

| Digitale Souveränität

AUSGABE 2
Cloud Computing





Digitale Souveränität

Herausgeber

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

Verantwortlich

Patrik Maeyer
Leiter Betriebswirtschaft, Prozesse und IT
Tel.: +49 30 2020–5452
E-Mail: p.maeyer@gdv.de

Autoren

Florian Baltruschat
Fabian Otto (BELTIOS)
Manuel Audi (BELTIOS)
Patrik Maeyer

Publikationsassistentz

Heike Borchardt, Nadine Luther

Redaktionsschluss dieser Ausgabe

07.07.2025

Bildnachweis

Titelbild - unsplash | Bahadr

Disclaimer

Die Analyse stellt eine allgemeine, unverbindliche Information dar. Die Inhalte wurden mit der erforderlichen Sorgfalt erstellt. Gleichwohl besteht keine Gewährleistung auf Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der darin enthaltenen Angaben oder Einschätzungen. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.

Inhalt

Vorwort	04
1. Cloud-Optionen für einen erhöhten Souveränitätsbedarf	05
2. Management digitaler Souveränität in der Cloud	07
3. Cloud-Strategien im Zeichen der Geopolitik	08
Szenario 1: Schnelle Erholung	08
Szenario 2: Konstante Unsicherheit.....	08
Szenario 3: Verschärfung.....	08
Entscheidungsbaum zur Feststellung eines erweiterten Souveränitätsbe- darfs	08
4. Fazit	11
Über die Autoren	12

Vorwort

In der laufenden Transformation zeigt sich die IT-Landschaft vieler Versicherer in Teilen noch als heterogenes Gefüge. In den kommenden Jahren wird sich das Bild spürbar verändern: Der Anteil an Cloud-Services wird deutlich steigen und der zentrale Mainframe weitgehend abgelöst, beziehungsweise als ein Baustein einer hybriden IT-Architektur bestehen bleiben.

In einer volatilen geopolitischen Lage – geprägt durch militärische Auseinandersetzungen, zunehmend protektionistische Märkte und technologische Machtkonzentrationen – müssen Cloud-Strategien laufend bewertet und gegebenenfalls angepasst werden. Es gilt, den bestmöglichen Weg zwischen Innovationskraft und Risikominimierung zu finden. Hierbei stellt sich auch die Frage: Welche Lösung sichert langfristig die digitale Handlungsfreiheit?

Dazu widmet sich die zweite Ausgabe der Studie gezielt dem Spannungsfeld zwischen Cloud Computing und digitaler Souveränität. Sie liefert konkrete Handlungsoptionen und Entscheidungshilfen, angefangen von der systematischen Bewertung von Cloud-Alternativen, über die Entwicklung eigener Souveränitätsstrategien entlang eines Reifegradmodells bis hin zur Einordnung geopolitischer Szenarien. Ziel ist es, IT-Verantwortliche in die Lage zu versetzen, Cloud-Infrastrukturen nicht nur sicher und leistungsfähig, sondern auch resilient und zukunftssicher zu gestalten.

1. Cloud-Optionen für einen erhöhten Souveränitätsbedarf

Cloud Computing ist eine zentrale technologische Grundlage für die fortschreitende digitale Transformation. Initiativen zur Modernisierung der Systemlandschaften, zur Nutzung von Potenzialthemen wie Künstlicher Intelligenz und zur Steigerung der organisatorischen Agilität basieren heute maßgeblich auf Cloud-Technologien. Dabei bilden

- etablierte Cloud-Betriebsmodelle: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS),
- Deployment-Modelle (Public Cloud, Private Cloud und Hybrid Cloud) sowie
- Cloud-Kategorien (Hyperscaler Cloud, Souveräne Cloud, EU Cloud und Offene Cloud)

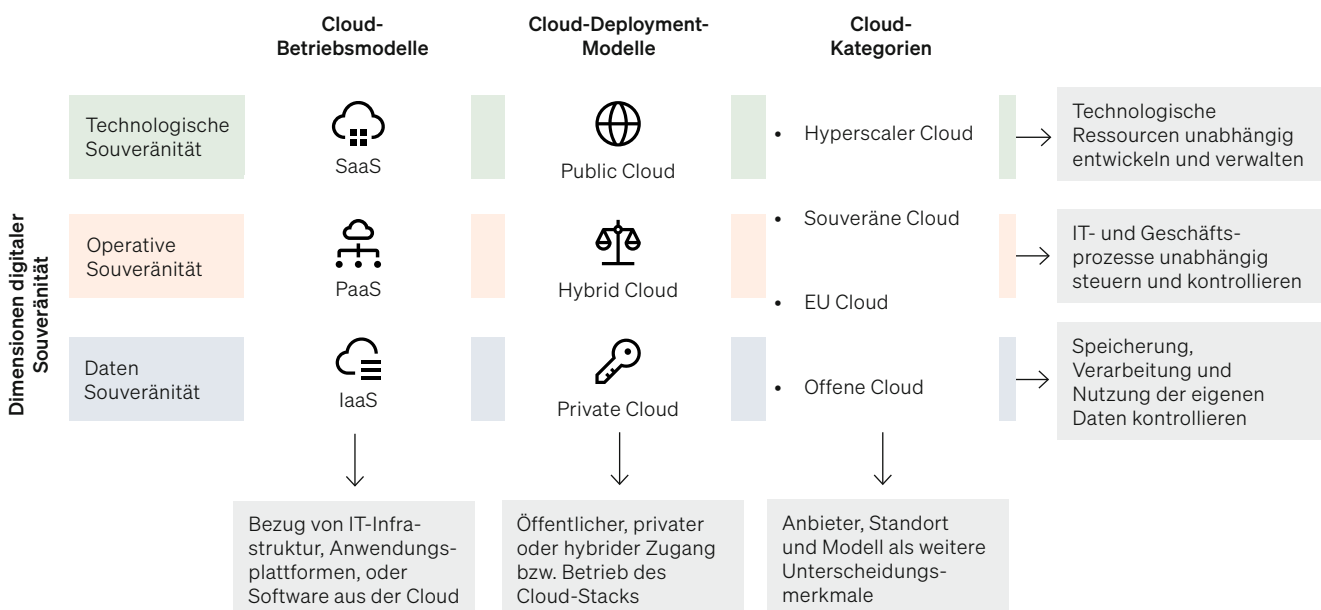
die vorherrschenden Bausteine für aktuelle IT-Strategien und -Architekturen (vgl. Abbildung 1).

Während die Auswahl der passenden IT-Infrastruktur lange Zeit primär von Kosten-Nutzen-Erwägungen geprägt war, rücken zunehmend Aspekte der digitalen Souveränität in den Fokus. Die im Weiteren beschriebenen geopolitischen Entwicklungen und eine damit einhergehende, kritischere Bewertung von Abhängigkeiten gegenüber globalen Anbietern, verstärken diese Tendenz (vgl. Kapitel 3). Die Fähigkeit zur selbstbestimmten Gestaltung der eigenen digitalen Prozesse und Datenverarbeitung gewinnt somit an Bedeutung.

Aus Sicht eines Versicherers stellt sich insbesondere die Frage nach der Auswahl des geeigneten Cloud-Anbieters – für den Start der eigenen Cloud-Journey oder für die Ergänzung des bestehenden Cloud-Setups in Form einer Hybrid-/ Multi-Cloud-Strategie. Zur Beantwortung dieser Frage erfolgt zunächst eine Einordnung der prototypischen Cloud-Kategorien auf der Makro-Ebene (vgl. Abbildung 2). Die Cloud-Kategorien umfassen

Cloud Computing und digitale Souveränität

Abbildung 1 · Übersicht der vorherrschenden Bausteine für Cloud-Strategien



Hyperscaler Clouds, Souveräne Clouds, Europäische Clouds und Offene Clouds. Diese werden anhand von zwei zentralen Dimensionen bewertet. Auf der einen Seite steht die Leistungsfähigkeit der Cloud, gemessen am Funktionsumfang und deren Skalierbarkeit. Dem gegenüber befinden sich die Kontrollmöglichkeiten mit den Ausprägungen „mehr Abhängigkeiten“ und „mehr Autarkie“.

In der Wechselwirkung beider Dimensionen ergibt sich ein Trade-Off: eine hohe Leistungsfähigkeit geht mit stärkeren Abhängigkeiten einher. Verdeutlicht wird dies durch die Kategorie der **Hyperscaler Clouds**, die diesem Bereich zuzurechnen ist. Hierbei handelt es sich um Public-Cloud-Angebote globaler Anbieter. Dank ihrer globalen Infrastruktur, weitreichenden Automatisierung und Standardisierung sowie Skalierbarkeit zeichnen sich diese durch eine hohe Leistungsfähigkeit aus. Dem gegenüber stehen jedoch auch Abhängigkeiten, z. B. in Form von Vendor-Lock-In-Effekten.

Einen Zwischenweg können hingegen Souveräne Clouds gefolgt von Europäischen Clouds bilden. **Souveräne Clouds** umfassen einerseits Cloud-Angebote mit erweitertem Datenschutz, der beispielsweise durch Transparenz, Datenhoheit und Kontrollierbarkeit, Offenheit und Vorhersehbarkeit erzielt werden soll. Andererseits umschließt die Kategorie der souveränen Clouds auch Hyperscaler mit hoher Überlebensfähigkeit ("Survivability"). Diese Cloud-Angebote sind resilienter gegenüber globalen Betriebsabhängigkeiten

und können daher in Krisensituationen zumindest zeitweise ohne externe Unterstützung weiter betrieben werden.

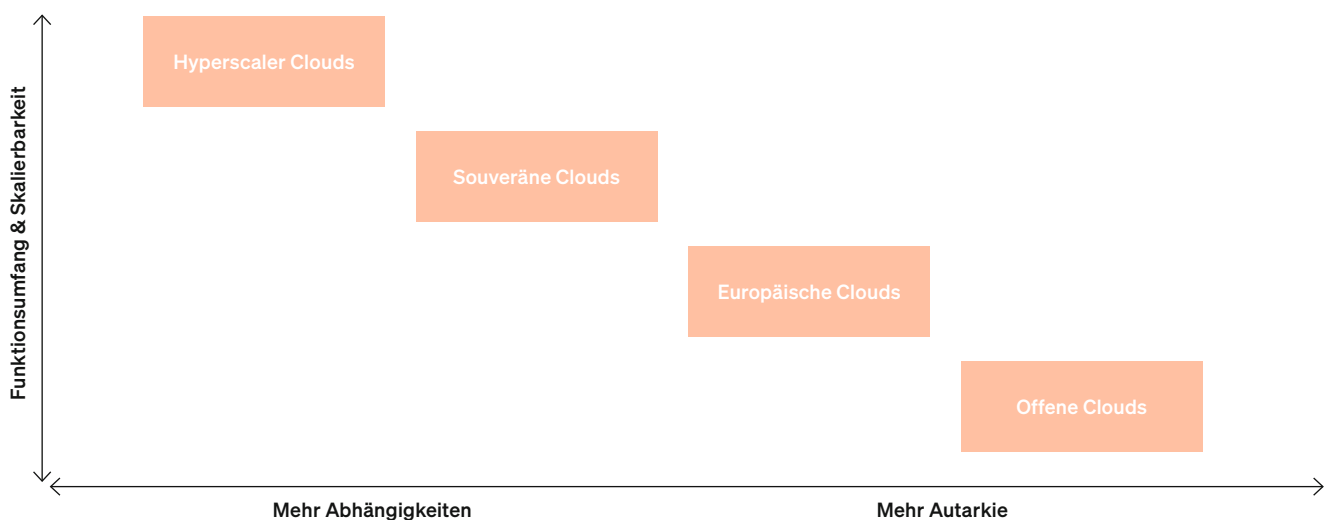
Noch einen Schritt weiter gehen **Europäische Clouds**. Die Lokalisierung steht hier im Vordergrund, um mehr Kontrollmöglichkeiten zu gewährleisten. Europäische Clouds werden daher häufig von EU-Unternehmen betrieben und nutzen europäische Software-Technologie bzw. eigene Implementierungen von Open-Source-Software. Die ex-ante Beschränkung auf europäische Lösungen hat jedoch Abstriche bei der globalen Skalierbarkeit und Verfügbarkeit zur Folge.

Schlussendlich bilden **Offene Clouds** das am stärksten auf Autarkie bzw. Unabhängigkeit ausgerichtete Angebot. Erreicht wird dies durch den überwiegenden Einsatz von Open-Source-Software sowie offenen Standards.

In der Praxis sind die Übergänge zwischen den verschiedenen Cloud-Kategorien fließend. Auch gibt es kein einheitliches Begriffsverständnis, sodass es unterschiedliche Auslegungen einer souveränen Cloud geben kann. In diesem Sinne erfolgt die Einordnung der Cloud-Kategorien prinzipienbasiert (vgl. Abbildung 2). Ergänzend zu den hier dargestellten Überlegungen ist außerdem zu berücksichtigen, dass sich bei allen vier Cloud-Kategorien unvermeidbare Abhängigkeiten ergeben können, z. B. im Bereich der IT-Hardware.

Einordnung verschiedener Cloud-Kategorien

Abbildung 2 · Leistung und Kontrolle als zentrale Dimensionen



Quelle: GDV & BELTIOS

2. Management digitaler Souveränität in der Cloud

Um die eigene digitale Souveränität in der Cloud zu steigern, ist es notwendig, mit einer Bestandsaufnahme zu beginnen. Hierfür kann nachfolgendes Steuerungsinstrument dienen, das Hilfestellung bei der Einordnung entlang der drei Säulen digitaler Souveränität sowie den Kompetenzen zur Umsetzung digitaler Souveränität gibt (vgl. Abbildung 3). Der geltende Rechtsrahmen, der ein wesentlicher Teil digitaler Souveränität ist, wird in diesem Instrument bewusst nicht explizit behandelt, da die bestehende Regulatorik i.d.R. an anderer Stelle im Unternehmen umgesetzt wird. Die nachfolgende Abbildung zeigt das Framework im Überblick.

Ausgehend vom übergeordneten Rechtsrahmen greift das Framework die drei Säulen digitaler Souveränität auf, die bereits im ersten Teil der Studie eingeführt wurden. Beginnend mit der technologischen Souveränität, über die operative Souveränität bis hin zur Daten-Souveränität werden konkrete Erfolgsfaktoren identifiziert, die zur Bewertung bzw. Erfüllung der Souveränität

herangezogen werden können. Nicht außer Acht gelassen werden sollten die digitalen Kompetenzen der Beschäftigten, Partner und Kunden. Sie bilden daher das Fundament des Frameworks und sind somit Ausgangspunkt aller weiteren Bewertungen. Je Säule sowie für die Kompetenzen gibt es Fragestellungen, die zur Selbsteinschätzung gedacht sind. Auf einer Skala von niedrig bis hoch kann eine Aufnahme der im Unternehmen bestehenden Reifegrade erfolgen. Strategische Handlungsempfehlungen schließen sich entsprechend an, sodass das Werkzeug auch die Grundlage zur Steigerung der digitalen Souveränität in der Cloud bildet.

Zur praxisnahen Verwendung empfiehlt sich die Online-Ressource, in der wir das Framework detailliert beschreiben und auf jeden genannten Aspekt eingehen: <https://www.msg.group/digitale-souveraenitaet/framework>



Framework zur Bestimmung der eigenen digitalen Souveränität

Abbildung 3 · Souveränität als mehrdimensionales Konzept



3. Cloud-Strategien im Zeichen der Geopolitik

Die Cloud-Strategie ist den direkten Einflüssen globaler politischer und wirtschaftlicher Entwicklungen ausgesetzt. Gerade geopolitische Verschiebungen und Unsicherheiten unterstreichen die Notwendigkeit eines resilienten Umfeldes. Unvermeidbare Abhängigkeiten wirken als wesentlicher Treiber für das verstärkte Streben nach digitaler Souveränität beispielsweise in Bezug auf Kostenstrukturen, Innovationskraft und strategische Handlungsoptionen.

Bislang handelte es sich bei der digitalen Souveränität um ein eher abstraktes Ziel, dessen betriebswirtschaftliche Begründung schwer herleitbar war. Dies ändert sich nun. Um die potenziellen Auswirkungen dieser komplexen Zusammenhänge greifbar zu machen und strategische Handlungsimpulse zu geben, skizziert dieses Kapitel drei mögliche Zukunftsszenarien und deren Konsequenzen sowie Handlungsoptionen für die Cloud-Strategien.

Szenario 1: Schnelle Erholung

In einem Szenario schneller Erholung stabilisieren sich die handelspolitischen Rahmenbedingungen rasch. Für Unternehmen geht dies mit einer Reduktion der externen Risiken einher. Cloud Computing kann im vollen Umfang genutzt werden und sich auf Aspekte wie Leistungsfähigkeit, Skalierbarkeit und Innovationspotenziale fokussieren. Die Cloud-Strategien und Provider-Auswahl sollten dennoch evaluiert werden, um für zukünftige Spannungen strategisch vorbereitet zu sein. Dies inkludiert die Schaffung von Transparenz und die bewusste Bewertung der bestehenden Abhängigkeiten von einzelnen Technologien und Anbietern. Erfahrungen aus der vorangegangenen Phase sollten dokumentiert und strategisch verankert werden.

Szenario 2: Konstante Unsicherheit

In einem Szenario konstanter Unsicherheit bleibt das geopolitische Umfeld angespannt, was zu Planungsunsicherheiten bei der Nutzung von Cloud-Diensten

führt. Um diesen Herausforderungen zu begegnen, ist es wichtig, die IT- und Cloud-Strategien anzupassen und die Resilienz zu stärken. Dazu gehört die strategische Einbindung alternativer Cloud-Lösungen, um Abhängigkeiten zu reduzieren und die Betriebsfähigkeit zu stärken. Ein Ansatz kann bspw. in Form einer Multi-Cloud-Strategie bestehen. Eine kontinuierliche Beobachtung der geopolitischen und regulatorischen Entwicklungen sowie eine flexible Cloud-Governance sind entscheidend, um auf Veränderungen schnell reagieren zu können.

Szenario 3: Verschärfung

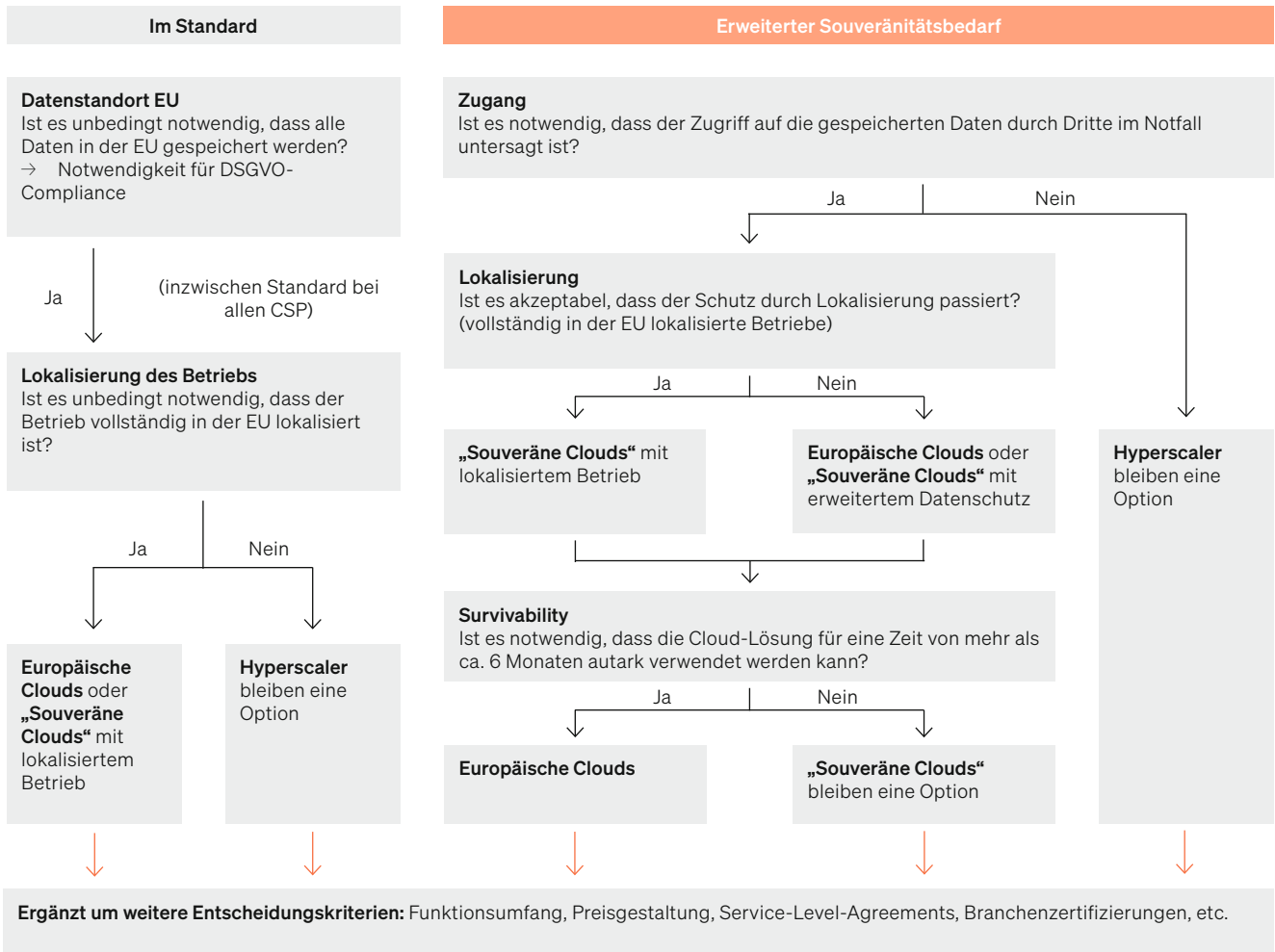
Eine weitere Verschärfung des geopolitischen Umfelds bis hin zu Black-Swan-Ereignissen würde eine grundsätzliche Neubewertung der Handlungsoptionen erforderlich machen. Unternehmen, die Cloud-Dienste nutzen, müssen sich insbesondere mit der Frage befassen, ob die Cloud-Dienste weiter uneingeschränkt zur Verfügung stehen werden oder ob kurzfristiger Handlungsbedarf entstehen könnte. Um flexibel zu bleiben, ist es sinnvoll, frühzeitig alternative Cloud-Lösungen und Strategien zur Anpassung zu prüfen. Die praktische Umsetzung von Veränderungen erfordert eine gute Vorbereitung und abgestimmte Prozesse.

Entscheidungsbaum zur Feststellung eines erweiterten Souveränitätsbedarfs

Reichen die Standard-Angebote im Hinblick auf die Souveränitätsanforderungen nicht aus, um die aus Unternehmenssicht definierten Ziele zu erfüllen, fällt der Blick auf mögliche Alternativen in Form von souveränen Cloud-Lösungen. Zur Orientierung und praxisnahen Hilfestellung in diesem komplexen Umfeld kann der nachfolgende Entscheidungsbaum dienen. Er zielt darauf ab, das vielfältige Angebot unterschiedlicher Cloud-Lösungen anhand weniger, aber zentraler Dimensionen der digitalen Souveränität zu strukturieren und vergleichbar zu machen.

Entscheidungsbaum zur Auswahl von Cloud-Alternativen

Abbildung 4 · Feststellung eines erweiterten Souveränitätsbedarfs



Quelle: GDV & BELTIOS

Es ist zu betonen, dass sich Cloud-Lösungen in zahlreichen weiteren Aspekten (u. a. Funktionsumfang, Preisgestaltung, Service-Level-Agreements, Branchenzertifizierungen) unterscheiden; der Fokus des Entscheidungsbaums liegt jedoch bewusst auf den kritischen Souveränitätsanforderungen. Das Modell basiert zudem teilweise auf Einschätzungen, insbesondere zur langfristigen Funktionsfähigkeit ohne Updates.

Der vorgestellte Entscheidungsbaum dient als Orientierungshilfe, um die komplexe Auswahl von Cloud-Alternativen auf drei kritische Souveränitätsdimensionen zu fokussieren:

- Schutz vor Zugriff durch Dritte
- Lokalisierung
- Überlebensfähigkeit ("Survivability")

Die Wahl des geeigneten Pfades und der daraus resultierenden Cloud-Lösung hängt maßgeblich von der individuellen Risikobewertung, den spezifischen Schutzbedürfnissen der jeweiligen Cloud-Anwendungsfälle und der strategischen Risikobereitschaft des einzelnen Unternehmens ab.

Schritt 1: Der Entscheidungsprozess zur Feststellung eines erweiterten Souveränitätsbedarfs beginnt mit einer zentralen Frage zum Schutz vor Zugriff durch Dritte: Ist es für den betrachteten Cloud-Anwendungsfall bzw. die verarbeiteten Daten notwendig, dass selbst im Notfall ein Zugriff durch Dritte in jedem Fall ausgeschlossen ist?

→ Wird diese Frage mit „Nein“ beantwortet, kann das gesamte Spektrum der zur Verfügung stehenden Cloud-Angebote in Betracht gezogen werden,

inkl. standardisierter Public-Cloud-Angebote von Hyperscalern.

- Wird diese Frage hingegen mit „Ja“ beantwortet, öffnet sich der Pfad zu weiteren Abwägungen bezüglich der Lokalisierung und Überlebensfähigkeit.

Schritt 2: Im nächsten Schritt beschäftigt sich der Entscheidungsbaum mit der Frage, ob die Lokalisierung des Cloud-Betriebs bspw. innerhalb der EU bereits eine ausreichende Maßnahme zur Erfüllung des erweiterten Souveränitätsbedarfs ist.

- Wird dieser Mechanismus als nicht ausreichend bewertet („Nein“), verweist der Baum zunächst auf eine breitere Kategorie von Lösungen: Europäische Clouds oder Souveräne Clouds mit erweitertem Datenschutz.
- Wird dieser Mechanismus hingegen als ausreichend erachtet („Ja“), um die notwendige Survivability im Krisenfall zu gewährleisten, verweist der Baum auf Souveräne Clouds mit lokalisiertem Betrieb.

Schritt 3: Schlussendlich muss die Notwendigkeit einer technologischen Unabhängigkeit bewertet werden: Ist es erforderlich, dass die gewählte Cloud-Lösung für einen Zeitraum von mehr als sechs Monaten ohne essenzielle Updates (wie Sicherheits-Patches oder kritische Funktions-Updates) stabil und sicher weiterbetrieben werden kann? Die Antwort auf die Frage der langfristigen Update-Unabhängigkeit führt zur finalen Differenzierung der geeigneten Cloud-Kategorien:

- Wird die Notwendigkeit einer Funktionsdauer von über sechs Monaten ohne Updates mit „Nein“ beantwortet (oder kann dieses Risiko für den Anwendungsfall akzeptiert werden), bleiben Souveräne Clouds (als allgemeine Kategorie, die auch spezielle Angebote von Providern umfassen kann, welche ggf. nicht die >6-Monate-Unabhängigkeit garantieren) eine valide Option.
- Ist diese langfristige technologische Unabhängigkeit von Updates jedoch unbedingt erforderlich („Ja“), um beispielsweise auch in einem langanhaltenden Krisenszenario den Betrieb und die Sicherheit zu gewährleisten, führt der Entscheidungspfad zu rein europäischen Clouds.

4. Fazit

Unternehmen müssen ihre Cloud-Strategien differenziert gestalten – abhängig vom eigenen Reifegrad, regulatorischen Anforderungen und der Bedeutung der Daten und der Cloud-Anwendungsfälle. Europäische und souveräne Cloud-Alternativen bieten dabei konkrete Handlungsoptionen für mehr Kontrolle und Krisenfestigkeit. Entscheidend ist, die Grundlagen frühzeitig schaffen.

Digitale Souveränität sollte als ein kontinuierlicher Gestaltungsprozess verstanden werden. Unternehmen müssen nicht nur technologische und regulatorische Aspekte sondern auch organisatorische Kompetenzen, Governance-Strukturen und kulturelle Voraussetzungen berücksichtigen.

Das vorgestellte Framework bietet eine Grundlage, um die jeweilige Ausgangslage zu bewerten und gezielte Maßnahmen zur Stärkung der Souveränität abzuleiten. Gleichzeitig macht der Entscheidungsbaum deutlich, wie wichtig es ist, Cloud-Alternativen entlang zentraler Souveränitätsdimensionen zu bewerten.

Wer seine Cloud-Strategie heute bewusst gestaltet, kann nicht nur geopolitischen Krisen besser begegnen, sondern stärkt auch Innovationskraft und Wettbewerbsfähigkeit. Digitale Souveränität wird damit zum Hebel für nachhaltigen Unternehmenserfolg im digitalen Zeitalter.

ÜBER DIE AUTOREN

Autoren

Patrik Maeyer

Leiter Betriebswirtschaft, Prozesse und IT

p.maeyer@gdv.de

Dr. Manuel Audi

Geschäftsführer BELTIOS & Leiter Business

Consulting Insurance

manuel.audi@beltios.com

Florian Baltruschat

Referent Betriebswirtschaft, Prozesse und IT

f.baltruschat@gdv.de

Fabian Otto

Principal BELTIOS, Business Consulting Insurance

fabian.otto@beltios.com

GDV

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in Berlin ist die Dachorganisation der Versicherer in Deutschland. Gegenüber Parlament, Regierung und Öffentlichkeit – national wie auf europäischer Ebene – vertreten wir die Interessen der Branche.

BELTIOS

Die BELTIOS GmbH ist eine spezialisierte Unternehmensberatung für die Versicherungs- und Finanzdienstleistungsbranche und Teil des Beratungsnetzwerks msg advisors. Als kompetenter Ansprechpartner für Fach- und IT-Abteilungen sowie das Management unterstützt BELTIOS Unternehmen in Transformationsprozessen und beim Aufbau digitaler Ökosysteme. Die rund 80 Mitarbeiter vereinen fundierte versicherungsmathematische, -fachliche und -technische Expertise.

Mehr Informationen zu digitaler Souveränität finden Sie online:

<https://advisors.msg.group/digitale-souveraenitaet/>



Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin

Besuchereingang: Leipziger Straße 121

Postfach 08 02 64, 10002 Berlin

Tel.: +49 30 2020-5000, Fax: +49 30 2020-6000

www.gdv.de, berlin@gdv.de