wir ein breites Portfolio ab: von Netzwerk- und IT-Security über Cloud- und Managed Services bis zu Open-Source-Technologien. Besonders in KRITIS-Bereichen verfügen wir über langjährige Erfahrung und tiefgehende Expertise.

Seit 2005 entwickeln wir uns kontinuierlich weiter. Heute beschäftigt die TechniData IT-Gruppe über 360 Mitarbeitende. Unser Handeln basiert auf Vertrauen, Verantwortung und langfristigen Partnerschaften. Firmensitz der TechniData IT AG, Holding der Gruppe, ist Karlsruhe.

UNTERNEHMENSPROFIL

**TECHNI
DATA**

it-gruppe

KONTAKT

Petra Moggioli

Leiterin Unternehmenskommunikation

E-Mail: petra.moggioli@technidata-it.com

Dennis Pudeck

Leiter Marketing & Produktmanagement

E-Mail: dennis.pudeck@technidata-it.com

TechniData IT AG

Albert-Nestler-Str. 28, 76131 Karlsruhe

Website: <https://www.technidata.de/>



Lizenz- und Studieninformation



Die hier dargestellte Studie wurde exklusiv in Zusammenarbeit mit adesso, Exxeta, MaibornWolff, Materna, msg und TechniData (Studienpartner) erstellt. Eine Zweitverwertung der Studienergebnisse ist nur unter Quellenangabe erlaubt. Eine Nutzung der Studie außerhalb der Studienpartnerschaft zu eigenen Marketing- oder Vertriebszwecken ist nicht gestattet. Die allgemeinen Geschäftsbedingungen sind hier in der aktuellen Version abrufbar: www.luenendonk.de/agb

Diese Studie ist nach deutschem und internationalem Veröffentlichungsrecht und entsprechenden Abkommen geschützt. Das Werk ist urheberrechtlich Eigentum der Lünendonk & Hossenfelder GmbH. Dieses Dokument darf ohne Einwilligung des Autors und Herausgebers außerhalb des Kundenunternehmens weder dupliziert, in anderen Datenbanksystemen oder privaten Rechnersystemen gespeichert noch an weitere Personen weitergeleitet werden.

Die folgenden Handlungen sind nicht erlaubt:

- Vervielfältigung zum weiteren Verkauf
- Verwendung in Beratungsprojekten für dritte Unternehmen
- Die Nutzung dieser Marktforschungsstudie durch KI-Systeme gemäß Art. 3 Nr. 1 Verordnung (EU) 2024/1689 erfordert die ausdrückliche Zustimmung der Lünendonk & Hossenfelder GmbH. Das Eingeben, Hochladen oder Verwenden der Inhalte für KI-Training oder automatisierte IT-Anwendungen ist strikt untersagt.

Die Marke Lünendonk® ist geschützt und ist Eigentum des Unternehmens Lünendonk & Hossenfelder GmbH. Bei Fragen zur Studienlizenz steht Ihnen das Team von Lünendonk & Hossenfelder gerne zur Verfügung (info@luendonk.de).

Alle Informationen dieses Dokuments entsprechen dem Stand zum Veröffentlichungsdatum. Alle Berichte, Auskünfte und Informationen dieses Dokuments entstammen aus Quellen, die aus Sicht der Lünendonk & Hossenfelder GmbH verlässlich erscheinen. Die Richtigkeit dieser Quellen wird vom Herausgeber jedoch nicht garantiert. Enthaltene Meinungen reflektieren eine angemessene Beurteilung zum Zeitpunkt der Veröffentlichung, die ohne Vermerk verändert werden können.

Über Lünendonk & Hossenfelder

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Digital & IT, Business Consulting, Audit & Tax, Real Estate Services, Personaldienstleistung (Zeitarbeit, IT-Workforce) und Weiterbildung.

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk®-Listen und -Studien“ heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalistinnen und Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Persönlichkeiten mit den Lünendonk B2B Service-Awards aus.



Mario Zillmann
Senior Partner

Telefon: +49 8261 73140-17
Mobil: +49 162 717 18 07
E-Mail: zillmann@lunenendonk.de



Tobias Ganowski
Senior Consultant

Telefon: +49 8261 73140-23
Mobil: +49 1525 914 16 16
E-Mail: ganowski@lunenendonk.de

IMPRESSUM

Herausgeber:
Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim
Telefon: +49 8261 73140-0
Telefax: +49 8261 73140-66
E-Mail: info@lunenendonk.de

Erfahren Sie mehr unter www.lunenendonk.de

Autoren:
Mario Zillmann, Senior Partner
Tobias Ganowski, Senior Consultant

Bilderquellen:
Titel © Adobe Stock / Johannes_1696883473
S. 62 © AdobeStock / M2L_489682374
S. 62 © iStock / NoSystem images_918035570