

STUDIE

DIGITALE SOUVERÄNITÄT 2026

**T Systems****8COM**
CYBER SECURITY**easy**
by conrizon**plusserver** **baramundi**



Ein aktuelles Studienprojekt von
CIO und COMPUTERWOCHE

Platin-Partner



Gold-Partner



Silber-Partner



Partner



Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen übernehmen, die auf fehlerhafte Informationen zurückzuführen sind.

Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch den Herausgeber.

Souveränität im Datenzeitalter: Was bedeutet das eigentlich?



Matthias Teichmann
Director Research

Lange haben deutsche Unternehmen gezögert, das Rechenzentrum im Keller einzumotten und in die Cloud zu migrieren. Inzwischen hat sich einiges getan: Deutsche Unternehmen liegen bei der Cloud-Nutzung im europäischen Durchschnitt. Und die meisten dieser Unternehmen würden zustimmen, dass die Cloud viele Vorteile hat und wirtschaftlich sinnvoll ist.

Trotzdem bietet das Thema noch immer reichlich Stoff für politische Diskussionen. Es geht um digitale Souveränität. Doch worin genau besteht das Problem? Geht es um Daten? Um Technologie? Um Abhängigkeiten? Oder darum, wer Zugriff auf die Informationen hat?

Die Unternehmen nutzen Cloud-Dienste, sie beziehen Anwendungen als Service, und sie speichern ihre Daten in der Cloud – meist in Rechenzentren innerhalb der EU, häufig jedoch bei amerikanischen Anbietern, den sogenannten US-Hyperscalern. Hätte man die freie Wahl, sähe das anders aus.

Lange galt es nur als ein Randthema, doch die Realität à la Snowden hat uns eingeholt: Seine Enthüllungen haben gezeigt, dass Überwachung keine theoretische Gefahr ist. Der US Cloud Act hat deutlich gemacht, dass rechtliche Grenzen virtuell sein können, wenn die Hard-

ware auf fremdem Boden steht. Und geopolitische Spannungen, die lange nur eine abstrakte Gefahr darstellten, haben längst konkrete Auswirkungen auf IT-Entscheidungen.

Eines ist klar: Digitale Souveränität ist komplex. Es bedarf größerer und kleinerer Weichenstellungen. Dabei müssen Entscheidungen immer in einem Spannungsfeld getroffen werden zwischen Sicherheit und Innovation, zwischen europäischen Werten und globalen Geschäftsmodellen sowie zwischen einem (theoretischen) Ideal und dem, was in der Praxis funktioniert. IT-Entscheider in Deutschland und Europa stehen daher vor der Frage: Welche Kompromisse sind akzeptabel? Und worauf können wir uns in diesen Zeiten eigentlich noch verlassen?

Unsere Studie versucht ein Verständnis dafür zu entwickeln, wie Organisationen heute denken, was sie antreibt und was sie leitet. Wie ernst nehmen die Unternehmen die Risiken? Welche Lösungen erscheinen ihnen praktikabel? Und wo liegen die eigentlichen Hürden: auf technologischer Seite, auf regulatorischer Seite – oder geht es am Ende doch wieder vorrangig um knappe Budgets?

Wir wünschen Ihnen eine spannende und erkenntnisreiche Lektüre

Inhalt

11

27

Die wichtigsten Ergebnisse

Management Summary.....	6
Das zentrale Ergebnis	
Souveränität hat viele Facetten	8
Die weiteren Key Findings	11
1. Souverän werden erfordert einen langen Atem	12
2. Ein Weg mit vielen Risiken	14
3. Fehlende Alternative	16
4. Hürden auf dem Weg zur Souveränität.....	18
5. Ohne Cloud ist alles nichts.....	20
6. Dienstleister sollten in das Vertrauen ihrer Kunden investieren	22
7. Wo Flexibilität an ihre Grenzen stößt.....	24

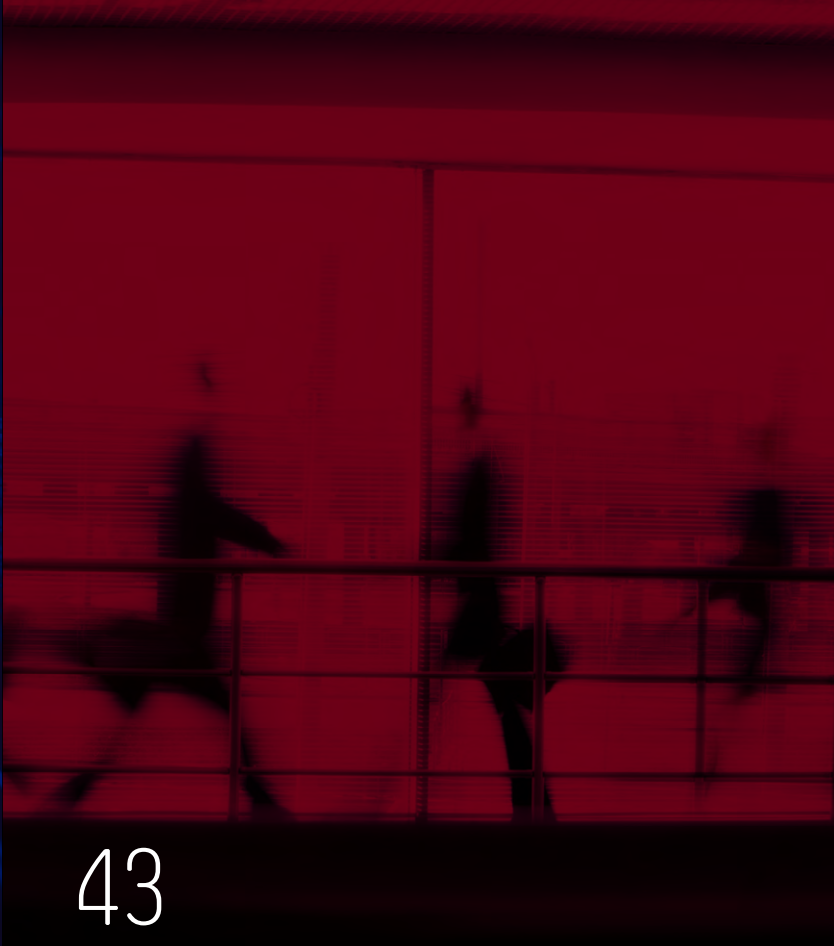
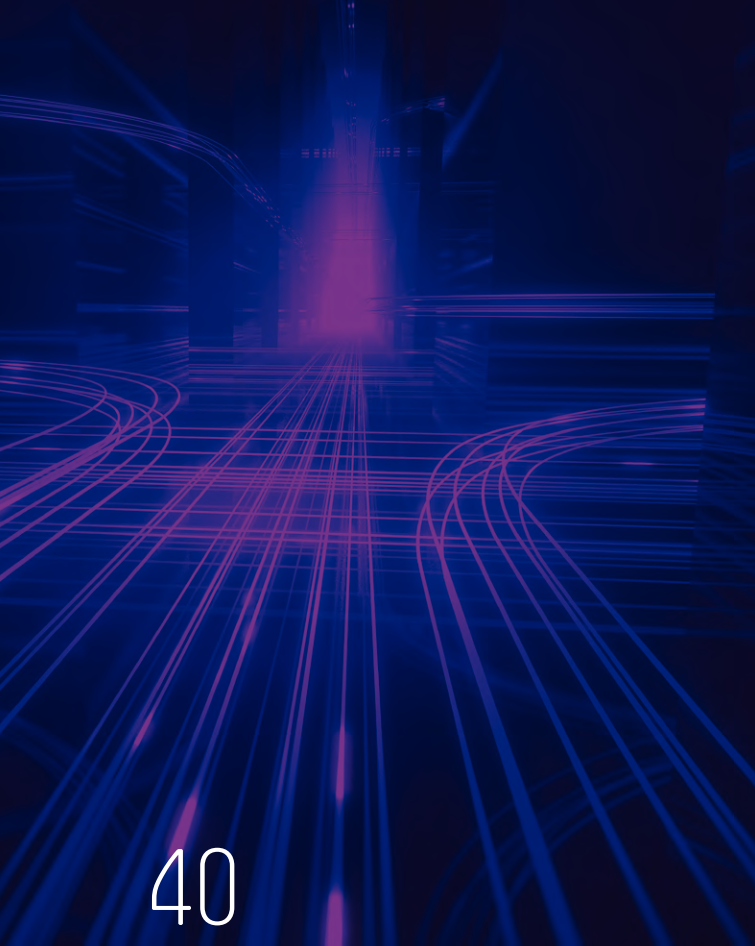
Editorial	3
------------------------	----------

Weitere Studienergebnisse

1. Sicherheit und Unabhängigkeit dominieren	28
2. KI-Piloten haben Vorrang	30
3. Open Source ist fest etabliert	32
4. Interoperabilität und räumliche Nähe sind Trumpf	34
5. Faktor Zeit spielt Providern in die Karten	35
6. Ort der Datenhaltung hat Top-Priorität	36
7. Digitale Souveränität bleibt ein indifferentes Ziel	38

Studiendesign

Impressum	57
Studiensteckbrief.....	58
Stichprobenstatistik.....	59
Studienkonzept, Round-Table-Moderation, Autor dieser Ausgabe	60
Studienreihe.....	61



Blick in die Zukunft

Souverän ohne Daten? 41

CIO-Agenda 2026

Daten zur allgemeinen Einschätzung der Marktlage 44



Die Studienpartner stellen sich vor

T-Systems International..... 48
8com 50
easy software..... 52
plusserver..... 54



Alle wollen es – aber sprechen alle vom Gleichen?

Selbstbestimmt im digitalen Raum zu handeln hat viele Facetten.



Dieser Weg wird kein leichter sein.

Digitale Souveränität setzt **Mut zum Risiko** und die **Trennung von Altlasten** voraus.



Resilienz und Regulatorik – geschenkt!

Auf dem Weg zur digitalen Selbstbestimmung starten die Unternehmen nicht bei Null – aber viele Faktoren **verengen ihre Spielräume**.



Only Europe – es wäre zu schön!

Die **technologische Abhängigkeit von US-Providern** lässt so manchen Traum platzen.



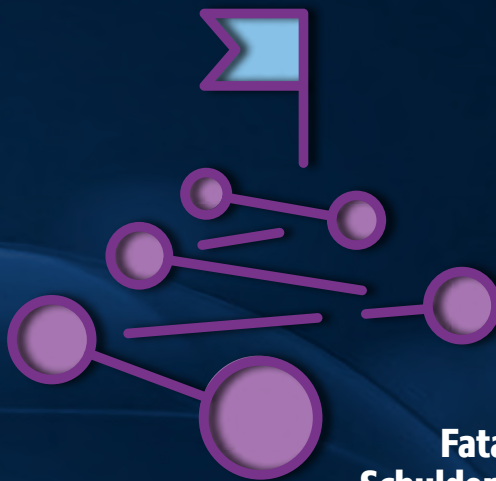
Schon wieder die Cloud

IT-Bezugsmodelle aus der Wolke sind **Teil des Problems** – und Teil der Lösung.



Mehr Beziehungspflege

Was Anwenderinnen und Anwender sich von den Dienstleistern wünschen würden.



Fatale Schuldenbremse

Viele IT-Altlasten stehen dem Ziel digitaler Souveränität im Weg.

Management Summary

Die Key Findings im Überblick



Keine Wahl ist auch eine Wahl.

Es gibt mehr als einen Grund, nicht den Provider zu wechseln.

Das zentrale Ergebnis

Souveränität hat viele Facetten

Den Unternehmen ist ihre digitale Souveränität immer wichtiger. Aber sie bringt viele Herausforderungen mit sich.

Dass der Begriff der digitalen Souveränität inzwischen mehr als ein Schlagwort ist, zeigt nicht nur die Aufmerksamkeit, die diesem Thema allorten gewidmet wird, sondern auch das verbreitete Meinungsbild von IT- und Business-Entscheidern.

So gaben bereits Anfang des Jahres im Rahmen der Studie „CIO-Agenda 2026“ mehr als 74 Prozent der Befragten an, sich intensiv mit diesem Thema zu beschäftigen und daraus entsprechende Strategien und Maßnahmen abzuleiten. Entsprechend vergleichbare Indexwerte der nun vorliegenden Untersuchung bestätigen diesen Trend. Weit über 60 Prozent der Unternehmen priorisieren ihre digitale Souveränität hoch bis sehr hoch. Ein Anteil, der den Auskünften der Studienteilnehmenden zufolge bis 2030 noch deutlich zunehmen dürfte.

Doch welche Bereiche sind den Unternehmen im Kontext der digitalen Souveränität überhaupt wichtig? Worauf legen IT- und Digitalverantwortliche letzten Endes den Fokus hinsichtlich der Fähigkeit, selbstbestimmt im digitalen Raum zu handeln?

Für fast ein Drittel der Anwenderinnen und Anwender ist demnach die technische Souveränität das Hauptanliegen. Damit gemeint ist die Frage, inwieweit sich IT-Infrastruktur und -Plattformen, Netzwerke, Geräte samt notwendiger Software-Patches über deren gesamten Lebenszyklus kontrollieren lassen. Interessant ist in diesem Zusammenhang auch,

dass die Großunternehmen diesen Aspekt noch einmal stärker gewichten als die mittelständischen und kleineren Firmen.

Mehr als ein Viertel aller Befragten führen im Ranking möglicher Mehrfachnennungen auch das Kapitel „Operative Souveränität“ ins Feld. Hier geht es konkret um die Beziehung zu Anbietern und Dienstleistern. Anders formuliert: um die Sicherstellung größtmöglicher Flexibilität bei einem Providerwechsel – Stichwort: Vendor Lock-in! Und auch hier zeigt sich ein heterogenes Meinungsbild: Während 35 Prozent der kleinen Unternehmen auf diesem Kriterium beharren, sind es bei den Mittelständlern lediglich 19 Prozent und bei den großen Firmen wiederum nur 23 Prozent.

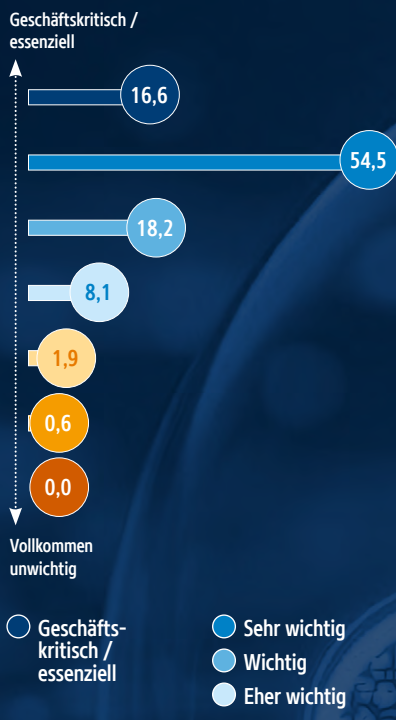
Fast ebenso wichtig ist den Befragten der Aspekt der Datensouveränität. Rund 23 Prozent wollen wissen: Wo liegen meine Daten? Wer kann darauf zugreifen? Und für 15 Prozent aller Unternehmen ist es zudem von Relevanz, wer auf welchen Daten das Modell trainiert und wer die Outputs sowie Guardrails kontrolliert.

Weitere Detailabfragen zu Aspekten, die die Anwenderinnen und Anwender mit digitaler Souveränität verbinden, sind ebenfalls aufschlussreich – und bestätigen das schon beschriebene Meinungsbild. So ist es 43 Prozent der Befragten am wichtigsten, nicht die Kontrolle über die eigenen Daten zu verlieren; bei den Großunternehmen geben dies sogar

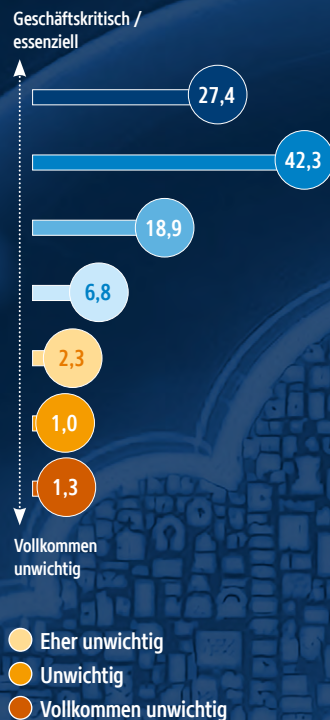
Wie wichtig ist Ihrem Unternehmen das Thema der digitalen Souveränität?

Angaben in Prozent. Basis: n = 312

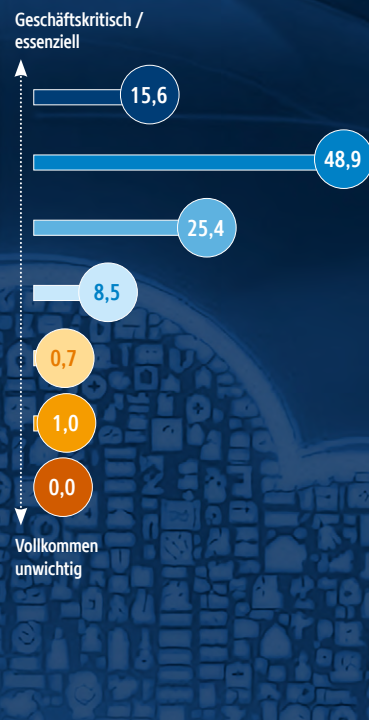
In technologischer Hinsicht



In puncto Daten / Datenhaltung / Datenzugriff

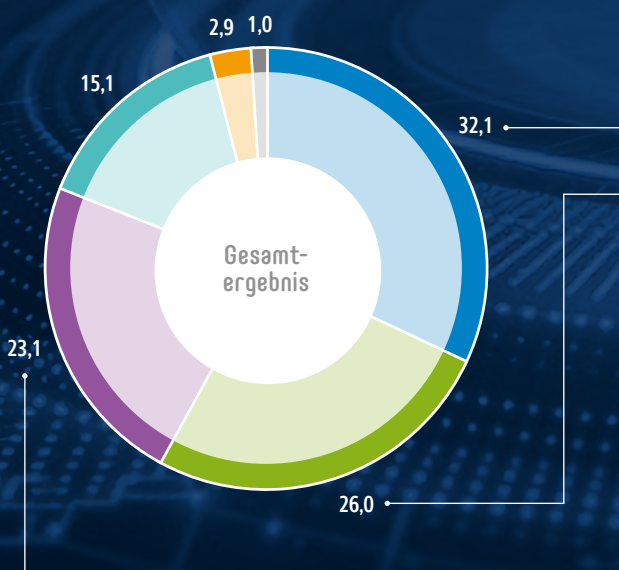


In operativer Hinsicht



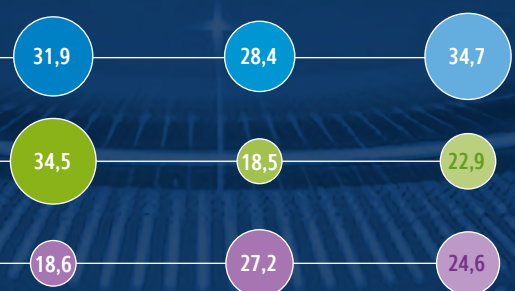
In welchem Bereich ist Ihrem Unternehmen die digitale Souveränität besonders wichtig?

Angaben in Prozent. Basis: n = 312



Ergebnis-Split nach Unternehmensgröße

< 500 Beschäftigte 500-999 Beschäftigte 1000 + Beschäftigte



- Technische Souveränität („Verstehe und kontrolliere ich die Technologie? Wer kontrolliert die Geräte, Patches, End-of-Life? Bin ich vom Hersteller abhängig?“)
- Operative Souveränität („Kann ich meinen Betrieb fortführen, wenn Anbieter X wegfällt? Habe ich Wechseloptionen?“)
- Daten-Souveränität („Wo liegen meine Daten? Wer kann darauf zugreifen?“)
- KI-Souveränität („Wer trainiert auf welchen Daten das Modell? Wer kontrolliert die Outputs und Guardrails?“)
- Kann ich so pauschal nicht beantworten
- Weiß nicht

mehr als 54 Prozent zu Protokoll. Noch stärker im Fokus steht das Thema IT-Sicherheit, das von mehr als der Hälfte der Unternehmen genannt wird. Zählt man den Aspekt Datenschutz und Regulierung noch dazu, hat dieser Komplex bei zwei Dritteln der Studienteilnehmerinnen und Studienteilnehmer Top-Priorität. Etwas überraschend ist indes, dass dieses Kapitel der Studie mit Blick auf die Frage nach der Nutzung europäischer Anbieter einen vergleichsweise sehr niedrigen Relevanzwert ausweist.

Noch einmal zum Thema Datenschutz: Bei der Frage, ob die Unternehmen über Daten verfügen, die sie als besonders schützenswert oder geschäftskritisch einstufen, nennen 66 Prozent der Anwenderinnen und Anwender in ers-

ter Linie personenbezogene Daten, etwa von Kunden und Mitarbeitenden, im Sinne der DSGVO. Den zweiten Platz im Ranking möglicher Mehrfachnennungen belegen mit einem Anteil von 49 Prozent besondere Kategorien personenbezogener Daten, etwa im Gesundheitswesen, oder biometrische Daten. Dritte Kategorie unter den Top 3 der Datenklassifizierung sind Daten, die den Kern von Geschäftsgeheimnissen bilden und entsprechenden gesetzlichen Schutz genießen.

Als weitere wichtige Datenkategorien werden Patente und technisches Know-how genannt, die in den Bereich „Geistiges Eigentum“ fallen. Ferner beschäftigen die Befragten kritische Infrastrukturdaten im Sinne der NIS2-Richtlinie sowie last, but not least, sensible Finanzdaten mit Insiderrelevanz.

Woran denken Sie bei „digitaler Souveränität“ in erster Linie?

Angaben in Prozent. Maximal zwei Nennungen. Basis: n = 312

Gesamtergebnis

Ergebnis-Split nach Unternehmensgröße

		< 500 Beschäftigte	500-999 Beschäftigte	1000 + Beschäftigte
IT-Sicherheit / Cybersecurity	50,6	49,6	54,3	49,2
Kontrolle über eigene Daten	42,9	38,1	33,3	54,2
Unabhängigkeit von Technologieanbietern	24,4	23,9	19,8	28,0
Einhaltung von Datenschutz / Regulierung	15,7	17,7	13,6	15,3
Innovationsfähigkeit	9,9	8,8	13,6	8,5
Transparenz von Technologien (z. B. KI)	9,6	10,6	11,1	7,6
Nutzung europäischer Anbieter	7,1	8,0	6,2	6,8
Einsatz von Open Source	5,8	7,1	9,9	1,7
Wertschöpfung in EU, volkswirtschaftlicher Nutzen	4,2	3,5	7,4	2,5
An etwas anderes	0,3	0,9	0,0	0,0
Weiß nicht	1,6	1,8	1,2	1,7

Die weiteren Key Findings

Die wichtigsten Daten, Analysen
und Insights der Studie

Souverän werden erfordert einen langen Atem

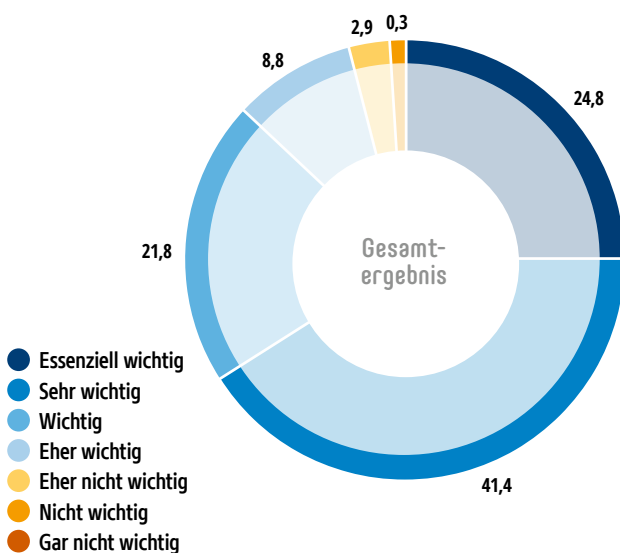
Zur Stärkung ihrer digitalen Souveränität bekennen sich alle Firmen – aber die Reise ist lang, und die notwendigen Maßnahmen sind vielfältig.

Mit der Bedeutung, die die IT- und Business-Verantwortlichen dem Thema Digitale Souveränität beimessen, steigen konsequenterweise auch deren Bemühungen, das eigene Unternehmen entsprechend besser aufzustellen. So ist es für zwei Drittel der Befragten ein essenziell wichtiges Ziel, die eigene digitale Souveränität zu stärken. Gut 20 Prozent sehen darin ein immerhin noch wichtiges Vorhaben.

Was sind nun aber die konkreten Maßnahmen der Unternehmen, die diese bereits umgesetzt haben? Im Ranking möglicher Mehrfachnennungen wird hier an erster Stelle eine Multicloud-Strategie genannt, für die sich 38 Prozent der Befragten entschieden haben. Es folgen mit respektablem Abstand die Nutzung souveräner Cloud-Lösungen (34 Prozent) sowie der Aufbau eigener Datenplattformen (31 Prozent). Bei den hier genannten Top-3-Maßnahmen wächst wiederum der prozentuale Anteil mit der Größe der jeweiligen Unternehmen.

Wie wichtig ist es aus Sicht Ihres Unternehmens, die eigene digitale Souveränität zu stärken?

Angaben in Prozent. Basis: n = 312



Weitere Schlüsselfaktoren, die nach Ansicht der Studienteilnehmenden zur Stärkung ihrer digitalen Souveränität beitragen, sind eine stärkere Fokussierung auf IT-Governance, die Diversifizierung von Anbietern und Lieferanten sowie die Nutzung von Open Source. Immerhin noch ein Viertel der Anwenderinnen und Anwender bekennen sich dazu, ihre internen IT-Kompetenzen auszubauen.

Mit den Ergebnissen und Auswirkungen bisher eingeleiteter Maßnahmen sind gut 60 Prozent der Studienteilnehmenden zufrieden. Ein weiteres Viertel der Unternehmen zieht aktuell eine befriedigende Bilanz.

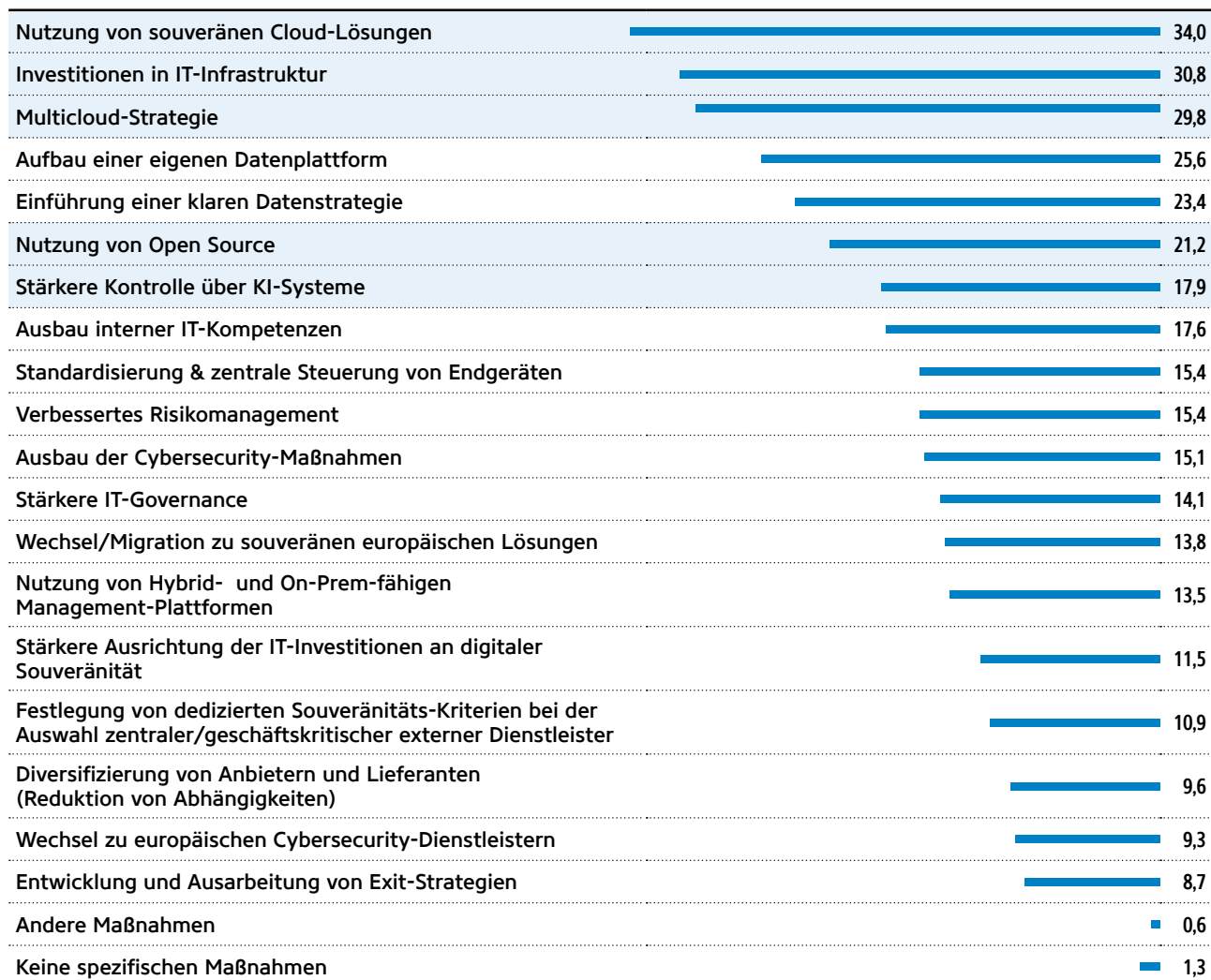
Bei diesem Einzelergebnis fällt auf, dass der Grad der Zufriedenheit tendenziell zunimmt, je größer das Unternehmen ist. Sehr stark differenziert sich hier auch das Meinungsbild innerhalb der unterschiedlichen Funktionsträgerinnen und Funktionsträger. Während 69 Prozent der Mitarbeitenden in Vorstand und Geschäftsführung bei den Maßnahmen zur Stärkung der digitalen Souveränität große Fortschritte sehen, beträgt dieser Anteil bei den Fachbereichsleitern lediglich 41 Prozent.

Das aktuelle Bild der Selbsteinschätzung und die Schwerpunkte bei den eingeleiteten Maßnahmen spiegelt sich auch in der Prognose bis 2029 wider. So plant rund ein Drittel der Unternehmen eine noch intensivere Nutzung souveräner Cloud-Lösungen, bei den mittelständischen Firmen beträgt dieser Anteil sogar 40 Prozent. Mehr als 30 Prozent der Anwenderinnen und Anwender ziehen es konkret in Betracht, noch stärker in ihre IT-Infrastruktur zu investieren. Letzteres ist kein überraschendes Einzelergebnis, sondern ein Trend, der sich auch in anderen Zusammenhängen immer wieder erkennen lässt – etwa, wenn es um den Abbau sogenannter technologischer Schulden geht.

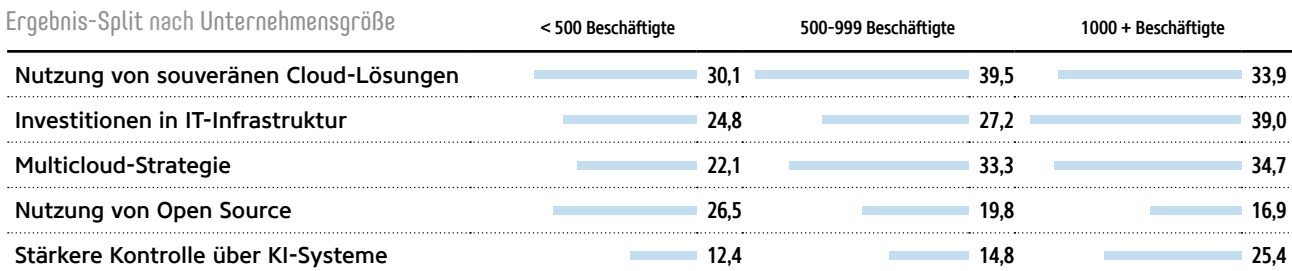
Welche Maßnahmen zur Stärkung der eigenen digitalen Souveränität plant Ihr Unternehmen für die nächsten zwei bis drei Jahre?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312

Gesamtergebnis



Ergebnis-Split nach Unternehmensgröße



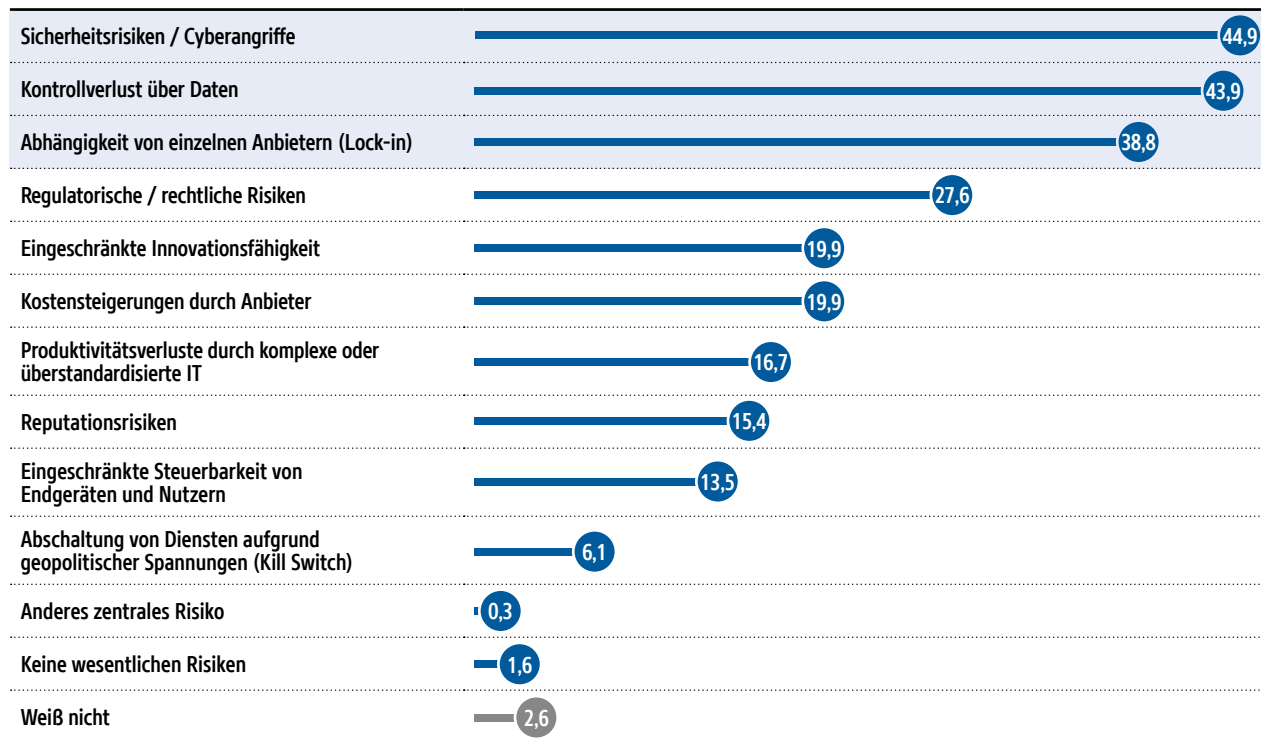
Auch die Handlungsfelder Multicloud-Strategie sowie Aufbau einer eigenen Datenplattform inklusive der Einführung einer klaren Datenstrategie genießen in den kommenden Jahren hohe Priorität. Stark im Kommen sind zudem der Einsatz von Open Source sowie die Implementierung stärkerer Kontrollmecha-

nismen für KI-Systeme. Ersteres steht deutlich stärker bei den kleinen Firmen im Vordergrund. Die Kontrolle und das Monitoring von KI-Workloads beschäftigt naturgemäß mehr die Großunternehmen, die bei der KI-Nutzung einen höheren Reifegrad aufweisen.

Welche zentralen Risiken bestehen aus Ihrer Sicht für Unternehmen infolge eines Mangels an digitaler Souveränität?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312

Gesamtergebnis



Ein Weg mit vielen Risiken

Digital souverän zu werden und zu bleiben ist kein Selbstläufer. Es warten viele Hindernisse und Unwägbarkeiten.

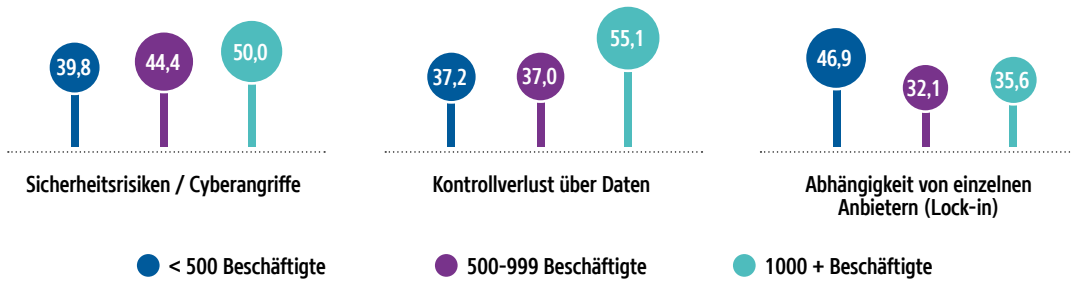
Wer das Thema Digitale Souveränität vernachlässigt, geht ohne Zweifel enorme Risiken ein. Aber was heißt das genau? Rund 45 Prozent der Studienteilnehmenden sehen vergleichbar mit anderen Einzelergebnissen der Untersuchung Cyberangriffe als größte Gefahr, dicht gefolgt vom Kontrollverlust über Daten. In beiden Fällen stuften die Großunternehmen ihre Bedrohungslage noch einmal deutlich höher ein als der Durchschnitt aller Befragten.

Als schwierig infolge mangelnder digitaler Souveränität erachten die Anwenderinnen und Anwender aber auch rechtliche beziehungsweise regulatorische Unsicherheiten sowie die zu große Abhängigkeit von einzelnen Anbietern. Zudem werden weitere interessante Aspekte im

Ranking möglicher Mehrfachnennungen als Risiken gesehen – etwa eine eingeschränkte Innovationsfähigkeit, Kostensteigerungen durch die Provider sowie Produktivitätsverluste durch eine „überstandardisierte IT“.

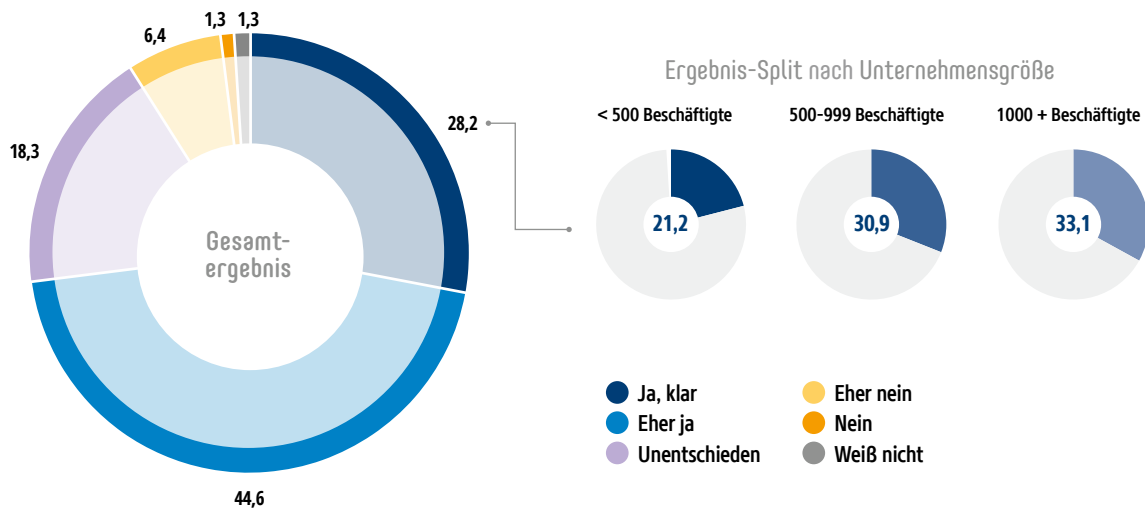
Bemerkenswert ist ferner: Weit über 70 Prozent der Firmen sind bereit, für mehr digitale Souveränität durchaus höhere Kosten in Kauf zu nehmen. Ein Statement, das sich wie ein roter Faden durch Unternehmen aller Größen zieht. Weitere 18 Prozent der Befragten sind noch unentschieden. Und noch ein Einzelergebnis sticht hervor: Ebenfalls 70 Prozent der Anwenderinnen und Anwender nehmen für mehr digitale Souveränität auch eine höhere Komplexität in Kauf.

Ergebnis-Split nach Unternehmensgröße



Sind Sie bereit, für mehr digitale Souveränität **höhere Kosten** in Kauf zu nehmen?

Angaben in Prozent. Basis: n = 312

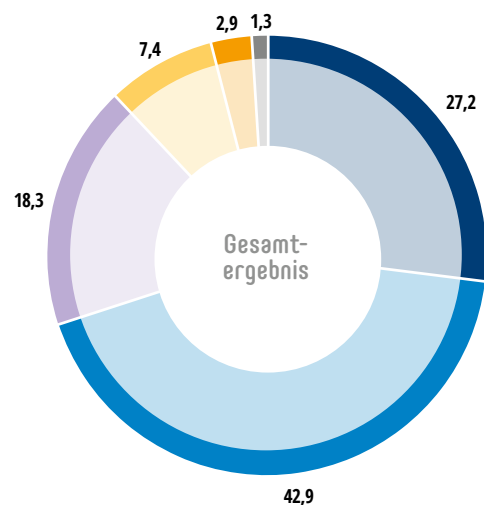


Gleichzeitig fließen in eine aktuelle Bewertung der Risiken auch die globalen Krisen und Spannungen mit ihren Auswirkungen auf Lieferketten und den Zugang zu Märkten ein. Hier zeigen sich die Studienteilnehmenden jedoch überraschend selbstbewusst. Gut 40 Prozent gehen davon aus, dass sie über eine sehr hohe oder hohe Resilienz verfügen. Weitere 35 Prozent sehen sich zumindest ausreichend gut aufgestellt.

Ähnlich positiv ist die Selbsteinschätzung der Befragten in puncto Regulatorik. Weit über die Hälfte (55 Prozent) fühlt sich im Hinblick auf NIS2, EU AI Act oder EU Cyber Resilience Act umfassend gewappnet, ein weiteres Drittel hat sich zumindest hinreichend gut mit diesen Themen beschäftigt.

Sind Sie bereit, für mehr digitale Souveränität eine **höhere Komplexität** in Kauf zu nehmen?

Angaben in Prozent. Basis: n = 312



Fehlende Alternative

Unternehmen in Europa können sich nur schwer von den US-Hyperscalern abnabeln.

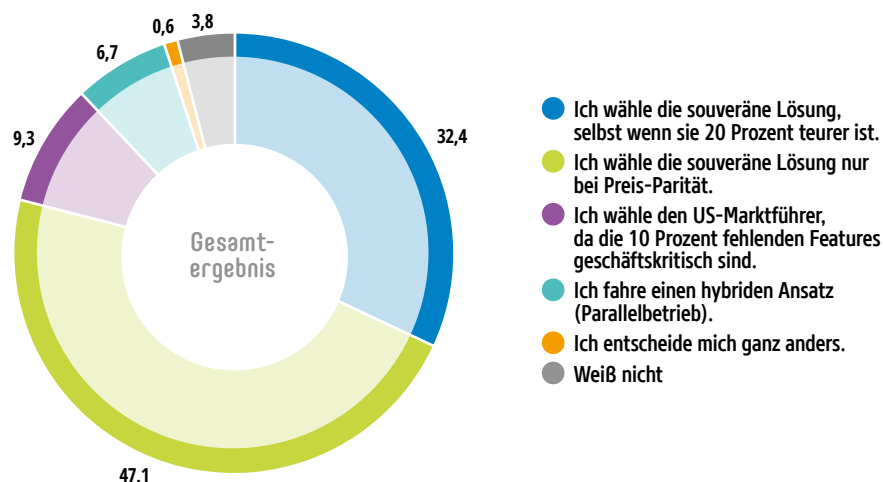
Bei der Herausforderung „Digitale Souveränität“ schwingt von je her die schon erwähnte geopolitische Komponente mit – spätestens seit dem Amtsantritt der zweiten Trump-Administration in den Vereinigten Staaten.

Insofern wurde im Rahmen der vorliegenden Untersuchung den Unternehmen auch eine Art „Gretchenfrage“ gestellt: „Angenommen, eine europäische Lösung bietet 90 Prozent der Funktionen eines US-Marktführers, garantiert aber hundert Prozent digitale Souveränität. Wie würden Sie entscheiden?“

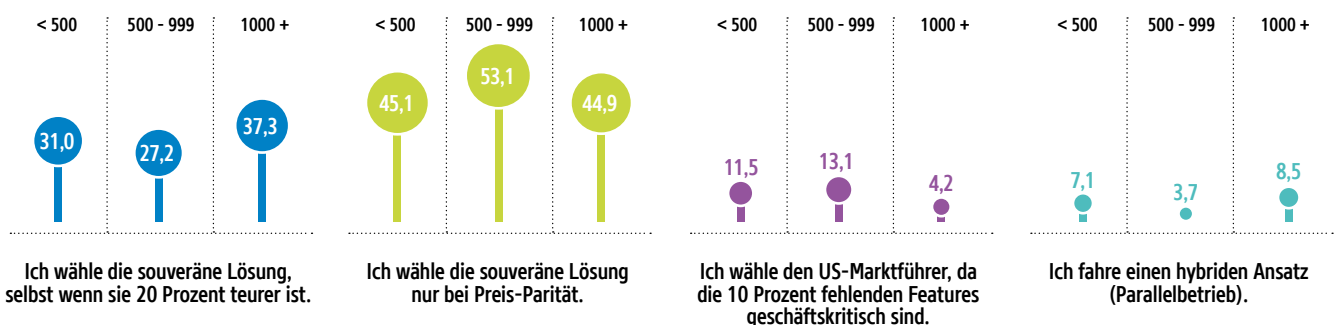
Die Antworten der Studienteilnehmenden sind auf den ersten Blick doch überraschend: Nur knapp ein Drittel der Befragten würde sich für die europäische und damit mutmaßlich souveräne Lösung entscheiden. Das Gros (47 Prozent) der Anwenderinnen und Anwender würde indes diesen Weg nur bei einer Preis-Parität gehen. Rund neun Prozent der Befragten würden sich dennoch für den US-Marktführer entscheiden. Für sie wiegen die fehlenden zehn Prozent an Funktionen schwerer, weil sie diese als geschäftskritisch ansehen.

Angenommen, eine europäische Lösung bietet 90 Prozent der Funktionen eines US-Marktführers, garantiert aber 100 Prozent digitale Souveränität. Wie würden Sie entscheiden?

Angaben in Prozent. Basis: n = 312

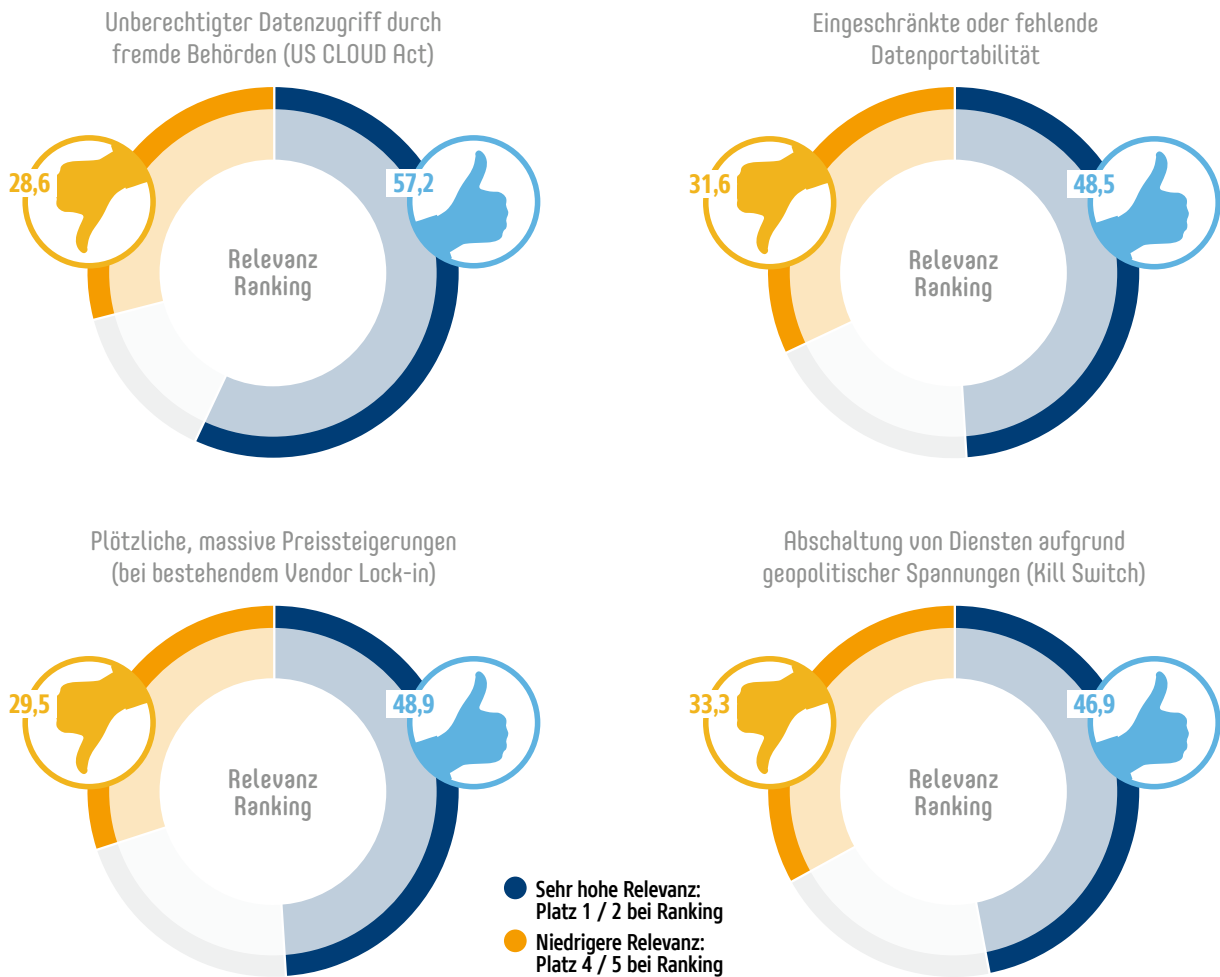


Ergebnis-Split nach Unternehmensgröße (Anzahl der Beschäftigten)



Welche der folgenden Szenarien bereiten Ihnen bei der Nutzung von Nicht-EU-Cloud-Anbietern die größten Sorgen?

Angaben in Prozent. Ranking nach Relevanz (Platz 1: Sehr hohe Relevanz bis Platz 5: Niedrige Relevanz). Basis: n = 283



Auch wenn in den Antworten noch ein heterogenes Meinungsbild zwischen den Unternehmen unterschiedlicher Größenordnungen mitschwingt, ist der Tenor insgesamt eindeutig: Die Auswahl des Providers hat entscheidend mit dessen Preis-Leistungs-Verhältnis zu tun – und sie dürfte derzeit auch noch von den unzureichenden qualitativen und quantitativen Alternativen in der europäischen Dienstleisterlandschaft beeinflusst sein.

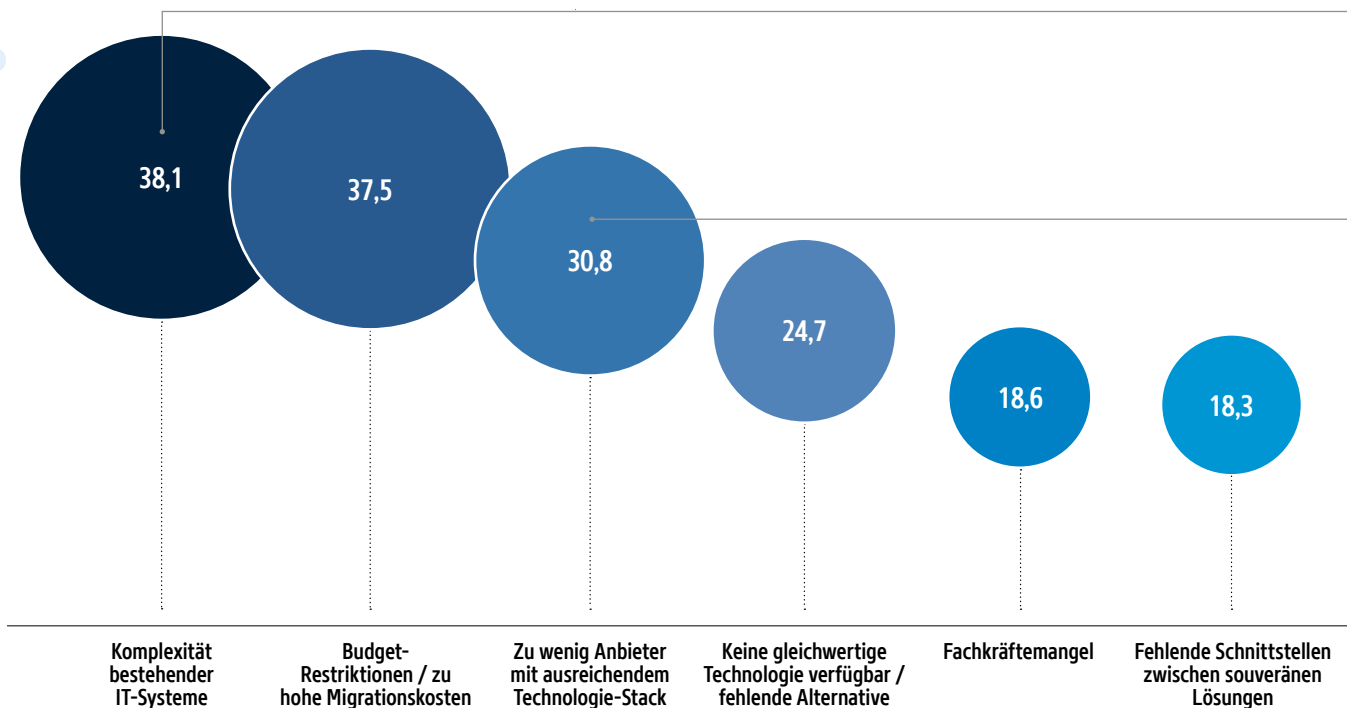
Ungeachtet dessen gibt es bei der Nutzung von Nicht-EU-Cloud-Anbietern auch große Vorbehalte. So befürchten deutlich mehr als

die Hälfte (57 Prozent) der Studienteilnehmenden einen unberechtigten Datenzugriff durch fremde Behörden – Stichwort: US Cloud Act. Fast 49 Prozent gehen zudem von einer eingeschränkten oder gar fehlenden Datenportabilität aus.

Des Weiteren gibt es Bedenken hinsichtlich der Gefahr plötzlich eintretender massiver Preiserhöhungen, insbesondere bei einem bestehenden Vendor Lock-in. Gleiches gilt für die Abschaltung von Diensten aufgrund geopolitischer Spannungen (Kill Switch) oder den Verlust der Innovationsgeschwindigkeit bei einem Anbieterwechsel.

Welche Hürden erschweren aktuell die Umsetzung digitaler Souveränität?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312



Hürden auf dem Weg zur Souveränität

Neben zu geringen Budgets und verbreiteter Risikoscheu erweist sich auch die Komplexität alter IT-Systeme als Hemmschuh.

Abgesehen von den Maßnahmen, die die Unternehmen zur Stärkung ihrer digitalen Souveränität ergreifen, sowie den Risiken, die sie in diesem Zusammenhang sehen, bleibt noch die Frage, welche Hürden sie aktuell in der Umsetzung sehen.

Rund 38 Prozent der Befragten verweisen hier auf die Komplexität bestehender IT-Systeme. Ein Umstand, der den Studienergebnissen zufolge vor allem auf den Mittelstand zutrifft. Knapp dahinter rangieren Budget-Restriktionen und zu hohe Migrationskosten. Platz drei im Ranking möglicher Mehrfachantworten belegt die Aussage, dass es aus Sicht der Anwenderinnen und Anwender zu wenig Anbieter mit einem ausreichenden Technologie-Stack gibt.

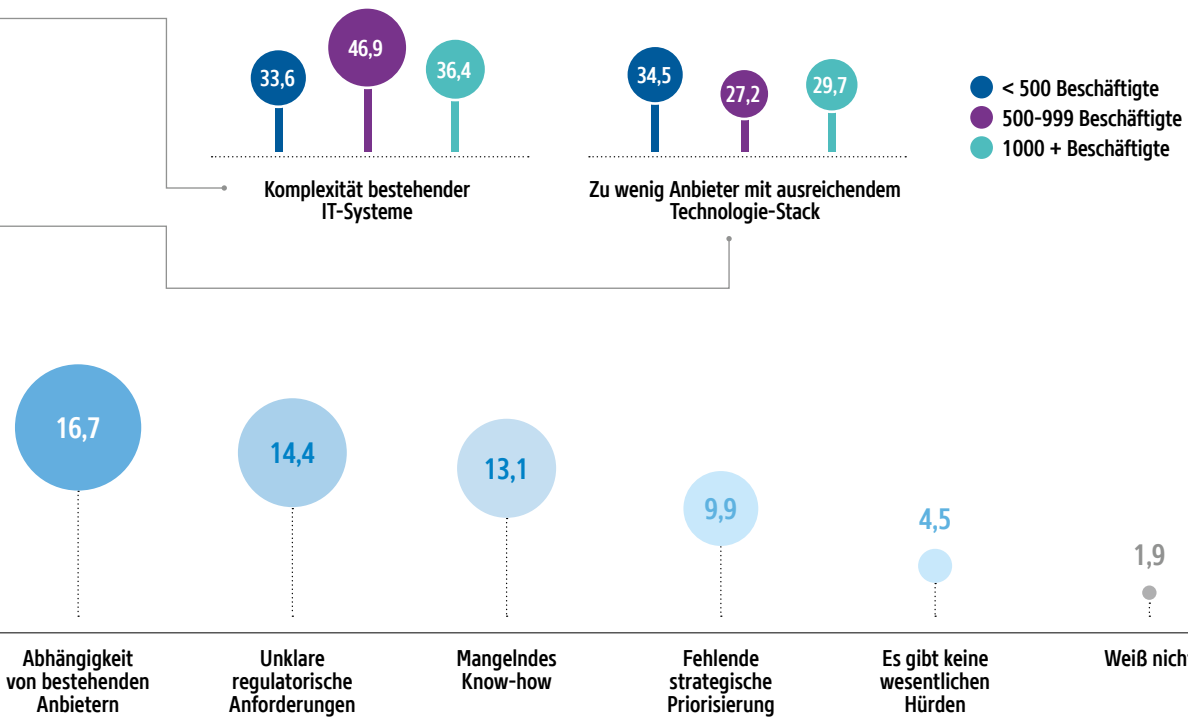
Mit gebührendem Abstand, aber dennoch mit statistischer Relevanz sehen die Befrag-

ten auch mangelnde Alternativen bei der Dienstleistungsauswahl, gefolgt von fehlenden Schnittstellen sowie dem immer noch vorhandene Fachkräftemangel.

Auch die Abhängigkeit von bestehenden Anbietern und unklare regulatorische Anforderungen spielen für die Unternehmen bei der Stärkung ihrer digitalen Souveränität eine eher hemmende Rolle. Und last, but not least entpuppt sich gelegentlich auch das fehlende interne Know-how als „Showstopper“.

Die Zahlen zeigen: Den einen Königsweg zur digitalen Souveränität gibt es offensichtlich nicht. Die Herausforderungen und Prioritäten können sich von Unternehmen zu Unternehmen erheblich unterscheiden.

Ergebnis-Split nach Unternehmensgröße



Ausgewählte Statements von Studienteilnehmenden zu folgender Frage:

„Wie sollte Ihrer Meinung nach ein digitales souveränes Unternehmen in drei bis fünf Jahren aussehen?“

„Strategische Unabhängigkeit, Datensouveränität, künstliche Intelligenz, Infrastruktur, Risikomanagement, Resilienz.“

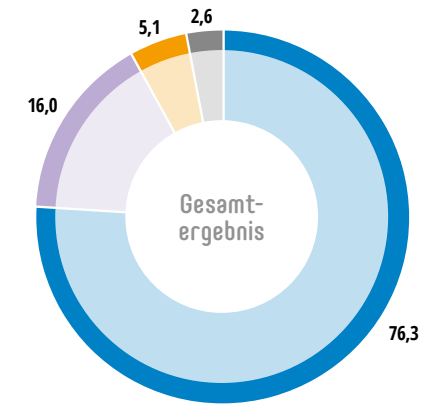
„Ich denke, in diesem Zeitraum ist ein Unternehmen kein autarkes Unternehmen mehr, sondern eines, das seine Abhängigkeiten kennt, kontrolliert und aktiv steuert. Es bewahrt die Handlungsfähigkeit, indem es die Kontrolle über Daten, Infrastruktur und KI-Technologien behält, ohne auf Innovationen zu verzichten.“

„In drei bis fünf Jahren zeichnet sich ein digital souveränes Unternehmen vor allem durch die vollständige Kontrolle über seine Daten und Kernprozesse aus. Es nutzt unabhängige Multicloud-Infrastrukturen und Open-Source-Software, um Knebelverträge und Abhängigkeiten von einzelnen IT-Giganten zu verhindern. (...) Eine starke Inhouse-Technologiekompetenz sichert dabei dauerhaft die eigene Innovations- und Lieferfähigkeit.“

„Es kontrolliert seine kritischen Daten und KI-Modelle vollständig, nutzt offene Standards und austauschbare Cloud-Dienste, vermeidet proprietäre Lock-in-Effekte und erfüllt alle Compliance-Anforderungen unabhängig von externen Anbietern.“

Nutzt Ihr Unternehmen Cloud-Services?

Angaben in Prozent. Basis: n = 312



● Ja
● Einführung konkret geplant
● Nein
● Weiß nicht

Ohne Cloud ist alles nichts

Die Cloud ist auf dem Weg zur digitalen Souveränität größter Risikofaktor und Hoffnungsträger zugleich.

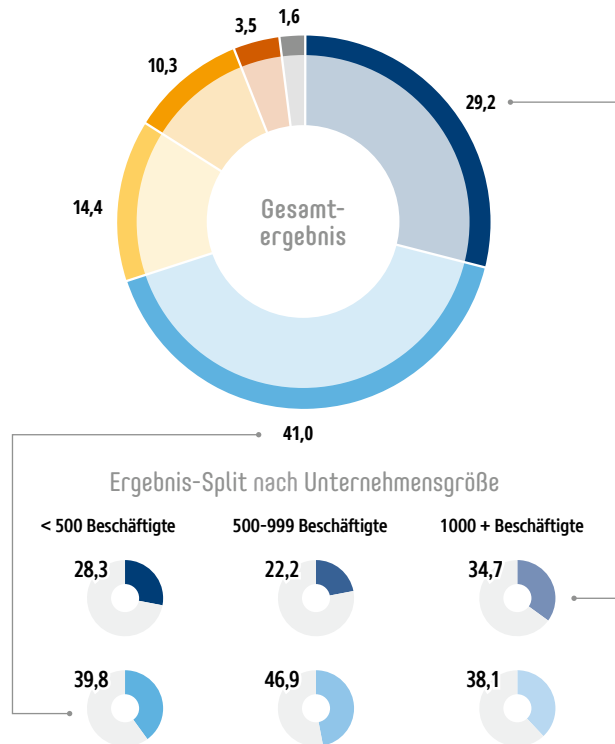
Bei der Realisierung digitaler Souveränität kommt einmal mehr die Cloud als weit verbreitetes IT-Betriebs- und -Bezugsmodell ins Spiel. Insofern ist der Status quo in Sachen Cloud-Strategien und -Nutzung bei deutschen Unternehmen auch in diesem Kontext mehr als aufschlussreich.

Zunächst bestätigt sich in der vorliegenden Untersuchung ein seit Längerem zu beobachtender Trend: Mehr als zwei Drittel aller Unternehmen nutzen Cloud-Services. Aber die Cloud ersetzt nicht zwingend und kompromisslos alte IT-Umgebungen, sondern wird vielerorts als komplementär gesehen.

Jedenfalls bleiben On-Premises-Systeme für rund 29 Prozent der Unternehmen ein fester Hauptbestandteil ihrer IT-Architektur, auch wenn diese womöglich schon mithilfe von Cloud-Technologien modernisiert wurden. Gut 40 Prozent der Befragten haben sich für den schon erwähnten komplementären Ansatz entschieden. Und nur rund 14 Prozent wollen sich komplett von der alten On-Pre-

Welche Rolle spielen On-Premises-Systeme heute in der IT-Strategie Ihres Unternehmens?

Angaben in Prozent. Basis: n = 312



● On-Premises bleibt fester Bestandteil unserer Architektur.
● On-Premises-Systeme sind Ergänzung zur Cloud.
● Auslaufmodell – wir bauen On-Premises aktiv und konsequent ab.
● On-Premises-Anteil sinkt, aber kein vollständiger Abbau geplant.
● On-Premises-Systeme spielen keine Rolle.
● Weiß nicht

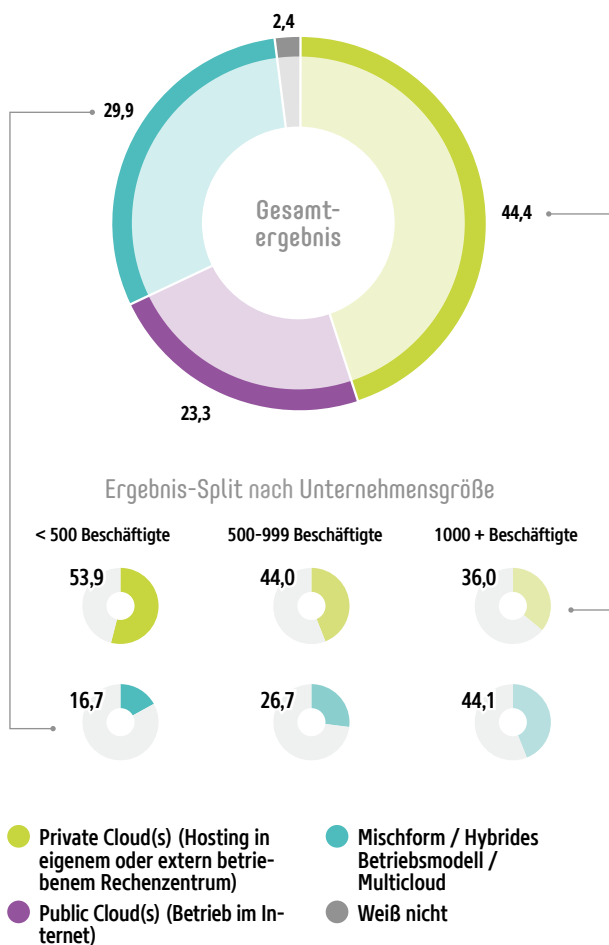
mises-Welt verabschieden. Bei weiteren zehn Prozent der Unternehmen soll der On-Premises-Anteil kontinuierlich sinken, aber nicht vollständig verschwinden.

Das mit Abstand beliebteste Cloud-Betriebsmodell ist die Private Cloud, die entweder im eigenen oder in einem extern betriebenen Rechenzentrum gehostet wird. Mehr als 44 Prozent haben sich für diesen Weg entschieden. Interessant ist hier die Umstand, dass der Anteil der Private Cloud in den kleinen Firmen mit 54 Prozent überproportional hoch ist.

Knapp 30 Prozent der Befragten wählten eine Mischform, also ein hybrides Betriebsmodell in der Multicloud, das wiederum die Großunternehmen in besonderem Maße bevorzugen. Die reine Public Cloud erfreut sich nur geringer Beliebtheit: Für sie können sich bis dato lediglich 23 Prozent der Unternehmen erwärmen.

Welches Betriebsmodell hat Ihr Unternehmen für die Cloud-Anwendungen gewählt?

Angaben in Prozent. Filter: Unternehmen, die Cloud-Services nutzen oder deren Einführung konkret planen. Basis: n = 288

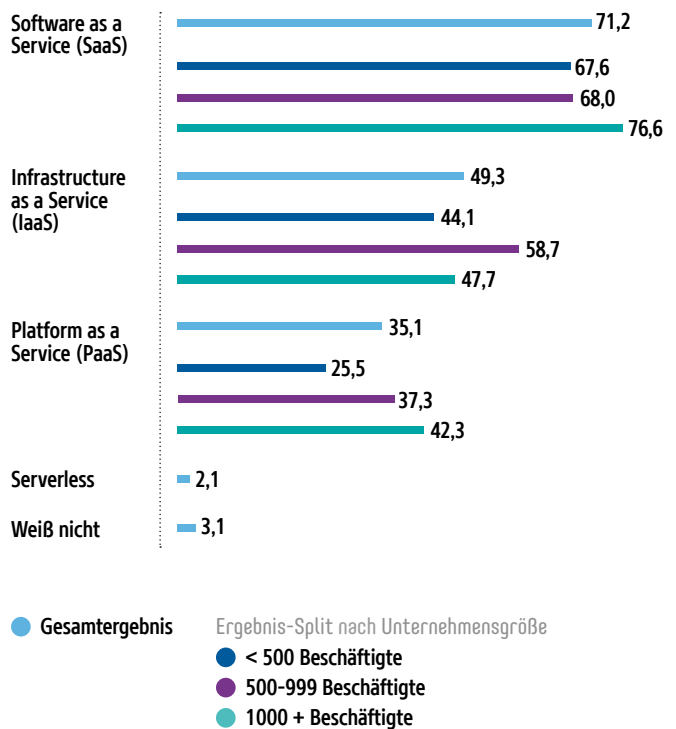


Bei der Nutzung unterschiedlicher Spielarten von Cloud-Services dominiert mit großem Abstand die Kategorie Software as a Service (SaaS), die 71 Prozent der Befragten zu schätzen wissen. Ebenfalls populär ist das Thema Infrastructure as a Service (IaaS), das im Ranking möglicher Mehrfachnennungen auf einen Anteil von 49 Prozent kommt. Auf Rang drei folgt die Nutzung von Platform as a Service (PaaS), eine Cloud-Domäne, die bei immerhin 35 Prozent der Unternehmen zum Einsatz kommt. Und bei allen genannten Cloud-Disziplinen zeigen sich erneut deutliche Unterschiede im Nutzungsverhalten der Unternehmen abhängig von ihrer Größenordnung.

Höchst aufschlussreich sind die Antworten der Studienteilnehmenden auf die Frage, in welchen Regionen sie hauptsächlich ihre Cloud-Infrastruktur betreiben. So setzen be-

Welche Arten von Cloud-Services nutzt Ihr Unternehmen?

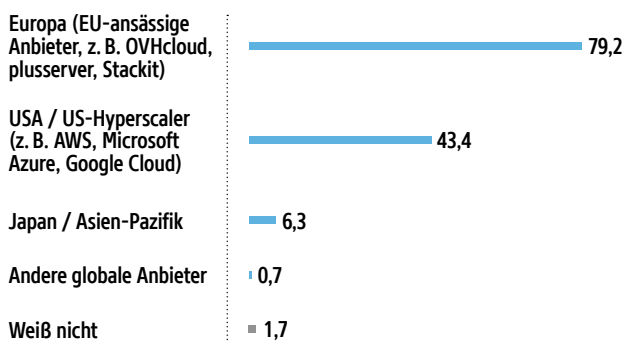
Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die Cloud-Services nutzen oder deren Einführung konkret planen. Basis: n = 288



reits 79 Prozent der Befragten auf die Zusammenarbeit mit in der EU-ansässigen Anbietern. Das ist mehr als ein Achtungserfolg für die hiesigen Provider. Rund 43 Prozent der Unternehmen unterhalten Geschäftsbeziehungen mit einem der US-Hyperscaler, und rund sechs Prozent vertrauen Daten Dienstleistern in Fernost an.

In welchen Regionen betreiben Sie Ihre primäre Cloud-Infrastruktur?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die Cloud-Services nutzen oder deren Einführung konkret planen. Basis: n = 288

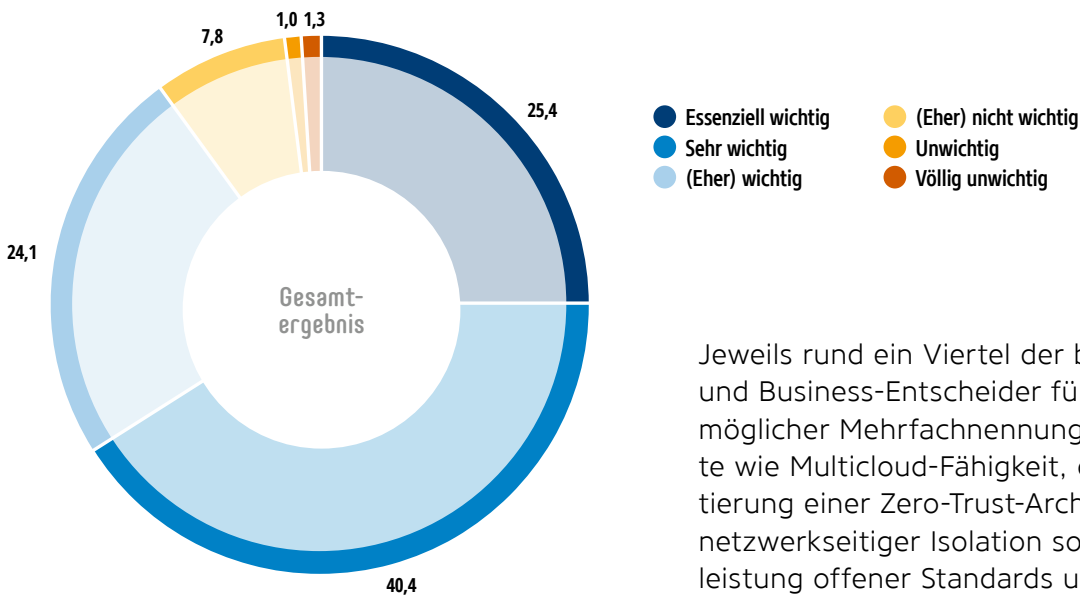


6 Dienstleister sollten in das Vertrauen ihrer Kunden investieren

Die Anwenderinnen und Anwender haben detaillierte Vorstellungen davon, was die Zusammenarbeit mit Providern aus ihrer Sicht stärken würde.

Wie wichtig ist die Verfügbarkeit einer souveränen, vollständig verwalteten Cloud-Plattform für die digitale Transformation und die Compliance-Initiativen Ihres Unternehmens?

Angaben in Prozent. Basis: n = 307



Digitale Souveränität ist nicht nur eine Frage der Unabhängigkeit und Sicherheit, sondern sie hat auch spürbare Auswirkungen auf die digitale Transformation von Unternehmen und deren Compliance-Vorgaben.

Rund zwei Drittel der Befragten bestätigen diese Sichtweise und betrachten eine vollständig souverän administrierte Cloud-Plattform als essenziell oder sehr wichtig. Ein weiteres Viertel der Studienteilnehmenden misst diesem Thema zumindest eine hohe Relevanz bei.

Bei den konkreten Features beziehungsweise Garantien, die das Vertrauen in eine souveräne Cloud-Plattform stärken würden, nennen die Anwenderinnen und Anwender in erster Linie sicherheitsrelevante Funktionen. Mehr als die Hälfte verweist hier auf eine Ende-zu-Ende-Verschlüsselung, auf Einblicke in Zugriffsprotokolle und Betriebsabläufe sowie auf eine effektive Verschlüsselungskontrolle (Bring Your Own Key / BYOK).

Jeweils rund ein Viertel der befragten IT- und Business-Entscheider führen im Ranking möglicher Mehrfachnennungen auch Aspekte wie Multicloud-Fähigkeit, die Implementierung einer Zero-Trust-Architektur samt netzwerkseitiger Isolation sowie die Gewährleistung offener Standards und APIs ins Feld.

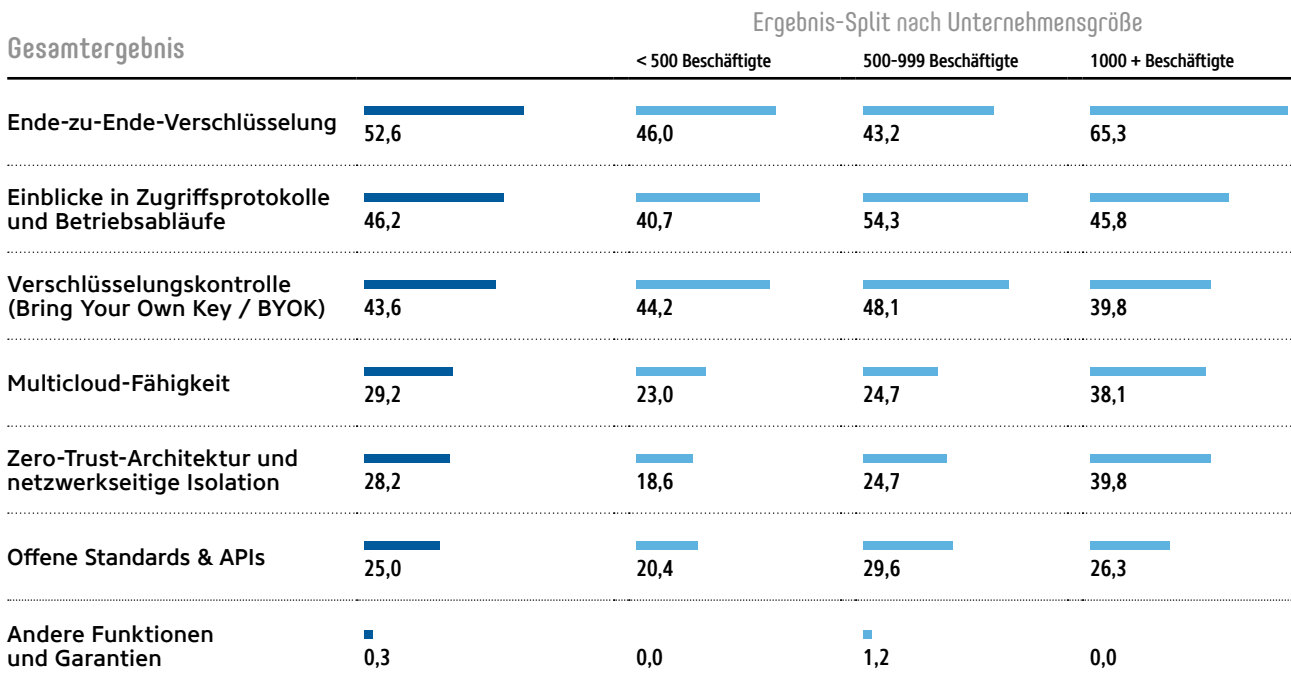
Mit Blick auf viele der genannten Themen ist wieder eine deutlich höhere Relevanz bei den größeren Unternehmen erkennbar. Ein Ergebnis, das in erster Linie den dort vorhandenen komplexeren IT-Architekturen geschuldet sein dürfte.

Apropos Architekturen: Wer hat eigentlich in den Unternehmen das „letzte Wort“ bei der Entscheidung über eine „Souveränitätsarchitektur“? In 23 Prozent der befragten Firmen ist dies der Vorstand / CEO. Bei nahezu der Hälfte der Unternehmen bleibt die Prokura in Sachen digitaler Souveränität jedoch beim CIO beziehungsweise der IT-Leitung.

Bemerkenswert an diesem Einzelergebnis sind zwei Dinge: Es gibt keine nennenswerten Unterschiede bei den Verantwortlichkeiten mit Blick auf Unternehmensgrößen. Und noch überraschender: In immerhin neun Prozent der Unternehmen entscheidet der CISO über den Weg zur digitalen Souveränität.

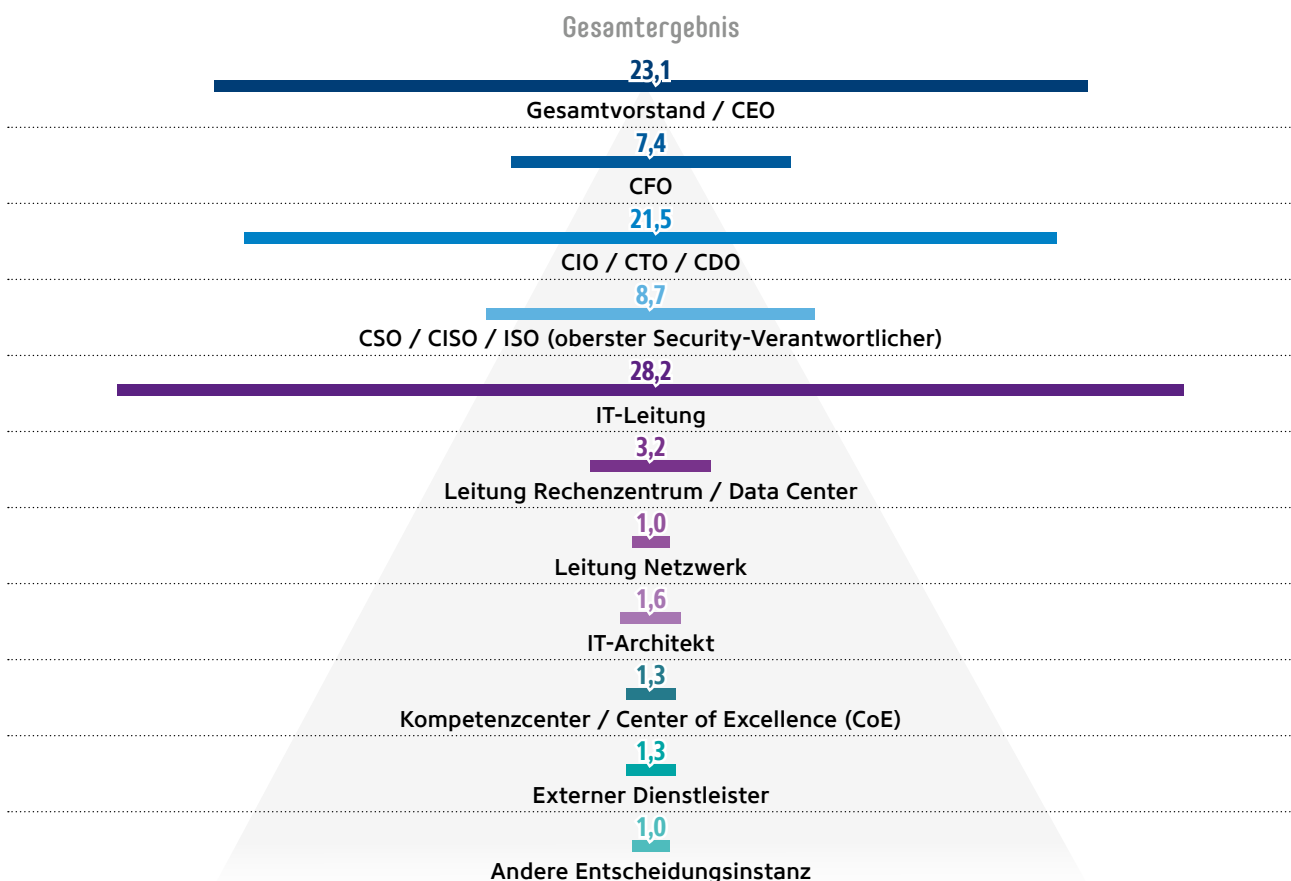
Welche der folgenden konkreten Funktionen oder Garantien würden Ihr Vertrauen in eine souveräne Cloud-Plattform stärken? Nennen Sie gern weitere konkrete Funktionen und Garantien, die Ihrem Unternehmen in diesem Kontext sehr wichtig wären.

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312



Wer in Ihrem Haus trifft die Letztentscheidung über die „Souveränitätsarchitektur“ (z. B. Cloud vs. On-Premises)?

Angaben in Prozent. Basis: n = 312

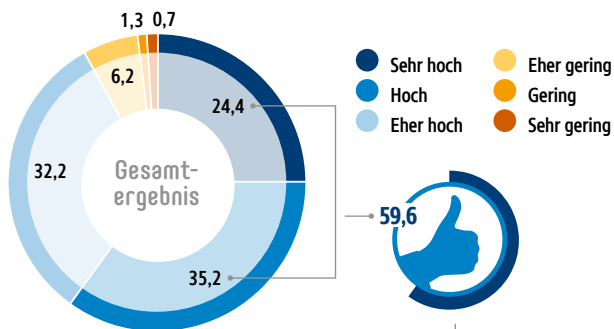


Wo Flexibilität an ihre Grenzen stößt

Die Unternehmen würden gern häufiger den Dienstleister wechseln – wenn sie es nur könnten.

Wie stufen Sie den aktuellen Abhängigkeitsgrad Ihres Unternehmens von einzelnen Technologieanbietern insgesamt ein?

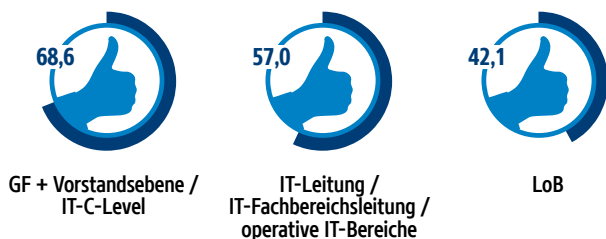
Angaben in Prozent. Basis: n = 307



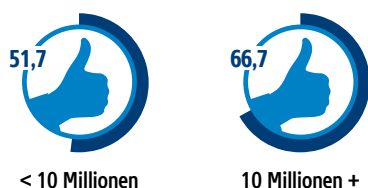
Ergebnis-Split nach Unternehmensgröße



Ergebnis-Split nach Funktion im Unternehmen



Ergebnis-Split nach jährlichen Aufwendungen in IT-Systeme



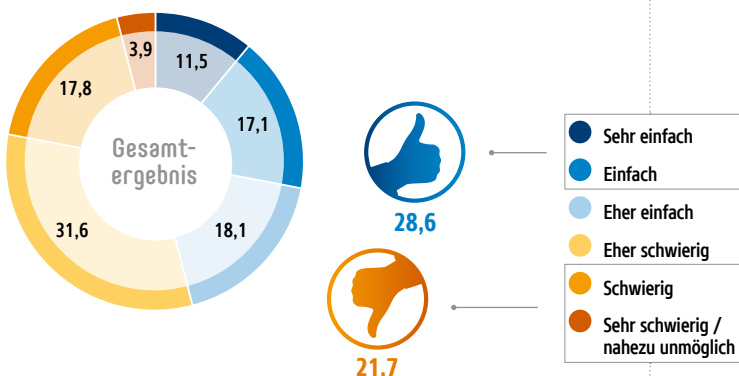
Entscheidungen in Sachen digitaler Souveränität zu treffen, bedeutet im Zweifel auch, den externen Dienstleister wechseln zu können. Und hier zeigt sich eines der Hauptprobleme. Die Unternehmen sind grundsätzlich in einer zu großen technologischen Abhängigkeit gefangen. Dies untermauert eine Reihe von Einzelergebnissen.

So stufen fast 60 Prozent der Befragten den Abhängigkeitsgrad Ihres Unternehmens als sehr hoch oder hoch ein. Im Mittelstand geben das sogar 72 Prozent der Anwenderinnen und Anwender zu erkennen. Und fragt man nur Vertreter aus dem IT-C-Level, so sind es sogar acht von zehn Befragten. Demzufolge gehen auch nur knapp 29 Prozent der Studienteilnehmenden davon aus, dass es grundsätzlich ein leichtes Unterfangen wäre, einen zentralen Hardware- oder Software-Lieferanten zu wechseln. Nahezu identisch ist das Meinungsbild bezüglich der Zusammenarbeit mit IT-Dienstleistern. Diese Zahlen lassen jedoch auch eine andere Interpretation zu: Immerhin ein Fünftel der Unternehmen sieht derzeit keine Chance – aus vertraglichen Gründen, mit Blick auf Budgets (Stichwort: Investitionsschutz und Abschreibungen) oder wegen mangelnder interner Ressourcen (Know-how) – seine IT weitestgehend komplett neu aufzustellen. Und bei rund zwei Drittel der Studienteilnehmenden könnte ein solcher Weg nur unter großen Schwierigkeiten und damit letzten Endes auch nur halbherzig beschritten werden.

In diese Erkenntnis spielt mit hinein, dass zwar einerseits 46 Prozent der Befragten ihre IT-Architektur als flexibel einstufen – der große Rest jedoch nicht.

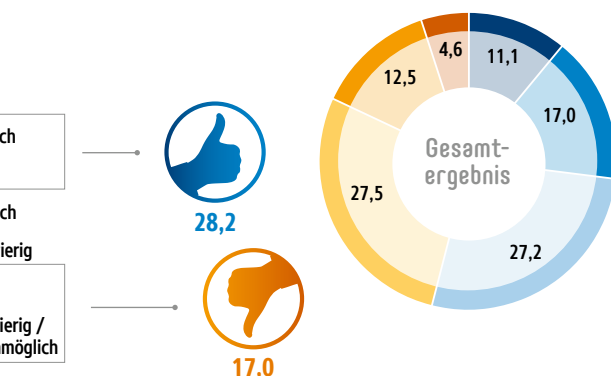
Wie einfach wäre es für Ihr Unternehmen, einen zentralen IT-Technologie-Anbieter zu wechseln?

Angaben in Prozent. Basis: n = 304



Wie einfach wäre es für Ihr Unternehmen, einen zentralen IT-Dienstleister zu wechseln?

Angaben in Prozent. Basis: n = 305



Ergebnis-Split nach Unternehmensgröße



Ergebnis-Split nach Unternehmensgröße



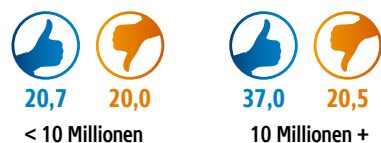
Ergebnis-Split nach Funktion im Unternehmen



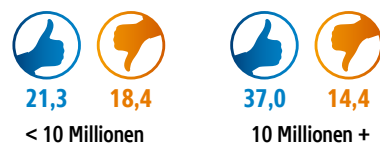
Ergebnis-Split nach Funktion im Unternehmen



Ergebnis-Split nach jährlichen Aufwendungen in IT-Systeme



Ergebnis-Split nach jährlichen Aufwendungen in IT-Systeme



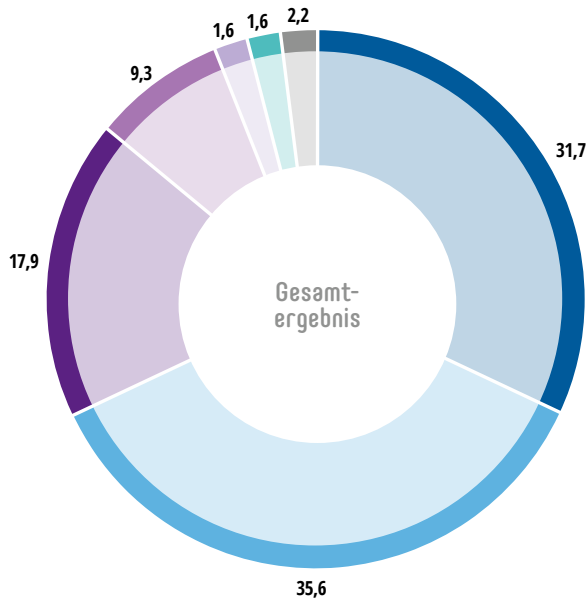
Zudem spielt in diesem Zusammenhang auch der Faktor Zeit eine große Rolle. In allen abgefragten Kerndisziplinen des IT-Managements wie beispielsweise Infrastruktur / Virtualisierung, ERP und CRM, Business Intelligence und Analytics sowie KI-Modelle würde es nach Angaben der Studienteilnehmenden tendenziell bis zu einem halben Jahr dauern, „das Pferd

zu wechseln“. Dieses Risiko und den damit verbunden Aufwand dürften sich die meisten Unternehmen aufgrund geopolitischer und konjunktureller Unwägbarkeiten aktuell kaum leisten wollen.

(Detailliertere Analysen dazu finden Sie unter „Sonstige Ergebnisse“)

Wer hat die Kontrolle über Ihre geschäftskritischen Daten?

Angaben in Prozent. Basis: n = 312



Die Kontrolle über geschäftskritische Daten ist ...

- ... vollständig intern
- ... überwiegend intern
- ... geteilt mit externen Anbietern
- ... überwiegend bei externen Anbietern
- ... vollständig bei externen Anbietern
- Das ist unklar und müsste geprüft werden.
- Weiß nicht

Und noch ein Thema ist hier von großer Relevanz: Wer hat in den Unternehmen die Kontrolle über die geschäftskritischen Daten? Und können die Anwenderinnen und Anwender überhaupt den Speicherort und die Datenflüsse in ihren jeweiligen Cloud-Architekturen nachvollziehen? Letzteres bejaht nur knapp die Hälfte der Befragten un-

eingeschränkt. Dies ist – bezogen auf alle Unternehmensgrößen – eine sehr alarmierende Erkenntnis, die vordergründig nur dadurch entkräftet wird, dass gleichzeitig rund zwei Drittel der Studienteilnehmenden davon ausgehen, weitestgehend selbst (intern) die Kontrolle über alle geschäftskritischen Daten zu haben.

Weitere Statements von den Studienteilnehmenden zu diesem Themenkomplex

„Wir bemühen uns, die Kontrolle über geschäftskritische Daten zu behalten. Doch in der Praxis ist dies nicht immer möglich oder umsetzbar.“

„Die Kontrolle über die geschäftskritischen Daten liegt beim Unternehmen. Die Speicherung und Verarbeitung erfolgt bei Cloud- und ERP-Providern. Die Zusammenarbeit erfolgt unter Einhaltung der DSGVO, sodass die unternehmerische Datenhoheit gewährleistet ist.“

„Wir testen im Moment verschiedene Möglichkeiten. Aktuell haben wir keinen Favoriten.“

„Das Unternehmen behält die vollständige Verfügungsgewalt über alle geschäftskritischen Daten. Externe Dienstleister unterstützen bei der technischen Umsetzung und Speicherung in der EU, ohne dass sie die alleinige Kontrolle über die Daten erhalten.“

„Wir haben einen externen IT-Dienstleister, der für geschäftskritische Daten mitverantwortlich ist.“

Weitere Studienergebnisse

Komplementäre Analysen
und Insights der Studie

Sicherheit und Unabhängigkeit dominieren

Im Mittelpunkt aller Souveränitätsbestrebungen stehen die Aspekte Datenschutz und Data Ownership.

Bei der Frage, aus welchen Gründen die Unternehmen bis dato schon souveräne Cloud-Lösungen implementiert haben oder dies konkret in Betracht ziehen, zeigen sich in der Untersuchung kaum Überraschungen.

Mehr als die Hälfte der Befragten nennen hier zuvorderst IT-Sicherheitsbelange oder Datenschutzgründe. Bei den Großunternehmen beträgt dieser Anteil sogar fast 70 Prozent. An zweiter und dritter Stelle folgen im Ranking möglicher Mehrfachnennungen die Aspekte Unabhängigkeit von kommerziellen Cloud-An-

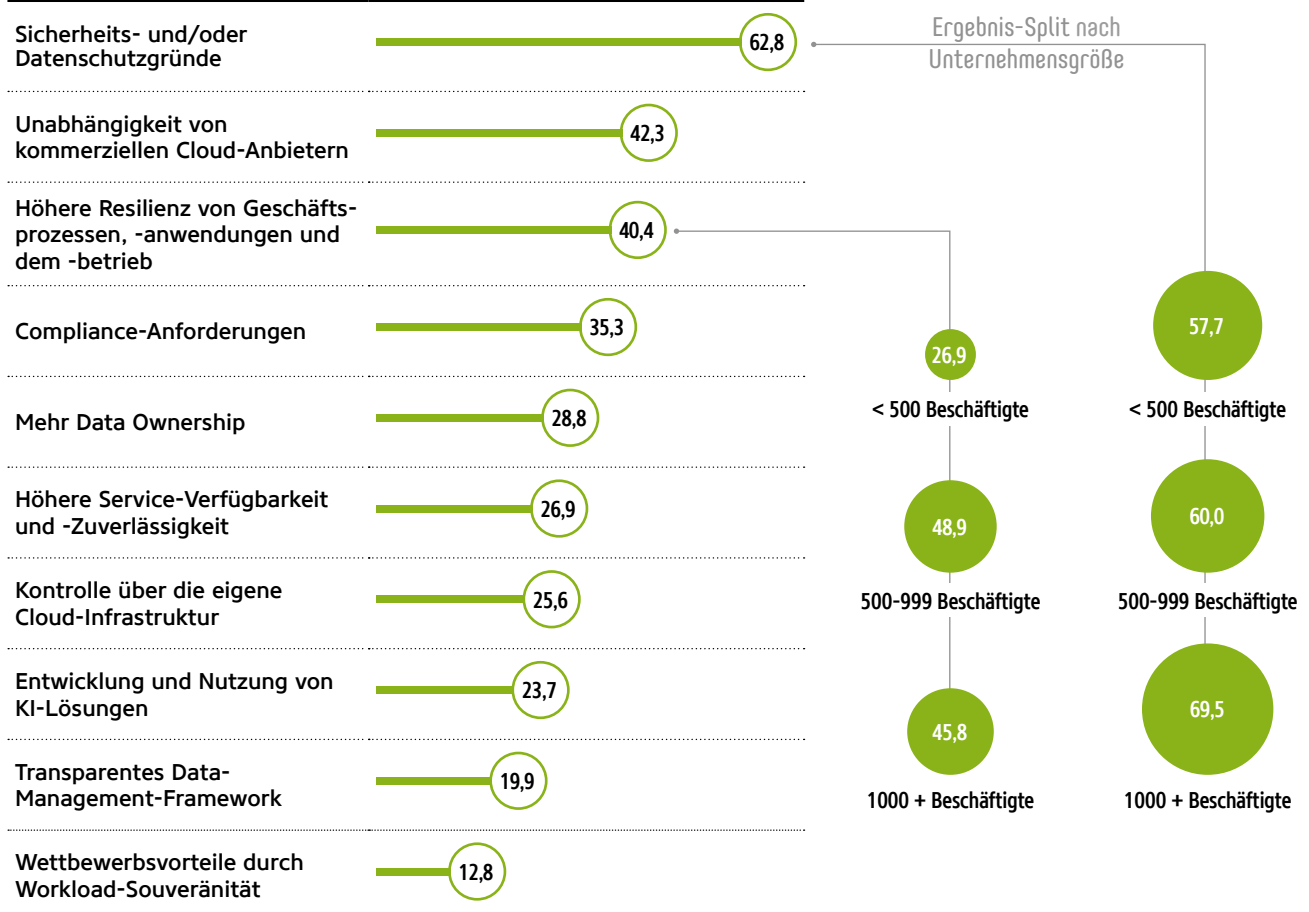
bietern sowie eine höhere Resilienz von Geschäftsprozessen, also dem IT-Betrieb.

Beide Themen hätte man auch als Hauptmotive im Kontext digitaler Souveränität vermuten können – aber am Ende geht es aus Sicht der Anwenderinnen und Anwender doch hauptsächlich um die übergeordnete Herausforderung der Informationssicherheit und des Datenschutzes. Interessant ist auch, dass vor allem die mittelständischen Firmen großen Wert auf ihre Unabhängigkeit und Resilienz legen. Große Bedeutung messen

Aus welchen Gründen hat Ihr Unternehmen souveräne Cloud-Lösungen implementiert oder zieht dies zumindest in Betracht?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die souveräne Cloud-Lösungen einsetzen. Basis: n = 156

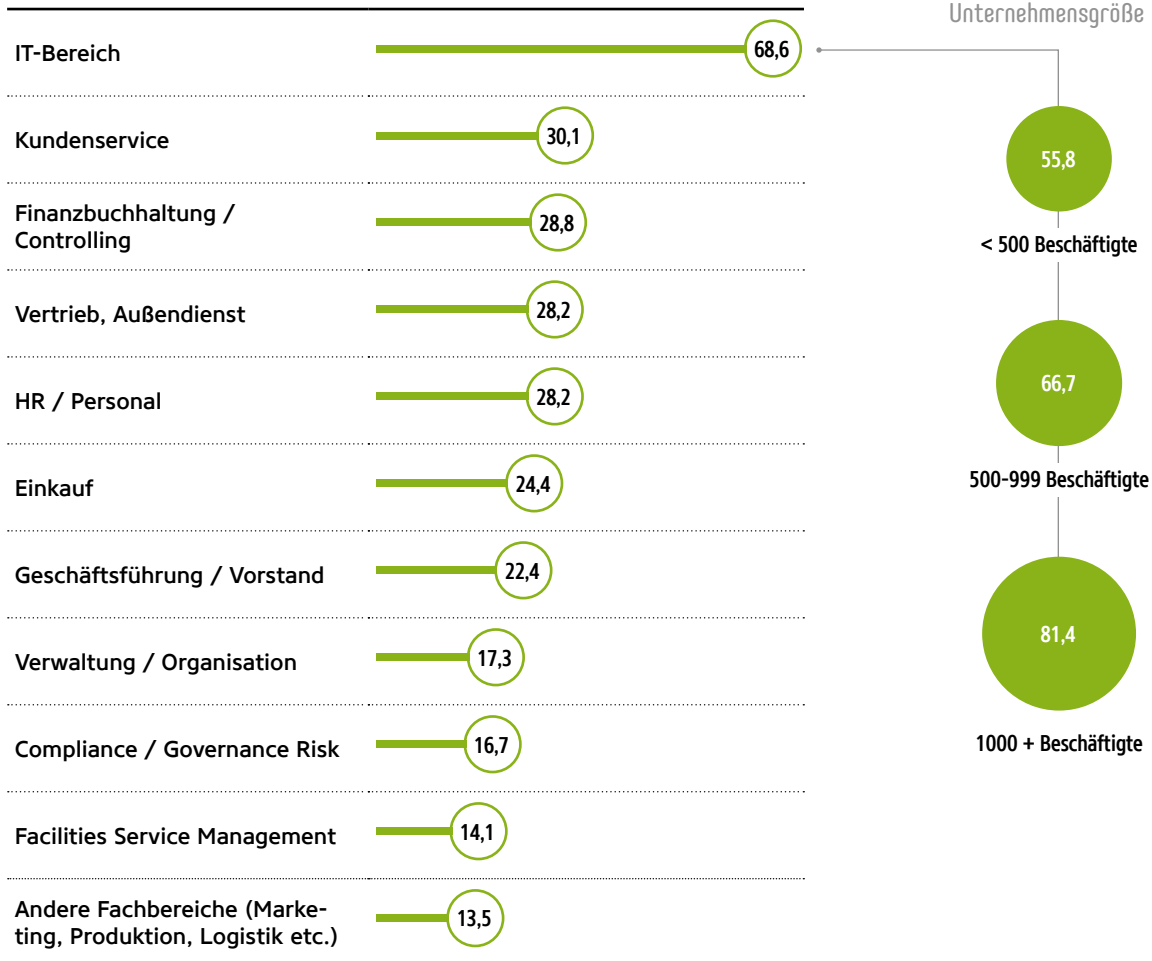
Gesamtergebnis



In welchen Bereichen Ihres Unternehmens kommen souveräne Cloud-Lösungen (künftig) zum Einsatz?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die souveräne Cloud-Lösungen einsetzen. Basis: n = 156

Gesamtergebnis



die Unternehmen beim Thema digitale Souveränität auch der Einhaltung von Compliance-Anforderungen bei.

Ausschlaggebend für die Nutzung souveräner Cloud-Lösungen sind den Studienteilnehmenden zufolge darüber hinaus die eigene Data Ownership, eine höhere Service-Verfügbarkeit und -Zuverlässigkeit sowie mehr Kontrolle über die eigene Cloud-Infrastruktur. Auch die Entwicklung und Nutzung von KI-Lösungen spielt eine wichtige Rolle. Jeweils rund ein Viertel der Befragten attestieren den genannten Themen eine hohe Relevanz.

Aufschlussreich ist auch der Blick in die Zukunft hinsichtlich der Frage, in welchen Geschäftsbereichen die Unternehmen in abseh-

barer Zeit auf die souveräne Cloud setzen wollen. Fast 70 Prozent nennen als erstes den IT-Bereich, bei den Großunternehmen sind es sogar über 80 Prozent. Es folgt mit großem Abstand der Kundenservice, knapp dahinter führen die Befragten die Bereiche Finanzbuchhaltung und das Controlling ins Feld.

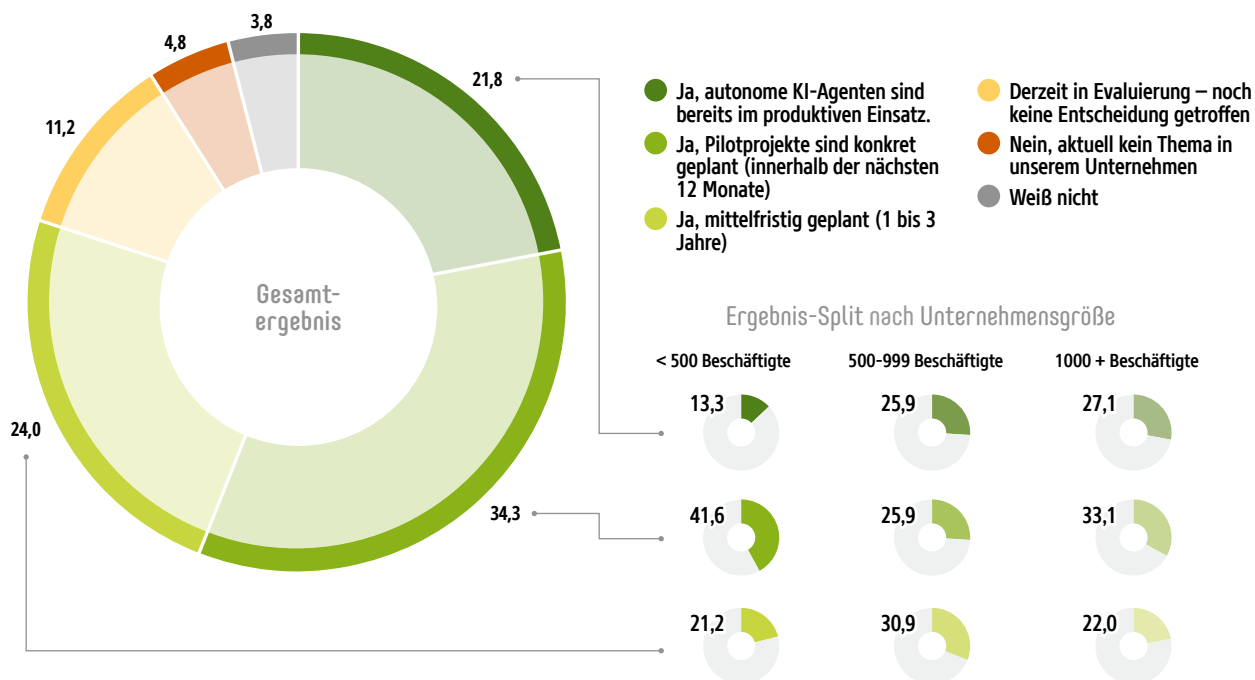
Ebenso bedeutsam für die künftige Nutzung einer souveränen Cloud-Architektur stufen die Anwenderinnen und Anwender (wiederum im Ranking möglicher Mehrfachnennungen) auch die Bereiche Vertrieb und Außendienst, HR/Personal sowie den Einkauf ein. Zumindest mittelfristig sollen zudem auch die allgemeine Verwaltung sowie der Vorstand beziehungsweise die Geschäftsführung einbezogen werden.

KI-Piloten haben Vorrang

Trotz aller Risiken ist den Unternehmen bei der Nutzung von KI-Agenten die Performance ihrer Workloads am wichtigsten.

Planen Sie den Einsatz autonomer KI-Agenten in Kernprozessen Ihres Unternehmens?

Angaben in Prozent. Basis: n = 312



Im Zuge des anhaltenden KI-Booms gewinnt derzeit vor allem die sogenannte agentenbasierte KI an Bedeutung. In dem Maße, wie Unternehmen hier ihre ersten Erfahrungen mit Piloten machen oder gemacht haben, hat dies auch enorme Auswirkungen auf die IT-Prozesse – und damit auch auf eine souveräne IT-Architektur.

Die vorliegende Untersuchung hat daher auch die Nutzung autonomer KI-Agenten abgefragt. Knapp 22 Prozent haben diese bereits im produktiven Einsatz, bei den Großunternehmen sind es sogar 27 Prozent. Rund ein Drittel der Studienteilnehmenden plant konkrete Pilotprojekte innerhalb der nächsten zwölf Monate.

Bemerkenswert ist hier, dass entsprechende Vorhaben in den kleinen Firmen noch einmal deutlich stärker im Fokus stehen als beim

Rest der Anwenderinnen und Anwender. Ein weiteres Viertel der Unternehmen hat das Thema jedoch binnen der kommenden drei Jahre auf der Agenda. Und hier wiederum ist es vor allem der Mittelstand, der mit solchen Plänen vorangeht.

Wie sehr die agenten-basierte KI derzeit die Unternehmen umtreibt, zeigt die Tatsache, dass lediglich fünf Prozent der Befragten zu Protokoll geben, sich derzeit nicht damit zu beschäftigen, weitere 15 Prozent sind noch in einer mehr oder weniger konkreten Evaluierungsphase.

Noch viel spannender ist im Zusammenhang mit der digitalen Souveränität, was für die Unternehmen im Falle einer Hosting-Entscheidung für KI-Agenten höhere Priorität hat: die Performance oder IT-Sicherheit.

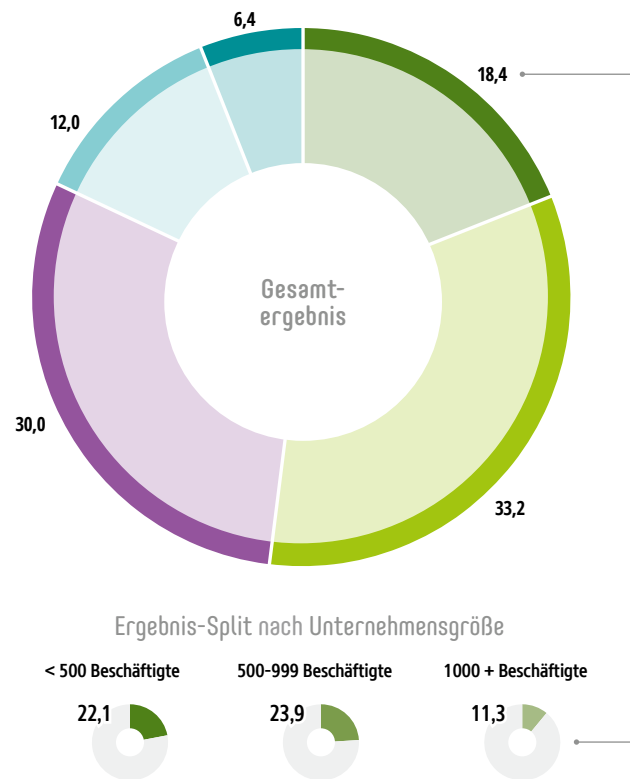
Rund 18 Prozent geben ein klares Votum ab und plädieren für die Performance im Sinne von Geschwindigkeit, Verfügbarkeit und Skalierbarkeit. Allerdings fällt auf, dass sich die Großunternehmen hier im Vergleich deutlich zurückhaltender äußern.

Exakt ein Drittel der Befragten gibt an, den Gesichtspunkt der Performance mehr im Auge zu haben, ohne Sicherheitskriterien im Kern zu vernachlässigen. Knapp ein Drittel vermeidet jegliche Priorisierung. Lediglich 18 Prozent legen einen stärkeren Fokus auf Datenschutz, Compliance und Kontrolle.

- Eindeutig die Performanz — Geschwindigkeit, Verfügbarkeit und Skalierbarkeit sind entscheidend
- Eher die Performanz, aber Sicherheit ist ein wichtiges Kriterium
- Beides gleichwertig
- Eher Sicherheit, aber Performanz darf nicht leiden
- Eindeutig die Sicherheit — Datenschutz, Compliance und Kontrolle haben Vorrang

Wenn Ihr Unternehmen eine Hosting-Entscheidung für KI-Agenten trifft: Was hat für Sie höhere Priorität: Performanz oder Sicherheit?

Angaben in Prozent. Filter: Unternehmen, die KI-Agenten in Kernprozessen einsetzen, dies konkret planen oder mittelfristig planen. Basis: n = 250



Ausgewählte Zitate von Studienteilnehmenden zur Priorisierung beim Hosting von KI-Agenten

„Performance oder kurzfristige Gewinne sollten niemals über der Bedeutung von Sicherheit und langfristigen Strategien stehen.“

„Beides ist essenziell für ein innovatives Unternehmen.“

„Sicherheit steht bei uns an erster Stelle.“

„Die Performance darf nicht aufgrund von Sicherheitsmaßnahmen leiden.“

„Ohne Sicherheit ist Performance nichts.“

„Wir priorisieren die Performance leicht höher, da Verzögerungen bei KI-Agenten direkt die Nutzererfahrung und Geschäftsprozesse beeinträchtigen würden. Gleichzeitig beziehen wir aber Sicherheitsstandards wie Verschlüsselung und Zugriffskontrollen als verbindliche Grundvoraussetzung ein.“

3 Open Source ist fest etabliert

Beim Betrieb souveräner IT-Architekturen sind Open-Source-Technologien inzwischen gesetzt.

Die Nutzung von Open Source gilt als einer der Hoffnungsträger beim Weg in die digitale Souveränität und rangiert in der vorliegenden Untersuchung unter den sechs wichtigsten Maßnahmen, die die Unternehmen ergreifen wollen. Insofern lohnt es sich, sich detaillierter die Bereiche anzusehen, in denen die Anwenderinnen und Anwender aktiv auf Open-Source-Standards setzen wollen.

Rund 56 Prozent der Befragten nennen hier in erster Linie den Betrieb ihrer Cloud-Plattformen sowie – damit zusammenhängend – den Bereich Virtualisierung. Bei den kleinen Firmen beträgt dieser Anteil sogar 65 Prozent. An zweiter Stelle rangiert im Ranking möglicher Mehrfachnennungen mit einem Anteil von fast 40 Prozent das Themen-

feld IT-Security. Hier wiederum fällt auf, dass die Großunternehmen Cyber Security im Kontext der Nutzung von Open Source noch einmal deutlich höher gewichten. Ein bemerkenswertes Einzelergebnis!

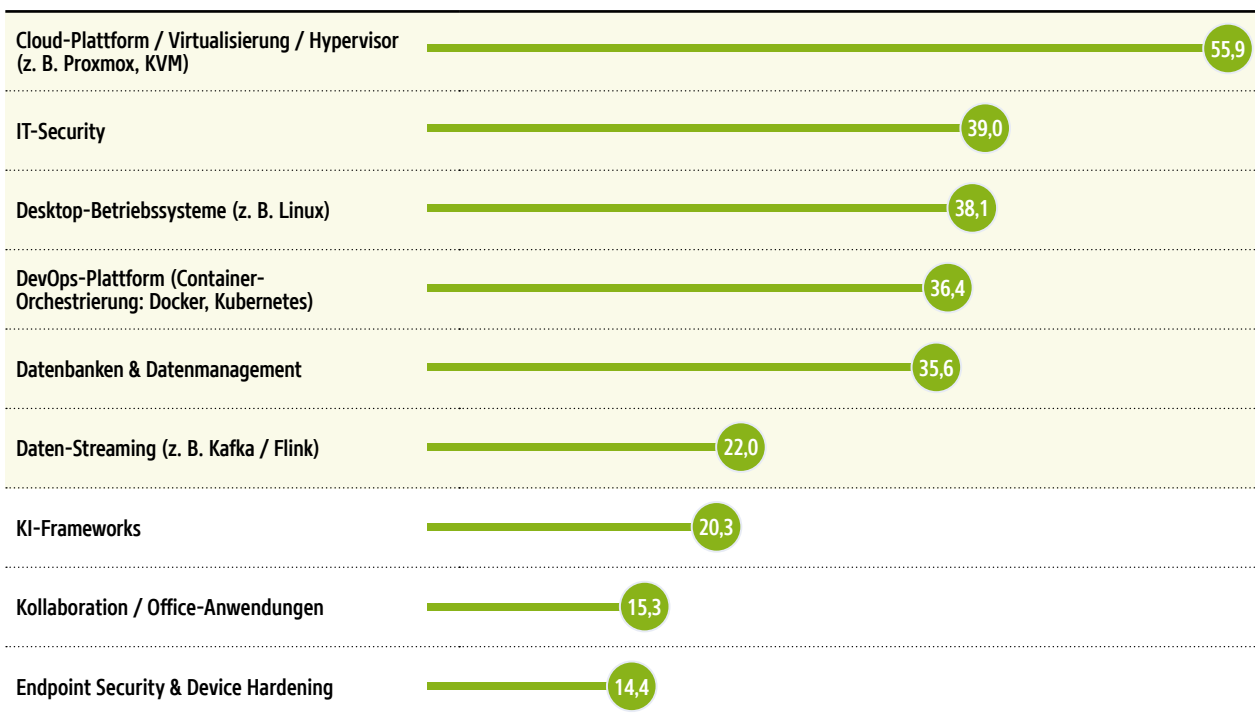
Nahezu gleichauf liegen in der Folge die Bereiche Desktop-Betriebssysteme (zum Beispiel: Linux) sowie DevOps-Plattformen – Stichworte: Container-Orchestrierung, Docker, Kubernetes. In diesen ureigenen Open-Source-Domänen gibt es auch mit Blick auf die Unternehmensgrößen ein einheitliches Meinungsbild. Gleiches gilt für Datenbanken und das Data Management.

KI-Frameworks sowie die klassischen Office-Anwendungen stehen indes nicht so

In welchen Bereichen setzen Sie aktiv auf Open-Source-Standards mit dem Ziel, digitale Souveränität zu sichern?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die Open-Source nutzen. Basis: n = 118

Gesamtergebnis

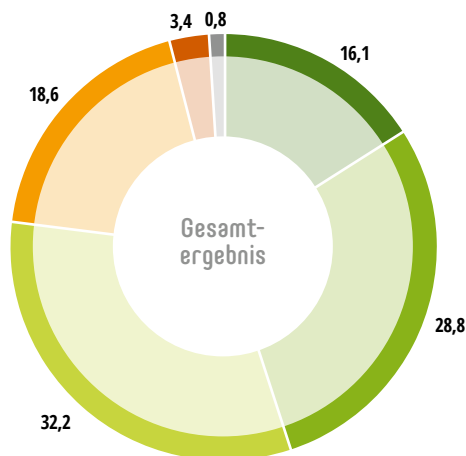


sehr im Fokus der Anwenderinnen und Anwender, wenn es um die Stärkung ihrer digitalen Souveränität geht. Lediglich 20 beziehungsweise 15 Prozent verfolgen hier aktuell entsprechend Pläne.

Grundsätzlich ist das einschlägige Know-how in den Unternehmen durchaus vorhanden, aber noch ausbaufähig ist. Lediglich 45 Prozent verweisen auf eine umfassende interne Expertise in Sachen Implementierung und Betrieb von Open-Source-Technologien. Ein weiteres Drittel reklamiert für sich solide Kenntnisse hinsichtlich ausgewählter Open-Source-Produkte. Knapp 19 Prozent der Befragten attestieren sich zumindest grundlegendes Open-Source-Wissen.

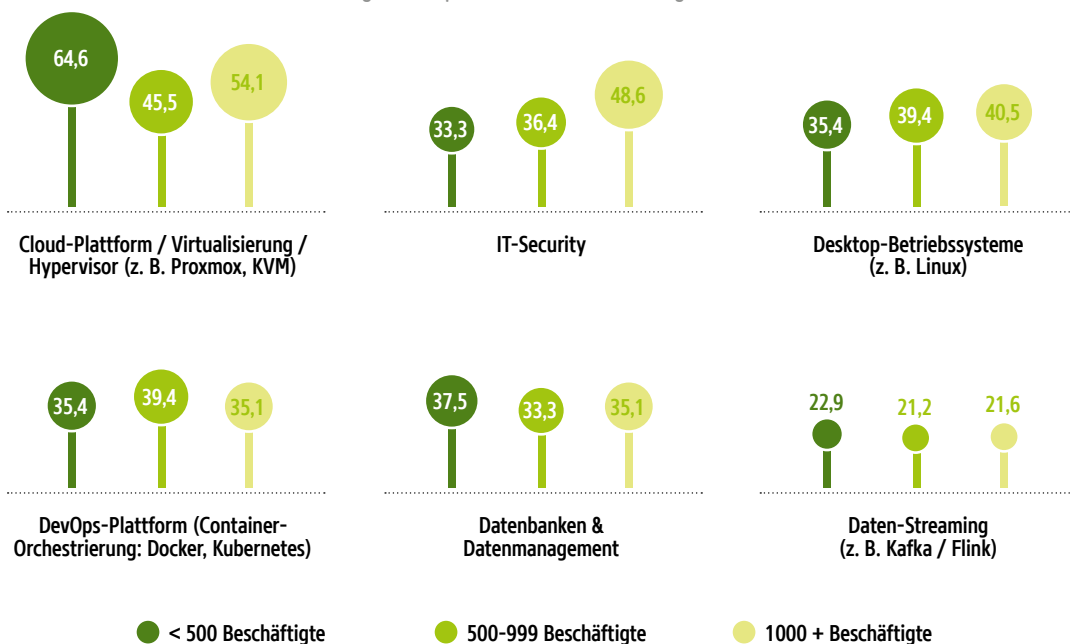
Besitzt Ihr Unternehmen die notwendige interne Fachkompetenz, um Open-Source-Lösungen nachhaltig zu implementieren, zu betreiben und weiterzuentwickeln?

Angaben in Prozent. Filter: Unternehmen, die Open-Source nutzen. Basis: n = 118



- Sehr hohe interne Expertise inkl. aktiver Weiterentwicklung
- Umfassende interne Expertise für Implementierung und Betrieb ist vorhanden
- Solides internes Know-how für ausgewählte Open-Source-Technologien ist vorhanden
- Grundlegendes Know-how ist vorhanden, jedoch mit Einschränkungen
- Nein, es besteht kaum internes Know-how im Bereich Open Source
- Weiß nicht

Ergebnis-Split nach Unternehmensgröße

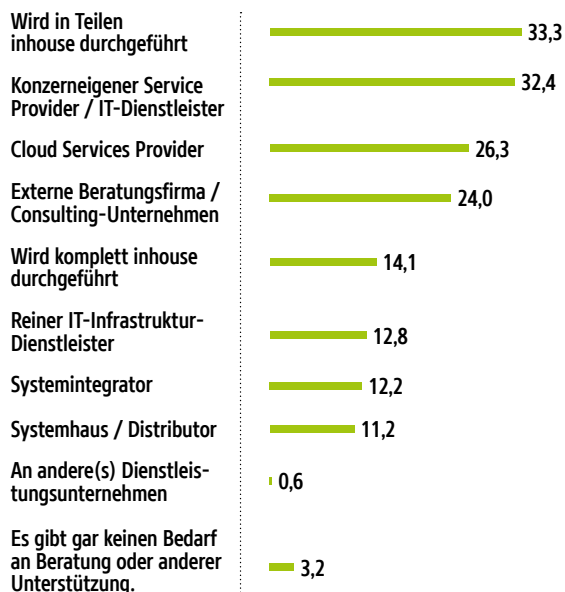


Interoperabilität und räumliche Nähe sind Trumpf

Bei den Kriterien für die Dienstleistungsauswahl dominieren bekannte Motive.

An welche Art von (externen) Dienstleistungsunternehmen wendet sich Ihr Unternehmen, wenn es um Maßnahmen zur Stärkung der eigenen digitalen Souveränität geht?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312



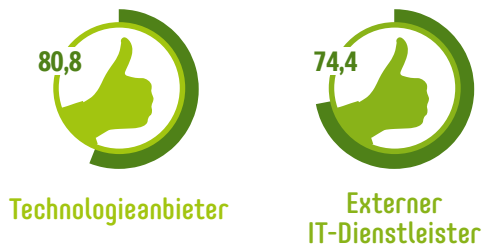
Digitale Souveränität hat bekanntermaßen sehr viel mit der Dienstleistungsauswahl zu tun. Unabhängig davon, welche Möglichkeiten die Unternehmen im Einzelnen für sich sehen, ist es auch interessant, zu erfahren, nach welchen Kriterien sie dabei vorgehen.

In zwei Drittel aller Fälle wenden sich die Anwenderinnen und Anwender an den konzern-eigenen IT-Dienstleister, für ein weiteres Viertel ist ein externer Cloud Provider die erste Wahl. Nahezu ebenso viele Studienteilnehmenden sprechen sich im Ranking möglicher Mehrfachnennungen für die Zusammenarbeit mit einem IT-Beratungshaus aus.

Fester Anker beim Fulfillment digitaler Souveränität sind den Anwenderinnen und Anwendern zufolge aber auch die reinen IT-Infrastruktur-Dienstleister, Systemintegratoren und Systemhäuser, die insgesamt mehr als 36 Prozent der Befragten zu Rate ziehen würden.

Ist der Unternehmenssitz eines Technologie-Anbieters oder externen IT-Dienstleisters für Sie ein maßgebliches Auswahlkriterium?

Angaben in Prozent. Dargestellt ist der kumulierte Wert für „maßgebliches Kriterium“ und „eines von mehreren maßgeblichen Kriterien“. Basis: n = 312.

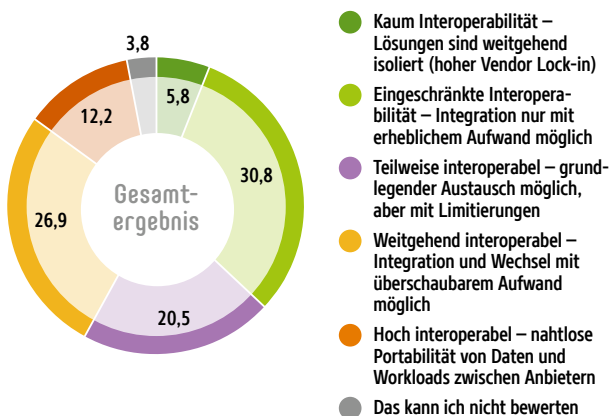


Inzwischen ist auch der Unternehmenssitz eines Technologie-Anbieters oder externen IT-Dienstleisters ein maßgebliches Auswahlkriterium. Mehr als 80 beziehungsweise 75 Prozent der Befragten bejahen dies. Nur für eine Minderheit von 17 beziehungsweise 22 Prozent ist dies ein nachgelagertes oder gar kein Entscheidungskriterium. Hier sind sich auch die Befragten über alle Firmengrößen hinweg sehr einig.

Darüber hinaus wurde auch die Frage nach der Interoperabilität zwischen den Cloud-Lösungen der europäischen Anbieter gestellt. Rund 37 Prozent stellen hier den in der EU ansässigen Providern kein gutes Zeugnis aus und sprechen von weitgehend isolierten Angeboten oder zumindest eingeschränkter Interoperabilität mit dem Charakter eines Vendor Lock-ins. Weitere 21 Prozent verweisen auf Limitierungen in ihrer Handlungsfreiheit, und nur rund 40 Prozent sind mit dem ihnen angebotenen Maß an Interoperabilität zufrieden.

Wie bewerten Sie die Interoperabilität zwischen Cloud-Lösungen europäischer Anbieter?

Angaben in Prozent. Filter: Unternehmen, die souveräne Cloud-Lösungen einsetzen. Basis: n = 156



Faktor Zeit spielt Providern in die Karten

Hinsichtlich ihrer Exit-Fähigkeit sind die Unternehmen bei einem etwaigen Dienstleisterwechsel nur bedingt flexibel aufgestellt.

Ein sehr entscheidendes Kriterium bei einem etwaigen Dienstleisterwechsel ist auch der Faktor Zeit. Konkret geht es hier um die Frage, wie viel Zeit der vollständige Wechsel zu einem anderen Anbieter beanspruchen würde – bezogen auf die einzelnen Bereiche einer unternehmensweiten IT-Landschaft.

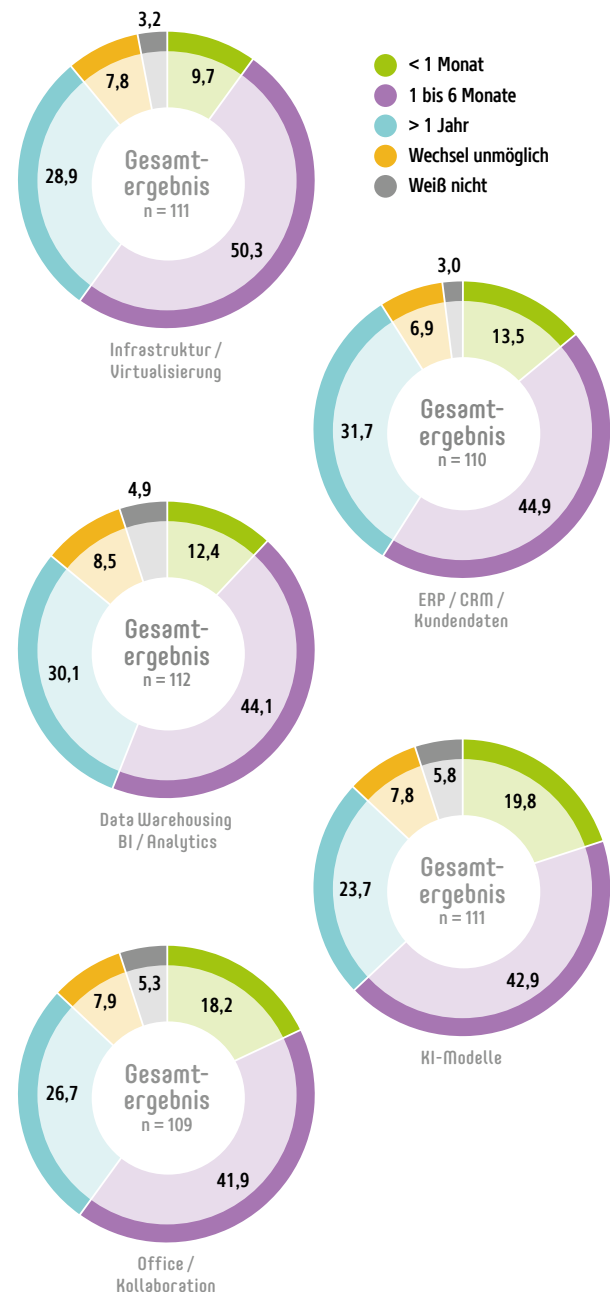
Numerisch betrachtet sehen die Anwenderinnen und Anwender bei der Nutzung von KI-Modellen die größten Hürden, wenn ein Providerwechsel anstünde. Rund 63 Prozent veranschlagen hier eine Übergangsperiode von bis zu einem halben Jahr. Sehr ähnlich sieht es in den Bereichen IT-Infrastruktur sowie Virtualisierung aus. Und sehr überraschend: Auch beim Thema Device Management gehen die Unternehmen von einer im Durchschnitt halbjährigen Transitionsphase aus. Letzteres dürfte wohl in erster Linie den längeren Lieferzeiten bei den Endgeräte-Herstellern geschuldet sein.

Auch bei den IT-Sparten und Systemlandschaften ERP, CRM, Data Warehousing, BI sowie Office und Collaboration Software nähme ein Dienstleisterwechsel bis zu sechs Monate in Anspruch, so die Annahme der Studienteilnehmenden.

Noch drei weitere Kernaussagen lassen sich aus den Einzelergebnissen zu dieser Frage ableiten: Mehr als ein Viertel der Befragten kalkuliert sogar mit mehr als sechs Monaten Übergangszeit im Falle eines Providerwechsels. Rund sieben Prozent halten einen Wechsel sogar grundsätzlich für unmöglich. Und: Das Meinungsbild ist über alle IT-Sparten und Unternehmensgrößen hinweg einhellig.

Wie schätzen Sie Ihre aktuelle Exit-Fähigkeit ein: Wie viel Zeit würde ein vollständiger Wechsel des Anbieters/Dienstleisters in den folgenden Bereichen schätzungsweise beanspruchen?

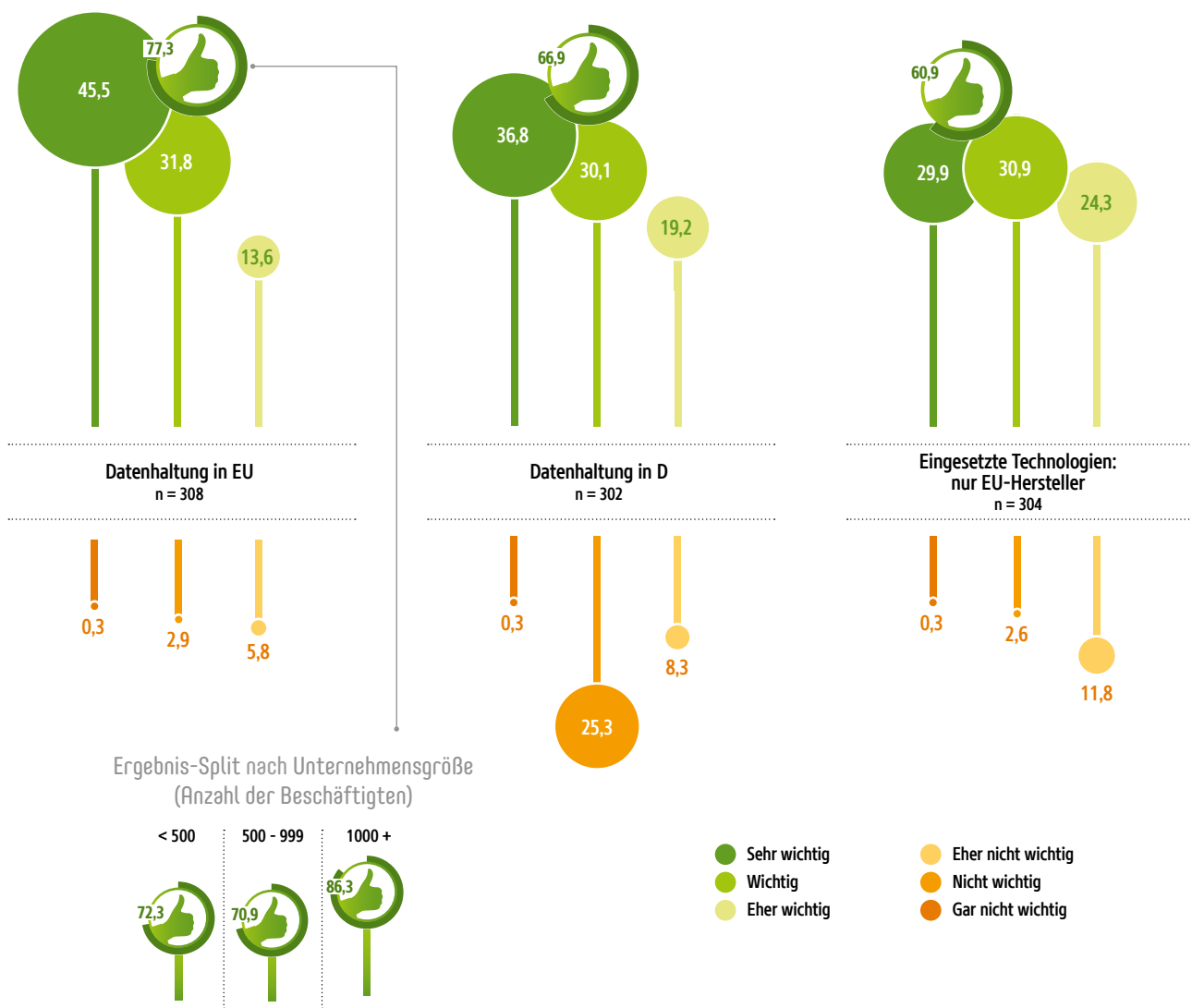
Angaben in Prozent. Basis: n = 303-308



Es bleibt also festzuhalten: Die Exit-Fähigkeit der Unternehmen kennt in puncto Geschwindigkeit ihre Grenzen und gestaltet sich damit im Hinblick auf die geforderte Agilität im Wettbewerb und den Geschäftsprozessen als schwieriges Unterfangen.

Wie wichtig sind Ihnen die folgenden Kriterien bei der Auswahl eines externen Managed-SOC-Dienstleisters (inklusive Incident Response)?

Angaben in Prozent. Basis: n = 302 - 308



Ort der Datenhaltung hat Top-Priorität

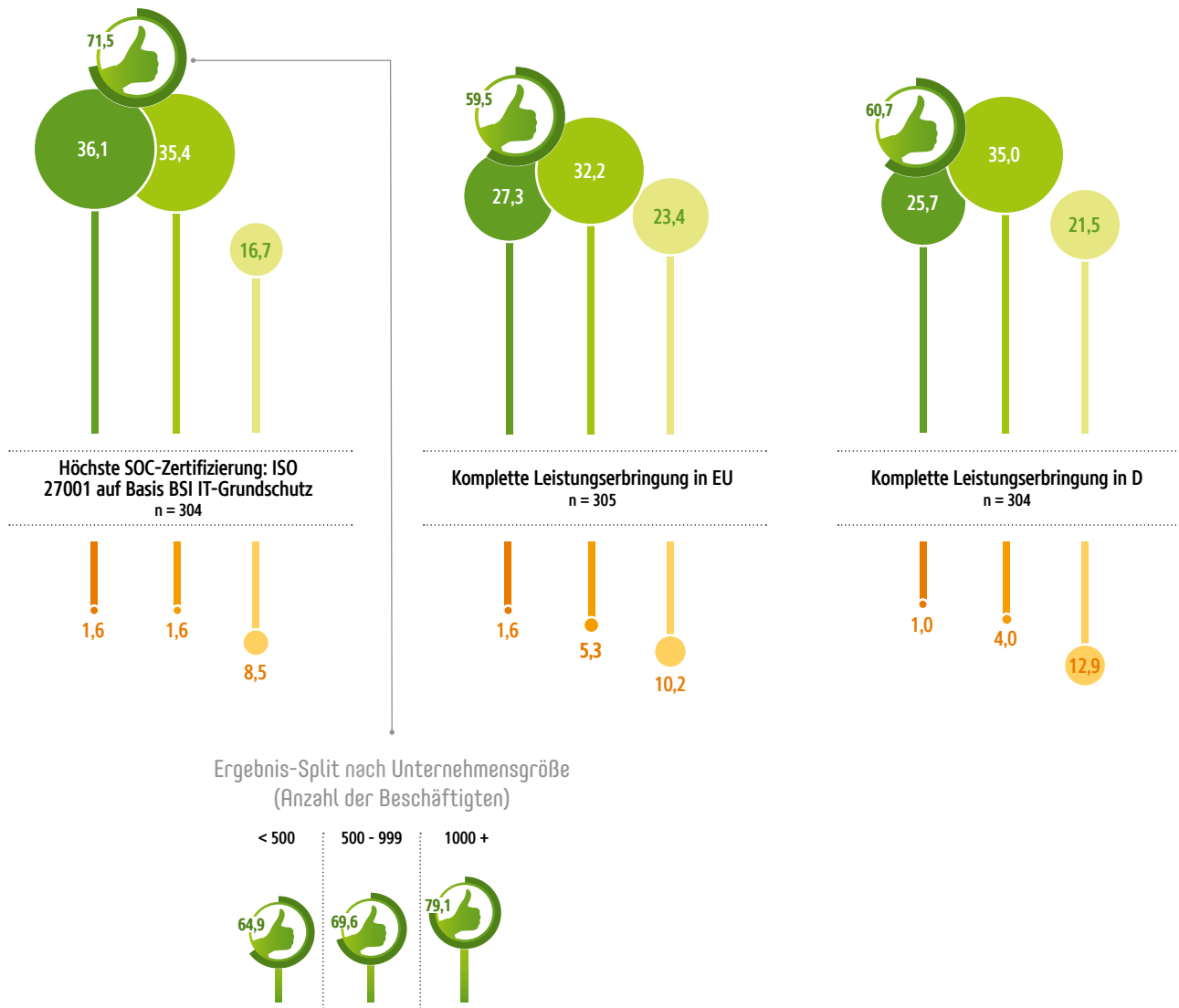
Nicht nur aber vor allem auch bei der Auswahl eines Managed-SOC-Dienstleisters ist dessen Herkunft entscheidend.

Eines der wichtigsten Themen im Kontext digitaler Souveränität ist IT-Sicherheit. No-lens volens kommt deshalb einschlägigen Dienstleistern, insbesondere im Bereich Security Operation Center (SOC), eine übergeordnete Bedeutung zu.

Was sind aber nun bei den Unternehmen, die eine eigene operative IT-Security-Organisation nicht vorhalten können oder wollen, die wichtigsten Auswahlkriterien für einen Managed-SOC-Dienstleister?

Mit absoluter Priorität wird hier die Datenhaltung in der EU gesehen, für die sich im Durchschnitt 77 Prozent der Befragten aussprechen, bei den größeren Unternehmen sind es sogar 86 Prozent. Exakt zwei Drittel der Studienteilnehmenden grenzen diese Anforderung regional sogar noch ein und plädieren für ein Hosting in Deutschland.

Neben dem Ort der Datenhaltung nennen die Unternehmen als zweitwichtigstes Kriterium bei der Entscheidung für einen Managed-SOC-



Dienstleister dessen höchstmögliche SOC-Zertifizierung, und zwar die ISO 27001 mit dem (entscheidenden) BSI-Zusatz „auf der Basis von IT-Grundschutz“. Für rund 72 Prozent der Anwenderinnen und Anwender ist diese Zertifizierung mehr oder weniger unabdingbar, bei den Großunternehmen stellen sogar 79 Prozent diese Anforderung.

Interessant ist in diesem Kontext auch, dass jeweils rund 60 Prozent der Befragten eine komplette Leistungserbringung in der EU oder in Deutschland voraussetzen. Und noch bemerkenswerter ist die Tatsache, dass ebenfalls 60 Prozent der Studienteilnehmenden erwarten, dass ihr Provider nur Techno-

logien von EU-Herstellern einsetzt. Im Einzelfall dürfte Letzteres spannend werden. Jedenfalls liegt hier die Vermutung nahe, dass dabei in erster Linie an Open-Source-Technologien gedacht wird.

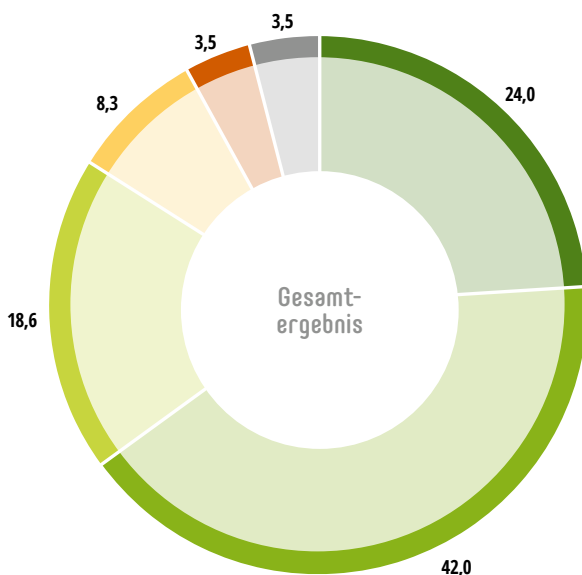
Last, but not least kommen bei den Auswahlkriterien auch zwei weitere bekannte Entscheidungsmuster zur Geltung. Mehr als die Hälfte der Unternehmen präferiert einen Provider, der seine personellen und technischen Ressourcen nicht nach dem „Follow-the-Sun“-Prinzip allokiert, also global aufgestellt ist. Und für fast zwei Drittel der Anwenderinnen und Anwender ist letzten Endes auch der Preis ausschlaggebend.

Digitale Souveränität bleibt ein indifferentes Ziel

Trotz eines grundsätzlichen Bekenntnisses der Unternehmen zur digitalen Selbstbestimmtheit gibt es unterschiedliche Sichtweisen darauf.

Ist „digitale Souveränität“ für Ihr Unternehmen ein Verkaufsargument gegenüber den eigenen Kunden und Geschäftspartnern?

Angaben in Prozent. Basis: n = 312



- Ja, wir nutzen das aktiv als wichtiges, zentrales Argument.
- Ja, wir nutzen das als Argument, aber eher ergänzend / situativ / kundenabhängig.
- Ja, wenn z. B. in Ausschreibungen gefordert
- Eher nein / kaum relevant
- Nein, das spielt in Richtung unserer Kunden und Geschäftspartner keine Rolle.
- Weiß nicht

Wie sehr die Unternehmen derzeit Anstrengungen unternehmen, ihre digitale Souveränität zu verbessern, zeigen die einzelnen Ergebnisse der vorliegenden Untersuchung eindeutig. Zusammenfassend belegen auch noch einmal ausgewählte Fragen zum Stimmungsbild die hohe Relevanz des Themas.

So nutzt beispielsweise knapp ein Viertel der Anwenderinnen und Anwender die eigene digitale Souveränität auch als Verkaufsargument gegenüber den eigenen Kunden und Geschäftspartnern. Mehr als 40 Prozent geben zu Protokoll, das Argument der digitalen Souveränität zumindest kundenabhängig

beziehungsweise situativ ins Spiel zu bringen. Weitere 19 Prozent der Unternehmen verweisen darauf bei Ausschreibungen, an denen sie sich beteiligen.

Nahezu die Hälfte der Befragten stimmt auch der Aussage zu, dass souveräne Cloud-Lösungen nicht nur die Sicherheit und Unabhängigkeit von Unternehmen, sondern auch die Selbstbestimmtheit ganzer Staaten stützt. In 46 Prozent der Unternehmen überwiegt auch die Überzeugung, dass in Zeiten wie diesen Rechtsraumsouveränität wichtiger denn je ist. Aspekte wie der Datenstandort, die Rechtsprechung, die Einhaltung von Compliance-Richtlinien, der Schutz vor externem Zugriff und die vertragliche Souveränität müssen rechtssicher geregelt sein, heißt es weiter.

Sehr indifferent sind die Reaktionen auf die These, wonach die Fokussierung auf digitale Souveränität notwendige technologische Innovationen ausbremst. Knapp 30 Prozent stimmen dieser Ansicht zu, knapp ein Viertel sieht dies komplett anders.

In der Tendenz sehr ähnlich ist das Meinungsbild der Anwenderinnen und Anwender bei zwei weiteren kontroversen Thesen. Jeweils rund ein Drittel teilen die Auffassung, wonach die Datensouveränität in einer souveränen Cloud-Lösung infolge der Abhängigkeit von den globalen Technologie-Giganten eine Illusion ist – und dass die Debatte um digitale Souveränität auf einer übertriebenen Angst vor Datenmissbrauch durch ausländische Mächte basiert. Umgekehrt vertreten jeweils knapp 25 Prozent die völlig gegenteilige Meinung.

Abschließend auch noch einmal zu der Frage nach den Hürden, die nach Ansicht der Unternehmen die Umsetzung der digitalen Sou-

Inwieweit stimmen Sie den folgenden Aussagen zu?

Angaben in Prozent. Basis: n = 308-311



„Souveräne Cloud-Lösungen stärken die Sicherheit und Unabhängigkeit nicht nur von Unternehmen und Behörden, sondern auch von ganzen Staaten!“



„Digitale Souveränität ist nur dann wirksam, wenn sie operativ einfach und effizient umsetzbar ist.“



„Die Verwendung freier Open-Source-Technologien, offener APIs und plattformabhängiger Orchestrierungswerkzeuge kann die Entwicklung souveräner Cloud-Lösungen unterstützen.“



„Datensouveränität durch souveräne Cloud-Lösungen ist eine Illusion – denn jede Cloud-Lösung ist per se abhängig von globalen Technologiegiganten, deren Soft- und Hardware sie nutzt!“



„In Zeiten wie diesen ist Rechtsraumsoveränität wichtiger denn je! Aspekte wie der Datenstandort, die Jurisdiktion, die Compliance-Sicherung, der Schutz vor externem Zugriff und die vertragliche Souveränität müssen rechtssicher geregelt sein!“



„Die Debatte um digitale Souveränität basiert auf einer übertriebenen Angst vor Datenmissbrauch durch ausländische Mächte, was nur die wenigsten Unternehmen wirklich betrifft.“

veränität erschweren. Rund 38 Prozent der Befragten nennen hier als erstes die Komplexität ihrer bestehenden IT-Systeme. Fast ebenso viele Studienteilnehmende verweisen auf Budget-Restriktionen und scheuen vor den ihrer Meinung nach zu hohen Migrationskosten zurück.

Es folgen im Ranking möglicher Mehrfachnennungen die Aspekte „Fehlende (technologische) Alternativen“, der vorherrschende Fachkräftemangel sowie unzureichende Schnittstellen. Zählt man zu den vermissten Technologie-Alternativen noch die vermeintlich zu geringe Auswahl bei Anbietern mit einem geeigneten Technologie-Stack hinzu, bedeutet dies im Umkehrschluss: Die Komplexität und Individualität zahlreicher Architekturen erschwert vielerorts die digitale Selbstbestimmung.

Welche Hürden erschweren aktuell die Umsetzung digitaler Souveränität?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 312



Blick in die Zukunft

© stock.adobe.com / envrfx (auch S. 5)

Die inhaltliche Einordnung
der Studienergebnisse –
eine Marktperspektive

Souverän ohne Daten?

Digitale Souveränität beschreibt die Fähigkeit von Individuen, Unternehmen und Staaten, digitale Technologien und Daten selbstbestimmt, sicher und unabhängig zu nutzen sowie zu gestalten. Sie zielt darauf ab, einseitige Abhängigkeiten von globalen Tech-Konzernen oder ausländischen Staaten zu vermeiden und die eigene Handlungsfähigkeit zu wahren. Soweit die Definition – oder besser gesagt: die graue Theorie.

Von Gerhard Holzwart

Im Alltag der IT- und Business-Verantwortlichen in den Unternehmen gestaltet sich die Herausforderung, digital selbstbestimmt zu agieren, dann doch etwas facettenreicher. In einer der Freitextantworten der vorliegenden Untersuchung hat einer der Studienteilnehmenden das künftig digital souveräne Unternehmen jedenfalls zutreffend charakterisiert: Es bewahrt seine Handlungsfähigkeit, indem es die Kontrolle über seine Daten, Infrastruktur und KI-Technologien behält, ohne auf Innovationen zu verzichten.

Was heißt das nun? Die IT- und Business-Verantwortlichen sollten, so könnte eine der Empfehlungen lauten, tunlichst zwischen der politischen und IT-spezifischen Dimension digitaler Souveränität unterscheiden.

Schon die Leaks von Edward Snowden zeigten 2013, dass ausländische Geheimdienste systematisch europäische Regierungs- und Wirtschaftsdaten abschöpften. Das Thema

Sicherheit bekam in der Folge schlagartig eine geopolitische Note. In der Folge wurde unter anderem das Projekt Gaia-X ins Leben gerufen, um eine souveräne europäische Dateninfrastruktur zu schaffen und die Dominanz der US-Hyperscaler zu brechen. Die Covid-Krise ab 2020 legte schließlich die digitale Verwundbarkeit von Schulen, Behörden und Unternehmen offen, was die Rufe nach technologischer Selbstständigkeit noch einmal drastisch verstärkte.

Von Gaia-X spricht heute kaum noch jemand. Aktuell berichten Beobachter indes von einer geopolitischen Fragmentierung. Die Zollpolitik der US-Administration unter Trump sowie der Krieg in der Ukraine und diverse Handelskonflikte lassen die digitale Souveränität fast zu einer Überlebensfrage im globalen Wettbewerb werden. Gleichzeitig rücken die künstliche Intelligenz und damit die Datensouveränität immer mehr in den Vordergrund.

Soweit zu den politischen und wirtschaftlichen Rahmenbedingungen, die die Firmen in ihre Strategien so weit wie möglich eingepreist haben. Sie streben ein Höchstmaß an technologischer und operativer Souveränität an. Also in der Lage zu sein, die eigene IT-Infrastruktur und -Plattformen samt Applikationen über den gesamten Lebenszyklus zu kontrollieren sowie gleichzeitig größtmögliche Flexibilität in den Beziehungen zu den Providern zu haben.

Die Unternehmen wollen personenbezogene Daten von Kunden und Mitarbeitenden noch besser geschützt wissen und wünschen sich weitestgehende Datensouveränität. Sie fragen: Wo liegen meine Daten? Wer kann darauf zugreifen? Wer trainiert mit welchen Daten – und wer kontrolliert die Ergebnisse?

Letzteres hat besondere Brisanz. Denn mit dem Boom von Large Language Models (LLMs) verschob sich der technische Fokus des Themas Souveränität inzwischen völlig in Richtung Kontrolle über Trainingsdaten, Rechenzentren und KI-Modelle. Doch Datensouveränität setzt Datenkontrolle und damit ein funktionierendes Datenmanagement voraus. Und hier haben die meisten Unternehmen immer noch große Defizite.

Natürlich haben die meisten Anwenderinnen und Anwender in den letzten Jahren enormes geleistet. Sie haben ihre Prozesse modernisiert und automatisiert, die Customer Experience optimiert, strategische Workloads in die Cloud transformiert – kurzum: ihre Unternehmen und Organisationen zum Teil neu erfunden. Aber haben sie die absolute Kontrolle über ihre Daten?

Die Frage stellt sich nicht nur im Zusammenhang mit dem Ort des Hostings und dem Sitz des Providers, sondern sie stellt sich vor allem auch in puncto Datenqualität. Einmal mehr ist in dieser Studie vom Bekenntnis der Unternehmen die Rede, in den Aufbau einer eigenen Datenplattform zu investieren sowie eine klare Datenstrategie zu implementieren. Doch seit wie vielen Jahren hören und lesen wir schon davon?

In jeder der derzeit unzähligen KI-Konferenzen für IT-Führungskräfte berichten die Redner und Rednerinnen davon, dass ein jedes LLM nur so gute Ergebnisse erzeugen kann, wie die entsprechend verfügbare Datenbasis an Qualität vorhält. Digital souverän zu werden und zu bleiben, ist also kein Selbstläufer – erst recht nicht im KI-Zeitalter.

CIO-Agenda 2026

**Daten zur allgemeinen Einschätzung
der Marktlage**

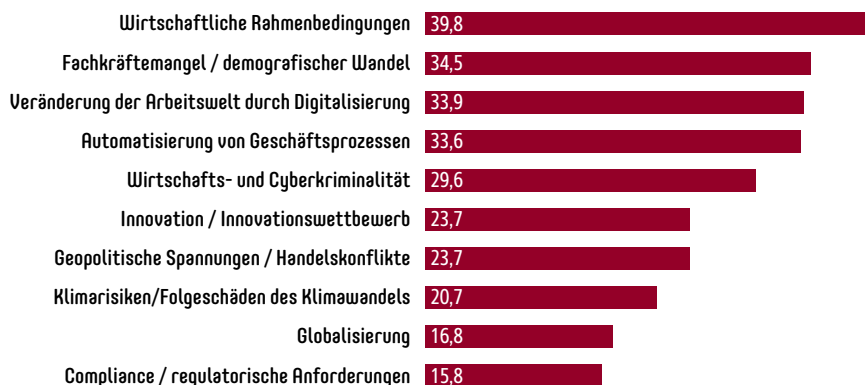
Exklusive Einblicke:
Wie IT-Verantwortliche das Business
in Gegenwart und Zukunft gestalten

2026 – Ein weiteres Jahr der Herausforderungen

Die Herausforderungen

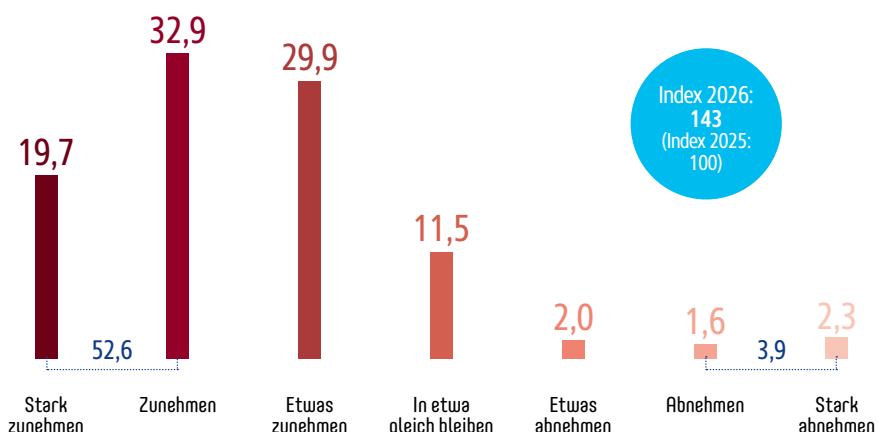
Welcher Art sind die Herausforderungen, vor denen Ihr Unternehmen 2026 vorrangig stehen wird?

(Mehrfachnennungen möglich)



Das Gesamtmaß der Herausforderungen

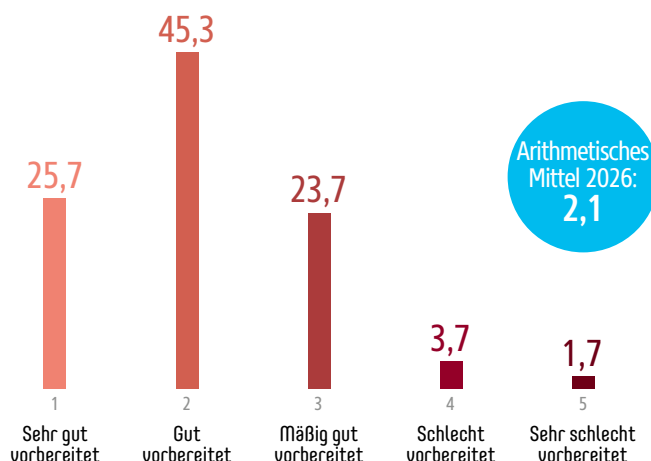
Wie wird sich das Gesamtmaß der Herausforderungen für Ihr Unternehmen im Jahr 2026 im Vergleich zu 2025 voraussichtlich entwickeln?



Grad der Vorbereitung

Wie gut ist Ihr Unternehmen auf diese Herausforderungen vorbereitet?

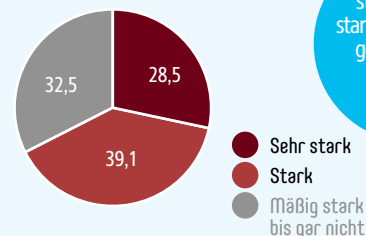
(Angaben auf einer Skala von 1 bis 5)



Generative KI

Nutzungsgrad

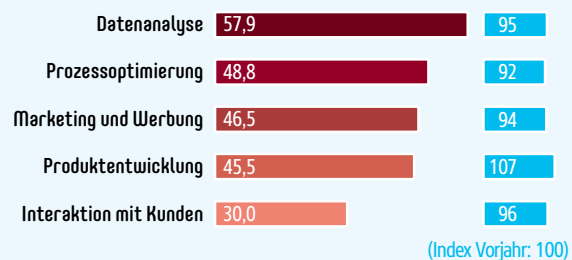
Wie stark wird generative KI in Ihrem Unternehmen genutzt?



Index starke bis sehr starke Nutzung von generativer KI:
2026: 114
(Index 2025: 100)

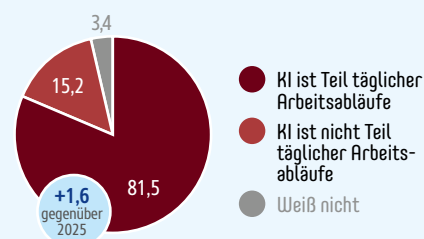
Anwendungsbereiche

In welchen Bereichen wird generative KI in Ihrem Unternehmen genutzt?



KI-Alltag

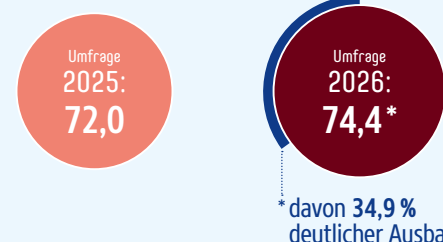
Ist generative KI Teil Ihrer täglichen Arbeitsabläufe, indem Sie entsprechende Tools aufrufen, Chatbots einsetzen oder auch KI integrativer Teil der IT-Systeme ist, mit denen Sie regelmäßig arbeiten?



Nutzungspläne

Welche Pläne hat Ihr Unternehmen bezüglich der Nutzung generativer KI in den kommenden 2 bis 3 Jahren?

Ausbau der Nutzung



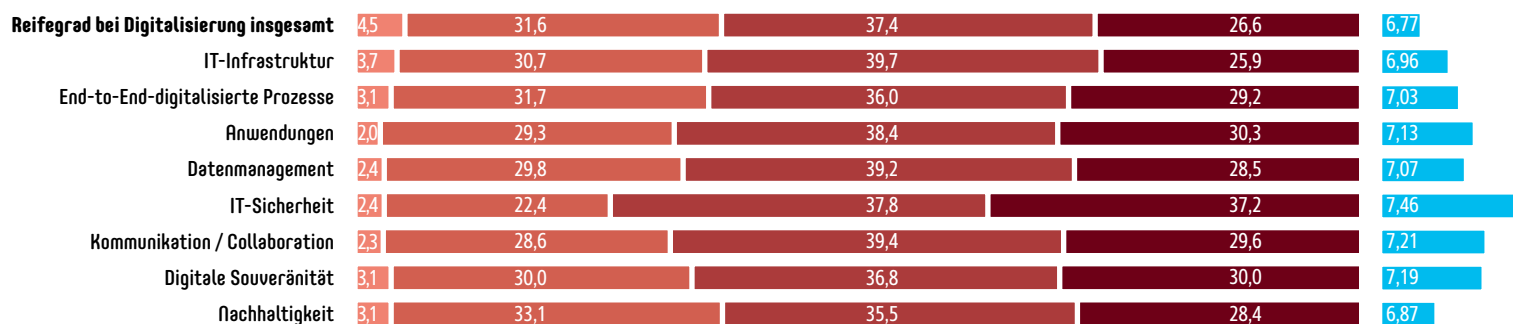
Digitale Transformation

Digitaler Reifegrad

Stellen Sie sich bitte die digitale Transformation als eine Wegstrecke von 0 bis 10 vor.
An welchem Punkt der Wegstrecke verorten Sie derzeit Ihr Unternehmen?

Bewertung auf einer Skala von 0 (In Sachen Digitalisierung stehen wir noch völlig am Anfang) bis 10 (Wir sind allerbestens für die digitale Zukunft aufgestellt)

Arithmetisches
Mittel



Darstellung auf einer Wegstrecke von 1 bis 10:

0 bis 1

2 bis 6

7 bis 8

9 bis 10

Technology Adoption

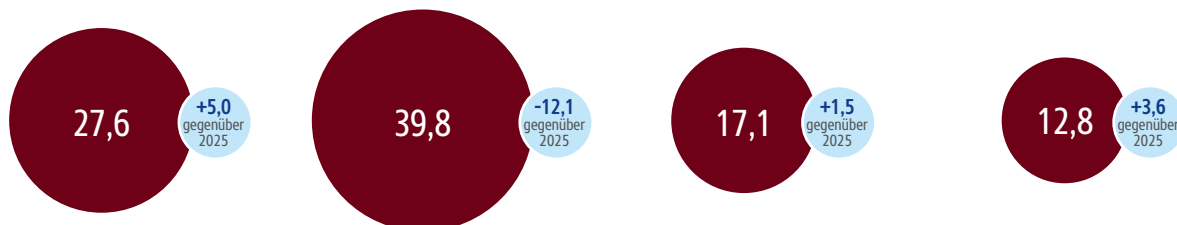
Welche der folgenden Beschreibungen charakterisiert Ihr Unternehmen am besten?

Innovators & Early Adopters
Unser Unternehmen ist ein Vorreiter der digitalen Transformation.

Early Majority
Unserem Unternehmen fällt es eher leicht, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen.

Late Majority
Unserem Unternehmen fällt es eher schwer, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen.

Laggards
Unser Unternehmen hat den Digitalisierungsinitiativen des Wettbewerbs nichts entgegensetzen.



Strategische Partnerschaften im digitalen Wandel

Mit welchen externen Partnern arbeiten Sie heute schon zusammen, um die Zukunftsfähigkeit Ihres Unternehmens zu sichern, Digitalisierungsprojekte umzusetzen oder neue Fachkräfte zu gewinnen? Mit wem planen Sie künftige Allianzen und strategische Partnerschaften?



CIO-Agenda 2026

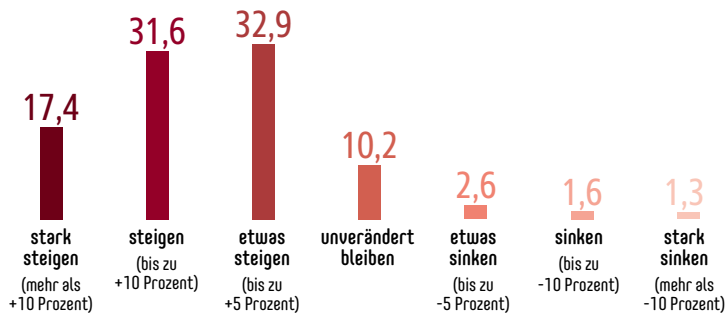
Alle Angaben in Prozent

Investitionen

IT-Budgets 2026

Wie wird sich das IT-Gesamtbudget Ihres Unternehmens im Jahr 2026 im Vergleich zu 2025 entwickeln?

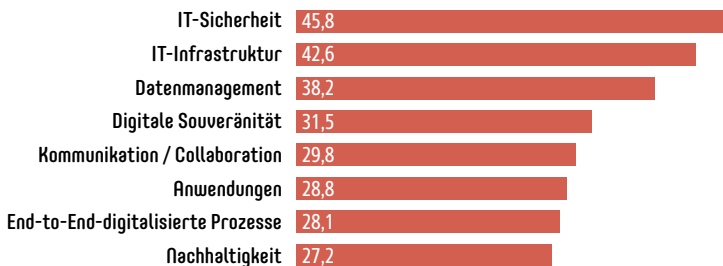
Das IT-Budget 2026 wird ...



Investitionsschwerpunkte in den nächsten drei Jahren

In welche der folgenden (IT-/Technologie-)Bereiche plant Ihr Unternehmen in den kommenden drei Jahren substantiell zu investieren?

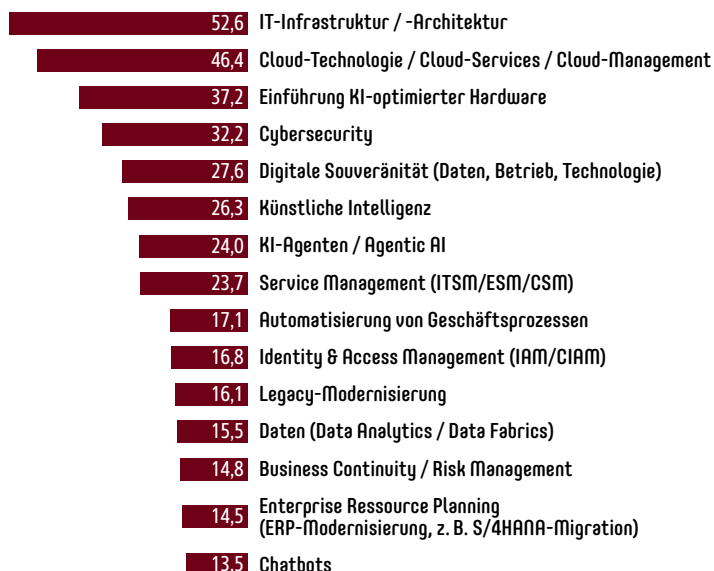
(Mehrfachnennungen möglich)



IT-Investitionsfelder in den nächsten drei Jahren

In welche der folgenden IT-Themen / Technologien plant Ihr Unternehmen in den kommenden drei Jahren zu investieren?

(Mehrfachnennungen möglich, Top-15-Antworten)



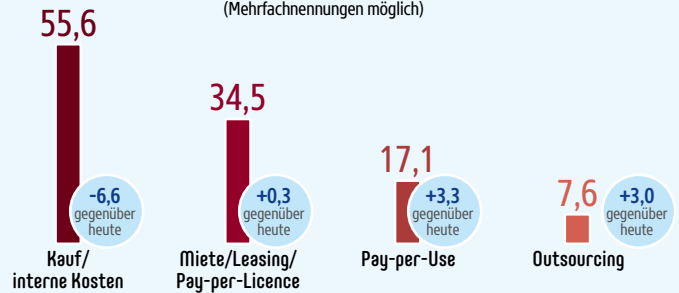
Beschaffungsprozesse

Wie sieht der IT-Beschaffungsprozess Ihres Unternehmens bei Hardware, Software und Services heute und zukünftig aus? Welche Facetten von Kauf über Miete bis hin zu Outsourcing umfasst der IT-Beschaffungsprozess jeweils?

Zukünftige Beschaffung von ...

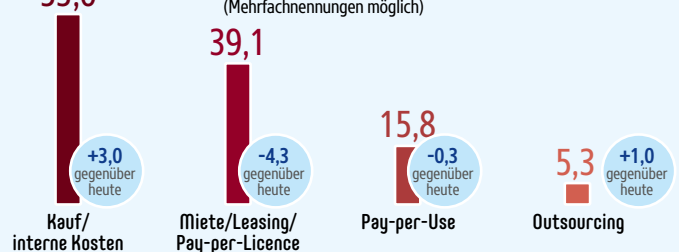
Hardware

(Mehrfachnennungen möglich)



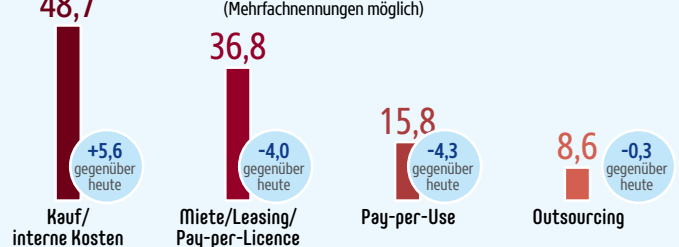
Software

(Mehrfachnennungen möglich)



Services

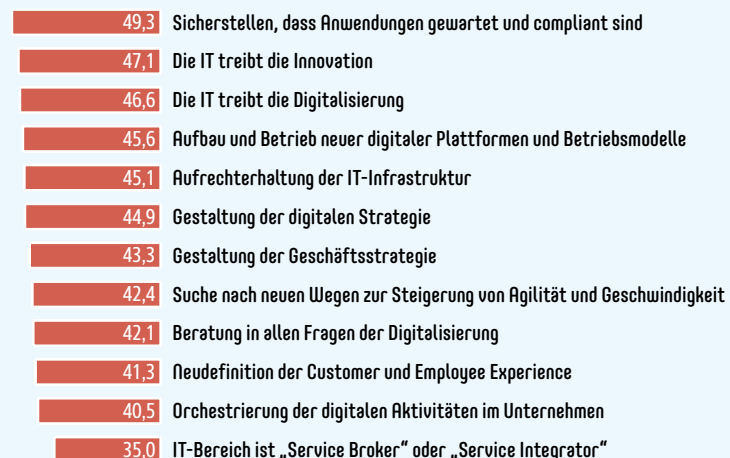
(Mehrfachnennungen möglich)



Die Rolle des CIO in fünf Jahren

Wie wird sich Ihrer Meinung nach der Fokus des CIOs / IT-Leiters bzw. IT-Bereichs in fünf Jahren verändert haben?

Verstärkter Fokus auf:



Die Studienpartner stellen sich vor

T-Systems International,
8com,
easy software, plusserver

*Die Vorstellung unserer Studienpartner wird von den beteiligten Unternehmen selbst erstellt.
Für die Porträts ist stets der jeweilige Studienpartner verantwortlich.*

Digitale Handlungsfreiheit beginnt in der Cloud

KI-Workloads skalieren, Compliance einhalten, flexibel handeln: Mit der richtigen Cloud-Architektur ist digitale Souveränität die beste Grundlage für Wettbewerbsfähigkeit und Innovation.



Souveränität und Innovation schließen sich bei T Cloud nicht aus. Unsere Lösungen ermöglichen es Unternehmen, beides optimal zu verbinden. Sicher, skalierbar und offen.

Thomas Weber

Vice President T Cloud Public

Wer heute KI-Modelle trainiert, Echtzeitdaten verarbeitet und zugleich NIS2, DSGVO und den EU AI Act einhalten muss, braucht Handlungsfreiheit. Die Fähigkeit, technologische Entscheidungen unabhängig, agil und im eigenen Tempo zu treffen. Genau diese Freiheit entsteht, wenn Unternehmen ihre Cloud-Architektur souverän aufstellen. Die zentralen Fragen: Wie lösen wir gewachsene Abhängigkeiten von einzelnen Anbietern? Wie gewinnen wir Flexibilität, ohne auf Skalierung zu verzichten? Und wie behalten wir die Kontrolle über unsere KI-Workloads?

Multi-Cloud für maximale Flexibilität

Souveränität ist kein Alles-oder-nichts-Prinzip, sondern eine Architekturentscheidung. Praktikabel und wirksam ist eine Multi-Cloud-Umgebung mit souveränem Kern. Hierfür vereint T Cloud mehrere Bausteine: T Cloud Public als vollständig in der EU betriebene Public Cloud mit Hyperscaler-Funktionen und -Leistung. T Cloud Private für regulierte und geschäftskritische Workloads sowie die Open Sovereign Cloud, die zu 100 Prozent auf Open Source setzt und maximale technologische Unabhängigkeit sichert – besonders wichtig für stark regulierte Branchen. Für KI-intensive Workloads ergänzt die Industrial AI Cloud in München das Setup mit 10.000 NVIDIA-GPUs für Training, Inferenz und Digital Twins.



Souveräne KI als Wettbewerbsfaktor

Doch wie viel Souveränität braucht ein Workload? Gemeinsam mit dem Unternehmen ermitteln wir die passende Cloud-Umgebung, abgestimmt auf Schutzbedarf und Regulatorik. Als Teil der Deutschen Telekom verbindet T-Systems dabei souveräne Cloud-Services mit sicherer Konnektivität.

Besonders bei KI macht T Cloud den Unterschied. Dank der nahtlosen Anbindung der T Cloud Public an die Industrial AI Cloud lassen sich KI-Anwendungen komplett souverän innerhalb der EU entwickeln und betreiben. Compliance-konform und ohne Datenabfluss in Drittstaaten. So entsteht Innovationskraft, die Unternehmen im Wettbewerb nach vorne bringt. Wir unterstützen sie auf diesem Weg – von der Strategie über die Migration bis zum Betrieb.

T Systems

T-Systems International GmbH

Friedrich-Ebert-Allee 140

53113 Bonn, Deutschland

0800 33 09030

info@t-systems.com

www.t-cloud.com



Kontrolle, Sicherheit, Unabhängigkeit



Digitale Souveränität braucht ein starkes SOC

Wer digitale Souveränität stärken will, benötigt volle Kontrolle über Daten, Prozesse und Sicherheitsmaßnahmen. Das 8COM SOC schafft Transparenz, schützt vor Cyberangriffen und sichert die Handlungsfähigkeit im Ernstfall.

Warum digitale Souveränität heute entscheidend ist

Die digitale Transformation hat Unternehmen und Behörden effizienter, vernetzter und leistungsfähiger gemacht. Gleichzeitig entstehen neue Abhängigkeiten von internationalen Technologieanbietern und teils globalen Lieferketten. Cyberangriffe, geopolitische Spannungen und regulatorische Anforderungen rücken digitale Souveränität immer stärker in den Fokus von Geschäftsleitungen und IT-Verantwortlichen.

Digitale Souveränität bedeutet dabei weit mehr als Datenschutz. Sie beschreibt die Fähigkeit einer Organisation, ihre digitalen Prozesse, Daten und Technologien eigenständig, sicher und rechtskonform zu steuern. Ziel ist es, jederzeit handlungsfähig zu bleiben, unabhängig von externen Risiken oder politischen Entwicklungen.

Ein wesentlicher Baustein hierfür ist ein Security Operations Center (SOC). Moderne Cyberangriffe erfolgen rund um die Uhr, sind hochgradig automatisiert und werden oft erst nach Tagen oder Wochen bemerkt. Ohne eine kontinuierliche Überwachung bleiben Angriffe häufig unentdeckt, bis bereits ein erheblicher Schaden entstanden ist. Ein SOC schafft Transparenz über die Sicherheitslage, erkennt Bedrohungen frühzeitig und ermöglicht eine schnelle Reaktion im Ernstfall. Es ist damit eine zentrale Voraussetzung für digitale Selbstbestimmung und Resilienz.

Doch nicht jedes SOC unterstützt digitale Souveränität gleichermaßen. Gerade beim Einsatz externer Managed Security Services sollten Unternehmen und Behörden genau prüfen, welche Rahmenbedingungen der Anbieter schafft.



Wie das 8COM SOC digitale Souveränität stärkt

Immer häufiger werden IT-Dienstleister selbst zum Einfallstor für Hacker, mit lukrativem Multiplikator-Effekt. Das 8COM SOC ist nach ISO 27001 auf Basis des BSI IT-Grundschutzes zertifiziert und wird in einem hochgesicherten Umfeld betrieben. Strenge Zutrittsregelungen, die physische Trennung sensibler Bereiche und revisionssichere Prozesse schaffen eine verlässliche Grundlage für den Schutz vor Lieferkettenangriffen. Die Leistungserbringung erfolgt ausschließlich in Deutschland, die Datenhaltung nach Möglichkeit ebenso, andernfalls in der EU.

Um technologische Abhängigkeiten zu vermeiden, verfolgt 8COM einen technologie-offenen Best-of-Breed-Ansatz. Die Auswahl der Sicherheitslösungen orientiert sich an den

Anforderungen der Kunden. Wo möglich, können deutsche oder europäische Technologien eingesetzt werden. Gleichzeitig werden Alternativen kontinuierlich bewertet, um auf regulatorische oder geopolitische Veränderungen flexibel reagieren zu können.

Mit mehr als 70 fest angestellten SOC-Mitarbeitenden, einem echten 24/7/365-Schichtbetrieb sowie eigenen Teams für Incident Response und digitale Forensik erkennt 8COM Bedrohungen frühzeitig und unterstützt bei deren Eindämmung. Da sämtliche Leistungen vollständig inhouse erbracht werden, entstehen keine Reibungsverluste durch die Übergabe an externe Dienstleister. Das ermöglicht kurze Entscheidungswege, schnelle Reaktionen und eine zügige Wiederherstellung der Betriebsfähigkeit.

⇒ Fazit

Digitale Souveränität entsteht nicht durch moderne Technologien, sondern durch die **Fähigkeit, Risiken jederzeit zu erkennen, zu bewerten und wirksam zu beherrschen**. Daran muss sich auch ein Security Operations Center selbst messen. Nur dann wird es vom reinen Sicherheitsinstrument zu einem strategischen Enabler unternehmerischer Handlungsfähigkeit.

8COM
CYBER SECURITY

8com GmbH & Co. KG
Europastraße 32,
67433 Neustadt an der Weinstraße

Telefon: +49 6321 48 446-0
E-Mail: info@8com.de

www.8com.de

wie intelligente dokumentenprozesse entscheidungen beschleunigen und unternehmen stärken

Unternehmen brauchen heute mehr als nur Dokumentenablage: Sie benötigen Lösungen und Strukturen, die Entscheidungen beschleunigen, Compliance sichern und Prozesse stabil halten. Mit intelligenten Dokumentenmanagement-Lösungen und automatisierten KI-gestützten Prozessen schafft easy die Grundlage für sichere DSGVO-konforme Abläufe, smarte datenbasierte Entscheidungen und Organisationen, die effizient und wettbewerbsfähig bleiben.

was macht easy auch in zukunft erfolgreich?

Andreas Zipser (CEO): Viele Unternehmen arbeiten in komplexen und fragmentierten Systemlandschaften. Sie brauchen Lösungen, die Daten nahtlos verbinden und Prozesse ohne Brüche steuern. Informationen müssen dort verfügbar sein, wo Entscheidungen entstehen. Hier setzt easy an: Wir entwickeln Lösungen, die Anwendungsfälle vereinfachen, Daten intelligent nutzbar machen und Teams befähigen, schneller und sicherer zu entscheiden.

was bedeutet compliance in zukunft?

Andreas Zipser: Compliance bedeutet in der Praxis auch digitale Souveränität – das Bewusstsein dafür wächst. Mit dem zunehmenden Einsatz von KI steigt die Bedeutung noch einmal deutlich. Unsere Lösungen unterstützen Unternehmen dabei, gesetzlichen Anforderungen gerecht zu werden und gleichzeitig effizienter zu arbeiten – durch automatisierte Prozesse und Document Intelligence. Wer Compliance heute richtig löst, schafft morgen die Grundlage für echten KI-Mehrwert.

wo sehen sie aktuell die grössten herausforderungen für unternehmen?

Andreas Zipser: Eine zentrale Aufgabe besteht darin, in gewachsenen IT-Systemen den Überblick über alle Unternehmensinformationen zu bekommen: Transparenz zurückzugewinnen, Kontrolle über Dokumente und Daten herzustellen, Prozesse steuerbar zu machen und Informationen über ihren gesamten Lebenszyklus auditierbar und effizient nutzbar zu halten.

welche trends werden die nächsten jahre prägen?

Andreas Zipser: Digitale Souveränität wird zum Leitprinzip. Steuerbare KI und Document Intelligence-Funktionen in Dokumentenmanagementsystemen werden zentrale Bausteine moderner Unternehmen. Technologie muss beherrschbar und vertrauenswürdig bleiben. Wir integrieren maßgeschneiderte KI-Agenten in unsere Lösungen und stellen Kunden ihre Daten gleichzeitig als sichere Grundlage für ihre eigene KI-Anwendungen bereit. So können sie souverän entscheiden, wie sie KI nutzen – ohne Abstriche bei Compliance und Revisionssicherheit.



**„digitale dokumenten-
prozesse schaffen trans-
parenz, reduzieren risiken
und ermöglichen effiziente
zusammenarbeit über das
gesamte unternehmen
hinweg.“**

Andreas Zipser,
CEO der easy software AG

Digitale Dokumentenprozesse sind ein zentraler Baustein leistungsfähiger Organisationen. In vielen Unternehmen sind sie jedoch historisch gewachsen: Informationen liegen parallel zum Beispiel in Papierakten, E-Mails und Fachanwendungen. Diese Medienbrüche erschweren den Zugriff, erhöhen den manuellen Aufwand und verhindern konsistente Informationsflüsse.

Moderne Dokumentenmanagement-Lösungen schaffen strukturierte Rahmenbedingungen. Sie ermöglichen es, Informationen systematisch zu erfassen, zu verwalten und entlang definierter Prozesse automatisch bereitzustellen. Dadurch wird nicht nur die Auffindbarkeit verbessert, sondern auch die Qualität von Abläufen stabilisiert. Gleichzeitig verändert sich die Rolle klassischer Archivsysteme grundlegend: Das Archiv wird zu einer aktiven Komponente mit integrierten Document Intelligence-Funktionen.

vom archiv zur aktiven informationsplattform

Im Mittelpunkt steht nicht mehr die Dokumentenablage, sondern die intelligente Nutzung von Informationen. Mit Document Intelligence werden Dokumente automatisiert klassifiziert, Inhalte verstanden und kontextbezogen bereitgestellt. Informationen fließen nahtlos in operative Systeme ein und bilden durchgängige Informationsströme, die unternehmensweit nutzbar sind.

Regulatorische Anforderungen lassen sich strukturell verankern: Revisionssicherheit, Nachvollziehbarkeit und klare Zugriffsmodelle sind integrale Bestandteile moderner Plattformen. Gleichzeitig ermöglichen flexible, cloud-fähige Architekturen und modulare Komponenten eine schrittweise Weiterentwicklung bestehender Landschaften. Mit automatisierten Workflows bis hin zu KI-gestützten Assistenzfunktionen trägt damit das Archiv zur aktiven Wertschöpfung und bildet die ideale Grundlage für KI-Agenten.

easy

by conrizon

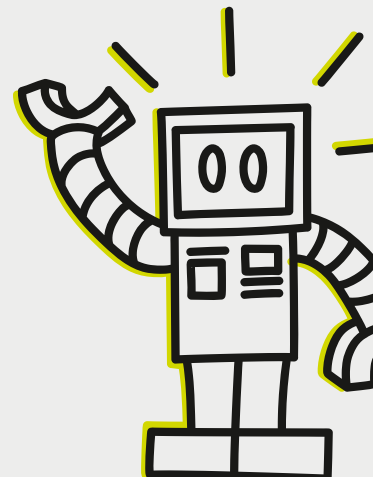
easy software AG

Jakob-Funke-Platz 1
45127 Essen

Telefon: +49 201 65069-0

E-Mail: info@easy-software.com

www.easy.de



Souveränität schafft Sicherheit in dynamischen Zeiten

Chief Executive Officer Dr. Marc Wilczek über die wachsenden Anforderungen an Unternehmen und wie digitale Souveränität diese verstärkt, aber auch lösen kann.

Dr. Wilczek, digitale Souveränität ist für deutsche Unternehmen aktuell wichtiger denn je. Wie definieren Sie digitale Souveränität und welche Bedeutung hat sie in der heutigen Wirtschaft?

Digitale Souveränität bedeutet, dass Unternehmen jederzeit die volle Kontrolle über ihre Daten behalten. Und zwar physisch, rechtlich sowie technisch. Das heißt, die Daten bleiben in Deutschland, unterliegen ausschließlich deutschem Recht und sind vor Zugriffsanforderungen wie durch den CLOUD Act geschützt. Und nicht nur die Daten, auch deren Management, sprich der Support, sollte in Deutschland angesiedelt sein.

Für Unternehmen sind Kriterien wie deutsche Standorte und eine deutsche Betriebsmannschaft keine bloßen Sicherheitsmerkmale mehr, sondern strategische Wettbewerbsvorteile. In einer dynamischen Zeit, die von disruptiven Technologien wie KI und geopolitischen Entwicklungen geprägt ist, gibt Souveränität die Sicherheit, neue Technologien zu nutzen, ohne Kompromisse bei Datenschutz oder Compliance einzugehen.

Welche Risiken sehen Sie für Unternehmen, die Daten in nicht-europäischen Cloud-Umgebungen speichern?

Technisch gesehen entstehen Abhängigkeiten, Vendor Lock-ins und Kontrollverluste. Rechtlich stehen Unternehmen vor widersprüchlichen Gesetzen: die europäische DSGVO gegenüber dem Einfluss

von außereuropäischen Gesetzen, die miteinander kollidieren können. Geopolitische Interessenskonflikte haben die Sorge vor einem früher unvorstellbaren „Kill Switch“ verstärkt, dass im Krisenfall der Zugang zu Software oder Daten abgeschaltet werden könnte.

Auf organisatorischer Ebene verkomplizieren sich Verträge und Governance-Strukturen, letztlich trägt die Instabilität dieser Umgebung zu höheren Kosten und zu erhöhten Haftungsrisiken bei. Die Folge ist ein Vertrauensverlust bei Kunden und Partnern, der in der heutigen datengetriebenen Wirtschaft teuer werden kann. Deshalb sollten diese Abhängigkeiten reduziert und damit die Risiken mitigiert werden.

Eine Möglichkeit ist die Wahl eines Anbieters mit EU-Rechenzentren. Wie wirkt sich der Einsatz eigener, in Deutschland betriebener und zertifizierter Datacenter konkret auf die digitale Souveränität Ihrer Kunden aus?

Unternehmen suchen heute einen Partner, der Verlässlichkeit, Sicherheit, Compliance und technologische Expertise vereint und gleichzeitig echte digitale Souveränität ermöglicht. Mit unseren vier DSGVO-konformen Datacenter in Deutschland bieten wir genau das. Unsere Zertifizierungen (u. a. ISO 27001 auf Basis von IT-Grundschutz, BSI C5 Typ II) sorgen dafür, dass physische sowie Prozesssicherheit auf höchstem Niveau gewährleistet sind. Die Interoperabilität unserer Services und Plattformen schafft Vertrauen und ermöglicht es Kunden, schnell auf regulatorische Änderungen zu reagieren.

Welche Trends erwarten Sie in den nächsten Jahren, die das Verständnis und die Umsetzung von digitaler Souveränität noch weiter verändern werden?

Regulierungen wie NIS2, DORA oder der EU AI Act werden Souveränität weiterhin stärken und als Pflichtkriterium etablieren. Technologisch wird die KI-Wirtschaft weiter Innovationen antreiben, aber gleichzeitig die Verantwortung für Betriebe erhöhen. Mit unserer eigenen souveränen KI-Plattform bieten wir genau

dafür eine Lösung. Auf Basis unserer OpenStack-Cloud können Kunden verschiedene LLMs DSGVO-konform und souverän nutzen.

Ich bin sicher, die geopolitischen Entwicklungen werden uns auch in Zukunft noch beschäftigen, und unser Marktumfeld wird generell dynamisch bleiben. All dies führt dazu, dass Souveränität nicht mehr optional ist. Sie wird in den nächsten Jahren nur noch mehr zur Grundlage jeder zukunftsfähigen Digitalstrategie werden.



„Souveränität ist nicht mehr optional. Sie wird zur Grundlage jeder zukunftsfähigen Digitalstrategie.“

Dr. Marc Wilczek
Chief Executive Officer
plusserver

Souveräne Cloud. Made & managed in Germany.

plusserver ist der Cloud-Provider mit der Digitalisierungsplattform „Made in Germany“. Schritt für Schritt begleitet plusserver Unternehmen aus dem Mittelstand sowie Konzerne bei ihrer IT-Modernisierung. Neben dem Cloud-Produktportfolio aus eigenen zertifizierten deutschen Rechenzentren, 24/7-Support in deutscher oder englischer Sprache sowie umfassenden Managed Services zeichnet plusserver den 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
Welserstraße 14, 51149 Köln
Telefon: +49 (0)221 8282 8550
E-Mail: beratung@plusserver.com
www.plusserver.com

Studiendesign

Alle wissenswerten Informationen
zu Aufbau, Methodik
und Stichprobe der Studie

Studienpartner

Platin-Partner

T-Systems International GmbH
Friedrich-Ebert-Allee 140
53113 Bonn
Telefon: +49 800 3309030
E-Mail: info@t-systems.com
Web: www.t-systems.com

Silber-Partner

easy software AG
Jakob-Funke-Platz 1
45127 Essen
Telefon: +49 201 65069-0
Telefax: +49 201 6506990
E-Mail: info@easy-software.com
Web: <https://easy-software.com>

Partner

baramundi software GmbH
Forschungsallee 3
86159 Augsburg
Telefon: +49 821 56708-0
E-Mail: info@baramundi.com
Web: www.baramundi.com

Gold-Partner

8com GmbH & Co. KG
Europastraße 32
67433 Neustadt an der Weinstraße
Telefon: +49 6321 48446-0
Telefax: +49 6321 4844629
E-Mail: info@8com.de
Web: www.8com.de

plusserver GmbH
Welserstraße 14
51149 Köln
Telefon: +49 221 82828550
E-Mail: beratung@plusserver.com
Web: www.plusserver.com

Gesamtstudienleitung

Matthias Teichmann
Director Research
Custom Research Team
Telefon: +49 172 8637540
matthias.teichmann@foundryco.com

Projektmanagement

Armin Rozsa
Research Manager
Custom Research Team
Telefon: +49 89 36086184
armin.rozsa@foundryco.com

Sales-Team

Daniela Häring
Account Managerin, Sales
Telefon: +49 152 90023492
daniela.haering@foundryco.com

Christine Nestler
Director, Sales
Telefon: +49 172 8111821
christine.nestler@foundryco.com

Ami Pepic
Senior Sales Manager
Telefon: +49 173 5703524
ami.pepic@foundryco.com

Regina Hermann
Senior Sales Manager
Telefon: +49 173 9706880
regina.hermann@foundryco.com

Impressum

**Studienkonzept /
Fragebogenentwicklung:**
Matthias Teichmann

**Endredaktion /
CvD Studienberichtsband:**
Matthias Teichmann

Analysen / Kommentierungen:
Gerhard Holzward, München

**Kommentierungen
CIO-Agenda 2026:**
Matthias Teichmann

**Hosting / Koordination
Feldarbeit:**
Armin Rozsa

**Artdirector &
Grafik CIO-Agenda 2026:**
Daniela Petrini, Reutte

Grafik:
Jutta-Maria Weber-Vidal, Würzburg

Umschlaggestaltung unter
Verwendung einer Illustration von
[©shutterstock.com/hasan as'ari](https://www.shutterstock.com/hasan-as-ari)

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

FoundryCo, Inc.

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086-0
Fax: +49 89 36086118

Vertretungsberechtigter:
Maria Savvidou, Geschäftsführerin

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Studiensteckbrief

Herausgeber	CIO und COMPUTERWOCHE
Studienpartner	Platin-Partner: T-Systems International GmbH Gold-Partner: 8com GmbH & Co. KG Silber-Partner: easy software AG plussserver GmbH Partner: baramundi software GmbH
Grundgesamtheiten	Oberste (IT-)Verantwortliche in Unternehmen der DACH-Region: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich und in den Fachbereichen (LoBs); Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT-Bereich
Teilnehmergenerierung	Persönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels
Gesamtstichprobe	312 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	12. bis 21. Mai 2026
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung und Durchführung	Custom Research Team von CIO und COMPUTERWOCHE in Abstimmung mit den Studienpartnern

Stichprobenstatistik

Branchenverteilung*

Land- und Forstwirtschaft, Fischerei, Bergbau.....	6,4%
Energie- und Wasserversorgung.....	8,3%
Chemisch-pharmazeutische Industrie, Life Science	10,6%
Medizin- und Labortechnik.....	10,9%
Metallerzeugende und -verarbeitende Industrie.....	11,2%
Maschinen- und Anlagenbau	9,6%
Automobilindustrie und Zulieferer	4,8%
Herstellung von elektrotechnischen Gütern, IT-Industrie	21,5%
Konsumgüter-, Nahrungs- und Genussmittelindustrie.....	7,4%
Medien & Kultur	2,6%
Baugewerbe, Handwerk	2,9%
Groß- und Einzelhandel (inkl. Onlinehandel).....	7,4%
Banken und Versicherungen.....	9,6%
Transport, Logistik und Verkehr.....	4,5%
Dienstleistungen für Unternehmen.....	10,9%
Hotel- und Gastgewerbe, Tourismus.....	1,6%
Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	5,8%
Schule, Universität, Hochschule	3,2%
Gesundheits- und Sozialwesen	4,2%
Anderer KRITIS-Sektor	0,3%
Sonstige Branchengruppe	5,1%

Unternehmensgröße deutschlandweit

Weniger als 100 Beschäftigte.....	5,1%
100 bis 249 Beschäftigte	16,0%
250 bis 499 Beschäftigte	15,1%
500 bis 999 Beschäftigte	26,0%
1000 bis 9999 Beschäftigte	26,0%
10.000 Beschäftigte und mehr.....	11,9%

Umsatzklasse deutschlandweit

Weniger als 20 Millionen Euro	11,9%
20 bis unter 50 Millionen Euro	18,3%
50 bis unter 100 Millionen Euro.....	18,9%
100 Millionen bis unter 1 Milliarde Euro.....	29,5%
1 Milliarde Euro und mehr	17,0%
Weiß ich nicht/keine Angabe	4,5%

Jährliche Aufwendungen in IT-Systeme

Weniger als 1 Million Euro.....	13,5%
1 bis unter 10 Millionen Euro	32,4%
10 bis unter 100 Millionen Euro.....	29,8%
100 Millionen Euro und mehr	17,0%
Weiß ich nicht/keine Angabe	7,4%

* Mehrfachnennungen möglich

Das Studienkonzept

Die Multi-Client-Studien von CIO und COMPUTERWOCHE sind mehr als nur Befragungen von C-Level-Verantwortlichen und IT-Fachleuten. Hinter den Marktforschungsprojekten steht ein nachhaltiges Studienkonzept, das auf eine Laufzeit von mindestens sechs Monaten ausgelegt ist.

Die Veranstaltung der initialen redaktionellen Round Tables, moderiert von leitenden Redakteuren und Redakteurinnen von CIO und COMPUTERWOCHE, steht zu Beginn eines jeden Studienprojekts.

Über den Verlauf der Round-Table-Veranstaltungen wird ausführlich berichtet, und die Themen, die den Branchenfachleuten besonders „auf den Nägeln brennen“, werden auch bei der Entwicklung des Studienfragebogens mitberücksichtigt. Die Unternehmen, die das Projekt als Partner begleiten, können eigene Ideen und Fragestellungen einbringen.

Etwa drei Monate nach der methodischen und inhaltlichen Ausgestaltung der Studie liegen die zentralen Ergebnisse in Form eines hochwertigen Survey Reports vor. Die Studienergebnisse werden auf Messen und Events, wie der Hannover Messe, dmexco oder it-sa, präsentiert, zum Teil in Form von Podiumsdiskussionen, bei denen sich die Studienpartner einem interessierten Fachpublikum stellen können.

Begleitet wird das gesamte Studienprojekt durch kontinuierliche Berichterstattung von CIO und COMPUTERWOCHE, zum Thema im Allgemeinen und zur Studie im Speziellen. Fachwissen und Kompetenz unserer Autoren und Autorinnen sowie unseres redaktionellen Teams tragen maßgeblich dazu bei, dass die Ergebnisse der Multi-Client-Studien richtig eingeordnet werden können. Berichtet und kommentiert wird auf allen modernen Medienkanälen; Infografiken, Bildergalerien und Video-Interviews tragen dazu bei, dass die Studien auf großes Interesse stoßen.

Der Autor dieser Studie



Gerhard Holzward

Der ehemalige COMPUTERWOCHE-Redakteur und -Eventchef war lange geschäftsführender Gesellschafter der h&g Editors und ist mittlerweile freiberuflich als Event Producer, ITK-Fachredakteur und Analyst tätig.

Round-Table-Moderation

Manfred Bremmer

Editorial Manager, COMPUTERWOCHE

Nachdem Manfred Bremmer bereits während seines Studiums als freier Journalist für die CW tätig war, stieg er Mitte 2001 fest als Onlineredakteur ein und blieb. Im Laufe der Jahre war Manfred in verschiedenen Ressorts tätig, darunter Unternehmen & Märkte, Communications und Mobile & Apps. Neben seiner Tätigkeit als Editorial Manager befasst sich der studierte Ethnologe mit zahlreichen IT-Trendthemen rund um die Digitalisierung und betreut den TechTalk-Podcast.

Jürgen Hill

*Chefreporter, Future Technologies
COMPUTERWOCHE*

Thematisch befasst sich der studierte Diplom-Journalist und Informatiker mit allen Facetten rund um Digitalisierung, KI / ML, IoT und Industrie 4.0.

Protokoll

Florian Stocker, München

Richard Ruf, München

Unsere Studienreihe



Folgen Sie uns auf LinkedIn:
<https://www.linkedin.com/showcase/research-services-germany>



T Systems

8COM
CYBER SECURITY

easy **plusserver**
by conrizon

 **baramundi**