



STATE OF DIGITAL SOVEREIGNTY 2025

Digitale Souveränität: zwischen Anspruch und Realität

Inhalt

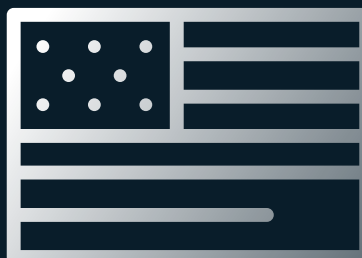
Executive Summary.....	3	Von der Abhängigkeit zur Eigenständigkeit: Erkenntnisse, Risiken und Handlungsempfehlungen	12
Digitale Souveränität: zwischen Anspruch und Realität	5	Das französische Vorbild: Förderung als entscheidender Impuls	13
Einigkeit in der Theorie: KRITIS braucht ein europäisches Fundament.....	5	Konkrete Risiken der digitalen Abhängigkeit	13
Abhängigkeit: am digitalen Tropf der US-Anbieter	6	Wechselhürden und Stärken europäischer Anbieter	14
Sichtbarkeit: Stärken Europas sind kaum bekannt	8	Ausblick: ein machbarer Weg zu mehr Eigenständigkeit.....	14
Wechselbereitschaft: Mehrheit hält an US-Lösungen fest.....	9		

Executive Summary

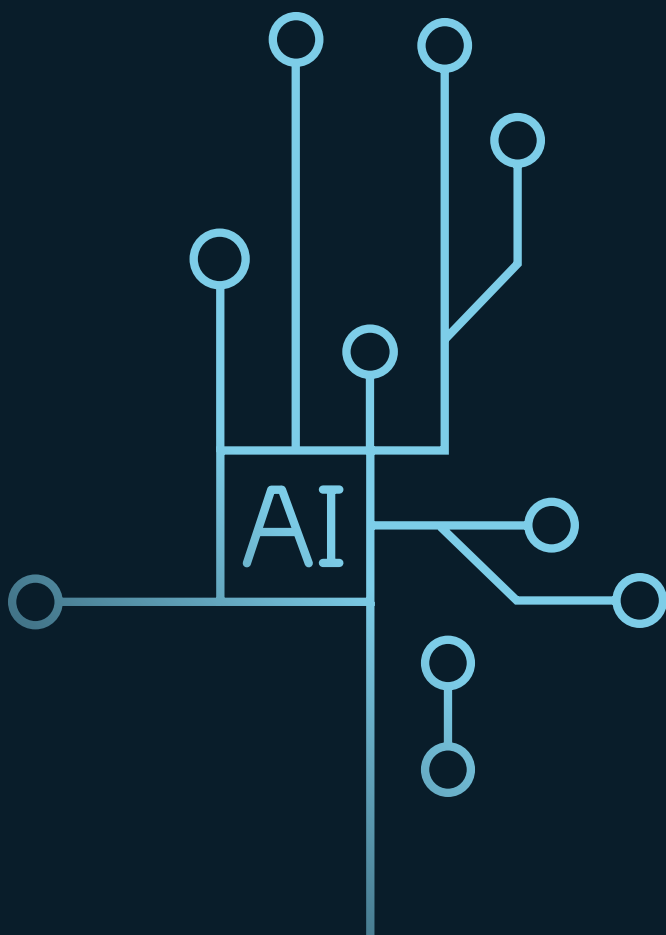
Digitale Souveränität steht in Deutschland seit Jahren im Fokus politischer Strategien und fachlicher Diskussionen. Ein Blick auf die tatsächliche Umsetzung in Unternehmensprozessen zeigt jedoch, dass zwischen den formulierten Ansprüchen und der gelebten Praxis weiterhin ein eklatanter Unterschied besteht.

Zwar sprechen sich **84,4 Prozent** der IT-Entscheider dafür aus, dass Staat und kritische Infrastrukturen vorrangig europäische Digitalprodukte nutzen sollten, doch in den eigenen Unternehmen dominieren weiterhin Lösungen aus den USA. Lediglich rund ein Drittel der Unternehmen plant, in den kommenden 24 Monaten europäische Software einzuführen. Fast die Hälfte schließt einen Umstieg derzeit aus.

Indessen sieht ein erheblicher Anteil der Unternehmen starke Abhängigkeiten von nicht-europäischen Anbietern in zentralen Bereichen wie Cloud Services und IT-Sicherheit (jeweils rund **40 Prozent**). Europäische Lösungen spielen bislang eine untergeordnete Rolle: Weniger als **25 Prozent** der Unternehmen nutzen europäische Cloud-Dienste. Im Bereich Kollaborations-Tools oder KI-Infrastruktur sind es etwa **10 Prozent**. Neben fehlender Umsetzungsbereitschaft besteht häufig auch ein Informationsdefizit über europäische Alternativen. Speziell in innovationsgetriebenen Feldern wie KI oder Cybersicherheit sind viele IT-Verantwortliche nicht hinreichend über europäische Pendanten informiert. Die Folge ist eine anhaltende Präferenz für US-Lösungen, trotz alternativer Angebote.



Obwohl europäische Softwarelösungen in vielen Bereichen wenig verbreitet und oft kaum bekannt sind, unterschätzen IT-Entscheider die eigene Abhängigkeit von nicht-europäischen Anbietern häufig. So geben nur **21,9 Prozent** an, europäische KI-Lösungen zu kennen, und lediglich **10,2 Prozent** nutzen diese. Dennoch stuft mehr als die Hälfte (**50,3 Prozent**) ihre Abhängigkeit in diesem Bereich als gering oder nicht existent ein. In der Cybersicherheit zeigt sich ein ähnliches Bild. Bekannt sind europäische Angebote nur **jedem Dritten**. Lediglich **20,5 Prozent** nutzen sie. Fast die Hälfte (**47,2 Prozent**) sieht aber nur eine schwache bis kaum vorhandene Abhängigkeit.



Festzuhalten bleibt: Deutsche Unternehmen sind weiterhin stark von US-amerikanischen IT-Anbietern abhängig – allerdings nicht in allen Bereichen. In klassischen Domänen wie ERP, Finanz- und Personalsoftware sind europäische Anbieter mit Marktanteilen von **30 bis 40 Prozent** vertreten.

Grundsätzlich zeigen sich deutsche IT-Entscheider offen für einen Umstieg auf europäische Alternativen – unter klaren Voraussetzungen. **7 von 10** Unternehmen würden auf europäische Anbieter umsteigen, wenn Leistung und Sicherheit vergleichbar sind. Besonders wichtig ist dabei die Datenspeicherung: Für **62,5 Prozent** der Befragten ist die garantierte Speicherung der Daten in der EU ein entscheidendes Kriterium für die zukünftige Nutzung europäischer Software.



Symbolischer *Tech-Patriotismus* allein reicht nicht

Um tatsächlich einen nachhaltigen Wandel hin zu digitaler Souveränität anzustoßen, bedarf es mehr als symbolischer Bekenntnisse. Gefragt sind deshalb sowohl die Hersteller, indem sie überzeugende Produkte auf den Markt einbringen, als auch die Politik. Letztere kann durch wechselfreundliche Rahmenbedingungen oder Förderprogramme einen Kurswechsel unterstützen und durch die Präsentation von Leuchtturmprojekten die öffentliche Aufmerksamkeit auf heimische Tech-Unternehmen lenken. Solange Preis, Performance und politischer Wille nicht synchron zünden, bleibt digitale Unabhängigkeit Wunschdenken.

Digitale Souveränität: zwischen Anspruch und Realität

Digitale Souveränität gilt in Politik und Wirtschaft als zentrale Voraussetzung für langfristige Wettbewerbsfähigkeit. Bislang fehlten jedoch belastbare Daten darüber, wie stark deutsche Unternehmen in zentralen Technologiebereichen tatsächlich auf außereuropäische Anbieter angewiesen sind, in welchen Feldern bereits europäische Alternativen genutzt werden und welche Faktoren einen Wechsel begünstigen könnten.

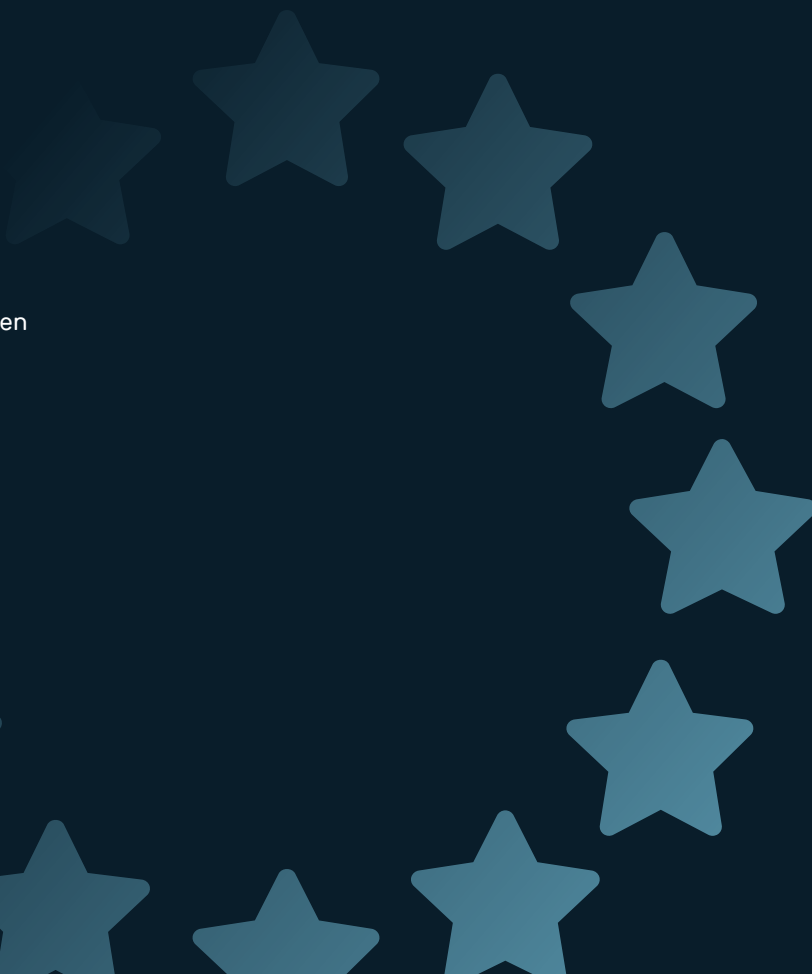
Die vorliegende Untersuchung schließt diese Lücke.

Auf Basis einer repräsentativen Civey-Befragung von 1.500 IT-Entscheidern erfasst sie in acht Bereichen – darunter Cloud Services, Cybersecurity und KI-Infrastruktur – den aktuellen Stand der digitalen Souveränität in Deutschland. Der Report macht sichtbar, in welchen Feldern bereits tragfähige europäische Optionen existieren, wo noch Nachholbedarf besteht und welche Hebel Politik und Wirtschaft ansetzen können, um digitale Unabhängigkeit zu fördern.

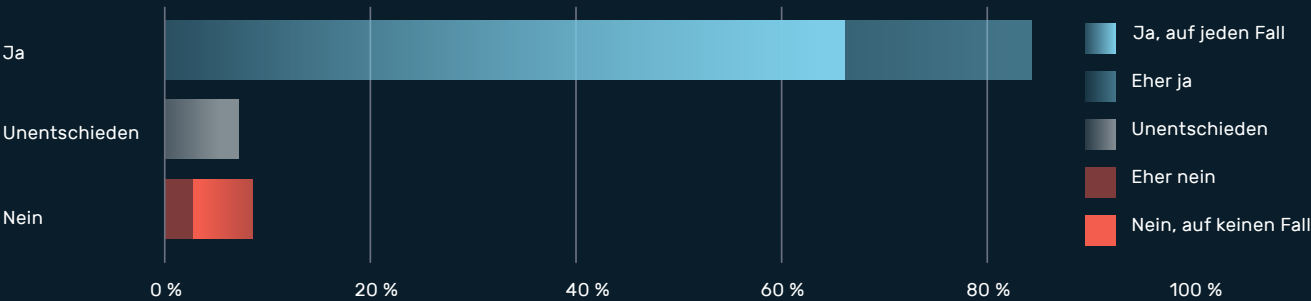
Damit liefert die Untersuchung eine solide Grundlage, um die Debatte über digitale Souveränität mit konkreten Daten und Handlungsempfehlungen zu untermauern.

Einigkeit in der Theorie: KRITIS braucht ein europäisches Fundament

Die Antwort auf die Frage, ob Staaten und Betreiber kritischer Infrastrukturen eher europäische Anbieter nutzen sollten, um unabhängig von außereuropäischen zu sein, beantworten die IT-Verantwortlichen sehr eindeutig: **84,4 Prozent** sagen Ja. Bemerkenswert: Das klare „Ja, auf jeden Fall“ überwiegt sogar das moderatere „Eher ja“. Nur insgesamt 8,3 Prozent sind dagegen, der Rest unentschieden. Das ist ein eindeutiges Votum und ein klarer Handlungsauftrag an die Politik. Die Botschaft: Gerade bei kritischer Infrastruktur – von Energie, Wasser, Verkehr bis zu Finanzen und Gesundheit – verlangen die Fachleute den Einsatz europäischer Lösungen. Man möchte diese zentralen Bereiche nicht in außereuropäischer Hand sehen oder hält es für strategisch gefährlich, hier nicht selbst Herr der Lage zu sein.



Sollten Staaten und Betreiber kritischer Infrastruktur in Europa Ihrer Meinung nach eher europäische Anbieter für digitale Produkte nutzen, um unabhängig von außereuropäischen Anbietern zu sein?



IT-Entscheider sind sich einig: Der öffentliche Sektor und Betreiber kritischer Infrastrukturen sollen auf europäische Lösungen setzen.

Das Stimmungsbild der befragten Unternehmen steht im Einklang mit politischen Tendenzen: Die Europäische Union und die Bundesregierung treiben eine strengere Regulierung von Cloud- und Kommunikationsdiensten für kritische Infrastrukturen voran, wie etwa die NIS-2-Richtlinie und nationale Gesetzesinitiativen zeigen. Maßnahmen wie der geplante Ausschluss

bestimmter Anbieter aus sicherheitskritischen Netzen verdeutlichen, dass künftig vor allem „vertrauenswürdige“ Anbieter zum Zuge kommen sollen. Die Wirtschaft signalisiert hierfür grundsätzlich Zustimmung, insbesondere wenn es um die öffentliche Hand und KRITIS geht. Bei der eigenen IT-Infrastruktur sind Unternehmen jedoch deutlich zögerlicher.

Abhängigkeit: am digitalen Tropf der US-Anbieter

Abhängigkeit von nicht-europäischen Lösungen in verschiedenen Bereichen
Zusammengefasste Ergebnisse

Bereich	Stark	Unentschieden	Schwach / Gar nicht
ERP	19,8 %	12,0 %	68,2 %
CRM	25,0 %	12,6 %	62,4 %
Cloud Service	39,7 %	12,7 %	47,6 %
Kollaborations-Tools	36,6 %	12,6 %	50,8 %
Cybersecurity	39,5 %	13,3 %	47,2 %
Finanzen	16,8 %	12,0 %	71,2 %
HR	13,5 %	10,4 %	76,1 %
KI-Infrastruktur	36,6 %	13,1 %	50,3 %

Die Analyse zeigt, dass deutsche Unternehmen in sicherheitsrelevanten Technologiebereichen weiterhin stark auf nicht-europäische Anbieter angewiesen sind. **39,7 Prozent** der IT-Entscheider berichten von einer starken bis sehr starken Abhängigkeit im Bereich Cloud Services. Im Bereich Cybersecurity geben **39,5 Prozent** eine ähnliche Einschätzung ab. Vier von zehn Unternehmen fühlen sich in diesen kritischen Bereichen ohne nicht-europäische Technologie kaum handlungsfähig. Auch die KI-Infrastruktur wird von **36,6 Prozent** als stark abhängig von nicht-europäischen Lösungen bewertet.

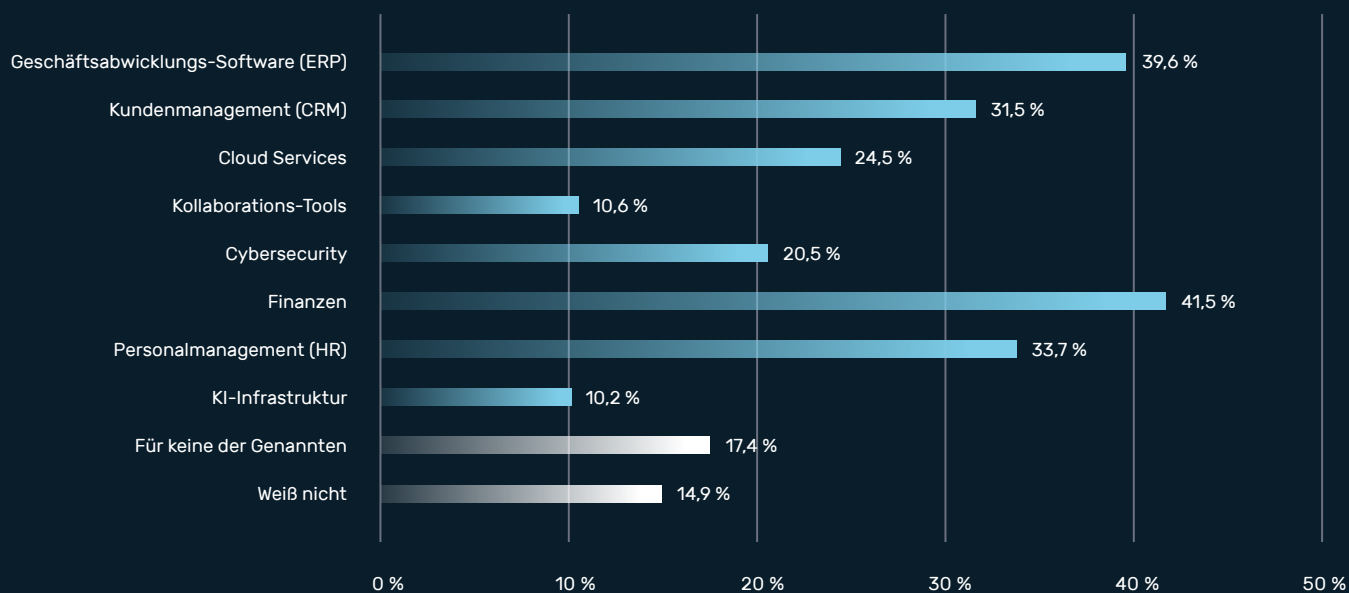
Demgegenüber bestehen in einzelnen Segmenten wie Finanzsoftware (**16,8 Prozent**) und ERP-Systemen (**19,8 Prozent**) geringere Abhängigkeiten, da hier europäische Anbieter traditionell eine stärkere Rolle spielen. Diese Bereiche der relativen Unabhängigkeit können jedoch nicht darüber hinwegtäuschen, dass in zentralen Feldern wie Cloud, KI, Sicherheit und Kollaboration nach wie vor überwiegend auf Nicht-EU-Anbieter gesetzt wird – gerade dort, wo sensible Daten verarbeitet und zukunftsweisende Entscheidungen getroffen werden.

Unternehmen wiegen sich in trügerischer IT-Souveränität

Obwohl europäische Software in vielen Bereichen nur selten zum Einsatz kommt, stufen IT-Entscheider ihren Grad der Abhängigkeit meist als sehr gering ein. Damit wird der Grad der eigenen Abhängigkeit stark unterschätzt und der Grad der Unabhängigkeit massiv überschätzt. So nutzen zwar nur **10,2 Prozent** europäische KI-Infrastrukturen, dennoch stufen mehr als die Hälfte der Befragten (**50,3 Prozent**) ihre Abhängigkeit von nicht-europäischen Lösungen in diesem Bereich als schwach bis nicht vorhanden ein. In der Cybersicherheit zeigt sich ein ähnliches Bild. Lediglich **20,5 Prozent** nutzen europäische Sicherheitslösungen. Fast die Hälfte (**47,2 Prozent**) sieht jedoch nur eine schwache bis kaum vorhandene Abhängigkeit.

20,5 %
nutzen europäische
Cybersecurity

Für welche dieser Unternehmensbereiche nutzt Ihr Unternehmen bereits europäische Software-Lösungen?



Geht es um die Nutzung europäischer Software-Produkte, gibt es in den Kategorien starke Unterschiede.

In Bereichen, in denen europäische Anbieter traditionell stärker vertreten sind, wie ERP- und Finanzsoftware, stimmen subjektive Wahrnehmung und tatsächliche Nutzung stärker überein. So empfinden **68,2 Prozent** der Befragten bei ERP-Systemen und **71,2 Prozent** im Finanzbereich nur eine geringe bis keine Abhängigkeit, was durch den vergleichsweise hohen Einsatz europäischer Lösungen (**39,6 Prozent** bei ERP und **41,5 Prozent** im Finanzbereich) gestützt wird.

Sichtbarkeit: Stärken Europas sind kaum bekannt

Ein erheblicher Anteil der IT-Entscheider ist mit europäischen Software-Alternativen nicht vertraut. Auf die Frage, für welche Bereiche sie europäische Software-Lösungen kennen, gibt etwas mehr als jeder zehnte IT-Manager an, keine zu kennen; weitere **16 Prozent** antworten mit „Weiß nicht“. Damit fehlt einem beträchtlichen Teil der Verantwortlichen der Überblick über verfügbare europäische Produkte in zentralen Kategorien der Unternehmenssoftware. Die fehlende Bekanntheit europäischer Lösungen ist ein gravierendes Hindernis für digitale Souveränität.

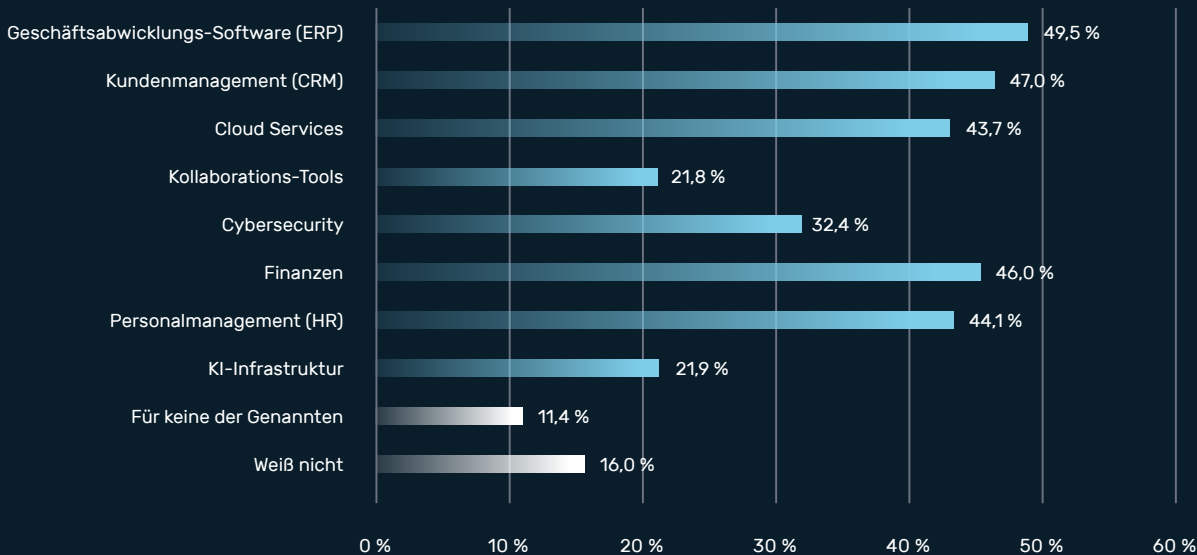
Eine detaillierte Betrachtung einzelner Softwarebereiche zeigt ein deutliches Gefälle in der Bekanntheit europäischer Anbieter. In klassischen

Segmenten wie ERP, CRM und Finanzsoftware sind europäische Lösungen relativ präsent: **49,5 Prozent** der Befragten kennen europäische ERP-Anbieter, **47,0 Prozent** nennen Namen im CRM-Bereich und **46,0 Prozent** im Finanzwesen. Diese Verankerung ist nicht zufällig, sondern spiegelt die lange Tradition europäischer – insbesondere deutscher – Softwareunternehmen in diesen Feldern wider.

Demgegenüber ist das Wissen um europäische Alternativen in neueren Technologiebereichen deutlich geringer. Nur **21,8 Prozent** der IT-Entscheider kennen europäische Lösungen für Kollaborations-Tools, obwohl diese während der Pandemie stark an Bedeutung gewonnen haben. Hier dominieren weiterhin US-Anbieter, während europäische oder Open-Source-Lösungen nur einem kleinen Kreis bekannt sind. Ein ähnliches Bild zeigt sich bei der KI-Infrastruktur: Lediglich **21,9 Prozent** können einen europäischen Anbieter benennen, was die geringe Sichtbarkeit Europas in diesem von US-Konzernen geprägten Zukunftsfeld unterstreicht.

Im Bereich Cybersicherheit ist die Bekanntheit europäischer Anbieter noch ausbaufähig: Nur **32,4 Prozent** der IT-Verantwortlichen sind sich europäischer Alternativen bewusst. Dies zeigt, dass sich einige europäische Unternehmen zwar bereits etabliert haben, gleichzeitig aber erheblicher Informations- und Entwicklungsbedarf besteht. Im Cloud-Segment ist die Situation etwas positiver: **43,7 Prozent** der Befragten kennen einen europäischen Cloud Service – ein im Vergleich zu anderen Technologiefeldern relativ hoher Wert.

Für welche dieser Unternehmensbereiche sind Ihnen europäische Software-Lösungen bekannt?



Bekanntheit europäischer Software-Anbieter nach Anwendungsbereich (Anteil der IT-Entscheider, die europäische Lösungen kennen)

Die Auswertung legt nahe, dass europäische Software dort besonders genutzt wird, wo sie seit Langem etabliert ist. In neueren digitalen Anwendungsfeldern hingegen ist die Verbreitung europäischer Lösungen gering. Im Bereich IT-Sicherheit setzen **20,5 Prozent** der Unternehmen auf europäische Produkte, was die Bedeutung spezialisierter europäischer Anbieter unterstreicht. Die Mehrheit verlässt sich jedoch weiterhin auf US-amerikanische Komplettlösungen. Auffällig ist, dass lediglich **17,4 Prozent** der Befragten angeben, in keinem Bereich europäische Software zu verwenden – mehr als **80 Prozent** nutzen mindestens eine europäische Lösung. Gleichwohl dominieren außereuropäische Produkte nach wie vor den Markt.

80 %

nutzen mindestens
eine europäische
Lösung

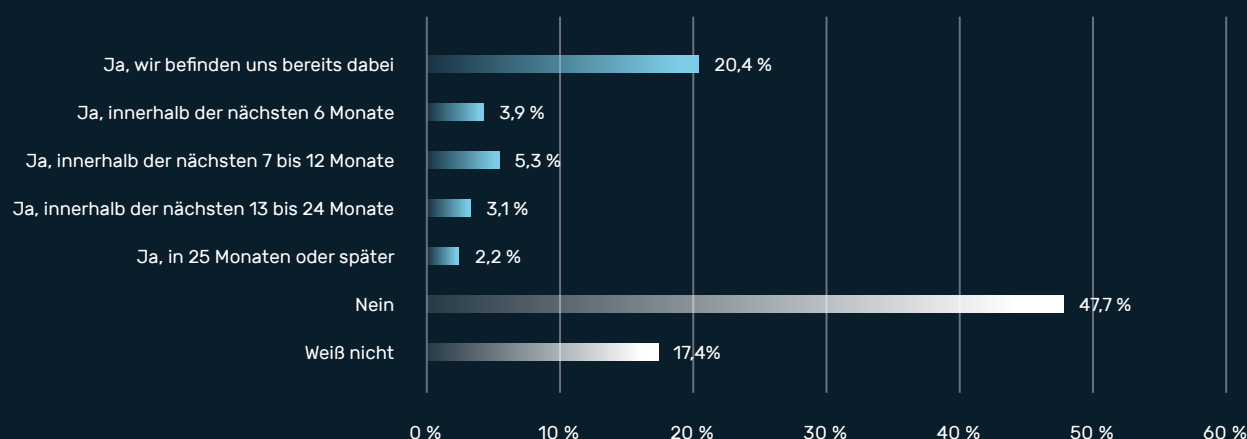
Wechselbereitschaft: Mehrheit hält an US-Lösungen fest

Unternehmen fordern zwar den konsequenten Einsatz europäischer Software-Lösungen im öffentlichen Sektor sowie für kritische Infrastrukturen, sind aber selbst in der Planung, zukünftig europäische Software-Lösungen einzuführen, deutlich zurückhaltender.

Nur **20,4 Prozent** der befragten Unternehmen befinden sich bereits aktiv in der Einführung einer oder mehrerer europäischer Lösungen. Weitere rund **15 Prozent** planen dies innerhalb der nächsten zwei Jahre (**3,9 Prozent** in den nächsten 6 Monaten, **5,3 Prozent** in 7 bis 12 Monaten, **3,1 Prozent** in 13 bis 24 Monaten, **2,2 Prozent** erst in 25 Monaten oder später). Über **47 Prozent** hingegen sagen: Nein, wir haben keine solchen Pläne. Ein knappes Fünftel ist unentschieden oder weiß es nicht (**17,4 Prozent**). Insgesamt bleibt die Mehrheit der Unternehmen vorerst bei bewährten Lösungen; ein umfassender Trend zu mehr digitaler Souveränität ist bislang nicht zu erkennen.



Plant Ihr Unternehmen zukünftig, eine oder mehrere europäische Software-Lösungen einzuführen?



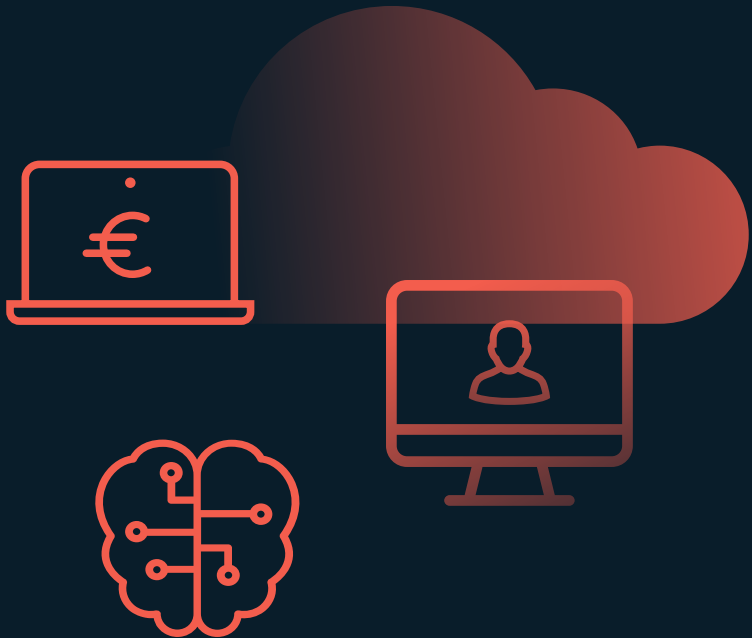
Fast die Hälfte aller IT-Entscheider plant innerhalb der nächsten zwei Jahre keine Einführung europäischer Software-Produkte.

Was hindert die Mehrheit, aktiv zu werden?

Ein wesentlicher Grund für die Zurückhaltung vieler Unternehmen liegt in den Herausforderungen und Risiken, die mit IT-Migrationen einhergehen. Solche Umstellungen sind komplex und betreffen oft zentrale Geschäftsprozesse. Veränderungen werden daher nur vorgenommen, wenn sie zwingend notwendig oder gesetzlich vorgeschrieben sind. Unternehmen handeln vor allem faktenbasiert und im Rahmen rechtlicher Vorgaben. Ohne signifikanten Mehrwert oder regulatorischen Druck gilt die Devise: „Never change a running system.“

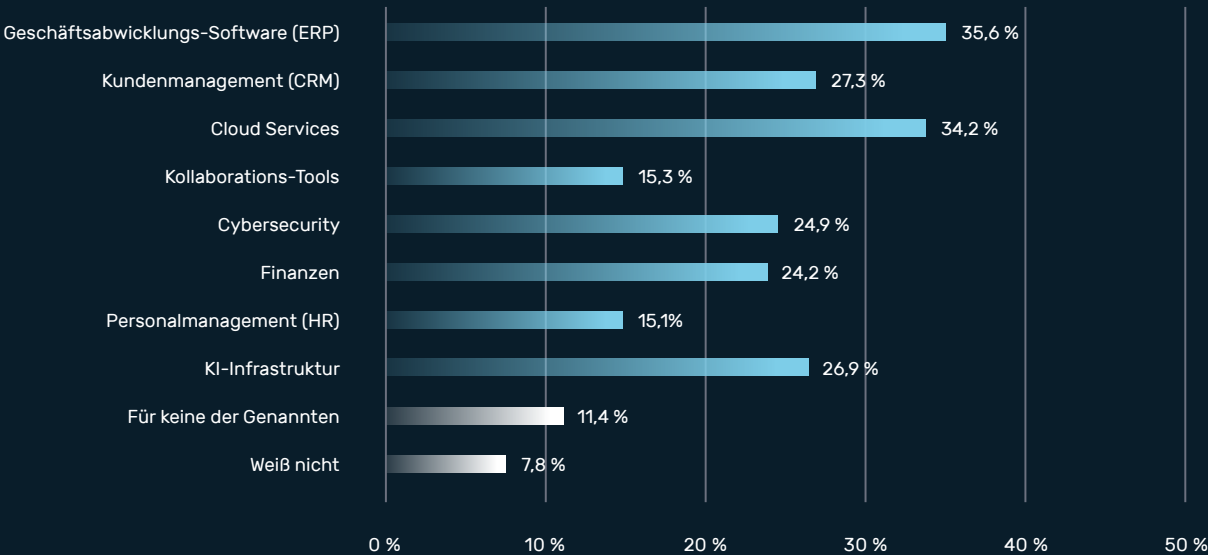
Die Analyse der Wechselabsichten zeigt, dass Unternehmen mit Umstiegsplänen vor allem in den Bereichen ERP (**35,6 Prozent**) und Cloud-Services (**34,2 Prozent**) aktiv werden wollen. Auch KI-Infrastruktur (**26,9 Prozent**), CRM (**27,3 Prozent**) und Finanzsoftware (**24,2 Prozent**) stehen im Fokus. Besonders im Cloud-Bereich, der zuvor als Abhängigkeitsschwerpunkt identifiziert wurde, gibt es bei einigen Unternehmen konkrete Bestrebungen, europäische Alternativen zu etablieren. Die Zahlen deuten zudem darauf hin, dass europäische Anbieter in den Bereichen Finanzen und CRM ihre bereits starke Marktstellung weiter ausbauen könnten.

Niedrig ist dagegen der Anteil im Bereich Kollaborations-Tools: Nur **15,3 Prozent** wollen in dieser von starker Abhängigkeit geprägten Kategorie in den nächsten 24 Monaten etwas ändern.



Für welche dieser Unternehmensbereiche plant Ihr Unternehmen, in den nächsten 24 Monaten eine europäische Software-Lösung einzuführen oder befindet sich bereits im Einführungsprozess?

IT-Entscheider, deren Unternehmen innerhalb der nächsten 24 Monate plant, eine europäische Software-Lösung einzuführen.



Bereiche, in denen Entscheider die Einführung europäischer Software-Lösungen planen.

Big Tech den Rücken kehren? Ja, aber ...

Die Wechselbereitschaft deutscher Unternehmen von etablierten, meist US-geprägten IT-Lösungen hin zu europäischen Alternativen ist grundsätzlich hoch – vorausgesetzt, die sachlichen Kriterien stimmen. Leistungsparität ist dabei das wichtigste Entscheidungskriterium: **69,9 Prozent** der IT-Entscheider würden auf europäische Software umsteigen, wenn diese die gleiche Funktionalität und Zuverlässigkeit wie die bestehende Lösung bietet. Datensicherheit ist nahezu ebenso relevant: **69,4 Prozent** nennen sie als Hauptmotiv für einen Wechsel. Auch Kostenvorteile spielen eine zentrale Rolle: zwei Drittel (**66,5 Prozent**) der Unternehmen wären bei deutlich niedrigeren Kosten bereit, auf europäische Lösungen umzusteigen. Über die Hälfte (**57,4 Prozent**) sehen zudem Förderprogramme als hilfreichen Anreiz.

Diese Ergebnisse zeigen, dass die Offenheit für europäische Alternativen vorhanden ist, sofern diese in den entscheidenden Punkten mit den etablierten Lösungen konkurrieren können. Neben den harten Fakten wie Leistung, Sicherheit und Kosten sind auch unterstützende Maßnahmen – etwa durch Förderprogramme oder regulatorische Rahmenbedingungen – wichtige Faktoren, um Unternehmen zu einem Wechsel zu bewegen.

69,4 %
nennen Datensicherheit
als Hauptmotiv
für einen Wechsel



Wechselbereitschaft auf Basis verschiedener Kriterien

Zusammengefasste Ergebnisse

Kriterium	Ja	Nein	Weiß nicht
Kostengründe	66,5 % 	22,3 % 	11,2 %
Vergleichbare Leistungen	69,9 % 	20,4 % 	9,7 %
Förderungen	57,4 % 	29,8 % 	12,8 %
Datensicherheit	69,4 % 	20,9 % 	9,7 %
Anerkennung	48,4 % 	37,3 % 	14,3 %
Verbot	57,8 % 	29,5 % 	12,7 %

Bei den Kriterien für einen Wechsel dominieren vor allem Leistung, Datensicherheit und Kosten.

Bereitschaft zur zukünftigen Nutzung europäischer Lösungen auf Basis verschiedener Kriterien
Zusammengefasste Ergebnisse

Frage	Hoch	Unentschieden	Niedrig
DSGVO-Konformität	59,4 % 	14,5 % 	26,1 % 
Datenspeicherung in der EU	62,5 % 	13,1 % 	24,4 % 
Lokaler Support	61,3 % 	13,7 % 	25,0 % 
Stärkung Euro-Wirtschaft	45,3 % 	22,8 % 	31,9 % 
EU-basierte Datenübertragung	51,9 % 	20,6 % 	27,5 % 
Preisvorteil	53,0 % 	22,3 % 	24,7 % 
CDN	37,0 % 	29,5 % 	33,5 % 

Europäische Datenschutzstandards und lokale Unterstützung sind für viele Entscheider die wichtigsten Kriterien für eine zukünftige Nutzung europäischer Lösungen.

62,5 Prozent der Befragten geben an, dass ihre Bereitschaft zur zukünftigen Nutzung europäischer Softwarelösungen hoch wäre, wenn die Datenspeicherung in der EU garantiert ist. Ein ähnlich hoher Anteil (**61,3 Prozent**) sieht lokalen Support als entscheidenden Faktor an. Auch die strikte Einhaltung der DSGVO überzeugt **59,4 Prozent** der IT-Entscheider. Diese Ergebnisse verdeutlichen, dass die Kernversprechen europäischer Anbieter – ein höheres Datenschutzniveau und Kundennähe – zentrale Verkaufsargumente darstellen. Darüber hinaus spielen auch ideelle Aspekte eine Rolle: Für **45,3 Prozent** der Befragten ist die Stärkung der europäischen Wirtschaft ein wichtiger Beweggrund, wenngleich dieses Motiv weniger stark wiegt als die konkreten, sachlichen Vorteile.

Von der Abhängigkeit zur Eigenständigkeit: Erkenntnisse, Risiken und Handlungsempfehlungen

In Deutschland klafft eine deutliche Lücke zwischen dem Wunsch nach digitaler Souveränität und der Realität in Unternehmen und Behörden. Die tatsächliche Abhängigkeit von außereuropäischen, meist US-amerikanischen, Technologieanbietern ist hoch und wird in ihren Konsequenzen massiv unterschätzt.

Gleichzeitig ist der politische Handlungsauftrag klar: Ein breiter Konsens von **84 Prozent** der IT-Entscheider fordert, dass der öffentliche Sektor und kritische Infrastrukturen europäische IT-Lösungen bevorzugen. Geht der Staat hier mit gutem Beispiel voran, könnte dies eine Wechselwelle auslösen, da die grundsätzliche Bereitschaft in der Wirtschaft vorhanden ist.

Das französische Vorbild: Förderung als entscheidender Impuls

Frankreich demonstriert mit dem 2021 gestarteten Programm „**Parcours de cybersécurité**“, wie staatliche Förderung die digitale Souveränität wirksam stärken kann.

- **Rahmen:** Unter der Leitung der nationalen Cybersicherheitsbehörde ANSSI wurden mit einem Budget von 176 Millionen Euro insgesamt 945 Einrichtungen unterstützt – darunter Kommunen, Krankenhäuser und weitere öffentliche Institutionen.
- **Umsetzung:** Das Programm umfasste standardisierte Audits und eine kofinanzierte Realisierung von über 3.000 konkreten Sicherheitsmaßnahmen wie die Härtung von Systemen, Netzwerksegmentierung und Backup-Strategien.
- **Ergebnis:** Der durchschnittliche Cyber-Reifegrad der Teilnehmer stieg signifikant von „D+“ auf „B“. Zudem investierten die Kommunen im Schnitt **30 Prozent** mehr als durch die Förderung vorgesehen war, was ein starkes Commitment belegt.

Die Erfahrungen aus Frankreich und Umfragedaten bestätigen: Finanzielle Anreize sind ein zentraler Hebel. Mehr als die Hälfte der Entscheider würde bei entsprechenden Förderungen einen Wechsel zu europäischen Anbietern erwägen. Sobald die finanziellen Hürden in Frankreich abgebaut waren, bevorzugten die Teilnehmer mehrheitlich europäische Dienstleister. Ein in Deutschland eingeführter „**Souveränitäts-Check**“ bei öffentlichen IT-Beschaffungen könnte die Prüfung europäischer Alternativen rechtlich verankern und deren Sichtbarkeit erhöhen.



Konkrete Risiken der digitalen Abhängigkeit

Die technologischen Abhängigkeiten europäischer Unternehmen von außereuropäischen Anbietern bergen konkrete Risiken mit unmittelbaren Auswirkungen:

- **Kontrollverlust:** Ein anschauliches Beispiel ist die Sperrung des E-Mail-Kontos des Chefanklägers des Internationalen Strafgerichtshofs durch Microsoft im Mai 2025. Diese Maßnahme, offenbar ausgelöst durch politische Sanktionen der USA, führte zu einem temporären Ausfall wichtiger Kommunikationswege und verdeutlicht die Gefahr einseitiger Abhängigkeiten von US-Anbietern.
- **Wirtschaftlicher Druck:** Steigende Lizenzkosten können Unternehmen und öffentliche Institutionen erheblich belasten. So sah sich die Stadt Kopenhagen mit einer Preissteigerung von **72 Prozent** für Microsoft-Produkte zwischen 2018 und 2023 konfrontiert, was sie zum Umstieg auf Open-Source-Alternativen wie LibreOffice bewegte. Ähnliche Entwicklungen sind auch in anderen europäischen Städten wie Lyon zu beobachten, die verstärkt auf offene und europäische Lösungen setzen, um Kosten zu kontrollieren und die eigene digitale Souveränität zu stärken.
- **Rechtliche Unsicherheit:** US-Gesetze wie der CLOUD Act und Section 702 des Foreign Intelligence Surveillance Act (FISA) verpflichten US-Anbieter zur Herausgabe von Daten an US-Behörden – unabhängig davon, ob die Daten auf europäischen Servern gespeichert sind. Dies untergräbt die europäische Datenschutzgrundverordnung (DSGVO), entzieht Unternehmen die Kontrolle über ihre Daten und gefährdet ihre Wettbewerbsfähigkeit.

Diese Beispiele verdeutlichen, dass die Abhängigkeit von außereuropäischen Technologieanbietern nicht nur theoretische Risiken birgt, sondern reale und unmittelbare Folgen für die digitale Souveränität, Wirtschaftlichkeit und Rechtssicherheit europäischer Unternehmen und Institutionen hat. Die Stärkung eigener digitaler Infrastrukturen und der Einsatz europäischer Lösungen sind daher zentrale Schritte, um diese Risiken zu minimieren.

Wechselhürden und Stärken europäischer Anbieter

Trotz der bekannten Risiken beabsichtigt fast die Hälfte der IT-Entscheider (**47 Prozent**), in den nächsten zwei Jahren keine Änderungen an ihrer bestehenden IT-Infrastruktur vorzunehmen. Eine wesentliche Ursache ist die mangelnde Kenntnis über leistungsfähige europäische Alternativen – ein Umstand, der die starke Marktposition außereuropäischer Anbieter weiter festigt.

Europäische Lösungen verfügen jedoch über klare Alleinstellungsmerkmale, die auch wirtschaftliche Vorteile bieten:

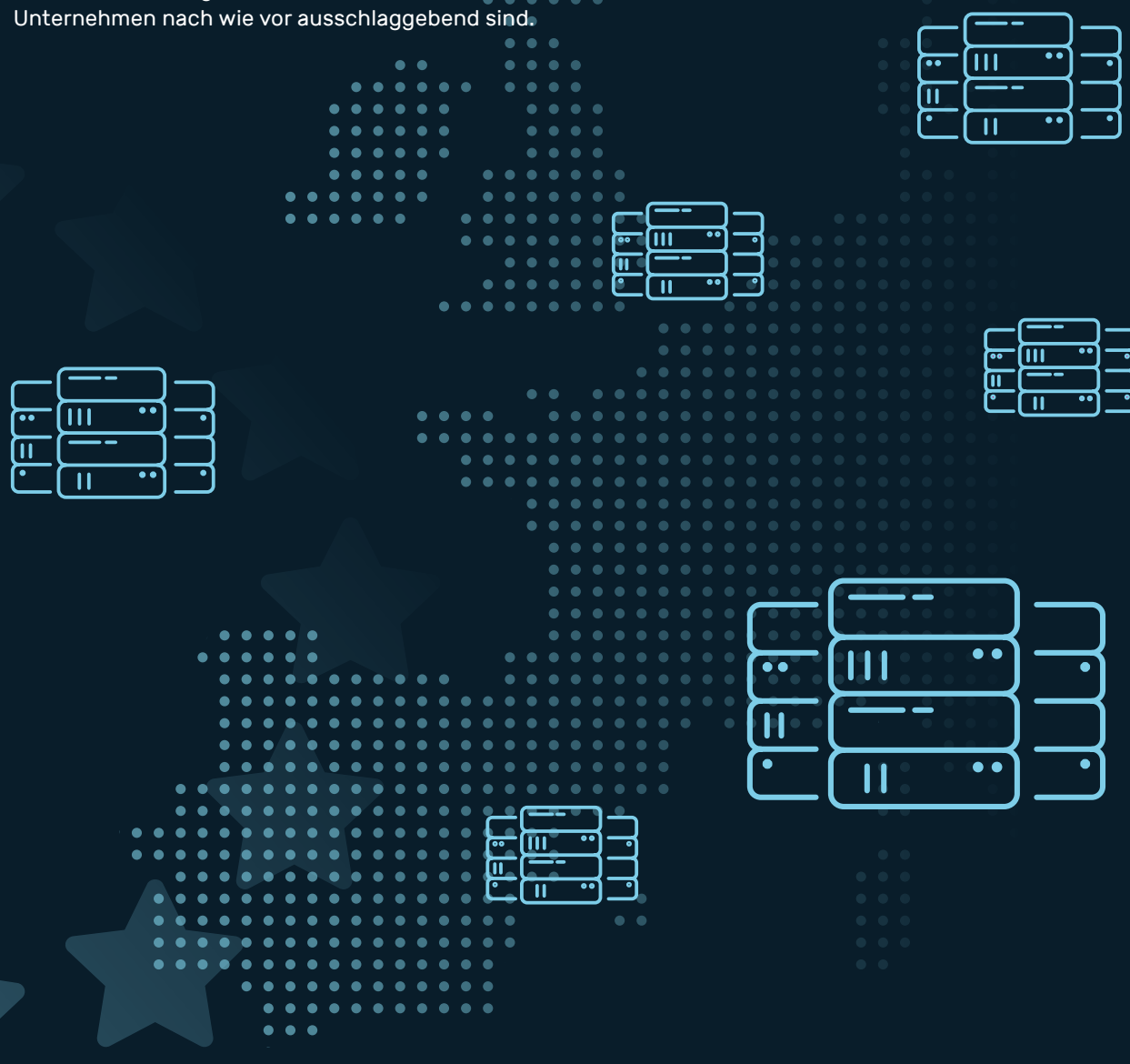
- **Rechtssicherheit** durch die Einhaltung von EU-Recht und DSGVO
- **Datenschutz** ohne Zugriffsmöglichkeiten ausländischer Behörden
- **Lokaler Service** mit kurzen Wegen und Ansprechpartnern vor Ort

Diese Vorteile allein sind jedoch nicht ausreichend. Um langfristig wettbewerbsfähig zu sein, müssen europäische Anbieter insbesondere bei Leistung und Preis überzeugen, da diese Faktoren für Unternehmen nach wie vor ausschlaggebend sind.

Ausblick: Ein machbarer Weg zu mehr Eigenständigkeit

Das Bewusstsein für die Notwendigkeit digitaler Souveränität ist so groß wie nie. Ziel ist nicht eine technologische Abschottung, sondern der Aufbau eines resilienten, innovativen und wettbewerbsfähigen digitalen Ökosystems, das auf europäischen Werten und Rechtssicherheit basiert.

Wenn die Politik jetzt mutige und verlässliche Rahmenbedingungen schafft und Unternehmen den Wechsel aktiv vollziehen, kann Europa seine digitale Eigenständigkeit schrittweise zurückgewinnen. Ein „Weiter so“ würde digitale Souveränität zum bloßen Lippenbekenntnis degradieren, während die Risiken der Abhängigkeit weiter anwachsen.



Zahlen, Daten, Fakten: Unsere Reports zu Cybersecurity & Digitaler Souveränität

Sie möchten mehr über die Cyberresilienz und den Stand der digitalen Souveränität in Deutschland erfahren? Unsere umfassenden Studien liefern Ihnen aktuelle Zahlen, exklusive Daten und fundierte Experteneinschätzungen zu den wichtigsten digitalen Herausforderungen für Deutschland.

Myra Cybersecurity Report H1 2025

Wie hat sich die Bedrohungslage entwickelt? Welche Branchen sind besonders gefährdet und mit welchen Angriffen müssen Unternehmen rechnen? Entdecken Sie die Fakten hinter den Schlagzeilen.

Alle Details in unserem Cybersecurity Report:



Myra State of Digital Sovereignty 2025

(Digital-Version der Studie + Zusatzmaterial)

Wo steht Deutschland im globalen Wettbewerb um technologische Unabhängigkeit? Erfahren Sie, warum digitale Souveränität ein entscheidender strategischer Faktor für Wirtschaft und Gesellschaft ist und welche Hürden zu überwinden sind.

Zur vollständigen Analyse:



Methodischer Hinweis: Die Ergebnisse basieren auf einer Civey-Umfrage unter 1.500 IT-Entscheidern in Deutschland im Zeitraum 2. April bis 10. Juni 2025. Die Befragung erfolgte online; bei Fragen mit Mehrfachnennungen konnten mehrere Bereiche ausgewählt werden. Die statistische Fehlertoleranz liegt bei ca. ± 5 Prozent. Digitale Souveränität ist hier definiert als die Fähigkeit, auf europäische Softwarelösungen zurückzugreifen, statt von außereuropäischen Anbietern abhängig zu sein.

Hinweis zur Sprache und Geschlechtergerechtigkeit:

Zur besseren Lesbarkeit wird in diesem Bericht das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten – sofern nicht explizit anders angegeben – gleichermaßen für alle Geschlechter.

Made in Germany



Myra schützt, was zählt. In der digitalen Welt.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor böartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihre Organisation. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

**Cyberangriffe sind teuer,
ein unverbindliches Gespräch kostet nichts.**

Myra Security GmbH

☎ +49 89 414141 - 345

🌐 www.myrasecurity.com

@ info@myrasecurity.com