Cloud Souveränität praktisch umsetzen

Ein praxisnaher Leitfaden

bitkom

Inhalt

1 Einleitung

Begriffsdefinition

Zu Beginn definieren wir zentrale Begriffe, da der Begriff »Cloud« in Praxis und Diskussionen oft unterschiedlich interpretiert wird. Ohne diese Präzisierung könnten Aussagen sonst fälschlicherweise nur auf einzelne Cloud-Varianten bezogen verstanden werden. Die folgende Begriffsklärung zu Deployment- und Service-Modellen sowie zur Digitalen Souveränität schafft eine gemeinsame Grundlage, auf die sich die weiteren Aussagen des Leitfadens stützen. Darauf aufbauend bietet der Leitfaden eine praxisorientierte Orientierungshilfe für Architektur, Governance und Beschaffung souveräner Cloud-Lösungen über alle Modelle hinweg und verweist bei Bedarf auf vertiefende Bitkom-Publikationen.

Cloud-Deployment-Modelle (»wo« und »wie betrieben«)[1]

- **Private Cloud:** ausschließlich für eine Organisation bereitgestellt; Hosting / Management intern oder durch Dritte.
- **Public Cloud:** über das Internet nutzbare Dienste für einen breiten Markt, typischerweise im Pay-per-Use-Modell (IaaS/PaaS/SaaS).
- **Hybrid IT / Hybrid-Cloud**: Kombination eigener Ressourcen (On-Premises) und externer Provider; *Make* und *Buy* werden je Use Case kombiniert.
- **Multi-Cloud:** parallele Nutzung von Diensten mehrerer Anbieter. Die Multi Cloud ermöglicht die parallele Nutzung von Cloud-Diensten und Cloud-Plattformen mehrerer Anbieter.
- **Community Cloud:** von mehreren Institutionen mit ähnlichen Interessen und regulatorischen Anforderungen geteilt, betrieben durch eine der Institutionen oder Dritte.
- **On- / Off-Premises:** Begriffspaar zur Ortsangabe der Leistungserbringung (eigenes RZ vs. externes RZ); unabhängig vom Servicemodell.

Diese Modelle sind topologisch (Lage und Struktur der Cloud-Ressourcen) zu verstehen und werden im Leitfaden bewusst vom Servicemodell getrennt betrachtet.

Cloud-Service-Modelle (XaaS – »was« wird als Dienst bezogen)[2]

- **IaaS:** Rechenleistung, Speicher, Netzwerk als Infrastruktur-Ressourcen; Abrechnung i. d. R. nutzungsbasiert; SLAs regeln Verfügbarkeiten.

[1] Bitkom ↗Whitepaper Hybride IT
[2] Bitkom ↗Whitepaper Hybride IT

- **PaaS:** Entwicklungs- / Laufzeitumgebungen als Plattform; Kunde verwaltet die eigenen Anwendungen, nicht die darunterliegenden Schichten.
- **SaaS:** komplett betriebene Anwendungssoftware als Dienst; Zugriff meist per Browser, kaum Eigenkonfiguration nötig.

Hinweis zur Verantwortlichkeit: Deployment- und Service-Modell bestimmen gemeinsam die operative Zuständigkeit (Stichwort: »*Shared Responsibility*«) und die notwendigen Governance-Regelwerke.

Zielpublikum

An wen sich dieser Leitfaden richtet

Dieser Leitfaden wurde mit Blick auf die technisch-operative Ebene geschrieben. Er richtet den Blick darauf, wie Unternehmen Souveränitätsanforderungen aus der strategischen Ebene konkret umsetzen können. Damit sind Interoperabilität, Wechselfähigkeit, offene Standards gemeint, die helfen, neben der erforderlichen Datensicherheit dafür zu sorgen, dass der Nutzer Daten und Workloads bedarfsgerecht steuern können. Dabei liefert der Leitfaden Anhaltspunkte und Empfehlungen, um den Stellenwert von Souveränität für die eigene Organisation festzulegen. Dieser Leitfaden hilft dann auf Basis einer solchen Entscheidung, Risiken und Mechanismen zu beleuchten und zu erläutern. Dabei bietet er keinen vollständigen Katalog an Risiken, sondern dient als Anregung für die eigene individuelle Bewertung von Maßnahmen. Durch die Anlehnung an bestehende Risikomanagement-Systeme möchten wir die praktische Umsetzung erleichtern.

Digitale Souveränität – Bezugspunkt des Leitfadens

Bitkom fasst den Kernbegriff prägnant: »Im Kern ist die Digitale Souveränität die Möglichkeit zur unabhängigen digitalen Selbstbestimmung.«[3]. Die ausführliche Bitkom-Definition betont Selbstbestimmung, Eigenständigkeit und Abgrenzung gegenüber Fremdbestimmung, ohne Autarkie zu verlangen. Diese Handlungs- und Gestaltungsfreiheit zielt darauf ab, technologische Lösungen einzusetzen, die Innovation und Kontrolle ermöglichen.

Wie dieser Leitfaden den Begriff »Cloud« verwendet

Wenn im Folgenden von Cloud die Rede ist, meint der Leitfaden grundsätzlich alle Deployment- und Service-Modelle (s. oben). Aussagen zu Architektur, Sicherheit, Compliance, Beschaffung, Betrieb, Exit-Strategien u. a. sind modellübergreifend formuliert und werden – sofern erforderlich – je Modell differenziert. Dadurch schließen wir Missverständnisse aus, bei denen »Cloud« ausschließlich als Public Cloud gelesen wird.

[3] ↗Digitale Souveränität – Bitkom

Ein Fallbeispiel: Die Fictura Mittelstand GmbH

Die Fictura Mittelstand GmbH ist ein fiktives mittelständisches Maschinenbauunternehmen aus Süddeutschland. 180 Mitarbeitende entwickeln und produzieren Spezialmaschinen für die Lebensmittelverarbeitung – ein solides, wachsendes Geschäft mit Kunden in ganz Europa. Im Zuge einer geplanten IT-Modernisierung steht eine strategische Entscheidung an:

Um zu wachsen, will die Fictura Mittelstand GmbH ihr Angebot an Spezialmaschinen für die Lebensmittelverarbeitung um digitale Services erweitern, zum Beispiel vernetzte Wartung, Fernüberwachung oder Auswertung von Produktionsdaten. Die IT der Firma kann solche Angebote nur schwer unterstützen: Neue Systeme lassen sich kaum anbinden, bestehende Anwendungen geraten schnell an ihre Grenzen. Darum prüft das Unternehmen im Rahmen eines Modernisierungsprogramms: Wie kann die Cloud helfen, bestehende Systeme zu erneuern und neue digitale Angebote aufzubauen?

In einer Geschäftsführungssitzung präsentiert die IT-Leitung die Optionen. Ein Teil des Teams ist überzeugt: Die Cloud bietet mehr Flexibilität, weniger Aufwand und bessere Verfügbarkeit. Die ERP-Systeme sollen gleich mit migriert werden. Auch eine KI-gestützte Analyseplattform für Vertriebsdaten steht zur Diskussion.

Dann meldet sich ein Geschäftsführer aus dem Technikbereich zu Wort:

»Das klingt spannend. Wenn wir jedoch mehr in die Cloud verlagern, sollten wir sicherstellen, dass Interoperabilität gewährleistet ist, offene Standards genutzt werden und Leistungen bei Bedarf über unterschiedliche Anbieter bezogen werden können. Gleichzeitig muss die Lösung in Bezug auf Sicherheit und Verfügbarkeit auch bei Störungen oder Ausfällen belastbar bleiben.«

Die Fragen sind bedacht und komplex. Die Diskussion nimmt Fahrt auf. Und schnell wird deutlich: Es geht nicht nur um IT-Infrastruktur, sondern um eine strategische Entscheidung des Unternehmens, ob und wie es fit für das digitale 21. Jahrhundert ist.

Eine Projektleiterin fragt:

»Das klingt alles ganz schön kompliziert. Haben wir intern die Leute, die sich mit Multi-Cloud auskennen? Das erfordert massive Schulungen!«

Ein anderer Geschäftsführer ergänzt:

»Wie sehr können wir uns eigentlich auf die Konditionen verlassen? Wenn der Anbieter plötzlich die Preise verdreifacht oder Services einstellt? Haben wir dann einen Plan B?«

Es geht nicht mehr nur um Technik. Die Diskussion hat eine neue Ebene erreicht:

- Rollen- und Rechtemanagement und Kontroll-Tools sollen den Zugriff auf die unternehmerischen Daten und Systeme sichern
- Datenschutz und Cybersicherheit sowie robuste Verschlüsselung sind essenziell für die Eigenständigkeit der IT-Struktur
- Der gesamte digitale Betrieb darf nicht von einem einzigen Anbieter abhängen – eine Multi-Cloud-Strategie oder eine Backup- und Migrationsstrategie müssen her

Am Ende ist klar: Die Cloud bietet viele Chancen, aber diese gehen einher mit einer robusten technischen Architektur, rechtlichen Rahmenbedingungen, einer klaren Risikoeinschätzung / -Bewertung und einem Konzept für Cybersicherheit und interne Schulungen.

Die Geschäftsführung vertagt die Entscheidung und beauftragt das Team, die technischen und rechtlichen Rahmenbedingungen auszuarbeiten. Was sind die konkreten Abhängigkeiten, die entstehen könnten und welche Maßnahmen brauchen wir, um handlungsfähig zu bleiben? Gibt es weitere, tieferliegende Risiken, die wir berücksichtigen und bewerten müssen?

Denn eines steht fest für die Geschäftsführung: Nichtstun birgt ein höheres strategisches Risiko als die Nutzung der Cloud. Die Fictura Mittelstand GmbH muss auch das Risiko bewerten, das entsteht, wenn nicht gehandelt wird. Globale Wettbewerber integrieren bereits KI-gestützte Analysen zur Optimierung ihrer Maschinen. Wenn wir jetzt aus übertriebener Vorsicht auf die leistungsfähigsten globalen Plattformen verzichten, zementieren wir einen technologischen Rückstand, der uns in drei Jahren unsere Marktfähigkeit kosten kann. Unsere Souveränität ist auch dadurch bedroht, dass wir irrelevant werden.

2 Warum Innovation, Open Standards, Cybersicherheit und Multi-Cloud jetzt strategisch entscheidend sind

Chancen von Cloud und KI

Cloud-Technologien und KI-Systeme haben sich in den letzten Jahren zu zentralen Innovationstreibern entwickelt. Sie ermöglichen Unternehmen, schneller zu skalieren, neue Geschäftsmodelle zu erschließen und komplexe Prozesse effizienter zu gestalten. Wer heute moderne Entwicklungs- und Datenplattformen nutzt, profitiert von:

- kurzfristiger Verfügbarkeit großer Rechenkapazitäten,
- global verfügbaren Werkzeugen für Entwicklung, Betrieb und Analyse,
- ständig wachsenden Funktionen, die als Dienste konsumiert werden können,
- hoher Sicherheit und Resilienz durch standardisierten Betrieb beim Cloud-Provider (z. B. Multi-Zone Regions, Geprüfte Backup-and-Restore-Prozeduren, Verschlüsselung von Daten »at-rest«, »in-transit«, »in-process« / »Confidential Computing« etc.)

Die Zahlen aus dem Bitkom Cloud Report 2025[4] zeigen, dass in der Nutzung die Private Cloud mit 74 Prozent deutlich vor Public-Cloud-Angeboten (59 Prozent) liegt. Viele setzen auch auf mehr als eine Cloud. 29 Prozent nutzen eine Hybrid-Cloud, also sowohl private als auch öffentliche Cloud-Dienste. Und 41 Prozent setzen auf Multi-Cloud, beziehen also Cloud-Dienste von unterschiedlichen Anbietern. Mit solchen flexiblen Deployment-Modellen hat der Kunde die Wahlfreiheit, seine Anwendungen dort zu verarbeiten bzw. Daten dort zu speichern, wo es für ihn am meisten Sinn macht (Kriterien: Sicherheit, Resilienz, Security, Performance, Skalierung, etc.).

Diese Kriterien können sich über die Zeit gesehen verändern und verlangen nach flexiblen Lösungen, um sich jederzeit neuen Anforderungen anzupassen. Diese Grundfähigkeit, Anwendungen flexibel »on-prem«, in der Cloud (public, private) oder in einer Kombination zu entwickeln und zu betreiben, kann als ein wesentlicher Baustein zur Digitalen Souveränität betrachtet werden.

[4] 2025, Bitkom Cloud Report

Handlungsfreiheit ist eine Machtfrage

Digitale Souveränität ist kein rein technisches Thema. Vertragliche, technische und organisatorische Optionen müssen gemeinsam gedacht und strategisch umgesetzt werden.

Dies ermöglicht die Prüfung von Resilienzkriterien in Bezug auf:

- Sicherheit und Datenschutz
- Wechseloptionen und Alternativangeboten
- Funktionalitäten und Innovationspotenzial

Digitale Souveränität bedeutet, die Kontrolle über die eigenen digitalen Systeme und Daten zu behalten. Es geht nicht nur um Technik, sondern vor allem darum, handlungsfähig und unabhängig zu bleiben, gerade dann, wenn sich Bedingungen ändern. Digitale Souveränität ist ein Spektrum, kein statischer Zustand. Sie umfasst Wahlfreiheit, Kontrolle und Fähigkeiten. Souveränität ist damit die Fähigkeit, technologische Entscheidungen eigenständig zu treffen, Daten und Infrastruktur selbstbestimmt zu kontrollieren und regulatorische Anforderungen zu erfüllen.

Das bedeutet: Selbst wenn Unternehmen vertraglich abgesichert scheinen, brauchen sie reale technische und organisatorische Mittel, um ihre Kontrolle im Ernstfall auch durchsetzen zu können. Wenn ein Anbieter Preise anpasst, Funktionen verändert oder durch gesetzliche Vorgaben Anpassungen notwendig werden, sind vertragliche Zusicherungen ein wichtiger Schutzmechanismus. Dennoch bleibt es für Unternehmen essenziell, eigene Alternativen und Strategien zur Risikominimierung zu entwickeln.

> Digitale Souveränität heißt nicht, alles allein zu machen, sondern bewusst so aufgestellt zu sein, dass man Systeme selbst steuern und im Notfall auch wechseln kann.

Souveränität beginnt dort, wo reale Wahlmöglichkeiten einschließlich Exit-Fähigkeit existieren, unabhängig davon, ob man sie gerade nutzt. Wer aktiv gestaltet, behält die Kontrolle, kann schneller auf Veränderungen reagieren und verhindert, dass er zum Getriebenen wird, durch Entscheidungen Dritter, auf die man keine Antwort hat.

Die richtigen Vertragselemente und interne Befähigung sind essenziell

Die Digitalisierung schreitet weltweit mit hoher Geschwindigkeit voran. Die Anwendung der künstlichen Intelligenz beginnt gerade erst ihr Potenzial zu entfalten. Dabei spielt das richtige Vertragswerk eine entscheidende Rolle, um nicht in die Abhängigkeit eines einzelnen Cloud-Providers zu gelangen. Um sich zukunftssicher

aufzustellen, ist es wichtig, technologische Entwicklungen bestmöglich nutzen zu können. Gleichzeitig sollten Unternehmen ihre Verhandlungsspielräume bei der Preisgestaltung wahren und zentrale Cybersicherheitsstandards einhalten.

Dafür empfiehlt sich ein vertragliches Konzept, das

- Interoperabilitätsklauseln,
- eine Multi-Cloud-Architektur und
- den Einsatz offener Standards vorsieht.

Ein weiterer Aspekt: Die Organisation entwickelt Kompetenzen, Prozesse und Datenstrukturen rund um Plattformen und Anbieter, die sich ihrerseits weiterentwickeln. Diese frühen Erfahrungen erzeugen einen Lernvorsprung, der sich über die Zeit potenziert, ähnlich einem Zinseszinseffekt. Wer hingegen zu lange zögert, läuft Gefahr, dauerhaft auf einem technologischen Rückstand zu operieren. Die digitale Souveränität bemisst sich deshalb nicht nur an der Fähigkeit zum Ausstieg, sondern auch an der Fähigkeit, neue Technologien souverän zu adaptieren, bevor Mitbewerber dadurch den Markt dominieren. Ein dynamisches Lern- und Schulungskonzept für das gesamte Unternehmen, inklusive der Geschäftsführung, ist daher von zentraler Bedeutung, um das digitale Potenzial und damit einhergehende Innovationsfähigkeit voll ausschöpfen zu können.

Technologien bringen Abhängigkeiten – es geht um bewusste Steuerung

Kein Unternehmen kann in der globalen Supply Chain vollständig unabhängig agieren. Die Nutzung externer Dienste und spezialisierter Technologieanbieter ist betriebswirtschaftlich sinnvoll und notwendig, um Innovationen voranzubringen und schnell neue Fähigkeiten für das Unternehmen aufzubauen. Entscheidend ist jedoch, dieses Zusammenspiel bewusst zu gestalten durch Fragen wie:

- Welche Risiken entstehen und wo ist ein Risiko tragbar? Welche Wahrscheinlichkeit ist damit verbunden?
- Wo muss ich Alternativen verfügbar halten und wie sind meine Cybersicherheitskonzepte ausgestaltet?
- Und wo brauche ich eigene technische Fähigkeiten und wie implementiere und steuere ich diese?

Digitale Souveränität entsteht nicht durch Abschottung, sondern durch technisch fundierte Kontrolle über kritische Ressourcen und Prozesse. Offene Standards, transparente Schnittstellen und – wo sinnvoll – die Beteiligung an Open-Source-Projekten können Abhängigkeiten relativieren, ein technologisch vielfältiges Ökosystem schaffen und damit die eigenen Handlungsoptionen erweitern.

3 Systematische Risikoabwägung, -bewertung, und -analyse

Digitale Souveränität ist kein binärer Zustand, sondern das Ergebnis strategischer Gestaltung. Um den unternehmerischen Handlungsbedarf richtig einzuordnen, müssen Organisationen verstehen, wo und wie Risiken für ihre digitale Handlungsfähigkeit entstehen, und zugleich bewerten, mit welcher Wahrscheinlichkeit diese Risiken eintreten. Der risikobasierte Ansatz ist nicht neu und hat im Rahmen der unternehmerischen Gestaltung an Bedeutung gewonnen durch die rasante technologische und auch regulatorische Entwicklung. Wie bereits oben ausgeführt, sind Interdependenzen nichts Neues, es geht um eine bewusste Risiko-Nutzen-Abwägung.

Im Folgenden werden fünf zentrale Risikofelder vorgestellt, deren Gestaltung in der Praxis substanziellen Einfluss auf die betriebliche und strategische Steuerungsfähigkeit hat.

Organisatorische Risiken

Fehlende Zuständigkeiten, fragmentierte Verantwortung und unklare Entscheidungswege verhindern in vielen Organisationen eine aktive Auseinandersetzung mit dem Thema digitale Modernisierung. Die Frage ist, ob die heutige Organisationsstruktur eines Unternehmens so aufgestellt ist, um eine Modernisierung und die notwendige digitale Transformation zu ermöglichen. Entscheidungen zur Cloud-Nutzung oder zum Einsatz externer KI-Dienste werden häufig isoliert getroffen – ohne eine übergreifende Steuerung oder Risikobewertung. Durch vertraglich festgelegte Vendor Lock-ins oder nur auf einen Cloud-Provider fokussierte Services entstehen Abhängigkeiten nicht aus strategischer Überzeugung, sondern aus operativem Pragmatismus.

Zudem mangelt es in vielen Unternehmen an Mechanismen, mit denen IT-bedingte Sourcing- und Architekturentscheidungen konsequent an übergeordneten Zielen wie Sicherheit, Resilienz oder Zukunftsfähigkeit ausgerichtet werden. Das äußert sich darin, dass die Unternehmen die Risiken für diese Ziele nicht ausreichend systematisch untersuchen und bewerten. Fehlt eine spezifische Cloud-Strategie, kann meistens auch keine effektive Enterprise-Architektur erstellt werden, um eine zielgerichtete und stetige Modernisierungsarbeit für das Unternehmen zu leisten.

Risikobezeichnung	Wirkung auf unternehmerische Zukunfts- / Handlungsfähigkeit	Anmerkung
Fehlende Zuständigkeiten	Es fehlt institutionalisierte Verantwortung zur Gesamtbetrachtung der unternehmerischen Zukunfts- / Handlungsfähigkeit digitaler Souveränität.	Ohne Zuständigkeiten wird das Thema operativ übersehen oder zu spät berücksichtigt.
Fragmentierte Entscheidungspfade	Strategisch wirksame Technologieentscheidungen folgen keiner einheitlichen und geschäftsstrategischen Bewertung.	Cloud- oder KI-Entscheidungen werden dezentral und isoliert getroffen – meist opportunistisch.
Unzureichende Governance und Prozesse	Es fehlt ein Regelwerk zur systematischen Steuerung von Interdependenzen.	Entscheidungen erfolgen ad hoc, nicht anhand transparenter Kriterien oder Schwellenwerte.
Fehlende unternehmensweite Cloud-Strategie	Moderne Cloud-Architekturen und -Technologien ermöglichen neben den originären Zielen einer modernen IT-Infrastruktur auch eine höhere digitale Souveränität durch ihre Flexibilität, Resilienz und Sicherheit.	Ignorieren von verschiedenen »Cloud-Deployment«-, und Architektur – Optionen, die eine flexible und zukunftsorientierte Anpassung an die strategischen Ziele des Unternehmens ermöglichen.

Technologische Interdependenzen

Viele moderne Plattformen – insbesondere im Cloud- und KI-Bereich – bieten hochgradig integrierte Funktionalitäten, die über proprietäre Schnittstellen bereitgestellt werden. Diese technische Bequemlichkeit birgt ein Risiko: Je stärker Systeme, Datenmodelle und Prozesse an eine bestimmte Plattform gekoppelt werden, desto schwieriger wird ein späterer Wechsel – sowohl technisch als auch wirtschaftlich. Auf der anderen Seite fördern integrierte Fähigkeiten die schnelle Umsetzung innovativer Ansätze und damit die Chance auf einen schnellen »Go-To-Market«.

Lock-in entsteht nicht nur durch Technologie, sondern auch durch fehlende vertragliche Absicherung, Gewöhnung und Integration in die gesamte IT-Landschaft. Fehlen Schnittstellen und ein Konzept zur modularen Entkopplung, steigt das Risiko eines Vendor Lock-ins und der spätere Wechsel zu Alternativen wird komplex und kostenintensiv.

Es kann sehr sinnvoll sein, der Innovation den Vorzug zu geben und einen neuartigen Service über eine proprietäre Schnittstelle anzubinden. Bei einer späteren Standardisierung solcher Services kann dann eine bewusste Migrationsentscheidung auf einen Standard getroffen werden, um die Souveränität zu erhöhen. Im gleichen Zug ist zu erwarten, dass Anbieter diese Standardschnittstellen ebenfalls implementieren. Das Beispiel OpenAI zeigt, wie eine API innovativ in den Markt drängt

und dann als standardsetzend für alternative Lösungen dient – Innovation und Souveränität gehen hier Hand in Hand.

Risikobezeichnung	Wirkung auf Souveränität	Anmerkung
Nutzung proprietärer Schnittstellen	Die technische Kopplung verhindert den Wechsel zu anderen Plattformen.	APIs und Datenformate sind oft nur bei einem Anbieter verfügbar – Migration wird erschwert.
Plattformverzahnung von Prozessen	Fachprozesse sind tief in spezifische Plattformlogik integriert.	Die Prozesslogik basiert z. B. auf einem proprietären Workflow- oder AI-Service.
Fehlende Modularität und Interoperabilität	Systeme sind nicht entkoppelt und schwer austauschbar.	Eine modulare Architektur erleichtert Substitution oder Redundanz – fehlt aber oft.
Vertraglich vorgesehener Vendor-Lock-In samt Strafen bei Umstieg	Die vertragliche Bindung kann den Wechsel zu anderen Plattformen erschweren.	Abmilderung durch explizite Interoperabilitäts- und Exit-Klauseln, portables Design und Multi-Cloud-Ansätze.

Kompetenzdefizite und Skill-Monokulturen

Digitale Zukunfts- / Handlungsfähigkeit setzt voraus, dass Organisationen die genutzten Technologien verstehen und aktiv gestalten können. In der Praxis zeigt sich jedoch häufig eine Monokultur an Fähigkeiten: Alle Teams sind auf einen Anbieter, ein Ökosystem oder ein bestimmtes Tool-Set spezialisiert. Kompetenzen auf einen Anbieter zu fokussieren, wirkt einerseits effizient, kann aber die Abhängigkeit von einzelnen externen Dienstleistern erhöhen und erschwert die Nutzung alternativer Plattformen.

Besonders kritisch ist das bei Cloud-Plattformen, deren Services oft tiefes Spezialwissen für Konfiguration und Absicherung erfordern. Fehlt entsprechendes Know-how im eigenen Haus, wird technologische Steuerung erschwert. Ist es nur für eine Plattform vorhanden, wird diese den Vorzug vor Alternativen erhalten und es entsteht eine Erfahrungs- und Wissensverdichtung in Bezug auf diese Plattform.

Diese »Skill-Gravitation« schafft also einen Feedback-Loop und damit einen sich selbst verstärkenden Lock-in. Um das zu verhindern, muss in die Ausbildung mehrerer funktional redundanter Teams auf verschiedenen Plattformen investiert werden. Dabei ist sorgsam zu beobachten, ob der Aufwand wirtschaftlich gerechtfertigt ist und ob es gelingt, die notwendige Zusammenstellung von Fachleuten langfristig an das Unternehmen zu binden.

Für kleinere Unternehmen erscheint es oft unrealistisch, umfassende Multi-Cloud-Kompetenzen aufzubauen. Trotzdem können sie ihre Handlungsfähigkeit sichern –

etwa durch den bewussten Aufbau einer steuerbaren Plattform (z. B. Kubernetes), den Einsatz offener Standards, portabler Datenformate und unabhängiger Backup-Strategien. Beim Einsatz externer Dienstleister ist darauf zu achten, dass die Steuerungs- und Lösungskompetenz im eigenen Haus verbleibt – Dokumentation und Know-How-Transfer können hier Abhängigkeiten reduzieren. Multi-Cloud-Nutzung ist heute leichter möglich als es der Einsatz von verschiedenen Technologien und Anbietern in der Vergangenheit war. Eine effektive Governance, die mit der Komplexität von Multi-Cloud-Ansätzen kompetent umgehen kann ist notwendig, um Souveränitätsziele bewusst steuern zu können. Natürlich beinhaltet diese auch die bedeutenden Schutzziele der IT-Sicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit als Grundvoraussetzung. Wer seine Informationen nicht wirksam schützen kann, ist nicht in der Lage, Souveränität zu gewährleisten.

Risikobezeichnung	Wirkung auf Souveränität	Anmerkung
Plattformzentrierte Skills	Das Know-how konzentriert sich auf eine Plattform – Alternativen werden verdrängt.	Teams nutzen automatisch, was sie kennen – andere Optionen wirken risikoreicher und aufwändiger.
Geringe interne Steuerungs- / Lösungskompetenz	Entscheidungen sind von externem Know-how abhängig.	Externe Dienstleister haben meist einen Informationsvorsprung – Organisationen können Abhängigkeiten nicht selbst erkennen oder reduzieren.
Mangelnde Multi-Plattform-Erfahrung	Die Suche und Beurteilung von Alternativen sind nicht belastbar.	Ohne Erfahrung mit anderen Plattformen können Stärken / Schwächen nicht objektiv eingeschätzt werden.

Wirtschaftliche Interdependenzen und getestete Exit-Optionen

Werden Cloud- oder KI-Dienste zu zentralen Komponenten kritischer Geschäftsprozesse, Fachanwendungen oder Entscheidungssysteme, entsteht eine enge technische und wirtschaftliche Verzahnung mit den jeweiligen Plattformanbietern. Geschlossene Ökosysteme können dabei besondere Vorteile bieten, etwa durch optimierte Integration, effiziente Datentransfers oder exklusive Funktionalitäten, die die Nutzungsintensität innerhalb des Ökosystems fördern – um den Preis eines höheren Commitments zu dieser Technologie. Daher ist es wichtig, dass Unternehmen die langfristigen strategischen Implikationen im Blick behalten und bewusst prüfen, wie sie technologische Abhängigkeiten aktiv gestalten und gegebenenfalls absichern können.

Veränderungen bei Preisen, Lizenzen, geopolitischen Rahmenbedingungen oder der Serviceverfügbarkeit können für Unternehmen herausfordernd sein, insbesondere dann, wenn schnelle technologische Anpassungen erforderlich sind. In solchen Situationen zeigt sich, wie gut ein Unternehmen auf alternative Optionen vorbereitet

ist und ob es flexibel reagieren kann. Zwar existieren in vielen Fällen Exit-Konzepte, doch deren praktische Umsetzbarkeit hängt stark davon ab, ob notwendige Schritte wie Datenexport, Systemreplikation oder organisatorische Anpassungen realistisch geplant und getestet wurden.

Risikobezeichnung	Wirkung auf Souveränität	Anmerkung
Hohe technische und organisatorische Exit-Kosten	Ein Anbieterwechsel ist wirtschaftlich nicht darstellbar / unattraktiv.	Die Migration würde hohe Projektkosten, lange Downtimes oder Neukonstruktionen erfordern.
Pfadabhängigkeit durch tiefe Integration	Anbieternahe Dienste sind oft komfortabler und effizienter nutzbar, wodurch externe Alternativen tendenziell an Attraktivität verlieren.	Günstige Traffickosten, automatische Authentifizierung u. a. fördern Plattformbindung.
Ungetestete Exit-Konzepte	Migrationspläne existieren nur auf dem Papier – nicht als geübte Notfalloption.	Ohne Tests und Budgetierung bleibt der Exit abstrakt – und wird im Krisenfall nicht als Option gesehen.
Technologische / Wirtschaftliche Abhängigkeit (Vendor Lock-in)	Anbieter kann Preise, Lizenzmodelle oder Nutzungsrechte einseitig ändern.	Unternehmen haben keine Handhabe, sich dagegen zu wehren – Verträge helfen nur begrenzt. Der Austausch mit Alternativanbietern bietet eine Stütze hier an.
Keine vorhandene Servicebeschreibung der eigenen IT-Dienste	Unzureichende Entscheidungs- und Bewertungsgrundlage für Cloud-bezogene Steuerung.	Ein eigener Servicekatalog ist eine Voraussetzung für die Überführung der Services in die Cloud oder von einem zum anderen Cloud-Serviceprovider.

Politisch-regulatorische Risiken

Cloud- und KI-Plattformen unterliegen den jeweiligen Rechtsordnungen der Länder, in denen sie betrieben oder kontrolliert werden. Verschiedene Gesetzesinitiativen der EU unterstützen das Vorhaben von resilienten und sicheren IT-, Cloud, sowie KI- Systemen (EU Cybersecurity Act mit EUCS und EUCC, NIS-2-Richtlinie, EU Data Act, EU AI Act, EU Cyber Resilience Act etc.). Damit stehen für den Cloud-, IT-Markt in der EU bereits heute praktische Tools und Methoden zur Verfügung, um die eigenen Cloud-Lösungen entsprechend den Vorgaben auszulegen (DevSecOps) und deren Sicherheitsniveaus zu überprüfen (Self-Assessment oder 3rd Party Assessment / Certification). Neben den nationalen Programmen z. B. vom BSI, wie IT-Grundschutz und C5-Katalog, existieren auch Programme und »Code of Conducts« auf europäischer Ebene (EUCC; EUCS, EU CoC).

Für international tätige Unternehmen ist es daher wichtig, regulatorische Rahmenbedingungen – auch in Drittstaaten – sorgfältig zu prüfen. Selbst bei EU-konformen Vertragsgestaltungen können politische oder regulatorische Eingriffe, etwa

durch Exportkontrollen, Sanktionen oder nationale Sicherheitsgesetze, die Nutzung digitaler Dienste beeinflussen. Ein Beispiel hierfür ist unter anderem die US-amerikanische Foreign Direct Product Rule (FDPR), die auch außerhalb der USA Auswirkungen auf Technologien haben kann, die auf US-Hardware oder -Software basieren. Solche extraterritorialen Effekte betreffen nicht nur staatliche Einrichtungen, sondern auch privatwirtschaftliche Akteure mit internationaler Ausrichtung. Umso wichtiger ist es, dass Unternehmen geopolitische Entwicklungen in ihre strategische Planung einbeziehen und gemeinsam mit Technologiepartnern belastbare Szenarien für den Umgang mit regulatorischen Veränderungen entwickeln.

Dieses Risiko ist jedoch nicht statisch, sondern hängt stark von den implementierten technischen und organisatorischen Schutzmaßnahmen ab. Unternehmen sollten prüfen, inwieweit Anbieter technische Souveränitätskontrollen anbieten, die einen Zugriff Dritter wirksam unterbinden. Dazu gehören beispielsweise Confidential Computing, bei dem Daten während der Verarbeitung verschlüsselt bleiben, clientseitige Verschlüsselung (Bring-Your-Own-Key), bei der der Anbieter selbst keinen Zugriff auf die Entschlüsselungsschlüssel hat, sowie vertragliche Zusicherungen für den Betrieb durch rein europäische Tochtergesellschaften mit lokalem Personal.

Risikobezeichnung	Wirkung auf Souveränität	Anmerkung
Eingeschränkte Vertragssicherheit	Vertragsrechte sind außerhalb der eigenen Jurisdiktion schwer durchsetzbar, besonders wenn außenpolitische Maßnahmen (z. B. Zölle, Exportrestriktionen) dagegenstehen.	Selbst gut formulierte SLAs oder Datenschutzerklärungen helfen wenig, wenn Rechte effektiv nicht durchgesetzt werden können.
Geopolitische Disruption	Politische Maßnahmen können zu Blockaden, Embargos oder Zugangseinschränkungen führen.	Unternehmen müssen den Zugriff auf zentrale Funktionen dauerhaft sicherstellen können.
Zugriff durch Drittstaaten (z. B. CLOUD Act)[5]	Datenzugriffe durch Behörden außerhalb der EU können – abhängig von der jeweiligen Rechtslage – erfolgen. Auch Metadaten können bereits sensible Informationen enthalten (z. B. über Personal, organisatorische Maßnahmen).	EU-Hosting schützt nur bedingt, wenn der Anbieter aus einem Drittstaat stammt.

[5] Notiz: Der US CLOUD Act regelt den Zugriff US-amerikanischer Behörden auf Daten, auch wenn diese außerhalb der USA gespeichert sind. Er verpflichtet Anbieter jedoch nicht zur Entschlüsselung von Daten, und internationale Abkommen können zusätzliche Schutzmechanismen schaffen. Diese werden derzeit (Stand: November 2025) zwischen der EU und den USA verhandelt.

Die in diesem Kapitel dargestellten Risikofelder zeigen, wie unterschiedlich und vielschichtig die Gefährdungen der digitalen Handlungsfähigkeit eines Unternehmens sein können. Praktisch bilden sich je nach Anwendungsfall und Unternehmenskontext unterschiedliche Risikoprofile heraus, die jedes Unternehmen individuell betrachten und bewerten muss. Im folgenden Kapital gehen wir näher darauf ein.

4 Bewertung digitaler Risiken als Bestandteil des Unternehmensrisiko-managements

Um wirksame Maßnahmen aus den zuvor genannten Risikofeldern abzuleiten, ist es notwendig, die eigenen Services sowie die Risiken systematisch zu bewerten, idealerweise im Rahmen bestehender Prozesse des Enterprise-IT-Managements und des Unternehmensrisikomanagements. Dadurch können geübte und etablierte Fähigkeiten genutzt und um den Aspekt der Souveränität erweitert werden.

Strategische Kopplung von Geschäftszielen und IT-Strategie

Die Kopplung von Geschäfts- und IT-Strategie entscheidet heute darüber, ob Unternehmen Technologie als Mittel der Kontrolle oder als Quelle von Abhängigkeit nutzen. Wer seine geschäftskritischen Dienste kennt, kann im Rahmen eines Enterprise-IT-Managements auch bewerten, welche davon besondere Souveränitätsanforderungen haben – und wo Risiken entstehen.

Der Weg dorthin ist pragmatisch:

Ein Servicekatalog bildet die Grundlage. Jeder Dienst wird hinsichtlich seiner Schutzbedarfe bewertet und mit den Angeboten potenzieller Cloud- oder KI-Anbieter verglichen. Stimmen Schutzbedarf und Schutzangebot überein, steht einer Nutzung nichts im Weg. Weicht der Anbieter davon ab, wird im Rahmen des Risikomanagements entschieden: akzeptieren, kompensieren – oder eine Alternative wählen.

So entsteht ein klares Bild, welche Services kritisch sind, welche Anbieter infrage kommen – und wo Handlungsbedarf besteht. Die operative Voraussetzung dafür: eine

IT, die ihre Dienste sauber beschreibt, bewertet und steuern kann. Dann wird Risikomanagement vom Kontrollinstrument zum strategischen Werkzeug – und digitale Souveränität zu einer bewusst getroffenen Entscheidung.

Souveränitätsgrad als Ergebnis der Risikobewertung

Digitale Souveränität lässt sich nicht absolut messen. Sie lässt sich jedoch nach Strategiekonformität bewerten – kontextabhängig, anwendungsbezogen und risikoorientiert. Ein bewährter Ansatz ist die Herleitung eines Souveränitätsgrads aus der Risikobewertung: Je höher die Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe für ein identifiziertes Risiko, desto kritischer die Abhängigkeit – und desto niedriger der Grad digitaler Handlungsfähigkeit im betrachteten Bereich.

So entsteht ein differenziertes Bild: Manche Systeme (z. B. Public-Cloud-Hosting für Webseiten) sind risikotechnisch hinsichtlich Souveränität unkritisch, andere (z. B. Lieferkettensteuerung über proprietäre KI-Systeme mit extraterritorialem Hosting) können sensibel sein. Entscheidend ist, die Risiken nicht pauschal, sondern geschäftsrelevant zu gewichten.

Die Einführung und Umsetzung einer Cloud- und KI-Strategie, die neben vielen anderen Kriterien (Skalierung, Sicherheit, Abhängigkeiten, eigene Geschäftsziele, etc.) auch nach Risikobewertungen ausgelegt sein sollte, ist die Grundlage für Entscheidungen zur Umsetzung von IT- Infrastruktur-, und Technologieprojekten für kritische Anwendungen und Geschäftsprozesse.

Ein Governance-Modell sorgt für die kontinuierliche Kontrolle und Umsetzung von Maßnahmen zur Erreichung der definierten Ziele und Roadmaps. Digitale Souveränität sollte hierbei immer als ein fester Bestandteil der übergeordneten strategischen Ziele angesehen werden.

Bewertungstiefe: strategisch und operativ

Die Bewertung sollte zwischen strategischer (z. B. bei Sourcing-Entscheidungen) und operativer Ebene (z. B. bei der konkreten Einführung oder Migration von Services) abgestimmt sein. Dabei gilt: Nicht alle Risiken lassen sich vermeiden – aber sie lassen sich bewusst eingehen, wenn ihre Tragweite bekannt ist und entsprechende Gegenmaßnahmen vorbereitet sind.

Ein Beispiel: Die Nutzung eines proprietären Datenbankdienstes eines extraterritorialen Anbieters kann sinnvoll sein, sofern sich das Unternehmen über regulatorische Anforderungen, Exit- und Kontrollmöglichkeiten im Klaren ist und dafür konkrete Handlungsoptionen definiert hat. Sind die Risiken akzeptabel und / oder ein Wechsel zu vertretbaren Kosten in annehmbarer Zeit möglich, steht der Nutzung nichts im Weg.

Vorteile des integrativen Bewertungsansatzes

Die Verknüpfung digitaler Souveränität mit etablierten Risikobewertungsverfahren bringt mehrere Vorteile:

- **Geringerer zusätzlicher Aufwand**: Bestehende organisatorische Routinen und Gremien können mitgenutzt werden.
- **Höhere Akzeptanz und schnellere Umsetzung**: Die Einbettung in vertraute Verfahren erleichtert das Verständnis und die Umsetzungsbereitschaft im Unternehmen.
- **Bessere Governance**: Souveränitätsaspekte werden frühzeitig adressiert und in Entscheidungsprozesse eingebunden.
- **Konkrete Ableitbarkeit von Maßnahmen**: Die Risikobewertung schafft eine belastbare Grundlage für Investitionen, Architekturentscheidungen und organisatorische Veränderungen.

Souveränität wird damit **nicht als abstraktes Ideal,** sondern als **steuerbares Schutzgut** im betrieblichen Kontext behandelt und als Teil eines fundierten digitalen Risiko- und Chancenmanagements.

5 Maßnahmen zur Stärkung der digitalen Handlungsfähigkeit

Die Analyse der Risiken in Kapitel 3 und ihre Bewertung nach Kapitel 4 zeigen: Digitale Souveränität ist kein Selbstläufer. Sie muss kontinuierlich angepasst werden. In diesem Kapitel geht es daher um konkrete, umsetzbare Maßnahmen, mit denen Unternehmen und öffentliche Einrichtungen ihre digitale Handlungsfähigkeit systematisch stärken können.

Die Maßnahmen sind entlang von sechs Handlungsdimensionen gegliedert. Sie adressieren jeweils mehrere Risikofelder gleichzeitig und zeigen, welche praktischen Hebel für mehr Kontrolle, Flexibilität und Resilienz genutzt werden können.

Skills für Plattformvielfalt aufbauen

Digitale Souveränität beginnt bei den Menschen. Wer nur eine Plattform beherrscht, wird zwangsläufig bei ihr bleiben, selbst wenn sich die Bedingungen verschlechtern.

Viele Unternehmen haben in den vergangenen Jahren stark auf einen Cloud-Anbieter oder ein technisches Ökosystem gesetzt. Dabei ist häufig eine Monokultur an

Kompetenzen entstanden: Teams kennen nur die Werkzeuge eines bestimmten Anbieters, Dokumentation und Prozesse sind auf dessen Services zugeschnitten, neue Mitarbeitende werden mit dem gleichen Technologie-Stack sozialisiert. Diese Situation erschwert den Wechsel – nicht aus technischer Unmöglichkeit, sondern aus Mangel an Können und experimenteller Erfahrung.

Um diese »Skill-Gravitation« aufzubrechen, braucht es bewusste Personalentwicklung:

- Schulungsprogramme in mindestens zwei Cloud-Stacks und den jeweils relevanten IAM- und Security-Konzepten,
- Training in offenen Standards (z. B. Terraform / OpenTofu, Kubernetes),
- Aufbau interner Communities, in denen Wissen über alternative Plattformen aktiv geteilt und gepflegt wird, und
- interne Projekte zur Einführung alternativer Technologien – auch wenn sie nicht sofort produktiv genutzt werden.

So entstehen echte Wahlfreiheit und die Grundlage für strategische Unabhängigkeit.

Kontrollierbare Infrastrukturschichten einziehen (Platform Engineering)

Ein zentrales Mittel digitaler Souveränität ist die Fähigkeit, technologische Alternativen nicht nur zu wählen, sondern auch tatsächlich nutzbar zu machen. In der Praxis bedeutet das, unterschiedliche Technologien effizient in die eigene Organisation zu integrieren – sowohl auf technischer Ebene als auch effizient und komfortabel für die jeweiligen Nutzer. Besonders deutlich wird das im Kontext moderner Anwendungsdienste wie KI, Softwareentwicklung, Datenanalyse oder IoT.

Organisationen, die Auswahlfreiheit ernst nehmen, stehen daher vor einer Herausforderung: Sie müssen unterschiedliche Technologien und Anbieter in zentrale Arbeitsabläufe integrieren und gleichzeitig eine einheitliche Bereitstellung und Steuerung ermöglichen.

Ein geeigneter Ansatz ist hier das Platform Engineering, d.h. der Aufbau interner Plattformen, die zentrale Funktionen für bestimmte Anwendungsbereiche bereitstellen, beispielsweise:

- eine Infrastruktur-Plattform als hochperformantes, hochverfügbares System für kritische Workloads bei gleichzeitig guter Skalierbarkeit.
- eine Infrastruktur-Plattform zur Verschlüsselung hoch-sensibler bzw. »Business-kritischen« Daten.
- eine Plattform für maschinelles Lernen, die sowohl externe Foundation Models als auch interne Modelle orchestrieren kann,
- eine Entwicklerplattform, die eine Auswahl verschiedener Cloud-Umgebungen bereitstellt und standardisierte Deployments ermöglicht, oder

- eine Datenplattform, die Datendienste verschiedener Anbieter über einheitliche Schnittstellen zugänglich macht.

Ein dediziertes Plattform-Team kümmert sich dabei um den Aufbau und die Ausgestaltung der internen Plattform für die jeweiligen Anwender-Teams. Bei Unternehmen mit kleinerem Umfang werden dies eher sehr grundlegende Plattformen sein (z. B. Cloud Foundation oder Multi-Cloud-Portale), bei größeren Konzernen lohnt sich eine weitergehende Spezialisierung der Plattformen, um weitere Skalierungspotentiale zu nutzen (z. B. eine Datenanalyseplattform, die alle relevanten Daten und Modelle für den eigenen Absatzmarkt bereitstellt).

Solche Plattformen reduzieren Komplexität und Aufwand für die Nutzerinnen und Nutzer und erlauben gleichzeitig eine zentralisierte Steuerung auf Ebene der Organisation (»Control Plane«). Neue Dienste können gezielt eingeführt, überwacht, weiterentwickelt oder im Ernstfall auch wieder ersetzt werden.

Durch diesen Plattformansatz lassen sich technologische Infrastrukturschichten kontrollierbar gestalten. So entsteht die Grundlage für Auswahl, Wechseloptionen und damit für strategische Handlungsfähigkeit.

Offenheit und Standardisierung fördern

Digitale Abhängigkeiten entstehen dort, wo keine Alternativen bestehen oder wo Alternativen technisch aufwendig sind. Proprietäre Formate, geschlossene APIs oder exklusive Integrationen schaffen eine Architektur, die sich selbst verriegelt.

In der Praxis bedeutet das:

- bevorzugter Einsatz von offenen Schnittstellen wie OpenAPI oder OCI,
- Portabilität durch eine souveränitätsfördernde Architektur und bevorzugte Technologien (z. B. containerbasierte Deployments, Open-Source-Datenbanken, Kubernetes statt Function-as-a-Service usw.)
- Portabilität durch deklarative Konfigurationen (z. B. Kubernetes-Manifeste),
- Nutzung von SDKs und Integrationsmustern, die einen schnellen, effizienten Markteinstieg fördern und im späteren Verlauf des Lebenszyklus des Produkts »geöffnet« werden können,
- aktive Auswahl von Diensten, für die es standardisierte Alternativen gibt (z. B. offene Datenbanken wie Postgres)

Auch der Einsatz von Open-Source-Komponenten kann zur digitalen Handlungsfähigkeit beitragen – nicht zwingend, weil sie selbst betrieben werden sollen, sondern weil sie weithin als Service verfügbar, transparent aufgebaut und in auch in Private-Cloud-Betriebsmodellen nutzbar sind. Marktverfügbare Produkte auf der gleichen technischen Basis können Ressourcenaufwände und Kompetenzaufbau sparen und gleichzeitig die Exit-Option in andere Hosting-Modelle offenhalten. Die zeitliche Verzögerung einer Migration, die eine direkte Reaktion zum Schutz der eigenen Souveränität verhindert, sollte in der Risikobewertung berücksichtigt werden. Gleiches gilt für die in diesem Szenario sprungartig anfallenden Kosten einer Migration

– im Vergleich zu einer kontinuierlichen Investition in alternative Technologien wie zuvor beschrieben.

Die »Make or Buy«-Entscheidung kann durch Cloud-Technologien so kleinteilig wie nie zuvor getroffen werden. Die Gestaltung eines anforderungsgerecht zusammengestellten Serviceportfolios auf Basis einer integrierten Multi-Cloud-Landschaft ist dadurch anspruchsvoller, aber auch flexibler und effizienter geworden als mit vorherigen Technologie-Stacks.

Standardisierung schafft Wahlfreiheit und reduziert die Kosten künftiger Entscheidungen. Es gilt darauf zu achten, dass Innovationen schnell zur Marktreife und wirtschaftlichem Erfolg getrieben werden müssen. Bei innovativen Technologien kann es wirtschaftlich Sinn machen, den Aspekt der Souveränität hintenanzustellen, um Chancen im Markt zu nutzen und Erfahrungen zu sammeln. Keinesfalls sollten große Innovationspotenziale aus Angst vor Abhängigkeiten ungenutzt bleiben. Mit zunehmender Reifung solcher Technologien sollten dann jedoch – wie hier vorgeschlagen – diese Risiken wieder regulär betrachtet und gegen die wirtschaftlichen Potenziale bewertet werden, um weitere Entscheidungen zu informieren.

Exit-Szenarien technisch und organisatorisch vorbereiten

Theoretisch haben viele Unternehmen Exit-Pläne. Praktisch sind sie oft unvollständig, ungeprüft und damit nutzlos. Ein belastbares Exit-Szenario ist kein ausgefülltes Word-Dokument, sondern ein durchdachtes und getestetes Vorgehen:

- Wie lassen sich Daten, Modelle und Konfigurationen exportieren?
- Welche Alternativen existieren – funktional, regulatorisch und wirtschaftlich?
- Wer ist im Unternehmen in der Lage, diese Migration zu steuern?

Zentrale Elemente eines funktionierenden Exit-Managements:

- Design for Exit: Bereits bei Einführung eines neuen Systems wird ein möglicher Exit mitgedacht und dokumentiert. Nutzung von möglichst portablem Infrastructure-as-Code, umgebungsbasierter Konfiguration und anderen cloud-nativen Best Practices (12-Factors) beachten.
- Testszenarien: Regelmäßige Migrationsproben, um Prozesse, Abhängigkeiten und Zeitaufwände realistisch einzuschätzen.
- Governance-Einbindung: Definition klarer Exit-Trigger (z. B. Preissteigerung, regulatorisches Risiko) und Entscheidungsprozesse.

Nur wer realistische Alternativen hat und nutzen kann, erweitert seinen Handlungsrahmen und kann Alternativmaßnahmen einleiten. Das ist der zentrale Hebel für digitale Souveränität.

Souveränität als Governance-Kriterium verankern

Digitale Souveränität darf kein Einzelthema der IT bleiben. Sie ist ein strategisches Steuerungsziel und muss als solches in alle relevanten Entscheidungsprozesse integriert werden.

Das bedeutet:

- Einführung eines »Souveränitäts-Checks« in Architektur- und Projektgremien,
- verbindliche Bewertung von Abhängigkeiten bei Einkauf und Vertragsgestaltung,
- Berücksichtigung von Souveränitätskriterien in regulatorischen Vorbereitungen (z. B. DORA-Exit-Anforderungen),
- Reporting an die Geschäftsführung oder Aufsichtsorgane.

Souveränität ist dabei kein »Showstopper«, sondern ein entscheidungsleitender, nicht blockierender Risikofaktor unter anderen wie z. B. IT-Sicherheit. Die Etablierung als Governance-Kriterium erhöht die Relevanz im Unternehmen und sorgt dafür, dass das Thema nicht nur bei Krisen, sondern proaktiv bearbeitet wird.

Souveränitätsfördernde Alternativen stärken

Digitale Handlungsfähigkeit ist nicht nur eine Frage einzelner Unternehmensentscheidungen, sondern auch eine Frage der Gesamtarchitektur des digitalen Ökosystems. Möchten Unternehmen eine vielfältige Cloud-Landschaft aufbauen, um Wahlfreiheit zu ermöglichen, müssen sie dazu unter Berücksichtigung der identifizierten Risiken (s. oben) alternative Angebote in ihr Portfolio integrieren.

Dabei geht es nicht darum, Anbieter allein nach geografischer Herkunft zu wählen, sondern für den jeweiligen Anwendungsfall das beste Angebot auszuwählen. In diese Auswahl fließen Leistungsumfang und Qualität des Angebots ebenso ein wie die unter Souveränitätsgesichtspunkten identifizierten Risiken (s. oben). **Ziel ist Wahlfreiheit auf Basis objektiver Kriterien (Sicherheit, Compliance, Interoperabilität, Exit-Reife) – unabhängig von der Herkunft der Anbieter. Partnerschaften mit europäischen und internationalen Anbietern, die diese Kriterien erfüllen, stärken Souveränität.**

Trotzdem lohnt sich die strategische Unterstützung für Unternehmen, aber auch für Staaten im Sinne einer strategischen Infrastrukturpolitik:

- **Open-Source-Projekte** können in speziellen Bereichen wie Cloud-Infrastruktur, Datenmanagement oder KI oft hohe Transparenz, erweiterbare Architektur und Unabhängigkeit von einzelnen Anbietern bieten. Sie können helfen, die Investitionshoheit zurückzugewinnen und eigene Fähigkeiten auszubauen, so dass diese im Wettbewerb bestehen.
- **Souveräne Cloud-Angebote** wie z. B. regionale Anbieter, partnerschaftliche Modelle, rechtlich eigenständige EU-Betreibermodelle mit oder ohne Einfluss außereuropäischer Technologielieferanten und Public-Cloud-Angebote mit dezidierten Souveränitäts-Tools (z. B. auch in Partnerschaft mit lokalen Anbietern)

können zusätzliche Absicherungen im Sinne von lokaler Kontrolle, EU-Personal, zentraler Treuhandfunktion, technischen Tools (z. B. Verschlüsselung und External Key Management) und Zugriffsbarrieren eröffnen. Dies schafft neue Optionen für regulierte Branchen, staatliche Stellen oder Unternehmen mit erhöhten Compliance-Anforderungen. Es ist erkennbar, dass nahezu alle Anbieter Souveränitätsstrukturen aufbauen, die in die eigene Betrachtung einbezogen werden können.

- **Branchenübergreifende Plattformprojekte**, z. B. für industrielle Datenräume oder digitale Identitäten, müssen mit Nachdruck zur Einsatzreife vorangetrieben werden und sich im Wettbewerb behaupten.

Für Unternehmen ergibt sich daraus eine klare Handlungsmöglichkeit: Sie können sich aktiv beteiligen – als Nutzer, Beitragende oder Mitgestalter, zum Beispiel durch:

- Pilotprojekte mit neuen innovativen Ansätzen,
- aktive Mitwirkung in europäischen Konsortien und Initiativen (z. B. IPCEI-CIS, Gaia-X, Digital Europe, Alliance for Industrial Data, Edge and Cloud, European Cloud Alliance),
- Förderung wettbewerbsfähiger Infrastrukturen durch eigene Beiträge oder Beteiligungen.

Dies stärkt die Wettbewerbsfähigkeit und sorgt dafür, dass in kritischen Situationen tatsächlich souverän gehandelt und investiert werden kann. So stärken Organisationen ihre eigene Handlungsfähigkeit und genau das ist die Grundlage echter digitaler Souveränität.

Maßnahmen-Risiken-Matrix: Orientierung durch Verknüpfung

Um die Wirkung der Maßnahmen besser einschätzen zu können, zeigt die folgende Matrix, auf welche Risikofelder aus Kapitel 3 die Maßnahmen besonders stark wirken. Die Matrix dient der Orientierung. Sie ersetzt keine unternehmensspezifische Bewertung.

Maßnahme	Org. Risiken	Techn. Lock-in	Skill-Monokultur	Exit-Kosten	Regulatorisches Risiko
Skills für Plattformvielfalt aufbauen					
Kontrollierbare Infrastrukturschichten					
Offenheit und Standardisierung fördern					

Maßnahme	Org. Risiken	Techn. Lock-in	Skill-Monokultur	Exit-Kosten	Regulatorisches Risiko
Exit-Szenarien vorbereiten					
Governance verankern					
Europäische Alternativen stärken					

= hohe Wirksamkeit = unterstützende Wirkung

= geringe direkte Wirkung

Digitale Souveränität lässt sich gestalten. Und zwar nicht durch Lippenbekenntnisse oder Verbote, sondern durch konkrete Maßnahmen, die in Architektur, Prozesse und Kompetenzen eingebettet sind. Um dabei effektiv vorzugehen und die kritischen Abhängigkeiten zu erkennen, sorgt ein risikoorientiertes Vorgehen, wie es hier vorgestellt wurde, für eine höhere Treffgenauigkeit von Maßnahmen.

Die in diesem Kapitel vorgestellten Ansätze bieten einen praxisnahen Werkzeugkasten für mehr digitale Handlungsfähigkeit – als Schutz, als Strategie und als Zukunftsinvestition.

6 Beispielhafte Risikobewertung: Die Fictura Mittelstand GmbH in der Praxis

Nach der aufgeworfenen Diskussion in der Geschäftsführung (vgl. Kapitel 1) hat die Fictura Mittelstand GmbH ein kleines internes Projektteam beauftragt, die Souveränitätsrisiken eines tiefgreifenden Cloud- und KI-Einsatzes systematisch zu bewerten. Ziel ist, die realen Abhängigkeiten greifbar zu machen – nicht theoretisch, sondern mit Blick auf konkrete Entscheidungen.

Das Team nutzt dazu eine einfache Bewertungsmatrix entlang zweier Achsen, die üblicherweise zur Risikobewertung herangezogen werden:

- **Eintrittswahrscheinlichkeit**: Wie wahrscheinlich ist es, dass dieser Risikofaktor in unserem Umfeld tatsächlich relevant wird?
  (Skala 1 = gering bis 5 = sehr hoch)
- **Schadensausmaß bei Eintritt**: Wie stark würde die digitale Handlungsfähigkeit des Unternehmens eingeschränkt?
  (Skala 1 = vernachlässigbar bis 5 = existenzbedrohend)

Daraus ergibt sich der **Risikoscore** (Produkt aus beiden Werten), der als Entscheidungsgrundlage dient.

Strukturell entspricht dieses Vorgehen, den üblichen Ansätzen zur Risikobewertung. Die Fictura Mittelstand GmbH möchte, die bereits im Unternehmen existierenden Methoden nutzen und die Souveränitätsrisiken als zusätzliches Set an zu bewertenden Risiken dort mit einbeziehen.

HINWEIS
Die in diesem Paper aufgezeigten Risikofaktoren können dafür ein Ausgangspunkt sein, sollten aber durch eine eigene interne Risikofindung überprüft und ergänzt oder gestrafft werden.

Für dieses Beispiel wurden fünf der **prägnantesten Risikofaktoren** (aus Kapitel 3) exemplarisch bewertet:

Fehlende Zuständigkeiten (Organisatorisches Risiko)

Bei der internen Bestandsaufnahme stellt Fictura fest, dass Entscheidungen zu Cloud- oder KI-Diensten in den letzten zwei Jahren überwiegend projektgetrieben getroffen wurden: Die Vertriebs-IT hat eigenständig ein Analyse-Tool eingeführt, die Produktions-IT nutzt einen anderen Anbieter für Wartungsdaten, und die Forschungsabteilung experimentiert mit einem dritten Dienst für Machine-Learning-Modelle. Eine zentrale Stelle, die diese Entwicklungen bewertet oder zusammenführt, existiert nicht. Dadurch haben sich Abhängigkeiten gebildet, die niemand gesamthaft überblickt. Da dieser Zustand schon heute sichtbar ist, bewertet das Team die Eintrittswahrscheinlichkeit als sehr hoch und den möglichen Schaden als relevant — weil unkoordinierte Architekturentscheidungen langfristige Verflechtungen schaffen, die schwer zu korrigieren sind.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risikoscore
5 (ist aktuell gegeben)	3 (führt zu unkoordinierten Entscheidungen)	15

Anmerkung: Entscheidungen zu Cloud-Nutzung erfolgen aktuell auf Projektbasis. Niemand prüft dabei systematisch die strategischen Auswirkungen. Dadurch besteht die Gefahr, dass sich kritische Abhängigkeiten »ungeplant« einschleichen.

Technologische Abhängigkeit durch spätes Handeln

Bei der Marktanalyse erkennt Fictura, dass mehrere internationale Wettbewerber KI-basierte Zusatzfunktionen bereits fest in ihre Maschinen integriert haben – etwa automatisierte Parameteroptimierung oder datengetriebene Diagnosemodelle. Diese Dienste setzen neue Kundenerwartungen und beeinflussen, welche Schnittstellen und Datenformate in der Branche zum Standard werden. Wenn Fictura zu spät eigene Lösungen entwickelt oder alternative Anbieter frühzeitig einbindet, muss sie später diese extern gesetzten Standards übernehmen – inklusive proprietärer Modelle, Formate oder Plattformen. Damit verliert das Unternehmen langfristig die Möglichkeit, selbst zu bestimmen, wie seine digitalen Services aufgebaut sind.

Das Team bewertet deshalb die Eintrittswahrscheinlichkeit als hoch (4), da sich die Branche sichtbar in Bewegung befindet, und das Schadenspotenzial als sehr hoch (5), weil der Verlust eigener Gestaltungshoheit Ficturas Wettbewerbsposition dauerhaft schwächen könnte.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risikoscore
4	5	20

Skill-Monokultur (Kompetenzdefizite)

Im technischen Betrieb zeigt sich, dass nahezu alle Automatisierungsabläufe und Betriebsprozesse auf die Funktionsweise eines einzelnen großen Plattformanbieters ausgerichtet sind. Skripte, Monitoring, Incident-Prozesse und Sicherheitsmechanismen basieren ausschließlich auf dessen Werkzeugen. Andere Plattformen wurden nie praktisch getestet und gelten intern pauschal als »zu aufwendig« oder »nicht kompatibel«. Das Unternehmen ist dadurch organisatorisch nicht in der Lage, alternative Dienste kurzfristig einzuführen oder parallel zu betreiben, selbst wenn dies aus regulatorischen oder wirtschaftlichen Gründen notwendig wäre. Deshalb wird die Eintrittswahrscheinlichkeit eines Problems als hoch bewertet. Das Schadensausmaß wird als mittel eingeschätzt, da Fictura zwar weiterarbeiten kann, aber strategisch an Flexibilität verliert.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risikoscore
4	3	12

Anmerkung: Der Betrieb denkt »AWS first« – andere Plattformen werden als inkompatibel und riskant eingestuft. Das behindert strategische Diversifikation und schränkt künftige Optionen ein.

Ungetestete Exit-Konzepte (Wirtschaftliches Risiko)

Bei der Analyse stellt Fictura fest, dass mehrere zentrale Geschäftsprozesse – etwa Ersatzteilbestellungen, Ferndiagnosen und die Übermittlung von Wartungsdaten – technisch eng an proprietäre Dienste eines einzelnen Plattformanbieters gebunden sind. In den vergangenen zwölf Monaten hat dieser Anbieter wiederholt Preise und Lizenzmodelle geändert, teilweise kurzfristig und mit direkter Auswirkung auf produktive Funktionen. Das Team hält daher weitere Einschränkungen oder Kostensteigerungen für sehr wahrscheinlich (5).

Der mögliche Schaden wird als maximal bewertet (5), weil Fictura derzeit keinen belastbaren Ausstiegsweg hat: Datenexporte wurden nie praktisch getestet, die mobile Service-App hängt direkt an proprietären Schnittstellen, und mehrere Kundenverträge verlangen kontinuierliche Diagnosefunktionen. Ein erzwungener Plattformwechsel würde erhebliche Verzögerungen verursachen, Vertragsrisiken auslösen und zentrale digitale Services zeitweise außer Betrieb setzen.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risikoscore
5	5	25

Marktpolitische Eingriffe durch ausländische Regierungen (Politisch-regulatorisches Risiko)

Für bestimmte internationale Servicefunktionen nutzt Fictura Cloud-Dienste eines Anbieters aus einem Drittstaat. Bei der Risikobewertung orientiert sich das Team an realen Fällen der letzten Jahre, in denen Regierungen Softwareexporte beschränkt oder Funktionen für einzelne Märkte untersagt haben, etwa im Zuge der US-Exportkontrollen gegenüber chinesischen Technologieunternehmen. Würde eine vergleichbare Maßnahme den von Fictura genutzten Dienst betreffen, könnten zentrale Funktionen wie Fernzugriff, Diagnosemodelle oder Update-Bereitstellung für Kunden außerhalb der EU kurzfristig eingeschränkt werden. Da solche Eingriffe vorkommen, bewertet das Team die Eintrittswahrscheinlichkeit als moderat (3), das Schadenspotenzial jedoch als hoch (4), insbesondere für die internationale Kundenbetreuung und Servicekontinuität.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risikoscore
3	4	12

Gesamtbewertung

Die fünf Einzelbewertungen ergeben zusammen ein deutliches Risikoprofil: Nicht ein einzelner technischer Fehler, sondern das Zusammenspiel aus organisatorischen Lücken, Kompetenzengpässen und struktureller Plattformabhängigkeit erzeugt die größte Verwundbarkeit. Vor allem wirtschaftliche Risiken – wie fehlende Exit-Fähigkeit – wirken sich unmittelbar auf die Handlungsfähigkeit des Unternehmens aus. Die Gesamtschau macht sichtbar, an welchen Stellen Fictura sofort aktiv werden muss und wo mittelfristige Anpassungen ausreichen. Die folgende Übersicht fasst die Ergebnisse zusammen.

Risikofeld	Risikofaktor	Score	Kritikalität
Wirtschaftlich	Ungetestete Exit-Konzepte	25	sehr hoch
Technisch	Plattformverzahnung von Prozessen	20	hoch
Organisatorisch	Fehlende Zuständigkeiten	15	mittel
Politische	Drittstaatlicher Zugriff	12	mittel
Kompetenzen	Skill-Monokultur	12	mittel

Fazit aus der Bewertung und Maßnahmenableitung

Die konsolidierte Bewertung macht deutlich: Die größte Verwundbarkeit der Fictura Mittelstand GmbH entsteht durch fehlende Exit-Fähigkeit, drohenden Verlust technischer Gestaltungshoheit und unklare Zuständigkeiten. Das alles führt dazu, dass das Unternehmen technologisch eher »getrieben« als gestaltend handelt.

Die Geschäftsführung beschließt daher drei unmittelbar wirksame Maßnahmen — alle darauf ausgerichtet, Handlungsfähigkeit zurückzugewinnen:

1. **Eine Exit-Probe, die nicht nur belastbare Wechselpfade schafft, sondern bewusst zum Kompetenzaufbau für mindestens ein weiteres Ökosystem genutzt wird.** Fictura führt eine realistische Exit-Probe für einen ausgewählten Dienst durch: Datenexport, Re-Deployment auf einer alternativen Plattform, Anpassung der Arbeitsabläufe. Dabei geht es nicht nur darum, einen Ausstiegsweg technisch nachzuweisen und finanziell zu bewerten – die Exit-Probe dient zugleich dem gezielten Kompetenzaufbau für ein zweites Ökosystem. Das Unternehmen lernt dabei, wie alternative Plattformen funktionieren, welche Schnittstellen relevant sind und wo technische oder organisatorische Hürden liegen. Exit-Fähigkeit wird so zu einem aktiven Lernprozess, der langfristige Handlungsfähigkeit sicherstellt.
2. **Den strategischen Aufbau technologischer Alternativen, bei denen Skill-Entwicklung integraler Bestandteil ist: Wer Alternativen nutzen will, muss sie verstehen.**

Um nicht von den Architekturentscheidungen eines einzigen Ökosystems abhängig zu werden, baut Fictura frühzeitig parallele Lösungswege auf: offene Modelle, interoperable Standards, alternative Plattformen für KI-Services oder maschinennahe Analytics. Dieser technische Aufbau wird bewusst mit Skill-Aufbau verbunden: Teams sollen nicht nur »eine Plattform können«, sondern die Grundlagen mehrerer Ökosysteme beherrschen. Die Einführung zusätzlicher Plattformen ist damit kein Selbstzweck, sondern ein gezielter Schritt, um Entscheidungsfreiheit zu sichern und zukünftige Standards aktiv mitgestalten zu können.

3. **Eine klare Governance-Struktur, die sicherstellt, dass Plattform- und KI-Entscheidungen systematisch bewertet, abgestimmt und gesteuert werden.** Fictura richtet ein Architektur- und Beschaffungsgremium ein, das souveränitätsrelevante Kriterien bewertet, Alternativen prüft und strategische Entscheidungen koordiniert. Damit wird die bisherige projektgetriebene Fragmentierung beendet. Diese Governance sorgt dafür, dass Skill-Aufbau und Technologieentscheidungen planvoll erfolgen – und nicht zufällig durch individuelle Vorlieben oder externe Dienstleister getrieben werden.

Diese Schritte adressieren die drei größten Risiken direkt und verbinden organisatorische, technische und kompetenzbezogene Maßnahmen zu einem konsistenten Gesamtansatz. Fictura gewinnt dadurch nicht nur digitale Souveränität zurück, sondern stärkt die Fähigkeit, Innovation selbstbestimmt und langfristig tragfähig einzusetzen.

7 Fazit: Strategische Vielfalt sichern & Handlungsfähigkeit erhalten

Digitale Souveränität ist kein Zustand, den man einmal erreicht und dann abhaken kann. Sie ist ein kontinuierlicher Gestaltungsauftrag für Organisationen, für Technologieentscheider, für die Politik. Denn mit jeder neuen Technologie, mit jeder Plattform, jedem Dienst entstehen neue Chancen, aber auch neue Abhängigkeiten.

In diesem Papier zeigen wir, dass nicht die Nutzung von Cloud- oder KI-Technologie das Problem ist, sondern die **unreflektierte, unvorbereitete, ungesteuerte Nutzung** – sie macht Organisationen verwundbar und langfristig steuerungsunfähig.

Die gute Nachricht: Digitale Souveränität lässt sich **bewusst gestalten**. Durch Transparenz über Risiken. Durch gezielte Maßnahmen zur Reduktion kritischer

Abhängigkeiten. Und durch strategische Entscheidungen, die Vielfalt ermöglichen und gleichzeitig Effizienz sicherstellen.

Der Schlüssel liegt in einem **risikobasierten Vorgehen:**
Organisationen müssen bewerten, welche Systeme und Prozesse besonders schutzwürdig sind und wo Souveränitätsrisiken real drohen. Diese Bewertung lässt sich mit bestehenden Risikomanagementprozessen verzahnen und erlaubt eine gezielte Priorisierung von Maßnahmen.

Die in diesem Papier vorgestellten Handlungsfelder bieten dafür konkrete Ansatzpunkte:

- **Kompetenzaufbau** für technologische Vielfalt,
- **Plattform-Engineering** für effiziente Integration von Alternativen,
- **Innovations- und Investitionsfreude**,
- **Exit-Strategien** als echte Option statt Papiertiger,
- **Verankerung in Governance-Zielen**, die Handlungsfähigkeit zum Entscheidungskriterium macht, und
- **Stärkung wettbewerbsfähiger Alternativen** für langfristigen wirtschaftlichen Erfolg.

Jetzt handeln – bevor externe Störungen die Kontrolle entziehen

Die vergangenen Jahre haben gezeigt, wie schnell sich Rahmenbedingungen ändern können: Geopolitische Konflikte, Handelsbeschränkungen, regulatorische Verschärfungen, abrupte Preisänderungen oder Serviceeinschränkungen – all das ist keine Science-Fiction, sondern gelebte Realität.

Organisationen, die auf solche Szenarien nicht vorbereitet sind, verlieren im entscheidenden Moment ihre Handlungsfähigkeit. Denn wer keine echten Alternativen kennt, kann im Zweifel nicht wählen.

Deshalb ist jetzt der Moment zu handeln.
Nicht aus Angst, sondern aus Weitsicht.
Nicht gegen eine bestimmte Technologie, sondern für nachhaltige Entscheidungsfreiheit.

Digitale Souveränität entsteht nicht durch das Ignorieren von Risiken, sondern durch die aktive Gestaltung von Optionen. Sie ist die Voraussetzung dafür, dass Innovation kein Glücksspiel, sondern eine souveräne Entscheidung bleibt. Denn Organisationen, die ihre technologische Zukunft aktiv gestalten, sind schneller, resilienter und freier.

Dieses Papier liefert den Bauplan.
Die Umsetzung liegt bei den Organisationen selbst.
Und sie beginnt mit einer einfachen Frage:

»Wie frei sind wir wirklich, und was tun wir, um es zu bleiben?«

8 Epilog: Die Fictura Mittelstand GmbH hat gehandelt.

Ein halbes Jahr später bei Fictura Mittelstand: Die Cloud-Nutzung wurde nicht gestoppt, sondern bewusst gestaltet. Statt »alles oder nichts« setzt das Unternehmen heute auf eine modulare Plattformstrategie. Das ERP-System läuft zunächst weiter on-premises, die KI-Analysen finden auf einer offenen Plattform mit klar definierten Exit-Optionen statt. Für Webentwicklung oder IoT-Anwendungen wurden eigene Plattformen eingerichtet, die den Nutzern fertige, kuratierte Services bereitstellen.

Ein kleines, aber entscheidendes Team wurde geschult, souveräne Architekturen aufzusetzen und zu betreiben. Offene Standards und portable Datenformate sind verbindlicher Bestandteil neuer Projekte. Der Einkauf prüft neue Services nicht nur auf den Preis, sondern auch auf einen Katalog von Kriterien zur Souveränität. Die Risiken wurden erhoben, bewertet, in das unternehmerische Risikomanagement integriert und passende Maßnahmen priorisiert.

Das Ergebnis? Keine völlige Unabhängigkeit – aber kluge Vielfalt. Die Fictura Mittelstand GmbH ist souveräner als zuvor.

Und sie weiß: Es ist ein fortlaufender Weg. Aber sie hat ihn begonnen.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Marvin Pawelczyk | Referent Künstliche Intelligenz & Cloud
T 030 27576-108 | m.pawelczyk@bitkom.org

Lucy Czachowski | Bereichsleiterin für KI & Cloud Resilienz und Infrastruktur
T 030 27576-320 | l.czachowski@bitkom.org

Verantwortliches Bitkom-Gremium
AK Cloud Services & Digital Ecosystems

bitkom.org