LÜNENDONK

Lünendonk®-Studie

Digitale Souveränität – Vom Risiko zur Resilienz

Balanceakt zwischen technischem Fortschritt und geopolitischer Realität

Eine Studie von Lünendonk & Hossenfelder in Zusammenarbeit mit

MATERNA

LÜNENDONK

Inhaltsverzeichnis

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 unkontrol-liertem Datenabfluss & extraterritorialen Zugriffen

93 %
Umsetzung regulatorischer Anforderungen

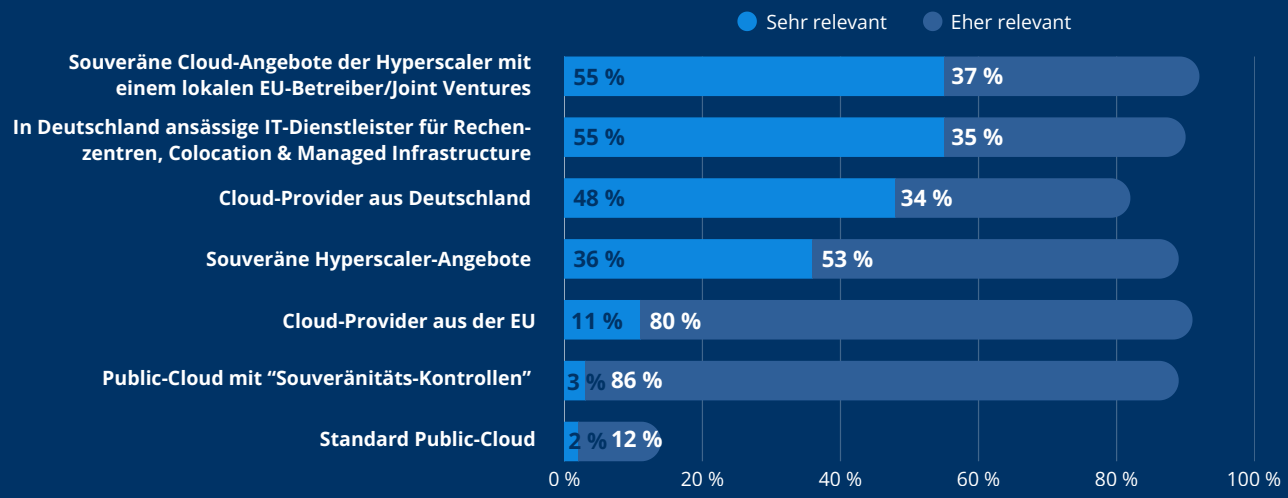
96 Prozent
ERWARTEN, DASS DIGITALE SOUVERÄNITÄT AUCH BEI EINER ENTSPANNUNG DER GEOPOLITISCHEN LAGE EIN ZENTRALES THEMA BLEIBT.

86 Prozent
halten höhere Investi-tionen in souveräne Angebote für sinnvoll, da die Opportunitäts-kosten 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

DEZEMBER 2022
Das ZenDiS (Zentrum für digitale Souveränität) wird im Auftrag des Bundesministeriums des Innern (BMI) gegründet mit dem Ziel, die digitale Souveränität in Bund, Ländern und Kommunen zu stärken.

OKTOBER 2024
Das ZenDiS launch Open Desk – eine souveräne Office- und Kollaborationssuite für die Öffentliche Verwaltung.

NOVEMBER 2024
Schleswig-Holstein beschließt seine Open-Souce-Strategie und setzt unter andrem auf die quell-offenen Software LibreOffice als Standard-Office-Lösung für die rund 25.000 IT-Arbeitsplätze. Bis Ende 2025 sollen rund 80 Prozent der Arbeits-plätze darauf umgestellt sein.

DEZEMBER 2024
Die Deutsche Rentenversicherung geht der Sozialversicherung, der Bundesagentur für Arbeit (BA) und der Deutschen Gesetzlichen Unfallver-sicherung (DGUV) vergeben eine gemeinsamen Cloud-Broker-Ausschreibung im Sinne ihrer Multi-Cloud-Strategie.

FEBRUAR 2025
Microsoft sperrt den E-Mail-Account von Karim Khan, Chefankläger am Internationalen Strafgerichtshof, auf Dekret des US-Präsidenten Donald Trump.

JULI 2025
Anton Carniaux, der Chefjustiziar von Microsoft France, bestätigt im Rahmen einer Anhörung vor dem französischen Senat, dass es keine Garantie dafür gibt, dass EU-Daten vor einer Übermittlung in die USA sicher sind und nie weitergegeben werden.

SEPTEMBER 2025
SAP kündigt an, 20 Milliarden Euro in die Erweiterungen des Sovereign-Cloud-Angebots bis 2035 zu investieren.

OKTOBER 2025
Der Internationalen Strafgerichtshofs vermeldet als Arbeitsplatz-Software Microsoft durch Open Desk zu ersetzen.

OKTOBER 2025
Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) veröffentlicht das Konzept zum Deutschland-Stack, einer sicheren, interoperablen, europäisch anschlussfähigen und souveränen Techno-logie-Plattform zur Digitalisierung der gesamten Verwaltung.

NOVEMBER 2025
Die Europäische Kommission veröffentlicht das Cloud Sovereignty Framework, einen 8-Punkte-Katalog, um Cloud-Services nach einheitlichen Souveränitätskriterien auszuwählen.

NOVEMBER 2025
Spatenstich für Schwarz Digits für ein Rechen-zentrum in Lübbenau im Spreewald mit einer Anschlussleistung von 200 Megawatt.

NOVEMBER 2025
Im deutsch-französischer "Gipfel zur Europäischen Digitalen Souveränität“ kündigen Bundeskanzler Merz und Präsident Macron gemeinsame Initiativen gegen Abhängigkeit von USA und China an.

NOVEMBER 2025
Die Deutsche Telekom und die Schwarz-Gruppe prüfen den Bau einer gemeinsam AI Gigafactory, einem Rechenzentrum mit 100.000 oder mehr Spezialchips für Künstliche Intelligenz.

JANUAR 2026
Die Deutsche Rentenversicherung Bund, die Bundesagentur für Arbeit sowie die IT-Dienst-leister Bitmarck und BG-Phoenics starten ein Pilotprojekt zu Open Desk als mögliche Alternative zu Microsoft 365.

JANUAR 2026
Die AWS European Sovereign Cloud (AWS ESC) geht in Brandenburg in Betrieb.

JANUAR 2026
Frankreich gibt bekannt, bis 2027 Zoom und Microsoft Teams durch die Videokonferenzplatt-form Visio in der Verwaltung zu ersetzen.

JANUAR 2026
Die Gesellschaft für Informatik bezieht Position, dass angesichts der Nationale Sicherheitsstrategie (NSS 2025) der USA die IT-Beschaffung im öffentlichen Sektor in Europa eine strategische Neuausrichtung benötigt – unter anderem durch verbindliche Souveränitätsprüfungen und ein Verbot von Rahmenverträgen mit US-Monopolanbietern.

FEBRUAR 2026
Das BSI und Schwarz Digits vereinbaren eine Partnerschaft zur Entwicklung souveräner Cloud-Infrastrukturen für die öffentliche Verwaltung.

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

Branche

Manufacturing & Automotive	21 %
Health	15 %
Transport, Verkehr	15 %
Öffentlicher Sektor	15 %
Energie, Utilities & Smart City	14 %
Banken	10 %
Versicherungen	10 %

Positionen

IT-Bereichsleiter	47 %
GRC-/Security-Verantwortliche	19 %
IT-Einkauf	18 %
CIOs	12 %
Business-Verantwortliche	4 %

Unternehmensgrößen

100 bis 500 Mio. €	26 %
Über 500 Mio. bis 1 Mrd. €	25 %
Über 1 bis 5 Mrd. €	26 %
Über 5 Mrd. €	23 %

Internationalisierungsgrad

Fokus auf EU	39 %
International	61 %

Deutschland 68 % | Österreich 16 % | Schweiz 16 %

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 Hyperscalers 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 Leadern. 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

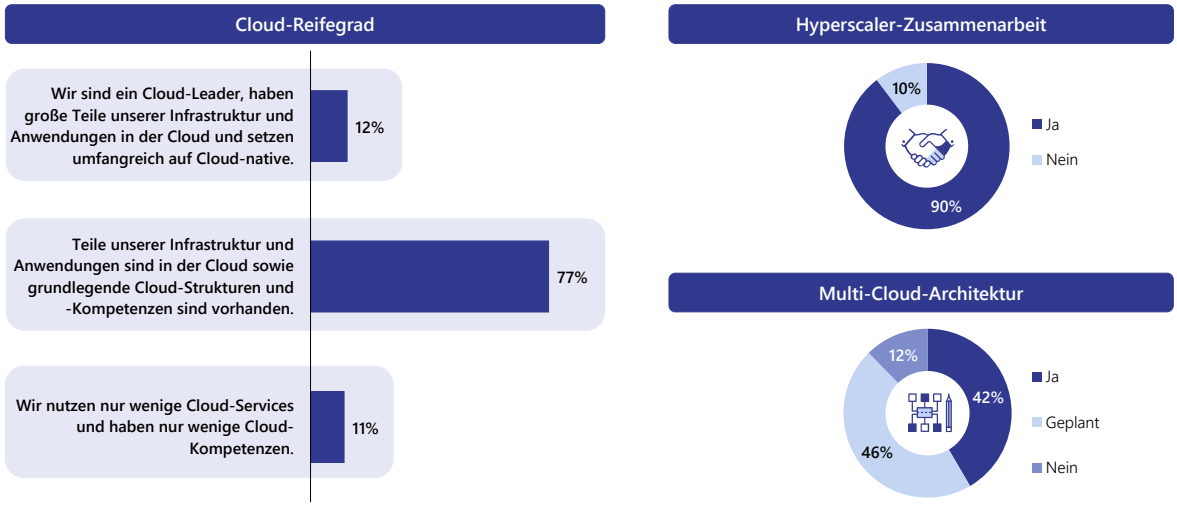


Abb. 2: Wie schätzen Sie den Cloud-Reifegrad Ihrer Organisation ein?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155
Ist Ihr Unternehmen Kunde von einem Hyperscaler?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155
Nutzt Ihre Organisation eine Multi-Cloud-Architektur und setzt somit 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

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 stufen 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 stufen 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

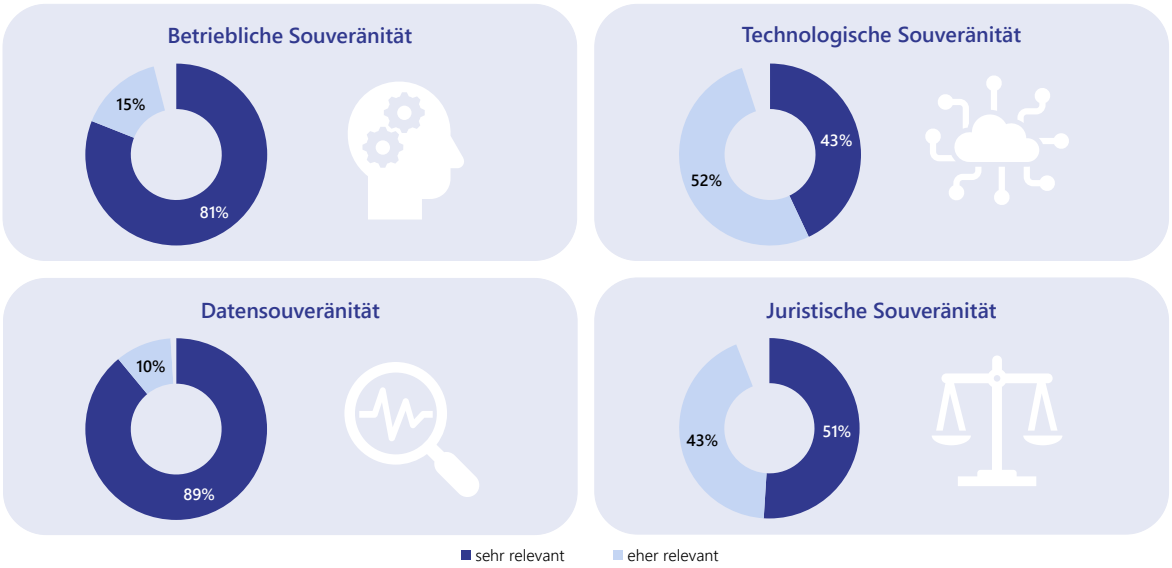


Abb. 4: Wie wichtig sind die folgenden Souveränitätsprinzipien für Ihre Organisation?; Skala von 1 = „nicht relevant" bis 4 = „sehr relevant"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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

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.

Digitale Souveränität wird in Zukunft deutlich wichtiger

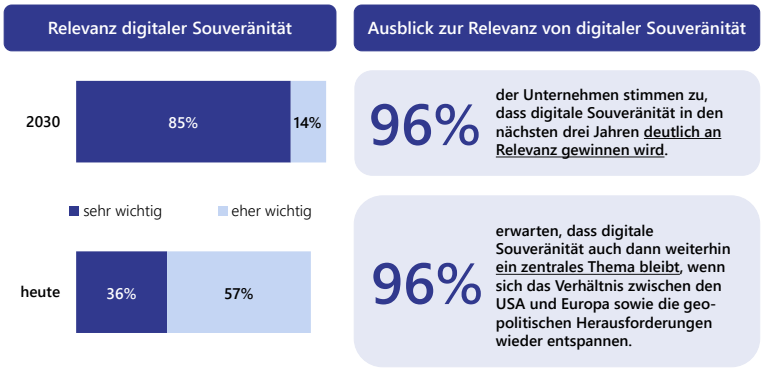


Abb. 6: Digitale Souveränität ist aktuell ein sehr zentrales Thema in der öffentlichen Diskussion. Wie wichtig ist digitale Souveränität für Ihre Organisation?; Skala von 1 = „unwichtig" bis 4 = „sehr wichtig"; heute und 2030; relative Häufigkeitsverteilung; alle Unternehmen; n = 155
Angenommen, das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

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 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 Eskalationsszenarien, 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

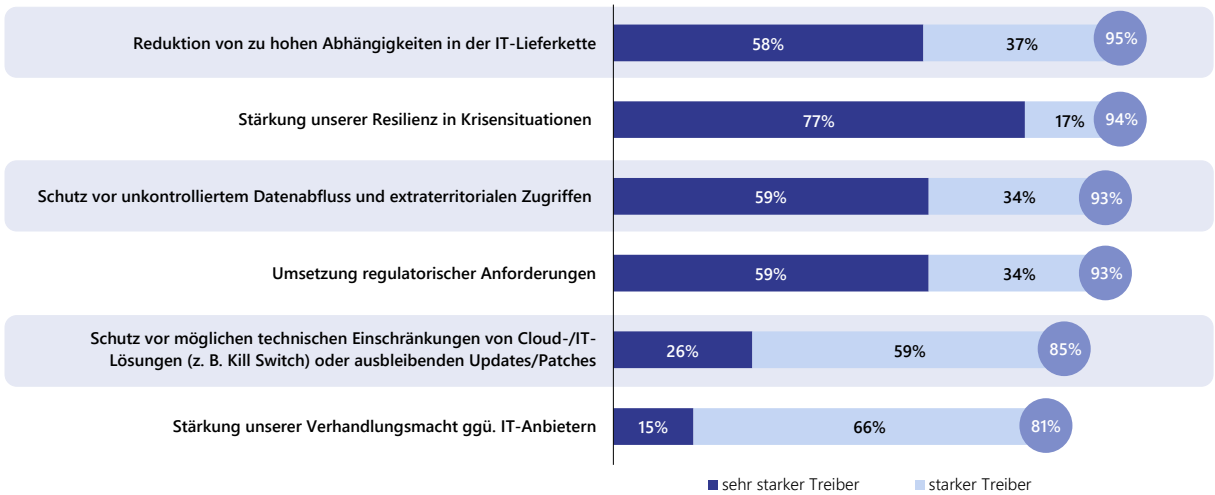


Abb. 7: Digitale Souveränität hat viele Facetten. Wie stark sind die folgenden Aspekte ein Treiber für Ihre Organisation, digitaler Souveränität auszubauen?; Skala von 1 = „kein Treiber" bis 4 = „sehr starker Treiber"; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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 Hyperscaler, 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 Alternativanbietern. 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

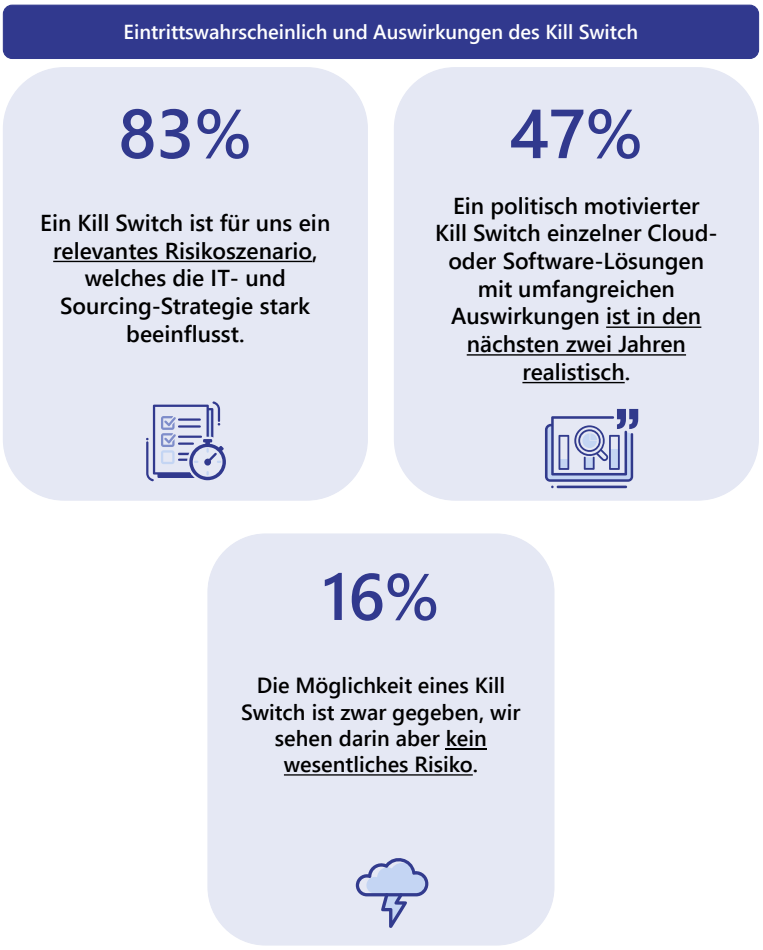


Abb. 8: Der Kill Switch, also die Einschränkung oder Abschaltung von digitalen Diensten für einzelne Personen, Organisationen oder ganze Staaten, ist ein viel diskutiertes Thema. Wie bewerten Sie die folgenden Aussagen in Bezug auf Ihre Organisation?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll 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

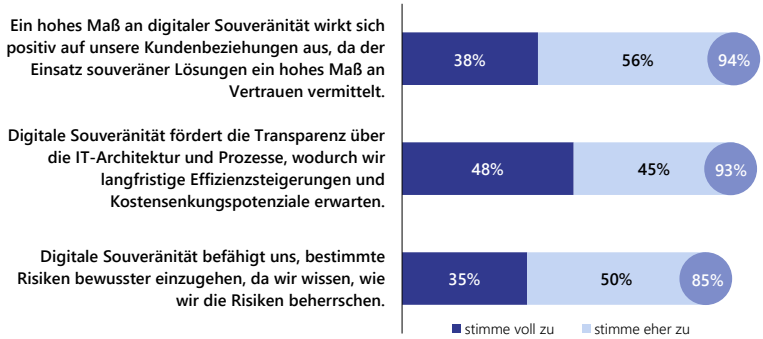


Abb. 9: Wie stehen Sie zu den folgenden Aussagen, wie digitale Souveränität in Ihrer Organisation aufgefasst wird?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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

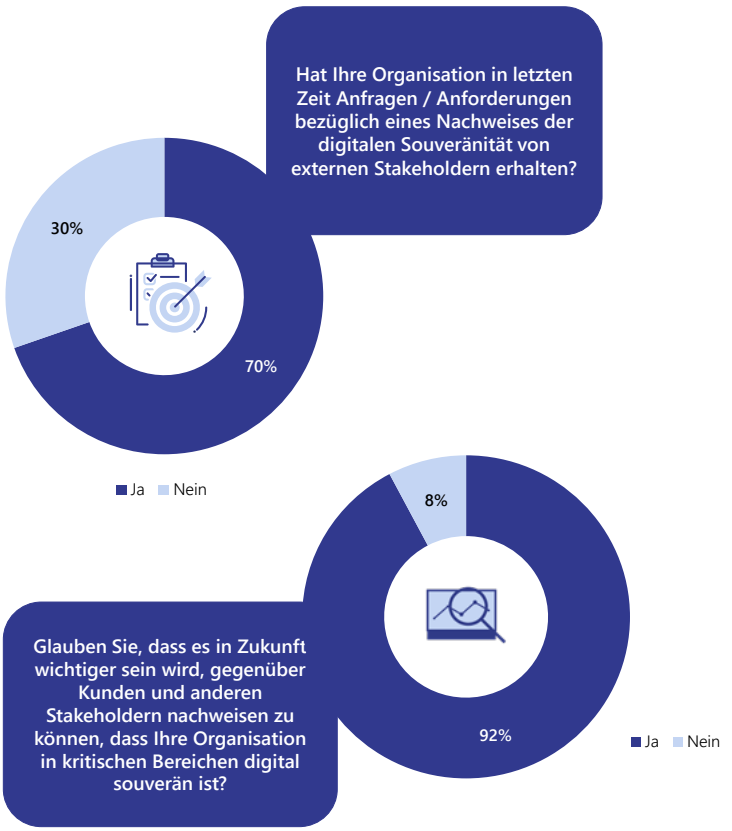


Abb. 10: Hat Ihre Organisation in letzten Zeit Anfragen / Anforderungen bezüglich eines Nachweises der digitalen Souveränität von externen Stakeholdern erhalten (z. B. Kunden, Banken, Versicherungen)?; relative Häufigkeitsverteilung; alle Unternehmen; n = 155
Glauben Sie, dass es in Zukunft wichtiger 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

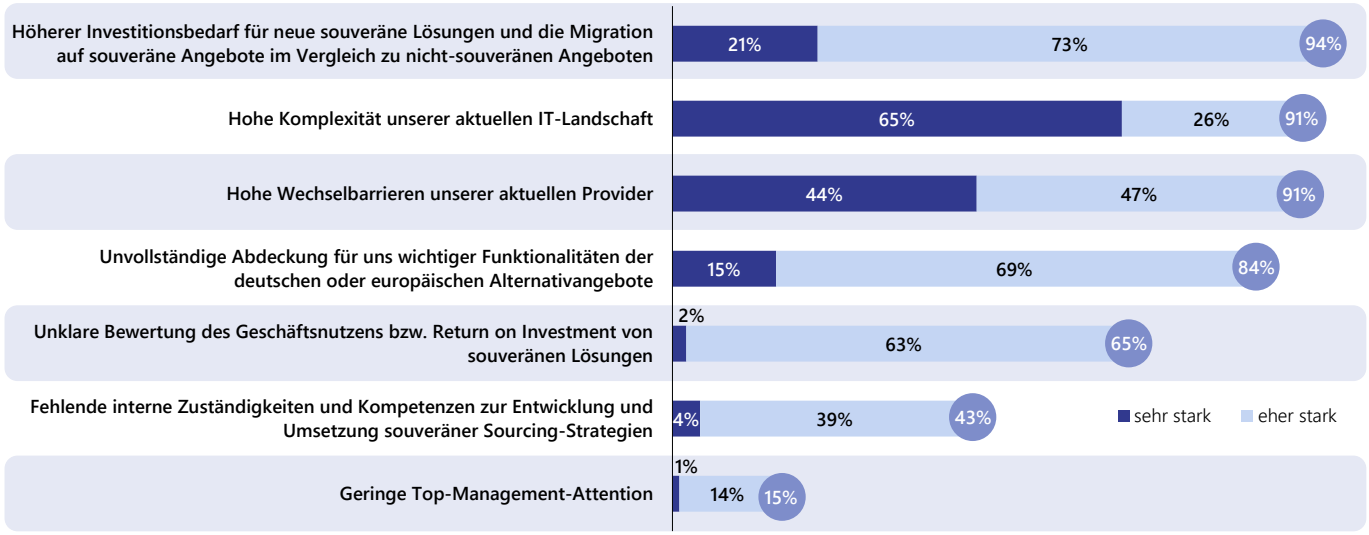


Abb. 11: Wie stark fordern Ihre Organisation die folgenden Aspekte beim Aufbau von mehr digitaler Souveränität heraus?; Skala von 1 = „gar nicht" bis 4 = „sehr stark"; relative Häufigkeitsverteilung; alle Unternehmen; n = 152

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 Strategiefrage: 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 substanzielle 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

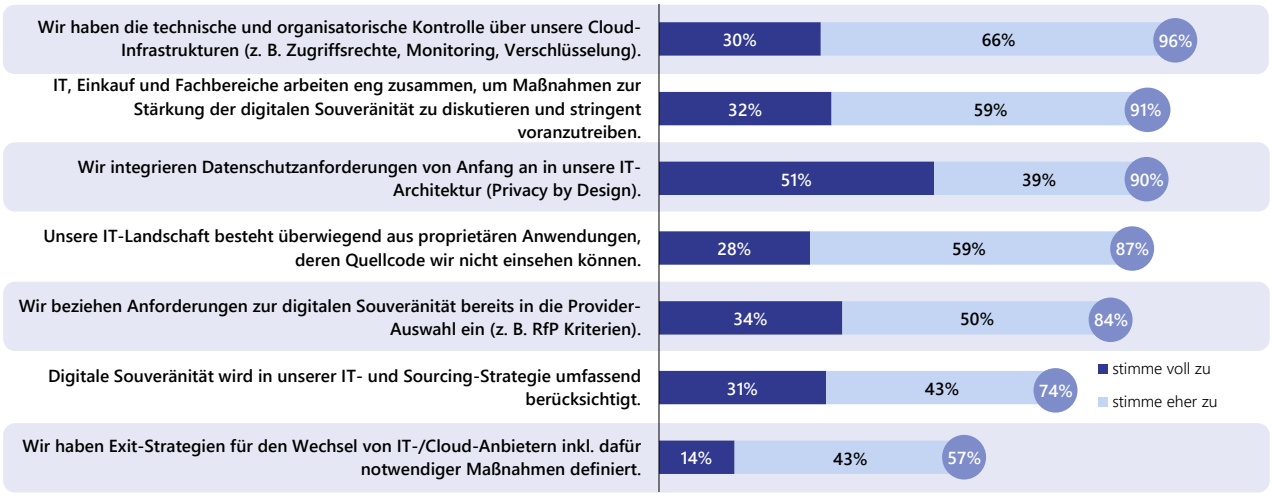


Abb. 12: Wie stehen Sie zu den folgenden Aussagen bezüglich Ihrer Sourcing-Strategie und IT-Landschaft?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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 Schnittstellenoffenheit 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 Wechselszenarien 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 Exportformate 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

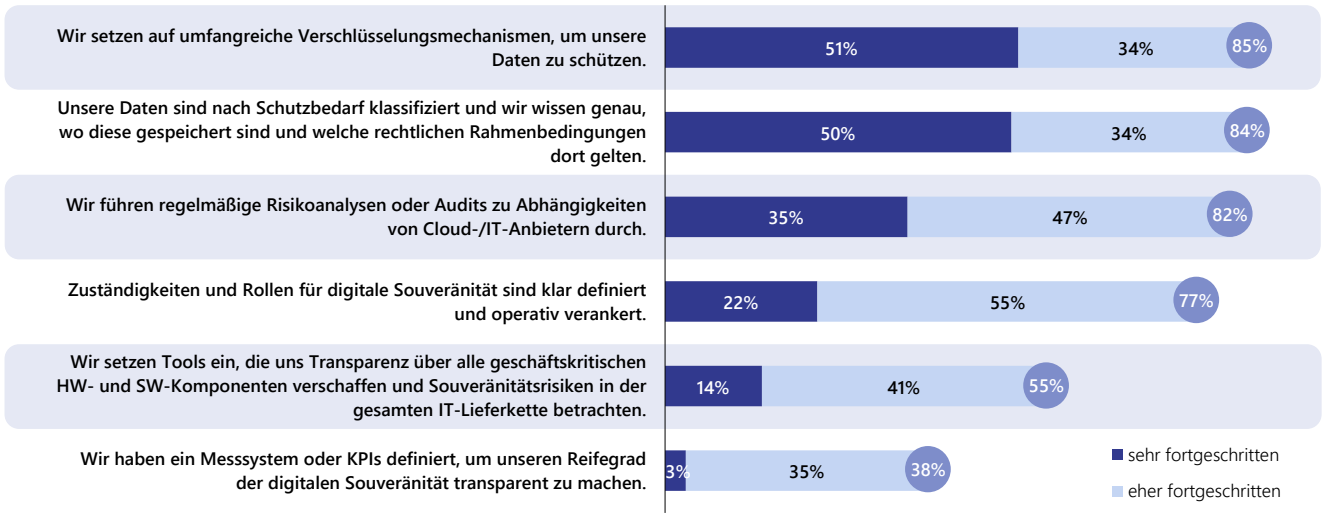


Abb. 13: Wie fortgeschritten ist Ihre Organisation bei den folgenden Maßnahmen?; Skala von 1 = „stehen am Anfang" bis 4 = „sehr fortgeschritten"; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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

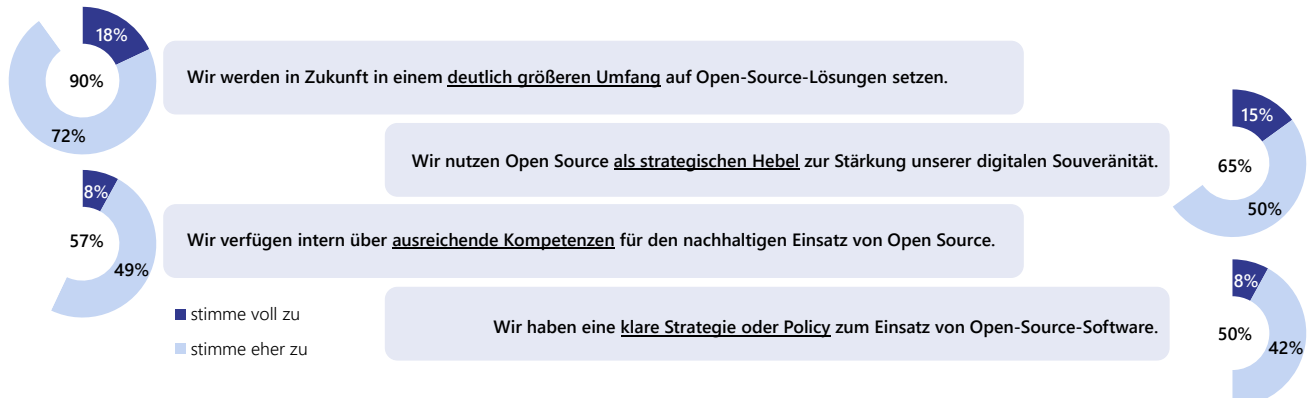


Abb. 14: Open Source ist ein weiteres Instrument zur Stärkung der digitalen Souveränität. Wie stehen Sie zu den folgenden Aussagen hinsichtlich Ihrer Organisation?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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 zwischengeschaltet 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

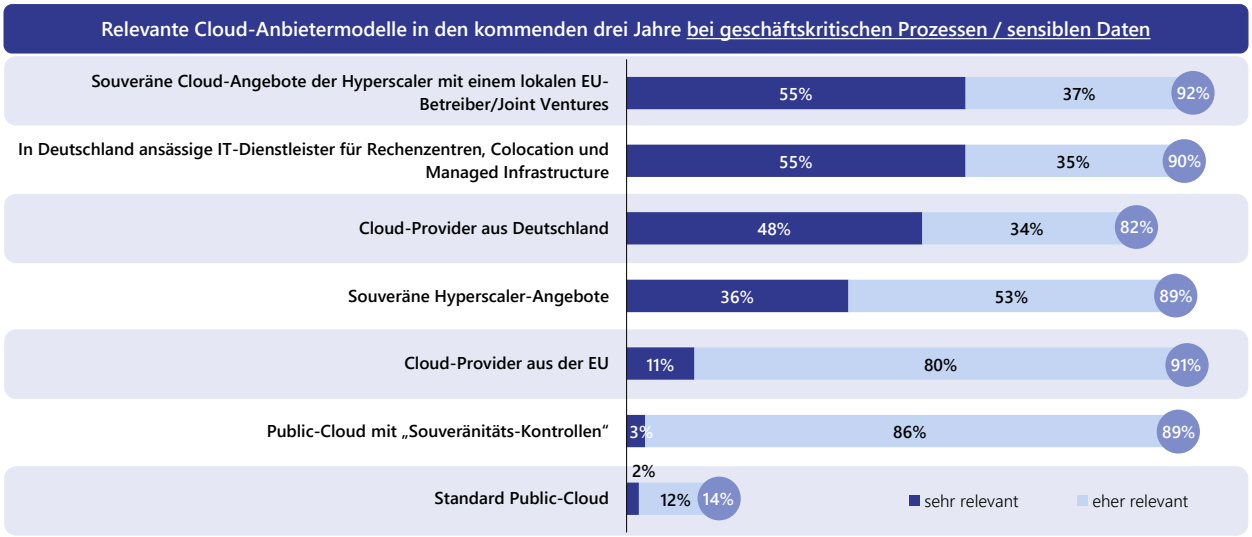


Abb. 15: Welche Rolle spielen folgende Anbietermodelle für Ihre Organisation mit Blick auf die kommenden drei Jahre; bei geschäftskritischen Prozessen / sensiblen Daten?; Skala von 1 = „nicht relevant" bis 4 = „sehr relevant"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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 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

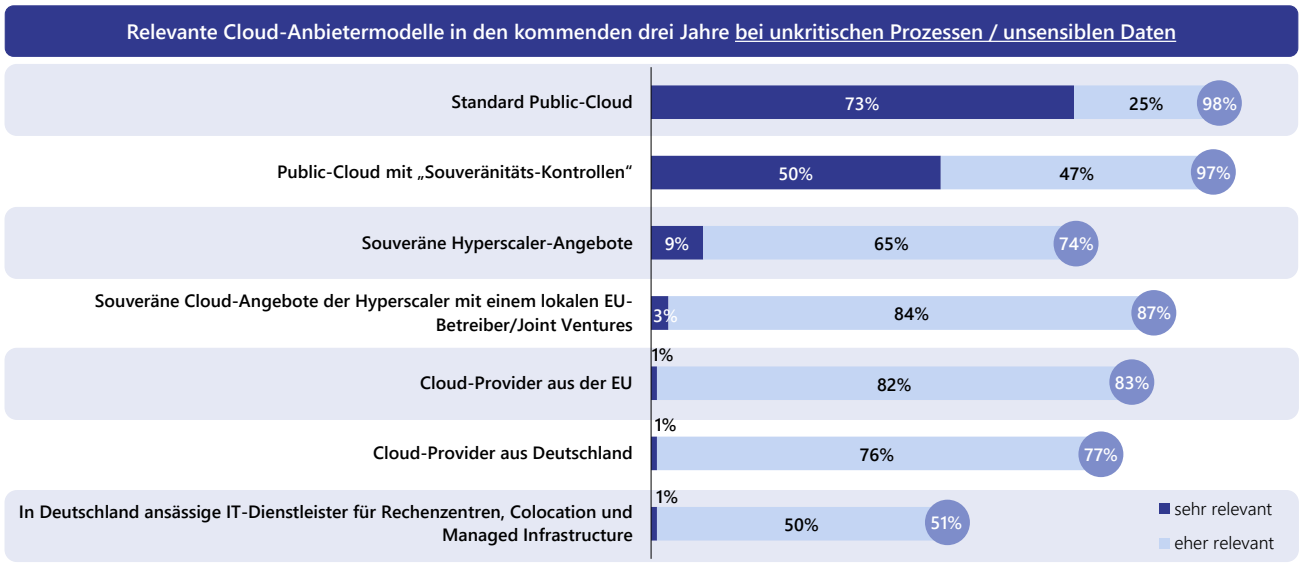


Abb. 16: Welche Rolle spielen folgende Anbietermodelle für Ihre Organisation mit Blick auf die kommenden drei Jahre; bei unkritischen Prozessen / unsensiblen Daten?; Skala von 1 = „nicht relevant" bis 4 = „sehr relevant"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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 Chefjustiziars 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

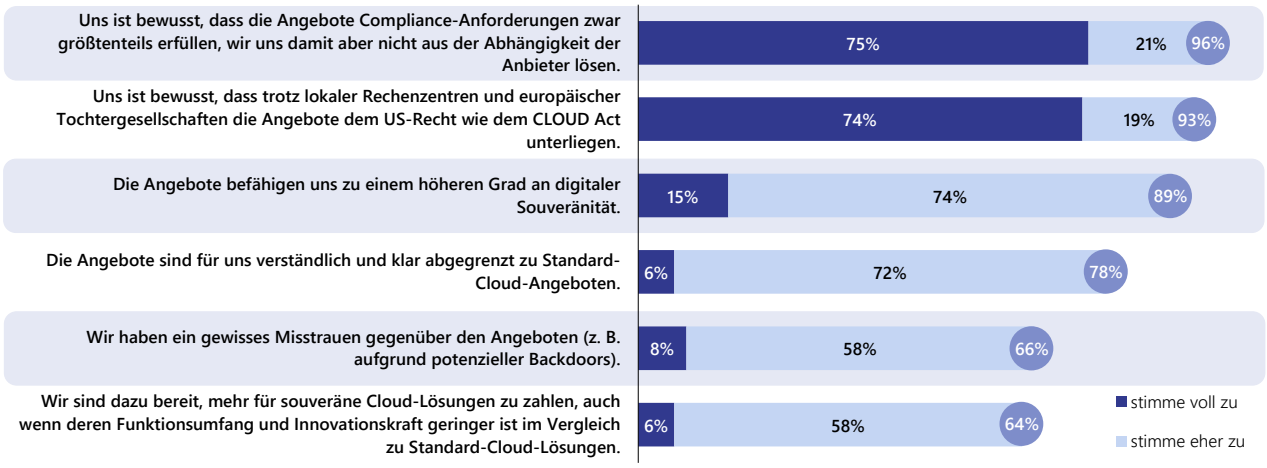


Abb. 17: Wie stehen Sie zu den folgenden Aussagen hinsichtlich der von den Hyperscalern angebotenen souveränen Cloud-Lösungen?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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

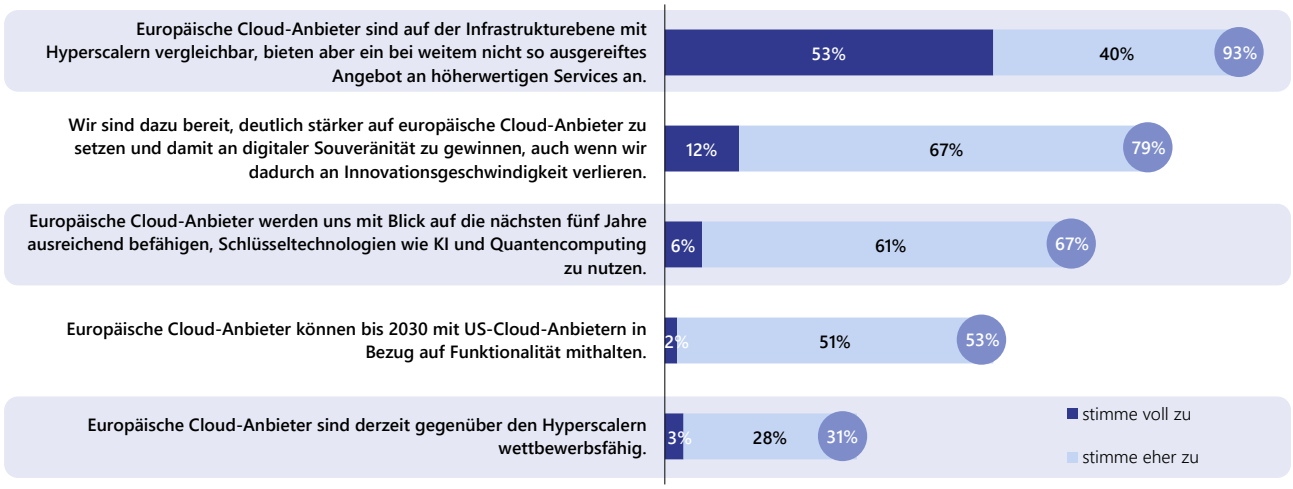


Abb. 18: Deutsche oder europäische Cloud-Provider sind eine Alternative zu den Hyperscalern. Wie stehen Sie zu den folgenden Aussagen?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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

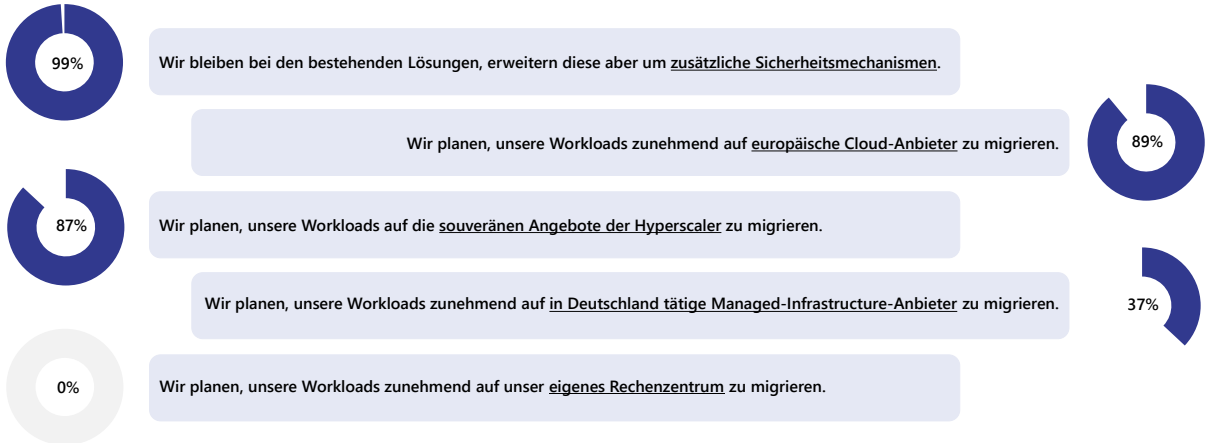


Abb. 19: Wie stehen Sie zu den folgenden Aussagen bezüglich der Workloads, die aktuell auf den Hyperscalern laufen?; Mehrfachauswahl; nur Hyperscaler-Kunden; n = 139

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

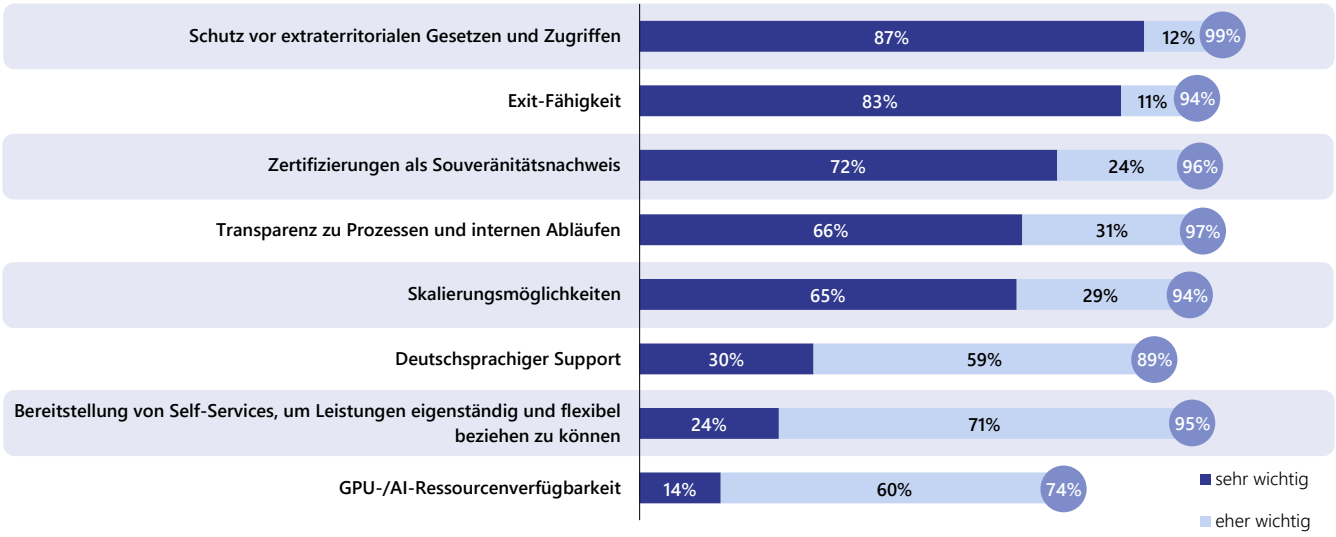


Abb. 20: Wie wichtig sind die folgenden Kriterien bei der Auswahl eines souveränen Cloud-Anbieters?; Skala von 1 = „unwichtig" bis 4 = „sehr wichtig"; relative Häufigkeitsverteilung; alle Unternehmen; n = 152

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

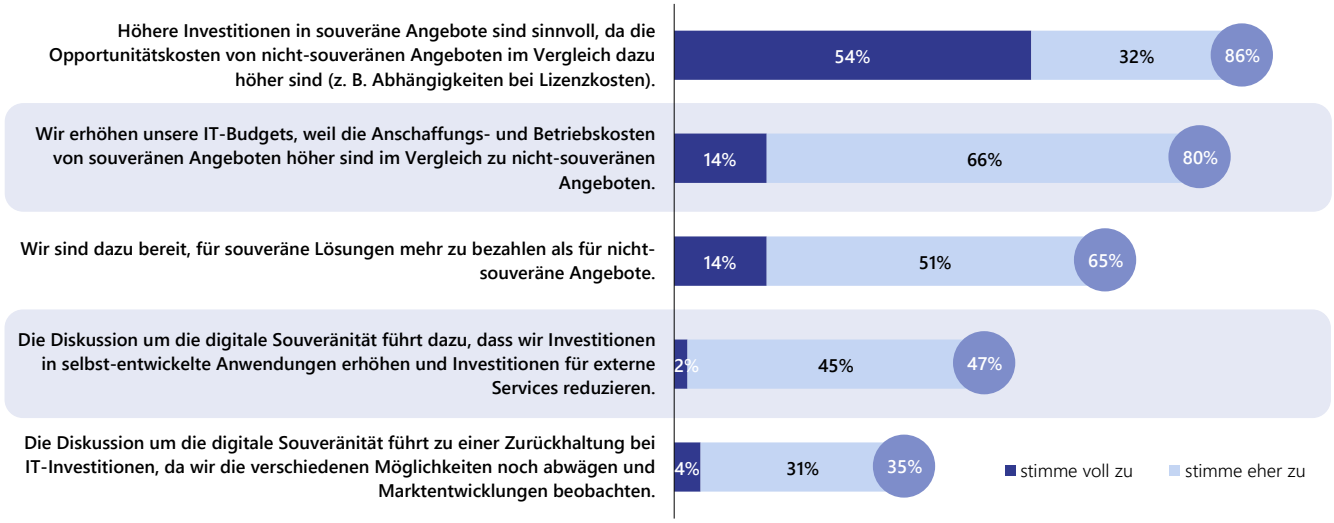


Abb. 22: Wie stehen Sie zu den folgenden Aussagen in Bezug auf Ihre Organisation?; Skala von 1 = „stimme nicht zu" bis 4 = „stimme voll zu"; relative Häufigkeitsverteilung; alle Unternehmen; n = 155

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

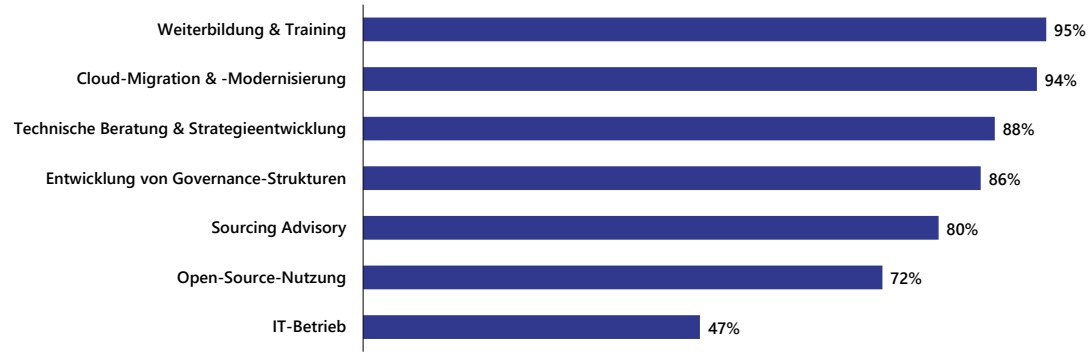


Abb. 23: In welchen Bereichen werden Sie künftig mit externen Partnern zusammenarbeiten, um Ihre digitale Souveränität zu stärken?; Mehrfachantwort; relative Häufigkeitsverteilung; alle Unternehmen; n = 154

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 außereuropäischen 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 Studienumsetzung:

- 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!

Lünendonk im Interview mit Materna

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

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 selbstbestimmter 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 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.

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/

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@luenendonk.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@luenendonk.de

Tobias Ganowski

Senior Consultant

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

IMPRESSUM

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

Erfahren Sie mehr unter www.luenendonk.de

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

Bilderquellen:
Titel © Adobe Stock / Johannes_1696883473
S. 38 © AdobeStock / M2L_489682374
S. 38 © iStock / NoSystem images_918035570