techconsult
TECHNOLOGY MARKET ANALYSTS
EIN UNTERNEHMEN DER heise group

EuroCloud
DEUTSCHLAND eco

EuroCloud Pulse Check 2025

Digitale Resilienz made in Europe:

Strategien für eine souveräne Cloud-Zukunft

EXOSCALE
member of A1 Digital

IONOS

plusserver

Informationen zur Studie

Erstellung durch

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

Tel.: +49 561 8109 0
Fax: +49 561 8109 101
E-Mail: info@techconsult.de
Web: www.techconsult.de

Veröffentlichung

September 2025

Autor

Pascal Brunnert

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group

In Zusammenarbeit mit

EuroCloud DEUTSCHLAND eco

Kontakt

EuroCloud Deutschland_eco e. V.
Lichtstraße 43h
50825 Köln

E-Mail: info@eurocloud.de
Telefon: +49 221 7000 48 0

Mehr erfahren

Sonstige Informationen

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser,

Künstliche Intelligenz und Cloud Computing verschieben die Grenzen dessen, was Unternehmen technologisch leisten können. Cloud ist dabei längst nicht mehr nur Infrastruktur – sie bildet die Basis für moderne KI-Anwendungen, die effizientere Prozesse, datenbasierte Entscheidungen und mehr Innovationskraft ermöglichen. Diese Entwicklung bestätigt unser „EuroCloud Pulse Check 2025".

Zugleich gewinnen digitale Souveränität und Resilienz angesichts wachsender geopolitischer Unwägbarkeiten an strategischer Bedeutung. Unternehmen achten verstärkt auf Sicherheit, Compliance und Datenkontrolle. Wie unsere Studie zeigt, können ihnen Hybrid- und Multi-Cloud-Ansätze helfen, Risiken zu streuen und Flexibilität zu gewährleisten.

Diese Architekturen sind jedoch hochkomplex und erfordern spezifisches Know-how aus verschiedenen IT-Bereichen. Kooperationen zwischen Cloud Providern, MSPs, Beratungs- und Systemhäusern, Software- und Hardware-Anbietern werden daher unverzichtbar, um Projekte effizient, sicher und skalierbar umzusetzen.

Eine Gruppe von Unternehmen, der wir diesmal im Pulse Check unser besonderes Augenmerk widmen, habe ich noch nicht genannt: die „Superscaler". Europäische Cloud-Anbieter, die sich als Alternativen zu den US-Hyperscalern positionieren, gewinnen an Relevanz im Markt. Sie verbinden technologische Leistungsfähigkeit mit Transparenz und Datensouveränität. Daher bieten sie sich insbesondere als Partner für geschäftskritische Workloads an.

Unsere Studie belegt: Digitale Souveränität, Cloud-Resilienz, KI-Fähigkeiten und partnerschaftliche Zusammenarbeit sind entscheidende Faktoren für die Zukunftsfähigkeit deutscher Unternehmen. Den Akteuren dabei vitale Plattformen zu bieten, über die sie sich auf Augenhöhe zu neuen Ansätzen und Best Practices, zu Erfolg und Scheitern austauschen können, ist Mission von EuroCloud Deutschland.

Wir hoffen, dass der diesjährige Pulse Check wertvolle Impulse für eine souveräne, resiliente und innovationsfähige Zukunft liefert.

Nicht zuletzt möchte ich mich zutiefst bei unseren Partnern A1 Digital, IONOS und plusserver bedanken. Sie haben mit ihrem konzeptionellen Input und ihrer finanziellen Unterstützung entscheidend zum Gelingen der Studie beigetragen.

Und jetzt? Viel Spaß beim Lesen und bleibt gesund!

Beste Grüße

Nils Kaufmann

Dr. Nils Kaufmann
Vorstand EuroCloud und Leiter EuroCloud Native (ECN)

Köln, im September 2025

Einleitung

Während traditionelle Infrastrukturen noch mit physischen Servern und starren Wartungszyklen kämpfen, haben Cloud-native Unternehmen bereits den nächsten Entwicklungssprung vollzogen. Wo früher IT-Teams wochenlang Hardware beschaffen und konfigurieren mussten, entstehen heute komplexe Anwendungslandschaften per Mausklick. Diese Geschwindigkeitsunterschiede entscheiden mittlerweile über Marktanteile: Wer seine Softwareentwicklung noch an lokale Server kettet, verliert gegen Konkurrenten, die ihre Services global skalieren und binnen Minuten neue Features ausrollen können. Cloud Computing ist längst über den Status eines IT-Trends hinausgewachsen und bestimmt heute die Architektur erfolgreicher Digitalunternehmen.

Doch wo Licht ist, ist bekanntlich auch Schatten: Die schiere Vielfalt an Cloud-Angeboten, Deployment-Modellen und Serviceoptionen kann selbst erfahrene IT-Verantwortliche vor Kopfzerbrechen stellen. Was gestern noch als innovative Lösung galt, kann heute bereits überholt sein. In diesem dynamischen Umfeld den Überblick zu behalten und die richtigen strategischen Entscheidungen zu treffen, erfordert fundierte Marktkenntnis und eine solide Datenbasis.

Genau hier setzt der EuroCloud Pulse Check an, der nun bereits in seine fünfte Runde geht – ein bewährtes Barometer für die deutsche Cloud-Landschaft. Diese kontinuierliche Bestandsaufnahme hat sich über die Jahre als verlässlicher Kompass für IT- sowie Business-verantwortliche etabliert und liefert wertvolle Einblicke in Trends, Herausforderungen und Entwicklungen des deutschen Cloud-Marktes.

Dabei setzt jede Ausgabe ihren eigenen thematischen Schwerpunkt, um den jeweils aktuellen Herausforderungen der Zeit Rechnung zu tragen.

Angesichts der anhaltenden geopolitischen Spannungen und einer zunehmend fragmentierten Weltordnung rückt in diesem Jahr die europäische und deutsche Resilienz sowie digitale Souveränität besonders in den Fokus. In Zeiten, in denen Lieferketten unterbrochen werden und Abhängigkeiten zu unkalkulierbaren Risiken werden können, stellt sich die europäische Frage nach technologischer Autonomie von globalen Partnern mit neuer Dringlichkeit. Wer seine digitalen Zügel nicht selbst in der Hand hält, könnte sich schnell in einer misslichen Lage wiederfinden.

Für die aktuelle Ausgabe wurden 258 Onlineinterviews mit IT- und Business-Verantwortlichen aus deutschen Unternehmen ab 50 Beschäftigten durchgeführt. Diese repräsentative Stichprobe ermöglicht es, einen umfassenden und belastbaren Überblick über den Status quo der Cloud-Nutzung in Deutschland zu zeichnen. Von etablierten Konzernen bis hin zu wachstumsstarken Mittelständlern – die Bandbreite der befragten Unternehmen spiegelt die Vielfalt der deutschen Wirtschaftslandschaft wider.

Am Puls der Zeit: Warum Unternehmen auf Diversifikation setzen

Status quo

Die Frage nach dem optimalen Cloud-Bereitstellungsmodell beschäftigt IT-Verantwortliche wie kaum eine andere strategische Entscheidung. Schließlich legt diese Weichenstellung den Grundstein für die gesamte digitale Infrastruktur eines Unternehmens. Die aktuellen Zahlen des EuroCloud Pulse Check offenbaren dabei eine bemerkenswerte Entwicklung: Die deutschen Unternehmen setzen zunehmend auf Flexibilität statt auf Gradlinigkeit.

Ein besonders auffälliger Trend zeigt sich bei der ausschließlichen Nutzung von Private Clouds. Hier ist ein deutlicher Rückgang zu verzeichnen: Während im vergangenen Jahr noch 22 Prozent der befragten Unternehmen ausschließlich auf Private-Cloud-Lösungen setzten, sind es 2025 nur noch 14 Prozent. Diese Entwicklung deutet darauf hin, dass die einst als Allheilmittel gepriesene Private Cloud ihre Monopolstellung in vielen Unternehmen verliert.

Der Gewinner dieser Verschiebung ist eindeutig die Hybrid Cloud, die sich mit 57 Prozent Nutzungsanteil zur absolut häufigsten Strategie entwickelte.

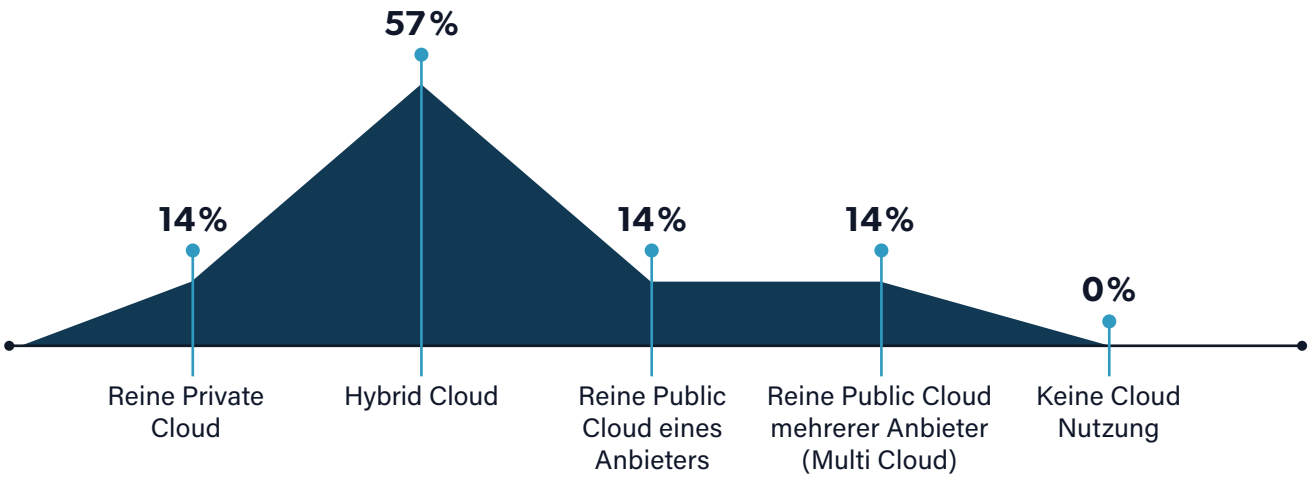
Bereits in den vergangenen Jahren zeichnete sich dieser Trend ab, als z. B. 2024 40 Prozent der Unternehmen auf hybride Modelle setzten. Die Gründe für diese Präferenz liegen auf der Hand: Hybride Ansätze versprechen Synergieeffekte durch das sprichwörtliche "best of both worlds". Unternehmen können kritische Workloads und sensible Daten in der Private Cloud behalten, während sie gleichzeitig die Skalierbarkeit und Kosteneffizienz der Public Cloud nutzen.

Besonders bemerkenswert ist dabei die verstärkte Betonung der Datensicherheit in der Public Cloud. Während früher die öffentliche Cloud oft als Sicherheitsrisiko betrachtet wurde, hat sich das Bewusstsein gewandelt. Moderne Public-Cloud-Anbieter investieren in Sicherheitsinfrastrukturen, die für einzelne Unternehmen schlichtweg unbezahlbar wären. Diese Sicherheitsstandards machen es Unternehmen leichter, vereinzelt auch sensible Workloads in die Public Cloud zu verlagern – allerdings weiterhin im Rahmen einer durchdachten Hybrid-Strategie.

Abbildung 1

Cloud-Strategien derzeit

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen



Ein Blick in die Zukunft

Interessant ist auch der Blick in die Zukunft: Die Hybrid Cloud wird ihre starke Position voraussichtlich behalten, denn 54 Prozent der Befragten planen, auch künftig auf dieses Modell zu setzen. Diese Stabilität unterstreicht, dass hybride Strategien nicht nur ein stetig wachsender Trend sind, sondern sich als nachhaltige Lösung etabliert haben – vor allem Angesichts schwieriger geopolitischer Weltlagen. Durch die Kombination aus Public und Private Cloud – vor allem von europäischen oder deutschen Anbietern – werden z. B. politische Zugriffsrisiken durch ausländische Regierungen verringert.

Eine bemerkenswerte Kehrtwende zeigt sich bei den strategischen Zukunftsplänen der Unternehmen. Während im letzten Jahr noch der Trend in Richtung einer einzigen Public Cloud zu gehen schien, hat sich das Blatt gewendet: Nun soll der Trend in Richtung Multi Cloud gehen. Aktuell setzen 14 Prozent der Unternehmen auf Multi-Cloud-Strategien, doch für die Zukunft planen bereits 22 Prozent eine entsprechende Ausrichtung.

Die strategische Aufteilung der Workloads auf verschiedene Cloud-Anbieter wird dabei zu einem zentralen Erfolgsfaktor. Unternehmen erkennen zunehmend, dass unterschiedliche Anwendungen und Services auch unterschiedliche Anforderungen haben.

Während ein Anbieter möglicherweise bei KI-Services hervorsticht, punktet ein anderer bei Datenbank-Performance oder Compliance-Features. Diese granulare Herangehensweise ermöglicht es, für jeden Workload die optimale Umgebung zu wählen und gleichzeitig Synergien zwischen verschiedenen Plattformen zu nutzen.

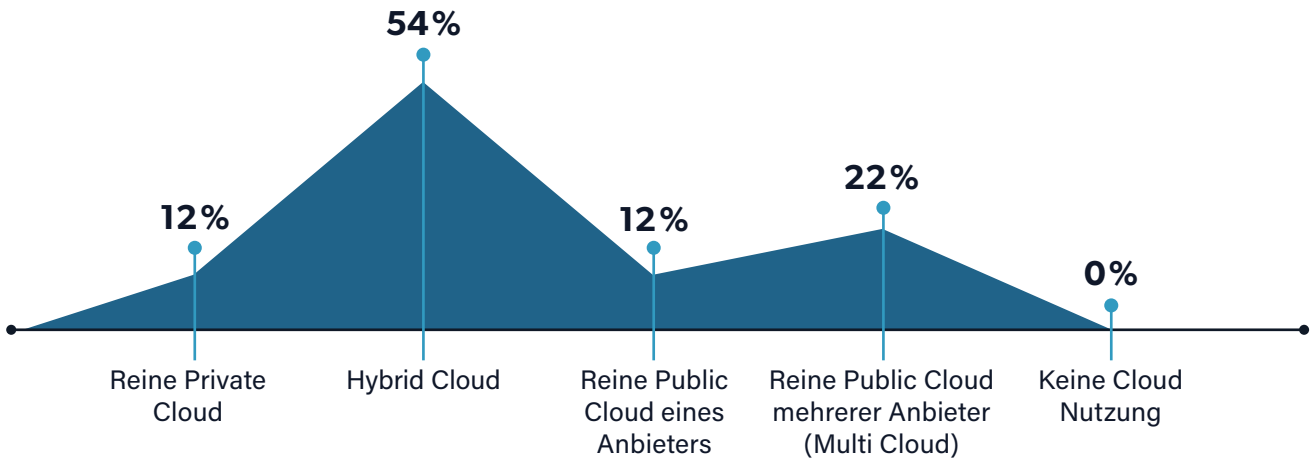
Ein weiterer treibender Faktor für Multi-Cloud-Strategien – aber auch hybride Ansätze – ist die bewusste Vermeidung eines Vendor-Lock-ins. Wer sich zu stark an einen einzelnen Anbieter bindet, macht sich nicht nur technisch abhängig, sondern versetzt sich auch bei zukünftigen Vertragsverhandlungen in eine schwierige Verhandlungsposition. Multi-Cloud-Ansätze schaffen hier die nötige Flexibilität und Verhandlungsgrundlage. Zudem reduzieren sie das Risiko von Ausfällen oder zukünftigen Service-Verschlechterungen bei einem einzelnen Anbieter erheblich.

Diese duale Entwicklung hin zu einer diversifizierten Cloud-Strategie – sowohl via Hybrid als auch Multi Cloud – spiegelt das gewachsene Bewusstsein für zukünftige Risiken wider. Wer alle Eier in einen Korb legt, macht sich angreifbar – eine Erkenntnis, die in Zeiten geopolitischer Unsicherheiten besonders an Gewicht gewinnt.

Abbildung 2

Cloud-Strategien zukünftig

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen



1. Wie Krisen Souveränität und Resilienz zur Unternehmenspriorität machen

Der bereits beschriebene Trendwechsel von der einzelnen Public Cloud zur Multi Cloud sowie die verstärkte Nutzung hybrider Modelle ist mehr als nur eine technische Kurskorrektur – er spiegelt einen grundlegenden Bedeutungswandel wider. Resilienz und Souveränität haben sich von Buzzwords zu strategischen Imperativen entwickelt, die das Fundament moderner Unternehmensstrategie bilden. Was einst als netter Zusatz galt, ist heute zur Überlebensfrage geworden.

Vor mehr als fünf Jahren sahen 67 Prozent der Unternehmen diese Faktoren als wichtig oder maßgeblich entscheidend an, wobei nur 25 Prozent sie als maßgeblich einstuften. Zum Zeitpunkt des Eintritts der COVID-19-Pandemie spielten Souveränität und Resilienz noch eine untergeordnete Rolle in der strategischen Planung vieler Unternehmen. Doch dann kam der große Realitätscheck. Plötzliches Homeoffice stellte IT-Abteilungen vor ungeahnte Herausforderungen: Der Mangel an Office-Hardware und Peripheriegeräten offenbarte die Fragilität globaler Lieferketten. Die komplette Umstellung der Arbeitsweise sowie gegebenenfalls des Geschäftsmodells stellte die Widerstandsfähigkeit der Unternehmen ungewollt auf den Prüfstand. Was über Nacht geschehen musste, hätte eigentlich Jahre der Vorbereitung erfordert und schon längst stattfinden sollen.

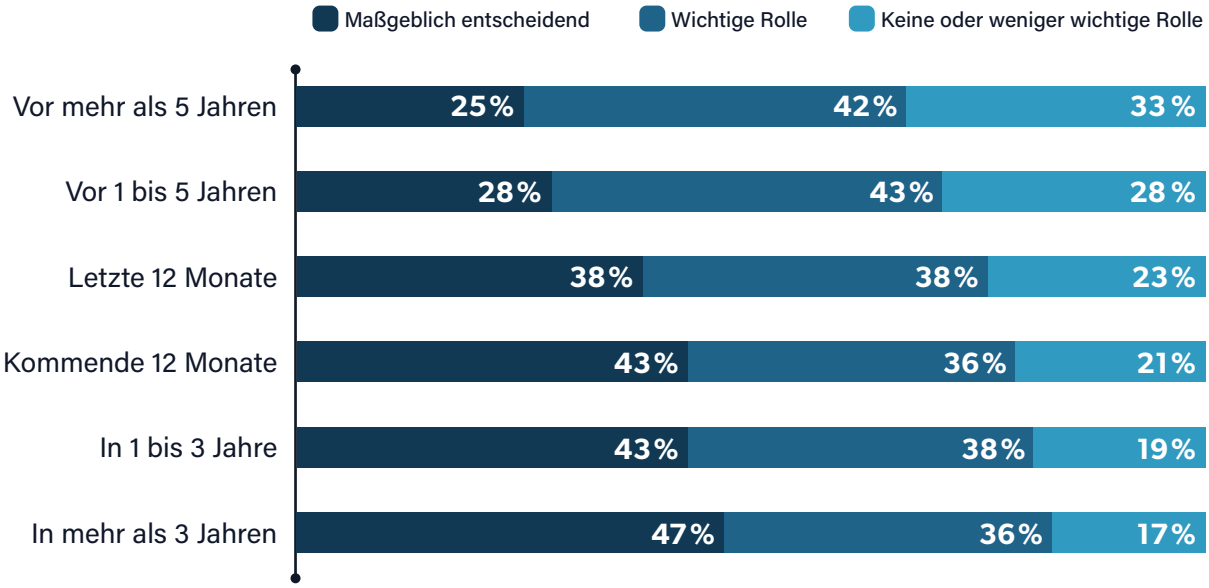
Vor fünf Jahren sahen nur 25 Prozent der Unternehmen Souveränität und Resilienz Faktoren als maßgeblich entscheidend für ihre Cloudstrategie an. COVID-19 und der Russland-Ukraine-Krieg verstärkten das Bewusstsein für Abhängigkeiten – die Bedeutung von Resilienz und Souveränität stieg auf 71 Prozent (28 Prozent maßgeblich entscheidend).

Während des anfänglichen Kriegsverlaufs zwischen Russland und der Ukraine wurde für deutsche Unternehmen deutlich, dass ihre Unternehmensresilienz sowie die Kontrolle über ihre Daten und Dienste deutlich mehr Aufmerksamkeit benötigen. Plötzlich waren eigene Lieferketten direkt betroffen und geopolitische Unsicherheiten sowie politische oder ethische Einschränkungen hinsichtlich Russlands zwangen Unternehmen dazu, ihre Abhängigkeiten zu überdenken. Was bis dahin als rein wirtschaftliche Entscheidung galt, wurde zur Frage der Unternehmensethik und strategischen Unabhängigkeit. Für diesen Zeitraum stieg die Bedeutung von Resilienz und Souveränität für die Cloudstrategie um 4 Prozentpunkte an – auf insgesamt 71 Prozent, davon 28 Prozent maßgeblich entscheidend.

Abbildung 3

Bedeutung von Resilienz und Souveränität in der Cloud-Strategie

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen



Im bisherigen Verlauf der zweiten Präsidentschaft Trumps werden Resilienz und Souveränität jetzt erneut stetig wichtiger, was sich vor allem hinsichtlich der kommenden Jahre – aber in Teilen auch schon in den letzten 12 Monaten – widerspiegelt. Geopolitische Unsicherheiten bei der Zusammenarbeit mit einem der engsten politischen und wirtschaftlichen Verbündeten des europäischen Handelsraums fordern mehr und mehr eine Sensibilisierung und Priorisierung resilienter sowie souveräner Prozesse – auch in der Cloud.

57 Prozent der befragten Unternehmen geben an, dass die Außenpolitik der aktuellen US-amerikanischen Regierung sie in ihrer bisherigen Infrastrukturstrategie verunsichert. Wenn selbst traditionelle Partnerschaften zwischen zwei wirtschaftlich eng gekoppelten Nationen ins Wanken geraten, wird strategische Autonomie zur Notwendigkeit.

Die Zahlen sprechen eine deutliche Sprache: Die Bedeutung von Souveränität und Resilienz in der Unternehmensstrategie hat sich über die Jahre kontinuierlich gesteigert. Je weiter in die Zukunft gedacht wird, desto bedeutender werden Souveränität und Resilienz für die Unternehmensstrategie. Die Steigerung von 67 Prozent auf 83 Prozent allgemein beziehungsweise von 25 Prozent auf 47 Prozent bei maßgeblich entscheidender Bedeutung zeigt: Deutsche Unternehmen haben ihre Lektion gelernt. Wer heute nicht in Resilienz investiert, könnte morgen das Nachsehen haben. Die Verinnerlichung dieser Erkenntnis spiegelt sich auch im Selbstbewusstsein der Unternehmen wider: 68 Prozent geben an, sehr gut auf zukünftige unsichere Wirtschaftslagen vorbereitet zu sein. Ob diese Einschätzung der Realität standhält, wird sich zeigen – aber die Richtung stimmt.

57 Prozent der deutschen Unternehmen zeigen sich durch die US-amerikanische Außenpolitik in ihrer Infrastrukturstrategie verunsichert – selbst traditionelle Partnerschaften geraten ins Wanken. Die Zahlen belegen einen kontinuierlichen Wandel, in dem Resilienz und Souveränität maßgeblich an Bedeutung gewinnen. Deutsche Unternehmen haben ihre Lektion gelernt.

2. Von der Strategie zur Praxis: Wie Unternehmen Datensouveränität konkret umsetzen

Um herauszukristallisieren, auf welche Weise die strategische Bedeutung von Souveränität sich auch praktisch widerspiegelt, ist es essenziell, die bereits ergriffenen Maßnahmen zur Daten- und Anwendungssouveränität genauer zu beleuchten. Denn zwischen dem Wunsch nach digitaler Autonomie und der konkreten Umsetzung liegt oft ein weiter Weg – und wie heißt es so schön: Der Teufel steckt im Detail.

Allgemeine Trends bei Souveränitätsmaßnahmen

Die Rangfolge der ergriffenen Maßnahmen zeigt, wo deutsche Unternehmen ihre Prioritäten setzen: An der Spitze stehen regelmäßige Sicherheitsprüfungen mit 42 Prozent – ein deutlicher Anstieg gegenüber dem Vorjahr, als nur 30 Prozent der Unternehmen regelmäßige Sicherheitsprüfungen durchführten. Unternehmen haben erkannt, dass sie nur rechtzeitig reagieren können, wenn sie den Status quo im Auge behalten. Kontinuierliches Monitoring ist zur Grundvoraussetzung geworden, um in einer sich schnell wandelnden Bedrohungslandschaft bestehen zu können.

Datenverschlüsselung folgt mit 38 Prozent auf dem zweiten Platz und etabliert sich als Standardmaßnahme für Datensouveränität. Denn bereits in der Vorjahresstudie gaben vier aus zehn Unternehmen (40 Prozent) an, Datenverschlüsselung als Kernelement ihrer Souveränitätsbemühungen zu betrachten. Besonders bemerkenswert ist hier der Handel, der dieses Jahr mit 48 Prozent deutlich über dem Durchschnitt liegt – ein Indiz dafür, dass kundennahe Branchen die Sensibilität ihrer Daten besonders ernst nehmen.

Die Sicherstellung der Datenqualität komplettiert das Spitzentrio mit 35 Prozent und hat im Vergleich zum letzten Jahr erheblich an Bedeutung gewonnen – von 24 Prozent um ganze 11 Prozentpunkte. Diese Entwicklung ergibt Sinn: Souveränität über schlechte oder unvollständige Daten ist wie ein Schloss ohne Fundament.

Kontinuierliches Monitoring wird zur Grundvoraussetzung für digitale Souveränität.

Abbildung 4

Maßnahmen zur Sicherstellung von Datensicherheit und -souveränität

Basis: 258 Unternehmen | Mehrfachantwort erlaubt

Branchenspezifische Ansätze: Verschiedene Wege führen nach Rom

Die Analyse nach Branchen offenbart interessante Unterschiede in den strategischen Herangehensweisen. Die Industrie hat über alle Branchen hinweg den höchsten Durchschnittswert und verfolgt damit den breitesten Ansatz. Diese Strategie der Souveränität über viele Bereiche hinweg hat ihre Berechtigung, birgt jedoch auch das Risiko, dass die nötige Tiefe fehlen könnte. Wer überall gleichzeitig präsent sein will, läuft Gefahr, nirgendwo wirklich stark zu sein.

Der Public Sector setzt verstärkt auf Open Source (39 Prozent) – eine logische Konsequenz des Strebens nach staatlicher Unabhängigkeit von der internationalen Wirtschaft. Wenn der Staat seine digitale Souveränität ernst nimmt, führt kein Weg an offenen Standards und transparenten Lösungen vorbei. Hier zeigt sich beispielhaft, wie politische Zielsetzungen technische Entscheidungen prägen.

Im Handel lässt sich ein starker Fokus auf die Delegation von Verantwortung erkennen. Mit 52 Prozent setzen überdurchschnittlich viele Handelsunternehmen auf Beauftragte für Datensouveränität und -sicherheit, während 42 Prozent explizit Beschäftigte mit der Kernaufgabe Datensouveränität und -sicherheit einsetzen.

Diese personalzentrierte Herangehensweise zeigt: Im Handel wird gelebt, dass Technologie allein nicht ausreicht – es braucht Menschen, die Verantwortung übernehmen und strategisch denken.

Banken und Versicherungen verfolgen zugleich einen technischen als auch rechtlichen Ansatz – ein doppelter Boden, der in regulierten Branchen durchaus sinnvoll ist. Mit 46 Prozent setzen sie überdurchschnittlich auf standardisierte, offene API-Infrastrukturen, während 42 Prozent Zusatzklauseln und Verträge mit Anbietern als Maßnahme zur Sicherstellung von Datensicherheit und Datensouveränität nutzen. Diese Kombination aus technischer Flexibilität und rechtlicher Absicherung spiegelt die besondere Verantwortung dieser Branchen wider: Hier geht es nicht nur um Unternehmensdaten, sondern um das Vertrauen der Kundschaft in das gesamte Finanzsystem.

Die Industrie diversifiziert, der Handel verteilt Verantwortungen, der Public Sector setzt auf Open Source und der Finanzsektor sichert sich in Technik sowie Recht doppelt ab.

Abbildung 5

Branchenspezifischer Fokus bei der Sicherstellung von Datensicherheit und Datensouveränität

Basis: 258 Unternehmen | Mehrfachantwort erlaubt

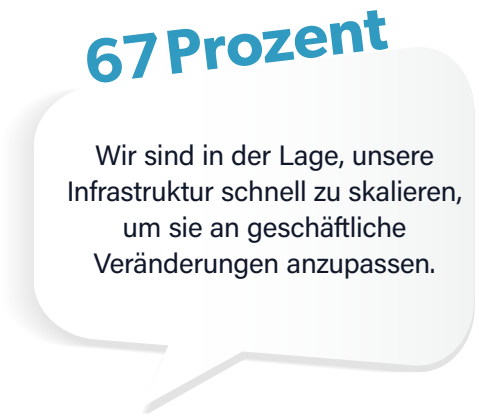
3. Die Anatomie der Resilienz: Fünf Schlüsselfaktoren für krisenresistente Unternehmen

Nachdem zunächst die Souveränität deutscher Unternehmen auf den Prüfstand gestellt wurde, gilt es nun herauszufinden, an welchen Stellen ihrer strategischen Planung Resilienz eine Rolle spielt. Auf Grundlage von 20 Items sollten die Befragten daher angeben, anhand welcher Kriterien sie die Resilienz eines Unternehmens feststellen. Denn Resilienz ist wie ein gutes Fundament – Ihre Stärke erkennt man erst unter extremer Belastung. Die Ergebnisse kristallisieren fünf zentrale Kriterien heraus, die das Fundament krisenresistenter Unternehmen bilden. Diese Quintessenz der Widerstandsfähigkeit zeigt, wo deutsche Unternehmen ihre Prioritäten setzen, wenn es um die Vorbereitung auf ungewisse Zeiten geht.

Abbildung 6

Fähigkeit zur schnellen Skalierbarkeit

Basis: 258 Unternehmen



1. Cybersicherheit

An der Spitze stehen Maßnahmen zur Cybersicherheit mit 37 Prozent – ein Ergebnis, das perfekt zu den Erkenntnissen des vorherigen Kapitels passt. Die dort beschriebenen regelmäßigen Sicherheitsprüfungen und Verschlüsselungsmaßnahmen finden hier ihre strategische Begründung. In einer Zeit, in der Cyberangriffe zur alltäglichen Bedrohung geworden sind, wird Cybersicherheit zum digitalen Immunsystem des Unternehmens. Wer hier spart, spart am falschen Ende.

2. Flexibilität der IT-Infrastruktur

Mit 35 Prozent folgt die Flexibilität der IT-Infrastruktur dicht dahinter. Hierunter fallen beispielsweise die Skalierbarkeit sowie die Möglichkeit zum Anbieterwechsel – Faktoren, die in der heutigen volatilen Geschäftswelt entscheidend sind. Bemerkenswert ist, dass 67 Prozent der Befragten angeben, in der Lage zu sein, ihre Infrastruktur schnell zu skalieren, um sie an geschäftliche Veränderungen anzupassen. Deutsche Unternehmen fühlen sich also gut für die Herausforderungen einer sich schnell wandelnden Geschäftswelt gerüstet. Ob diese Zuversicht berechtigt ist, wird sich in der nächsten Krise zeigen.

3. IT-Ausfallsicherheit

Maßnahmen zur IT-Ausfallsicherheit belegen mit 34 Prozent den dritten Platz. N+1 und Georedundanz sind hier die klassischen Beispiele – Konzepte, die bereits seit Ewigkeiten in der IT-Welt Bestand haben, aber in Zeiten zunehmender Digitalisierung neue Relevanz gewinnen. Wenn das gesamte Geschäftsmodell auf digitalen Prozessen basiert, wird jede Minute Ausfallzeit zur teuren Angelegenheit.

4. Innovationskraft

Mit 32 Prozent wird Innovationskraft als viertwichtigstes Resilienzkriterium eingestuft. Die schnellere und freiere Erarbeitung von Lösungsansätzen kann in Krisenzeiten zum entscheidenden Wettbewerbsfaktor werden. Unternehmen, die in der Lage sind, kreativ auf unvorhergesehene Herausforderungen zu reagieren, haben oft die Nase vorn. Innovation ist somit nicht nur ein Wachstumstreiber in guten Zeiten, sondern auch eine Überlebensstrategie in schlechten.

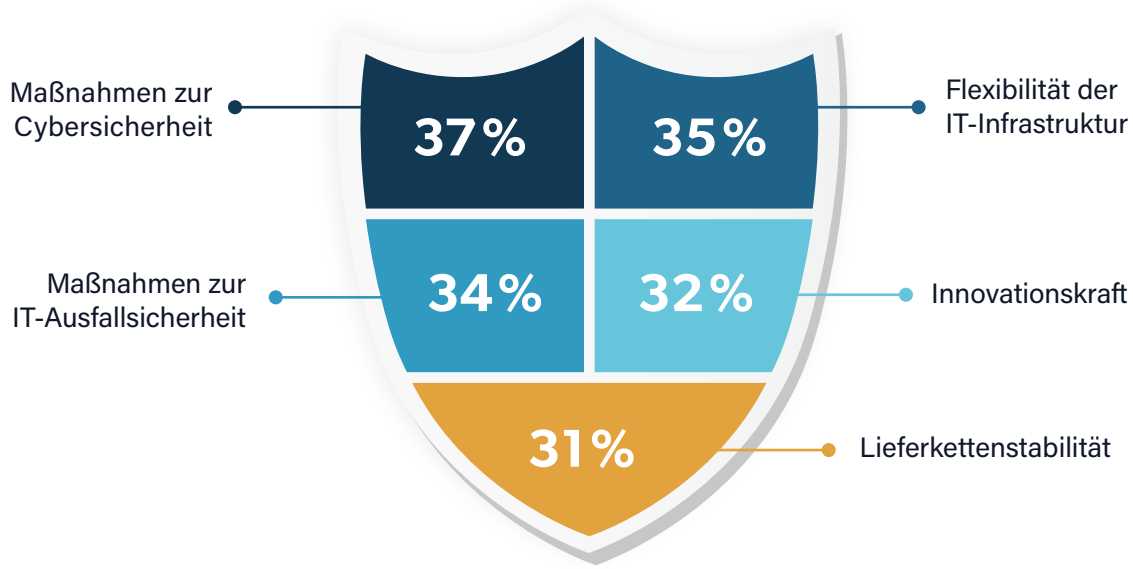
5. Lieferkettenstabilität

Den Abschluss der Top 5 bildet mit 31 Prozent die Lieferkettenstabilität. Geografische Streuung, mehrere Lieferanten, alternative Routen oder ausreichende Lagerbestände – all diese Maßnahmen zielen darauf ab, die Abhängigkeit von einzelnen Akteuren, Ländern oder Regionen zu reduzieren. Die COVID19-Pandemie und die geopolitischen Konflikte der letzten Jahre haben schmerzhaft vor Augen geführt, wie fragil globale Lieferketten sein können. Wer heute noch alles auf ein Pferd setzt, hat aus der Geschichte nicht gelernt.

Abbildung 7

Kriterien für ein resilientes Unternehmen

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



Diese fünf Säulen der Resilienz zeigen: Moderne Unternehmen denken ganzheitlich über Widerstandsfähigkeit nach. Es geht nicht mehr nur um technische Redundanzen, sondern um ein umfassendes Verständnis von organisationaler Robustheit, das von der Cybersicherheit bis zur Lieferkette reicht.

4. Europas Cloud-Antwort: Was sind eigentlich Superscaler?

Die Begrifflichkeiten

In der Cloud-Landschaft haben sich Hyperscaler längst als die großen Player etabliert – ein Begriff, der vielen IT- sowie Business-Entscheiderinnen und -Entscheidern geläufig ist wie der Name ihrer örtlichen Bäckerei. Diese digitalen Giganten zeichnen sich vor allem durch fünf charakteristische Kriterien aus: eine massive Skalierbarkeit (36 Prozent), Leistungsfähigkeit (34 Prozent), globale Verfügbarkeit (32 Prozent) und ein breites Portfolio (32 Prozent).

Im allgemeinen Sprachgebrauch sind hiermit meist US-amerikanische Cloud-Anbieter gemeint, allen voran Microsoft (50 Prozent), Google (46 Prozent), AWS (40 Prozent), IBM (37 Prozent) und Oracle (31 Prozent). Der Hyperscaler-Begriff hat sich so tief in das Bewusstsein der IT-Welt eingeprägt, dass er im Berufsalltag oftmals als Synonym sowohl für die genannten Unternehmen als auch für die Public Cloud als Ganzes verwendet wird.

Abbildung 8

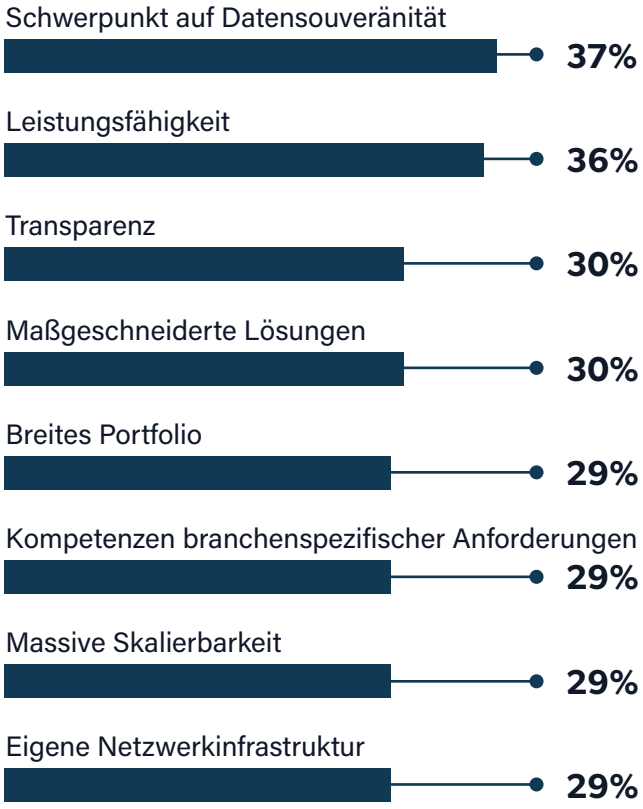
Kerneigenschaften eines Hyperscalers

Basis: 258 Unternehmen | Mehrfachantwort erlaubt

Abbildung 9

Kerneigenschaften eines Superscalers

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



Der Begriff „Superscaler" ist hingegen deutlich seltener bekannt, da der Begriff selbst erst relativ frisch ins Leben gerufen wurde. EuroCloud definiert Superscaler als regionale Antwort auf US-amerikanische Hyperscaler. Sie bieten ihre Cloud-Dienste meist mit einem regionalen, aber oft auch internationalen Fokus an – beispielsweise europaweit. Superscaler vertreiben im Vergleich zu Hyperscalern einen ähnlichen, zum Teil aber auch fokussierten Leistungsumfang bei gleicher Skalierbarkeit und legen verstärkt Wert auf den Datenschutz.

Angesichts der geopolitischen Situation sowie der bereits diskutierten Resilienzfaktoren gewinnen diese Cloud-Anbieter besonders an Relevanz. In einer Zeit, in der digitale Souveränität und strategische Unabhängigkeit zu Schlüsselfaktoren werden, bieten Superscaler eine Alternative, die sowohl technische Leistungsfähigkeit als auch regionale Verwurzelung verspricht. Sie sind der metaphorische David zu den amerikanischen Goliaths – sicherlich etwas kleiner, aber mit klar erkennbaren Vorteilen ausgestattet.

Deutsche Unternehmen bestätigen diese Einschätzung und sehen in Superscalern vor allem den Schwerpunkt auf Datensouveränität (37 Prozent) – ein direkter Gegenentwurf zu einer der grundlegenden Schwachstellen der Hyperscaler. Leistungsfähigkeit (36 Prozent) steht ebenfalls hoch im Kurs, beispielsweise auf Basis einer eigenen Netzwerkinfrastruktur, die eine massive Skalierbarkeit ermöglicht (jeweils 29 Prozent).

Besonders interessant ist die Betonung der Transparenz (30 Prozent) in Kosten und Prozessen – ein Aspekt, der an Hyperscalern oft bemängelt wird. Diese Kritik ist berechtigt, denn 64 Prozent der Befragten geben an, dass sie großen Wert auf Transparenz und Kontrolle über alle Abläufe sowie Zugriffe von Services und Infrastruktur legen. Hier klafft eine deutliche Lücke zwischen Anspruch und Realität bei den US-amerikanischen Anbietern.

Maßgeschneiderte Lösungen (30 Prozent) trotz eines breiten Portfolios (29 Prozent) runden das Profil ab. Diese scheinbare Paradoxie löst sich auf, wenn man die Kompetenzen bei branchenspezifischen Anforderungen und Regularien (29 Prozent) betrachtet. Superscaler sind in der Breite an den Angeboten von Hyperscalern angelehnt, bieten aber individuellere Möglichkeiten, um einen regionalen Fokus zu betonen – global gedacht, lokal gemacht.

Wer gilt als europäischer Superscaler?

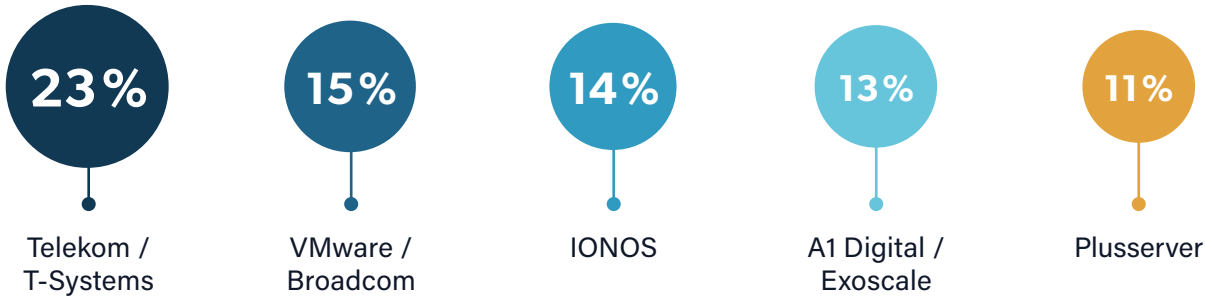
Auf Basis dieser Definition wurden vor allem international ausgerichtete Cloud-Anbieter mit starker Präsenz in Deutschland von den befragten Unternehmen als Superscaler eingestuft. An der Spitze steht die Telekom beziehungsweise T-Systems mit 23 Prozent, gefolgt von VMware/Broadcom (15 Prozent) und IONOS (14 Prozent). Weitere Kandidaten sind Fujitsu, STRATO, A1 Digital / Exoscale, Tencent, Bechtle und DATAGROUP (jeweils 13 Prozent) sowie Plusserver (11 Prozent).

Die im Vergleich zum Hyperscaler-Begriff deutlich gleichmäßigere Verteilung der Nennungen zeigt, dass in vielen Fällen die Größe und Bekanntheit des Cloud-Anbieters einen maßgeblichen Einfluss darauf hat, inwiefern er als ernstzunehmende Konkurrenz zu US-amerikanischen Hyperscalern wahrgenommen wird. Hier offenbart sich ein klassisches Henne-Ei-Problem: Ohne kritische Masse keine Wahrnehmung, ohne Wahrnehmung keine kritische Masse. Die Superscaler stehen somit vor der Herausforderung, nicht nur technisch zu überzeugen, sondern auch mental Marktanteile zu erobern.

Abbildung 10

Europäische Superscaler

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



5. Wo sind europäische Superscaler eine bevorzugte Alternative?

Die Frage nach den bevorzugten Einsatzgebieten europäischer Superscaler offenbart ein klares Muster: Deutsche Unternehmen setzen im Kern auf europäische Alternativen, wenn es um die Speicherung, Verarbeitung und Absicherung geschäftskritischer Daten geht. Hier zeigt sich das sprichwörtliche "Vertrauen ist gut, Kontrolle ist besser" in seiner reinsten Form – und Kontrolle bedeutet in diesem Kontext vor allem geografische und rechtliche Nähe, die ein Gefühl der Sicherheit und Greifbarkeit hervorruft.

Wo Europa besonders punktet

An der Spitze der bevorzugten Leistungen europäischer Cloud-Anbieter stehen mit leichtem Abstand Backup & Disaster Recovery (66 Prozent). Wenn das digitale Gedächtnis eines Unternehmens auf dem Spiel steht, wollen deutsche Firmen offenbar wissen, wo ihre Daten liegen und wer Zugriff darauf hat. Hier zahlt sich die regionale Verwurzelung der europäischen Superscaler aus.

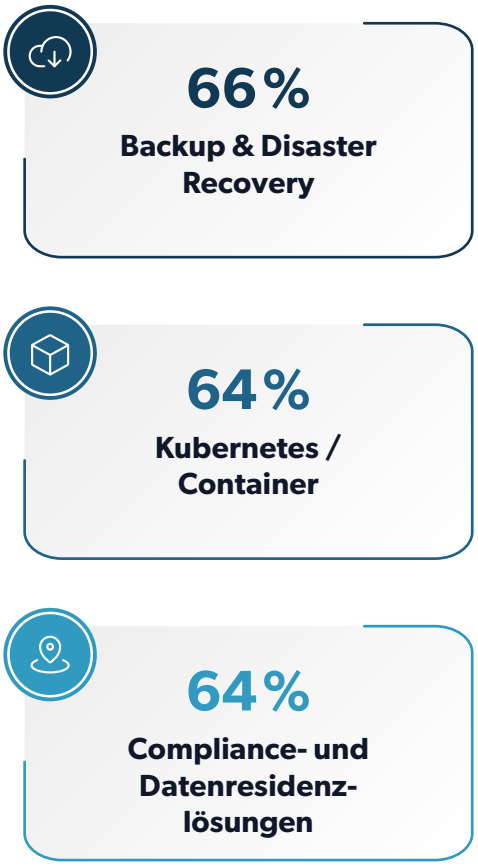
Dicht dahinter folgen Kubernetes- beziehungsweise Container-Lösungen mit 64 Prozent. Diese moderne Orchestrierungstechnologie ist das Rückgrat vieler digitaler Transformationsprojekte. Auch bei innovativen Technologien wollen Unternehmen nicht zwangsläufig auf US-amerikanische Hyperscaler setzen. Die Superscaler haben hier offenbar ihre Hausaufgaben gemacht und können technisch mithalten.

Compliance- und Datenresidenzlösungen komplettieren mit ebenfalls 64 Prozent das Spitzentrio. Hier liegt der Vorteil europäischer Anbieter auf der Hand: Sie kennen die regulatorischen Anforderungen von innen heraus und können maßgeschneiderte Lösungen anbieten, die von vornherein DSGVO-konform sind. Was bei Anbietern außerhalb des europäischen Raums oft ein nachgelagertes Add-on darstellt, ist hier Teil der DNA.

Abbildung 11

Top 3 Einsatzfelder europäischer Cloud-Anbieter

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



Weitere Schwerpunkte: Breite Präferenz für kritische Services

Die zusätzlichen Schwerpunktbereiche abseits der Top 3 zeigen, dass die Präferenz für Superscaler keineswegs auf Nischenbereiche beschränkt ist. Security-as-a-Service, einschließlich DDoS-Schutz und Firewalls, erreicht 63 Prozent – ein deutliches Signal, dass deutsche Unternehmen ihre Sicherheitsinfrastruktur lieber in europäische Hände legen möchten. Angesichts der steigenden Bedrohungslage durch Cyberangriffe aus dem nicht-europäischen Ausland ist dies mehr als verständlich.

Virtuelle Maschinen – ebenfalls mit 63 Prozent vertreten – bilden das Fundament vieler Cloud-Strategien. Da deutsche Unternehmen auch hier bevorzugt auf europäische Anbieter zurückgreifen möchten, liegt die Vermutung nahe, dass sich diese inzwischen auch bei den Grundlagen der Cloud-Infrastruktur nicht vor den Hyperscalern verstecken müssen. Hinsichtlich Datenanalyse und Data Warehousing (63 Prozent) – Bereiche, in denen sensible Geschäftsdaten verarbeitet werden und Datenschutz oberste Priorität hat – können europäische Anbieter dann zusätzlich ihre Stärken spielen lassen.

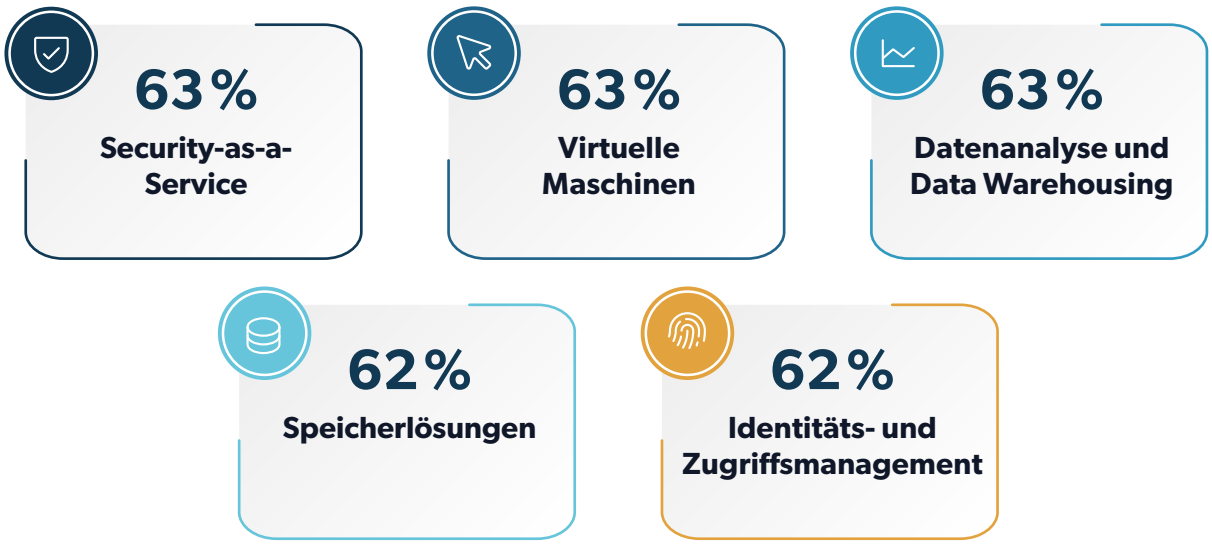
Speicherlösungen wie Object, File und Block Storage erreichen 62 Prozent und unterstreichen den bereits erwähnten Trend: Wenn es um die Aufbewahrung von Daten geht, setzen deutsche Unternehmen bevorzugt auf europäische Partner. Das Identitäts- und Zugriffsmanagement (IAM) rundet mit ebenfalls 62 Prozent die Liste ab – ein besonders sensibler Bereich, da hier die Schlüssel zum digitalen Königreich verwaltet werden.

Die durchweg hohen Werte in diesen Bereichen zeigen: Europäische Superscaler werden nicht als Notlösung oder Kompromiss betrachtet, sondern als vollwertige Alternative zu den amerikanischen Hyperscalern. Besonders dort, wo Vertrauen, Compliance und regionale Nähe eine Rolle spielen, haben sie die Nase vorn. In Sachen kritischer Infrastruktur setzen deutsche Unternehmen lieber auf Partner vor der eigenen Haustür.

Abbildung 12

Weitere bevorzugte Einsatzfelder europäischer Cloud-Anbieter

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



6. Worauf im Auswahlprozess besonders zu achten ist

Entscheidungskriterien

Zoomen wir etwas heraus: Auf der Meta-Ebene lässt sich erkennen, dass deutsche Unternehmen in jedem Bereich – mal mehr und mal weniger stark – europäische Clouds präferieren. Wenn dem so ist, warum dominieren europäische Anbieter nicht den deutschen Cloud-Markt? Es entsteht der Eindruck, dass es nicht gelingt, den richtigen Fit zu finden, um den Sprung in die Unabhängigkeit von US-amerikanischen Clouds zu wagen. Umso wichtiger ist es, die richtigen Kriterien herauszuarbeiten, anhand derer sich der passende Partner finden lässt.

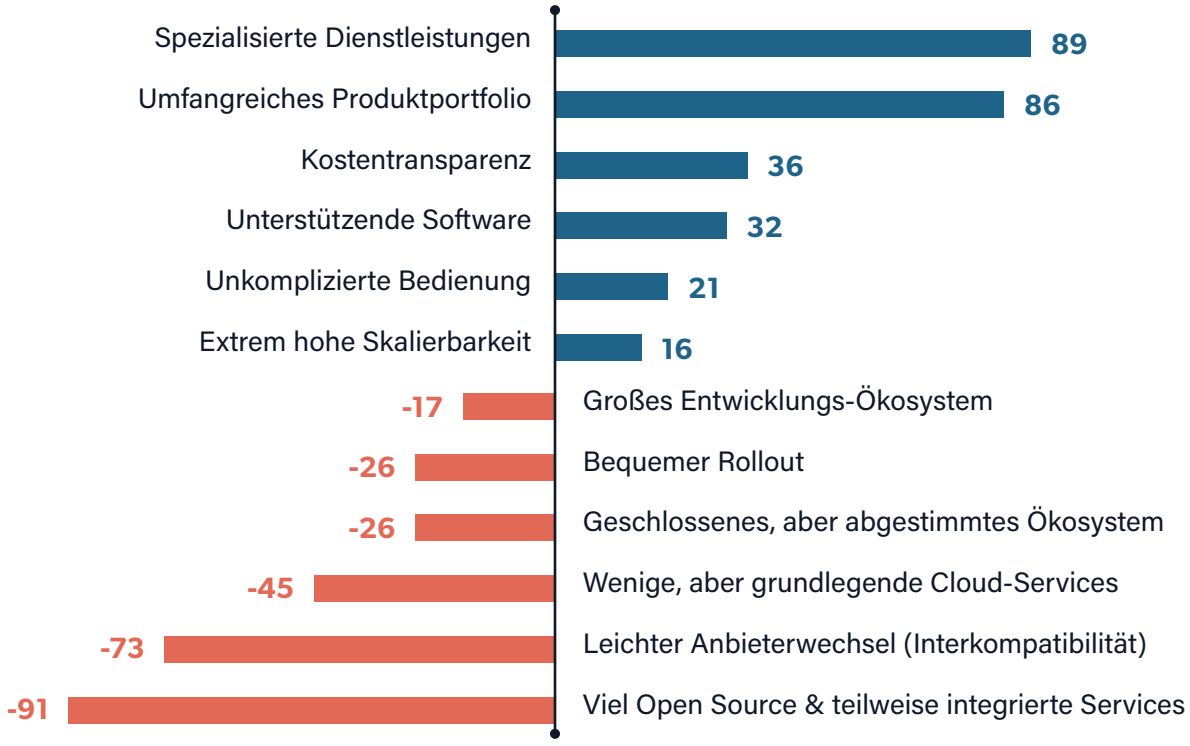
Um die Bedeutung verschiedener Eigenschaften im Auswahlprozess zueinander in Relation zu setzen, wurde das Maximum Difference Scaling verwendet. Bei diesem Verfahren müssen die Befragten in mehreren Durchläufen aus einer zufällig zusammengestellten Auswahl von vier Eigenschaften sowohl die wichtigste als auch die unwichtigste Eigenschaft auswählen. Diese Methode zwingt zu klaren Prioritäten und verhindert so, dass alle Kriterien als "sehr wichtig" eingestuft werden – ein typisches Problem bei klassischen Bewertungsskalen.

Die Ergebnisse sind aufschlussreich: Spezialisierte Dienstleistungen für Bereiche wie KI oder Data Analytics sowie ein umfangreiches Produktportfolio sind demnach im Auswahlprozess eines geeigneten Partners mit großem Abstand am relevantesten. Deutsche Unternehmen wollen also nicht nur einen Cloud-Anbieter, sondern einen strategischen Partner, der sowohl in die Breite als auch in die Tiefe gehen kann – gleichzeitig Generalist und Spezialist.

Abbildung 13

Bedeutung der Eigenschaften im Auswahlverfahren

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



Vor allem der Blick ans untere Ende der Prioritätenliste verspricht spannende Einblicke: Eine offene Architektur, die meist mit Open Source sowie teilweise integrierten Services einhergeht, und ein leichter Anbieterwechsel sind die mit Abstand am seltensten betonten Auswahlkriterien. Hier offenbart sich ein interessanter Widerspruch: Während in den vorherigen Kapiteln Multi-Cloud-Strategien und die Vermeidung von Vendor Lock-in als wichtige Trends identifiziert wurden, scheinen diese Aspekte bei der konkreten Anbieterauswahl eine untergeordnete Rolle zu spielen. Die tatsächliche Notwendigkeit eines Anbieterwechsels wird oft als eher unwahrscheinlich eingestuft, obwohl die drastischen Konsequenzen im konkreten Eintrittsfall durchaus wahrgenommen werden. Es ist, als würde man theoretisch die Wichtigkeit von Notausgängen betonen, aber bei der Hotelauswahl trotzdem hauptsächlich auf die Zimmerausstattung achten.

Ein bequemer Rollout ist überraschenderweise ebenfalls weniger relevant für den Auswahlprozess. Stattdessen liegt das Augenmerk verstärkt auf Kostentransparenz, allgemein unterstützender Software sowie einer unkomplizierten Bedienung, die keine zusätzliche Beratung erfordert. Dies spiegelt den Pragmatismus deutscher IT- und Business-Verantwortlichen wider: Man will Lösungen, die funktionieren, transparent sind und nicht unnötig kompliziert werden.

Best Practices

Um den theoretischen Erkenntnissen dieser Studie eine praktische Dimension zu verleihen, wurden die Teilnehmenden in einer offenen Frage direkt dazu befragt, welche drei Tipps sie Unternehmen geben würden, die ihre Cloud-Strategie so resilient wie möglich umsetzen wollen. Die Antworten liefern einen ungeschminkten Einblick in die Praxis und zeigen, wo der Schuh wirklich drückt:

An der Spitze steht unangefochten das Thema Sicherheit und Compliance, das von über der Hälfte der Befragten (52 Prozent) als entscheidend eingestuft wird. Genannt werden unter anderem eine starke Verschlüsselung, Rollen- und Identitätsmanagement (IAM), Zero Trust, Penetrationstests und regulatorische Compliance. Ein Teilnehmer bringt es auf den Punkt: “Sicherheit und Compliance von Anfang an priorisieren” – Sicherheit ist kein Nachgedanke, sondern muss von Anfang an mitgedacht werden.

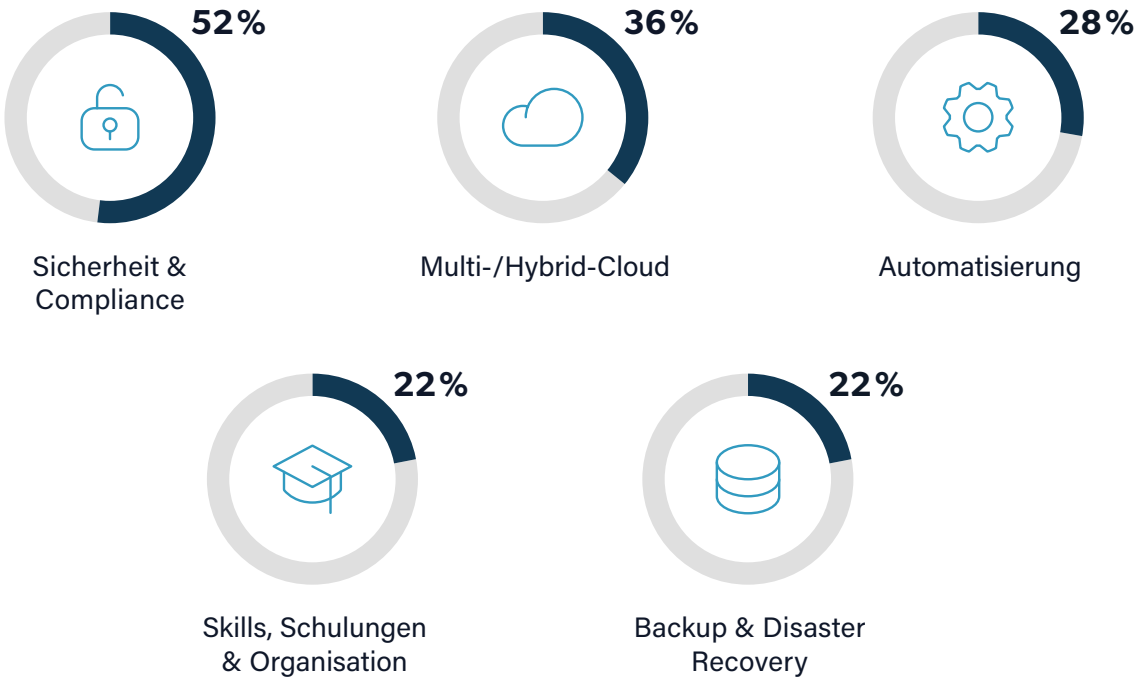
Deutlich mehr als ein Drittel der Expertinnen und Experten (36 Prozent) empfiehlt explizit Multi- oder Hybrid-Cloud-Strategien, vor allem zur Vermeidung von Vendor Lock-in und zur Erhöhung der Ausfallsicherheit. “Kombinieren Sie mehrere Cloud-Anbieter” lautet eine beispielhafte Empfehlung. Dies spielgelt die praktische Umsetzung der bereits diskutierten strategischen Trends wider.

Während Multi-Cloud-Strategien und die Vermeidung von Vendor Lock-ins als wichtige Trends gelten, spielen offene Architekturen und einfacher Anbieterwechsel bei der Anbieterauswahl kaum eine Rolle.

Abbildung 14

Themenfelder einer resilienten Cloud-Strategie aus der Praxis

Basis: 258 Unternehmen | Mehrfachantwort erlaubt



28 Prozent der Befragten sehen wiederum in Automatisierung und Infrastructure as Code zentrale Hebel für Resilienz. Terraform, CloudFormation, Orchestrierung, Self-Healing und Auto-Scaling werden als konkrete Werkzeuge genannt. "Automatisieren Sie alles, einschließlich Failover- und Wiederherstellungsverfahren" – dieser Rat zeigt, dass Automatisierung nicht nur Effizienz, sondern auch Verlässlichkeit bedeutet.

Etwa jede oder jeder fünfte Befragte (22 Prozent) betont die menschliche Komponente: Skills, Schulungen, klare Verantwortlichkeiten und "Resilienz als gemeinsame Verantwortung". Technologie allein macht noch keine Resilienz – es braucht Menschen, die wissen, was zu tun ist. Klar abgegrenzte Aufgaben und offensiv kommunizierte Pläne sind hier entscheidend. Ein Teilnehmer formuliert dies kurz und schmerzlos: "Verantwortlichkeiten und Prozesse klar definieren."

Ebenso viele Verantwortliche (22 Prozent) nennen Backup und Disaster Recovery als essentiellen Tipp für eine resiliente Cloud-Strategie – inklusive Replikation, DR-Runbooks und klar definierte Recovery Point und Recovery Time Objectives (RPO/RTO). "Implementierung von automatisierten Disaster-Recovery-Lösungen" ist eine häufige Empfehlung, die vor allen Dingen verdeutlicht, dass der Worst Case durchdacht und geübt werden muss.

Die Stimmen aus der Praxis bestätigen in ihrer Gesamtheit die strategischen Erkenntnisse dieser Studie: Resilienz ist kein Zufallsprodukt, sondern das Ergebnis durchdachter Planung, konsequenter Umsetzung und kontinuierlicher Verbesserung. Wer diese Lektionen beherzigt, ist für die Unwägbarkeiten der digitalen Zukunft gut gerüstet.

Die Praxis zeigt: Resilienz entsteht durch eine gut durchdachte Planung und konsequente Umsetzung. Nur eine Kombination aus Technologie, Mensch und Prozessen gilt als zukunftssicherer Ansatz.

7. Fazit

Die fünfte Ausgabe des EuroCloud Pulse Check zeichnet das Bild einer deutschen Cloud-Landschaft im Wandel – und dieser Wandel ist mehr als nur eine technische Evolution. Wir erleben einen fundamentalen Paradigmenwechsel hin zur strategischen Unabhängigkeit, der die Art und Weise, wie Unternehmen über ihre digitale Infrastruktur denken, von Grund auf verändert.

Die Hybrid Cloud dominiert mit 57 Prozent nicht nur die aktuelle Nutzung, sondern spiegelt eine bewusste Orchestrierung verschiedener Cloud-Modelle wider. Unternehmen setzen nicht mehr auf das Prinzip "einer für alles", sondern auf strategische Verteilung ihrer digitalen Assets. Der Multi-Cloud-Trend verstärkt sich zusätzlich und zeigt: Diversifikation gegen Vendor Lock-in ist nur eines von vielen Motiven. Dahinter stecken oft durchdachte Datensouveränitäts- und Resilienzstrategien – und natürlich auch Kostenoptimierung. Wer seine Eier auf verschiedene Körbe verteilt, schläft ruhiger.

Die strategische Bedeutung von Cloud-Souveränität steigt kontinuierlich, und die Zahlen sprechen eine deutliche Sprache: 57 Prozent der Unternehmen zeigen sich verunsichert durch die US-Außenpolitik unter Trump. Geopolitische Krisen fungieren damit als Katalysator für eine europäische Cloud-Emanzipation. Gleichzeitig fühlen sich 68 Prozent inzwischen gut auf zukünftige unsichere Wirtschaftslagen vorbereitet – ein Selbstbewusstsein, das zeigt: Die Lektionen der vergangenen Krisen sind angekommen.

Europäische Superscaler etablieren sich zunehmend als Alternative zu US-Hyperscalern und punkten mit regionalen Stärken. Der Fokus eines Superscalers liegt per Definition auf Datensouveränität, Transparenz und maßgeschneiderten Lösungen – genau das, was deutsche Unternehmen in unsicheren Zeiten suchen. Bevorzugt werden sie in geschäftskritischen Bereichen wie Backup & Disaster Recovery oder Compliance-Lösungen, wo Vertrauen und rechtliche Sicherheit oberste Priorität haben.

Die praktische Umsetzung nimmt endlich Fahrt auf: Regelmäßige Sicherheitsprüfungen sind deutlich gestiegen, Datenverschlüsselung und Datenqualitätssicherung stehen im Fokus der Unternehmen. Interessant sind die branchenspezifischen Ansätze: Die Industrie fährt breit auf, der Handel delegiert Verantwortung an spezialisierte Rollen, und der Public Sector setzt konsequent auf Open Source. Jede Branche findet ihren eigenen Weg zur digitalen Souveränität.

Dennoch bleiben Herausforderungen bestehen, die nicht von der Hand zu weisen sind. Es klafft weiterhin eine Lücke zwischen der Präferenz für europäische Anbieter und der tatsächlichen Marktdominanz amerikanischer Hyperscaler. Spezialisierte Services und Portfolio-Breite erweisen sich als wichtigste Auswahlkriterien, während Kostentransparenz wichtiger ist als offene Architektur oder einfacher Anbieterwechsel. Hier zeigt sich: Zwischen strategischen Absichten und operativen Entscheidungen liegt manchmal noch ein weiter Weg.

Dennoch: Die Zukunft klingt europäisch. Was wir beobachten, ist mehr als nur ein Trend – es ist eine strategische Revolution. Cloud-Unabhängigkeit entwickelt sich von einer theoretischen Überlegung zu einer praktischen Notwendigkeit. Europäische Superscaler positionieren sich dabei als Dirigenten einer neuen digitalen Ära, in der regionale Stärken, rechtliche Sicherheit und technische Exzellenz Hand in Hand gehen.

Der EuroCloud Pulse Check 2025 zeigt: Deutsche Unternehmen haben verstanden, dass digitale Souveränität kein Luxus, sondern eine Existenzfrage ist. Wer heute die Weichen richtig stellt, wird morgen nicht nur resilient, sondern auch souverän agieren können. Die europäische Cloud-Landschaft steht vor einer spannenden Zukunft – und diese Zukunft hat bereits begonnen.

Studiendesign und Stichprobe

Die Studie „Digitale Resilienz made in Europe: Strategien für eine souveräne Cloud-Zukunft“ wurde im Rahmen des EuroCloud Pulse Check 2025 von der tech**consult** GmbH im Auftrag der EuroCloud-Mitglieder A1 Digital, IONOS sowie Plusserver konzipiert und durchgeführt. Insgesamt wurden 258 IT- sowie Business-Verantwortliche aus deutschen Unternehmen ab 50 Beschäftigten nach Status quo und Zukunft ihrer Cloud-Strategie, dem Einfluss geopolitischer Unsicherheiten sowie den Kernthemen Souveränität und Resilienz auf ebendiese. Das Studiendesign ermöglicht Blickwinkel aus unterschiedlichen Aufgabenfeldern – von IT-Security und Cloud-Architektur über Compliance bis hin zum thematischen Schwerpunkt der diesjährigen Ausgabe: Souveränität und Resilienz.

Segmentverteilung der Stichrobe

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen

	Gesamt
Industrie	**31%**
Handel	**9%**
Dienstleistung	**41%**
Banken und Versicherung	**9%**
Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen	**9%**

Größenklassenverteilung der Stichprobe

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen

	Gesamt
50 bis 249 Beschäftigte	**22%**
250 bis 499 Beschäftigte	**19%**
500 bis 999 Beschäftigte	**29%**
1.000 oder mehr Beschäftigte	**31%**

Positionsverteilung der Stichprobe

Basis: 258 Unternehmen | Durch Rundungsdifferenzen kann die Summe der Prozentwerte unter Umständen von 100 abweichen

	Gesamt	
Vorstand / Geschäftsführung	9%	Management
Chief Information Officer (CIO) / Chief Technology Officer (CTO) / IT-Leitung	25%	Management
Resilienzmanagement (CRO, Head of Business Continuity usw.)	1%	Management
Chief Compliance Officer (CCO) / Leitung Compliance	4%	Management
Compliance Management / Specialist / Analyst	4%	Management
Controlling	2%	Management
CDO / Projektleitung Digitalisierung	1%	Management
Fachbereichsleitung, Projektleitung	2%	Management
Produktmanagement	3%	Management
Leitung IT-Infrastruktur / RZ	9%	IT-Mitarbeitende
Applikationsverantwortliche	1%	IT-Mitarbeitende
Leitung Software-Entwicklung	2%	IT-Mitarbeitende
IT-Management	25%	IT-Mitarbeitende
Software-/App-Entwicklung	2%	IT-Mitarbeitende
Software-Architekt	2%	IT-Mitarbeitende
IT-Systemadministration / Network Engineering	3%	IT-Mitarbeitende
Cloud-Architektur	3%	IT-Mitarbeitende
IT-Security-Spezialist/-Spezialistin	2%	IT-Mitarbeitende
Data Scientist	1%	IT-Mitarbeitende

EXOSCALE
member of | A1 Digital

Wie souverän sind wir?

Digitale Souveränität ist ein wesentlicher Erfolgsfaktor für Sicherheit, Resilienz und Innovation. Dennoch ist dies für europäische Unternehmen aktuell eine immense Herausforderung. Dr. Elisabetta Castiglioni, CEO der A1 Digital, sieht jedoch eine große wirtschaftliche Chance für Unternehmen.

Digitale Souveränität ist in aller Munde, aber was bedeutet das für A1 Digital?

Elisabetta Castiglioni: Bereits vor den aktuellen Ereignissen war „Digitale Souveränität" für A1 Digital ein zentrales Thema. Hierbei sehen wir Souveränität kurzgefasst als die Fähigkeit und das Bewusstsein von Unternehmen, selbstbestimmt entscheiden zu können und in einem selbst definierten Rahmen unabhängig zu agieren. Im digitalen Kontext sehen wir hierbei insbesondere kritische digitale Infrastruktur als zentrales Element in Form von Cloud, IoT Konnektivität, privaten Netzwerken und Cyber Security. Hierbei haben wir schon seit 2017 unsere souveräne europäische Cloud Exoscale aufgebaut und haben somit eine wichtige europäische Alternative geschaffen.

Welche Risiken und Chancen sehen Sie bezüglich digitaler Souveränität?

Elisabetta Castiglioni: Wenn europäische Unternehmen keine gezielten Maßnahmen zur digitalen Souveränität ergreifen, könnten Risiken für ihre wirtschaftliche Stabilität entstehen, da die Abhängigkeit von nicht-europäischen Technologieanbietern strategische Innovation und Entwicklungen einschränkt. Mit der zunehmenden Digitalisierung von Wertschöpfungsketten stellt diese ein Risiko für die Wettbewerbsfähigkeit und somit auch für den Wohlstand Europas dar. Daher müssen wir in Europa unsere Talente und unser Wissen in Kerntechnologien der Zukunft besser bündeln. Eine engere geographische Zusammenarbeit aus Forschung, Entwicklung und Wirtschaft sehen wir als große Chance, um digitale europäische Innovationen und somit Investitionen langfristig wirtschaftlicher erfolgreicher zu machen.

Was bedeutet die Vision Ihres Unternehmens „Leading to A Sovereign Digital Future – together“?

Elisabetta Castiglioni: Die A1 Digital ist ein verlässlicher Partner mit dem Ziel, unseren Kunden einen Weg zu einer souveränen digitalen Zukunft zu zeigen und gemeinsam die Reise dorthin zu bestreiten. Mit unserem Portfolio ermöglichen wir unseren Kunden, einen Großteil der Komplexität an uns abzugeben und gemeinsam eine digitale Infrastruktur für Innovation aufzubauen. Für ein Raffinerie Unternehmen in Deutschland haben wir als Partner gemeinsam eine digitale Lösung zur Überwachung von Teilen der Produktionsanlage entwickelt - angefangen von der vollständigen IoT Systemlösung inklusive Konnektivität bis hin zur Softwareplattform auf unserer Exoscale Cloud. Zudem hat das Unternehmen durch unsere hohe Kundennähe ein Verständnis für Digitalisierung entwickelt und somit die Basis für weitere souveräne digitale Entwicklungen in der Zukunft.

Dr. Elisabetta Castiglioni
CEO, A1 Digital

Über A1 Digital Deutschland GmbH

“Leading to a Sovereign Digital Future – Together”

A1 Digital ist ein europäischer Partner für digitale Infrastruktur und Lösungen mit dem Ziel, Unternehmen gemeinsam in eine souveräne digitale Zukunft zu führen.

Zu den Angeboten gehören Exoscale – eine europäische Cloud-Plattform, Managed Connectivity in über 180 Ländern, vertikale IoT Branchenlösungen mit Erfahrung von über 1 Million ausgelieferten Geräten und skalierbare Netzwerklösungen, ergänzt durch 24/7 Managed Cyber Security Services auf Telco-Niveau. Exoscale ist Mitglied von A1 Digital, wurde 2011 gegründet und gehört zur Telekom Austria Group. Der Cloudanbieter mit Sitz in der Schweiz und Rechenzentren in fünf europäischen Ländern unterstützt Unternehmen und Engineers ihre Workloads und Anwendungen sicher in der Cloud zu betreiben. Mit der benutzerfreundlichen, zuverlässigen und performanten Cloud-Plattform ist Exoscale der ideale Partner für Cloud-native Anwendungen. Der Fokus auf Sicherheit und Datenschutz ermöglichet zudem eine reibungslose und DSGVO-konforme Nutzung der Cloud.

A1 Digital Deutschland GmbH
c/o Unicorn
Rosenheimer Straße 116
81669 München

Wolfgang Brücker
Senior Partner Manager Exoscale
Telefon: +49 1743143407
Mail: **wolfgang.bruecker@a1.digital**

Web: **https://www.a1.digital/de/europaeische-cloud/**
E-Mail: **info@a1.digital**

EXOSCALE
member of A1 Digital

IONOS

Warum europäische Datensouveränität kein Luxus, sondern Voraussetzung ist

Ein Statement von IONOS zur souveränen Cloud-Zukunft in Europa

Europäische Datensouveränität ist keine Zukunftsvision, sondern eine operative Notwendigkeit. Sie ermöglicht die unabhängige Kontrolle über digitale Infrastrukturen – technisch, rechtlich und operativ. Wer heute souverän handelt, stärkt nicht nur seine digitale Resilienz, sondern sichert langfristige Innovations- und Wettbewerbsfähigkeit.

Trotz wachsender Sensibilität ist Europa noch immer auf außereuropäische Cloud-Infrastrukturen angewiesen. Ein Vorfall mit geopolitischer Tragweite hat dies deutlich gemacht: Nachdem der Internationale Strafgerichtshof gegen US-Soldaten ermittelte, wurde dem Chefankläger durch einen US-Dienstleister der Zugriff auf sein E-Mail-Konto verweigert – infolge politischen Drucks. Dieser Eingriff zeigt, wie schnell digitale Infrastrukturen zu geopolitischen Hebeln werden können.

Der Schlüssel zur Unabhängigkeit liegt in souveränen Cloud-Lösungen, die europäischen Rechtsrahmen, technologische Transparenz und Anbieterneutralität vereinen. Entscheidend ist:

- **Datenverarbeitung nach europäischem Recht**
- **Schutz vor extraterritorialen Zugriffsrechten wie dem US Cloud Act oder dem FISA**
- **Transparente, interoperable Technologien ohne Anbieterbindung**
- **Kontrolle über Speicherung, Zugriff und Migration von Daten**
- **Und nicht zuletzt: der Aufbau einer zukunftsweisenden IT-Industrie in Deutschland und die Stärkung der lokalen Wertschöpfung**

Europäische Initiativen setzen neue Standards

Mit Projekten wie IPCEI-CIS, dem EuroStack-Ökosystem oder der gemeinsam von IONOS, Aruba und Dynamo entwickelten SECA-API (Sovereign European Cloud API) entstehen derzeit neue Standards. Die SECA-API erlaubt die anbieterübergreifende Verwaltung von Cloud-Infrastrukturen auf Basis eines offenen, überprüfbaren Standards

Umsetzung auf Unternehmensebene: Schritte zu mehr Datensouveränität

Organisationen, die europäische Datensouveränität aktiv umsetzen möchten, können konkrete Maßnahmen ergreifen:

- **Bestehende Cloud-Verträge auf Verlagerungsklauseln und Zugriffsrechte prüfen.**
- **Infrastrukturentscheidungen an Compliance, Transparenz und Reversibilität ausrichten**
- **Anbieter bevorzugen, die in der EU entwickeln, betreiben und rechtlich verankert sind.**
- **Sicherheitskonzepte überprüfen, Exit-Strategien etablieren, Open-Source nutzen.**

Europäische Datensouveränität ist Voraussetzung – keine Option

Als zuverlässiger europäischer Cloud-Anbieter bietet IONOS nicht nur ein souveränes Produktportfolio, sondern Souveränität auf allen Ebenen. Die gesamte Infrastruktur ist in Europa verwurzelt: entwickelt, betrieben und rechtlich abgesichert nach EU-Standards. Kundendaten werden ausschließlich in ISO-27001-zertifizierten Rechenzentren in Deutschland und der EU verarbeitet – ohne Zugriff durch Drittländer, geschützt vor extraterritorialen Gesetzen wie dem US CLOUD Act.

Die Plattform basiert auf einem eigenen Tech-Stack – inklusive eigener IaaS-Plattform, eigener Rechenzentren, eigener Netzwerkarchitektur. Diese technologische Unabhängigkeit ist ein strategischer Vorteil für Unternehmen, die auf Resilienz, Kontrolle und Compliance angewiesen sind.

Digitale Souveränität ist kein Luxus. Sie ist Grundlage für Selbstbestimmung, Resilienz und vertrauenswürdige Digitalisierung „Made in Europe“.

Daniel Benad
Advisor Alliance Partnerships Strategy & Planning

Über IONOS SE

IONOS ist der führende europäische Digitalisierungs-Partner für kleine und mittlere Unternehmen sowie den öffentlichen Sektor. IONOS hat rund 6,4 Millionen Kundinnen und Kunden. Die selbst entwickelte souveräne Cloud-Plattform von IONOS mit mehr als 100.000 Servern läuft verteilt auf sieben Rechenzentren in Deutschland und 18 weiteren in Europa. IONOS wird regelmäßig staatlich geprüft und zertifiziert – inklusive C5-Testat, ISO 27001 und BSI IT-Grundschutz-Zertifizierung – und bietet sicheren Datenschutz und 100 % DSGVO-Konformität.

Mit Hauptsitz in Deutschland betreibt IONOS alle Dienste unter deutscher Jurisdiktion. Die Daten bleiben im Hoheitsgebiet Deutschlands – ausländische Dienste und Drittstaaten haben keinen Zugriff. So erhalten Kundinnen und Kunden vollständige digitale Souveränität und maximale Rechtssicherheit.

IONOS SE
Revaler Str. 30
10245 Berlin

Erez Tetelmann
Director B2B Cloud Marketing
Mail: **cloud-marketing@ionos.com**
Web: **https://cloud.ionos.de**

IONOS

Keine Souveränität - keine Resilienz!

plusserver als Partner für digitale Handlungsfähigkeit

Die vorliegende Studie macht deutlich: Digitale Resilienz ist kein optionales Ziel mehr, sondern ein zwingender Erfolgsfaktor. Wer digitale Abhängigkeiten in Kauf nimmt, gefährdet nicht nur seine Wettbewerbsfähigkeit, sondern die Zukunftsfähigkeit des gesamten Unternehmens. In Zeiten geopolitischer Unsicherheit braucht es eine Cloud-Strategie, die Sicherheit, Skalierbarkeit und Souveränität gleichermaßen vereint.

IT-Ausfallsicherheit durch deutsche Rechenzentren

Genau hier setzen wir bei plusserver an. Mit unseren zertifizierten Rechenzentren in Köln, Düsseldorf und Hamburg schaffen wir die Grundlage für höchste Ausfallsicherheit. Georedundanz nach BSI-Standard, n+1-Architekturen sowie umfassende Backup- und Disaster-Recovery-Lösungen sorgen dafür, dass Unternehmen ihren Betrieb auch dann fortführen können, wenn das Unvorhersehbare eintritt. Auch die vorliegende Untersuchung bestätigt: IT-Ausfallsicherheit zählt heute zu den fünf entscheidenden Kriterien digitaler Resilienz.

Cybersecurity und Cloud Services aus einer Hand

Resilienz geht jedoch über reine Redundanz hinaus. IT-Sicherheit gilt als digitales Immunsystem. Hier hat plusserver mit der Integration der Cosanta GmbH als eigenständige Tochtergesellschaft 2025 einen strategischen Meilenstein geschaffen: Gemeinsam mit dem deutschen Managed Security Service Provider bieten wir IT-Security und Cloud Services aus einer Hand – verlässlich, auditierbar und „Made in Germany". Unseren Kunden ermöglichen wir damit einen effektiven Schutz des operativen IT-Betriebs vor Cyberrisiken sowie Compliance mit der gültigen Regulatorik gemäß den Anforderungen des BSI. In der Analyse gilt das Thema Cybersicherheit als wichtiger Baustein einer robusten IT-Infrastruktur.

Flexibilität als Schlüssel zur Handlungsfähigkeit

Ebenso entscheidend für digitale Resilienz ist Flexibilität. Das bedeutet: Unternehmen müssen ihre Infrastruktur im Moment des Bedarfs anpassen können – in der Regel schneller, als es klassische IT erlaubt. Mit unserem neuen Self-Service-Shop ermöglichen wir die sofortige Buchung und Skalierung von Cloud-Ressourcen. Diese Konsumierbarkeit stärkt die Handlungsfähigkeit von Unternehmen, weil sie ohne Umwege auf neue Anforderungen reagieren können.

Abhängigkeiten reduzieren & Innovationskraft sichern

Was plusserver von globalen Hyperscalern unterscheidet, ist unser konsequenter Fokus auf Souveränität. Wir sind ein Cloud-Provider „Made in Germany“ mit dem Anspruch, Unabhängigkeit und Wahlfreiheit zu sichern. Mit der pluscloud open bieten wir die erste produktive Open Source Cloud auf Basis des Sovereign Cloud Stacks an, entwickelt für maximale Transparenz und Datenschutz. Ergänzend steht mit der pluscloud VMware eine Public Enterprise Cloud auf Industriestandard zur Verfügung, die als Sovereign Cloud von VMware/Broadcom ausgezeichnet ist. Gemeinsam mit Services wie Managed Kubernetes, Datenbanken und Storage entsteht so ein Ökosystem, das sowohl Skalierbarkeit als auch einfache Wechselmöglichkeiten bietet – und damit genau jene Interoperabilität, die die Studie als strategische Absicherung gegen Vendor Lock-ins hervorhebt.

Der Anspruch von plusserver ist es, Kunden nicht nur in die Cloud zu begleiten, sondern ihnen eine Plattform zu geben, auf der sie resilient und souverän agieren und ihre Innovationskraft entfalten können – heute und in Zukunft. Resilienz ist keine kurzfristige Reaktion auf Krisen, sondern die Voraussetzung für nachhaltige digitale Transformation. plusserver setzt sich dafür ein, diese Resilienz in Europa sichtbar zu machen und mitzugestalten.

Andreas Kadler
CEO, plusserver

Über plusserver GmbH

plusserver ist ein Cloud-Provider mit der Digitalisierungsplattform „Made in Germany“. Schritt für Schritt begleitet plusserver Unternehmen aus dem Mittelstand sowie Konzerne bei ihrer IT-Modernisierung. Neben einem eigenen Cloud-Produktportfolio aus eigenen zertifizierten deutschen Rechenzentren, 24/7-Support in deutscher oder englischer Sprache sowie umfassenden Managed Services zeichnet plusserver der Grundsatz für Datensouveränität und Interoperabilität aus. plusserver war das erste Unternehmen, das mit der pluscloud open eine Open Source Cloud produktiv umgesetzt hat, die vollständig auf dem Sovereign Cloud Stack basiert und so den höchsten Datenschutzstandards entspricht.

plusserver GmbH
Welserstr. 14
51149 Köln

Tanja Sessinghaus
Marketing / Communications
Telefon: +49 174 2810523
Mail: **Tanja.Sessinghaus@plusserver.com**
Web: **www.plusserver.com**

plusserver

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group

Informationen zur Studie

Autor der Studie

Pascal Brunnert
Senior Analyst

Telefon: +49 561 8109 176
E-Mail: pascal.brunnert@techconsult.de

Impressum

techconsult GmbH
Baunsbergstr. 37
34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Mail: **info@techconsult.de**
Web: **www.techconsult.de**

Über techconsult GmbH

Seit über 30 Jahren ist tech**consult** – als Research- und Analystenhaus – ein verlässlicher Partner für Anbieter und Nachfrager digitaler Technologien und Services. Mehr als 35.000 Interviews/Jahr mit Entscheidern, auf der Business- und Technologie-Ebene, Lösungsanwendern sowie Technologie- und Serviceanbietern, bilden die neutrale Grundlage unserer Beratungs- und Projektaktivitäten.

So werden Nachfrager in ihrer digitalen Standortbestimmung und strategischen Planung ebenso unterstützt, wie in konkreten Sourcing-Prozessen, um fundierte Entscheidungen auf Basis datengestützter Fakten zu treffen. In der Entwicklung und Umsetzung individueller Go-To-Market-Strategien, profitieren Anbieter sowohl strategisch als auch taktisch von der marktorientierten Unterstützung unserer Analysten und des tc-Partnernetzwerks.

In Zusammenarbeit mit

EuroCloud DEUTSCHLAND eco

Kontakt

EuroCloud Deutschland_eco e. V.
Lichtstraße 43h
50825 Köln

E-Mail: info@eurocloud.de
Telefon: +49 221 7000 48 0

Mehr erfahren

Über EuroCloud Deutschland_eco e. V

EuroCloud Deutschland_eco e. V. ist der Verband der Cloud-Computing-Wirtschaft. Er setzt sich für Akzeptanz und bedarfsgerechte Bereitstellung von Cloud Services am deutschen Markt ein sorgt mit Orientierungshilfen, praxisnahen Empfehlungen und Events dafür, dass Anwender und Anbieter von Cloud Services passgenau zusammenfinden. Zudem unterstützt EuroCloud bei zahlreichen Fragen rund um Datenschutz und Sicherheit, Interoperabilität und Standards sowie Recht und Compliance. Unter dem Dach des Verbands agiert die Initiative EuroCloud Native (ECN). Sie versteht sich als Anlaufstelle und Fachforum für Dienstleister und Lösungsanbieter, die sich auf Technologien fokussieren, die originär für die Cloud entwickelt wurden.

Eine Studie von

techconsult
TECHNOLOGY MARKET ANALYSTS
EIN UNTERNEHMEN DER heise group

Unterstützt durch

EuroCloud
DEUTSCHLAND eco

Impressum

techconsult GmbH
Baunsbergstr. 37
34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Mail: info@techconsult.de
Web: www.techconsult.de