

Souveränität ist nicht mehr optional

Digitale Souveränität als strategischen Hebel für Vertrauen, Resilienz und Wettbewerbsvorteile nutzen



C-Level-Briefing

Kritische Abhängigkeiten managen: Jetzt eine Pflicht für das Board!

Digitale Souveränität steht ganz oben auf der Agenda von Vorständen und Führungsteams. Geopolitische Fragmentierung, zunehmende Regulierung, extraterritoriale Zugangsgesetze und die Konzentration kritischer digitaler Fähigkeiten auf eine kleine Anzahl globaler Anbieter verändern die technologische Risikolandschaft. Die Einführung von KI beschleunigt diesen Wandel. Datensensibilität, automatisierte Entscheidungsfindung und die Abhängigkeit von komplexen digitalen Lieferketten erhöhen die operative und strategische Exposition.

Organisationen müssen daher die Kontrolle über kritische Daten, Systeme und digitale Abläufe behalten und gleichzeitig Innovationen weltweit skalieren. Cybersecurity ist dafür zentral: Sie ist die Voraussetzung für digitale Souveränität. Souveräne Zielsetzungen werden erst dann wirksam, wenn Kontrollen implementiert, überwacht und im Betrieb über Identitäten, Privilegien und Verschlüsselung hinweg nachweisbar gemacht werden.



Die folgenden Do's & Don'ts setzen eine klare Orientierung für Organisationen, die digitale Souveränität von einem erklärten Ziel in etwas verwandeln wollen, das sie entwerfen, betreiben und nachweisen können.

Do's

- ✓ Mit der Geschäftskritikalität beginnen
- ✓ Digitale Souveränität Workload für Workload umsetzen
- ✓ Cybersecurity als Grundlage etablieren
 - Identitäten, Berechtigungen, kryptografische Schlüssel und Betriebsabläufe absichern
- ✓ Digitale Souveränität über den gesamten Technologie-Stack hinweg gewährleisten
- ✓ Eine einheitliche, umgebungsübergreifende Kontroll- und Steuerungsebene schaffen
- ✓ Zielkonflikte und Abwägungen transparent machen
- ✓ Wahlfreiheit durch offene Standards und Portabilität sicherstellen
- ✓ Leitplanken für digitale Souveränität auf KI-Agenten ausweiten
- ✓ Digitale Souveränität als Managed Sovereignty etablieren und ihren Nachweis kontinuierlich im laufenden Betrieb erbringen

Don'ts

- ✗ Nicht überall dasselbe Maß an digitaler Souveränität anwenden
- ✗ Digitale Souveränität nicht auf Cloud, Anbieter oder Zertifizierungen reduzieren
- ✗ Dokumentierte Compliance nicht mit tatsächlicher Kontrolle verwechseln
- ✗ Nicht davon ausgehen, dass Datenresidenz allein das Problem löst
- ✗ Nicht nur eine Ebene optimieren und die übrigen vernachlässigen
- ✗ Nicht zulassen, dass jede Plattform zu einer isolierten Souveränitätsinsel wird
- ✗ Nicht davon ausgehen, dass maximale Kontrolle ohne Kosten, Reibungsverluste oder Auswirkungen auf die Time-to-Market erreichbar ist
- ✗ Keine unumkehrbaren Herstellerabhängigkeiten (Vendor Lock-in) schaffen
- ✗ Autonome Systeme nicht ohne Richtlinien, Protokollierung, Eskalationsmechanismen und Kill-Switch-Funktion über Workflows hinweg agieren lassen
- ✗ Digitale Souveränität nicht bereits mit Vertragsabschluss, Zertifizierung oder abgeschlossener Migration als erreicht betrachten

Atos Definition der digitalen Souveränität

Digitale Souveränität ist die Fähigkeit einer Organisation, die Kontrolle, Entscheidungshoheit und Verantwortung über ihre Daten, Infrastruktur, Anwendungen und digitalen Betriebsabläufe zu behalten und gleichzeitig kritische Abhängigkeiten sowie Risiken durch externe Rechtsräume, Anbieter oder Technologien kontinuierlich zu steuern und zu beherrschen.

Kontext

Digitale Souveränität ist seit Jahren ein wiederkehrendes Thema. Je nach politischer Lage, regulatorischen Entwicklungen oder bedeutenden Sicherheitsvorfällen rückte sie mal stärker, mal weniger stark in den Fokus der Unternehmensführung. In Phasen relativer Stabilität wurde sie häufig als politisches oder regulatorisches Thema betrachtet oder als Spezialanforderung für Behörden, Verteidigungseinrichtungen und stark regulierte Branchen eingeordnet.

Diese Sichtweise hat sich grundlegend geändert. Digitale Souveränität ist heute zu einer strategischen Kernanforderung geworden.

Geopolitische Spannungen, eine zunehmende regulatorische Verdichtung, extraterritoriale Rechtsvorschriften sowie die Konzentration kritischer digitaler Fähigkeiten auf wenige globale Technologieanbieter haben die Risikolandschaft nachhaltig verändert. Hinzu kommt, dass steigende Lizenz- und Plattformkosten die Abhängigkeit von einzelnen Anbietern verstärken und langfristige finanzielle Bindungen schaffen, die sich nur schwer wieder auflösen lassen.

Parallel dazu beschleunigt der rasante Einsatz Künstlicher Intelligenz diese Entwicklung zusätzlich. Sensible Daten, automatisierte Entscheidungen und komplexe digitale Lieferketten erhöhen die operativen, finanziellen und strategischen Folgen eines möglichen Kontrollverlusts erheblich.



Zusammen haben diese Kräfte die Souveränität von einer kontextuellen Überlegung zu einer strukturellen Angelegenheit für Unternehmen und Institutionen gleichermaßen gemacht. Das Tempo und die Priorität variieren je nach Geografie und Sektor, aber die Richtung ist beständig: Organisationen stärken ihre Souveränitätsposition zunehmend als Reaktion auf sich wandelnde Risikobewertungen.

Ein überwiegender Anteil der CxOs bettet inzwischen einen Souveränitätsansatz in ihrem IT-Stack ein.

IDC schätzt, dass

84%¹

der Unternehmen, die Cloud-Technologien einsetzen, derzeit bereits souveräne Cloud-Lösungen nutzen oder deren Einsatz planen, und Gartner geht davon aus, dass

50%

aller Unternehmen eine Strategie zur digitalen Souveränität bis 2029 implementiert haben wird - gegenüber lediglich 10% heute.²

Digitale Souveränität entwickelt sich damit zu einer strategischen Kernkompetenz. Sie ermöglicht Organisationen kritische digitale Abhängigkeiten aktiv zu steuern, architektonische Wahlfreiheit zu erhalten, die Kontrolle über Daten, Technologien und Betriebsprozesse dauerhaft zu sichern.

Atos bringt in diese Diskussion jahrzehntelange Erfahrung beim Betrieb hochkritischer, regulierter und souveräner IT-Umgebungen ein. Seit vielen Jahren entwickelt, implementiert und betreibt das Unternehmen Systeme, in denen Kontrolle, Sicherheit und Resilienz unverzichtbare Voraussetzungen sind. Diese Erfahrung bildet die Grundlage für einen praxisorientierten Ansatz zur digitalen Souveränität, der auf klaren Überzeugungen und operativer Erfahrung basiert.

1. Geschäftskritisch und nicht mehr optional

Wir sind überzeugt, dass digitale Souveränität nun fest auf Ihrer Agenda für 2026 steht. Die Gründe hierfür sind vielfältig: geopolitische Entwicklungen, neue regulatorische Anforderungen, Maßnahmen zur Risikominimierung nach Krisen, zunehmende Abhängigkeiten von einzelnen Technologieanbietern, sowie die Erkenntnis, dass digitale Souveränität ein strategischer Hebel für Wachstum und Differenzierung sein kann.

Unternehmen stehen heute gleichzeitig unter unterschiedlichsten Souveränitätsanforderungen. Sie müssen ihre Geschäftskontinuität auch unter außergewöhnlichen Bedingungen sicherstellen, sensible Daten und geistiges Eigentum schützen, strengere regulatorische Vorgaben erfüllen, Erwartungen von Kunden, Investoren und Behörden erfüllen, sowie Reputationsrisiken

in einer zunehmend kritisch beobachteten digitalen Welt beherrschen.

Digitale Souveränität dient jedoch nicht ausschließlich der Risikominimierung. **Sie ist auch eine strategische Chance.** Richtig umgesetzt schafft sie Vertrauen, stärkt die Glaubwürdigkeit einer Marke und entwickelt sich zunehmend zu einem echten Wettbewerbsfaktor.

Kunden und Geschäftspartner erwarten immer häufiger, dass Unternehmen nachweisen können, ihre Daten, Systeme und technologischen Abhängigkeiten wirksam zu kontrollieren. Bereits heute stellt digitale Souveränität bei öffentlichen Ausschreibungen vielfach ein entscheidendes Bewertungskriterium dar. Gleichzeitig entwickelt sich der Markt in Richtung

messbarer Anforderungen und überprüfbarer Nachweise.

Stakeholder werden künftig erwarten, dass digitale Souveränität anhand konkreter Kennzahlen belegt werden kann, beispielsweise durch geringere Konzentrationsrisiken, schnellere Reaktionen auf regulatorische Änderungen, höhere Wirksamkeit der implementierten Kontrollen, sowie eine höhere Resilienz geschäftskritischer Workloads.

Digitale Souveränität ermöglicht zudem eine nachhaltige, langfristige digitale Transformation. Indem Sie die Wahlfreiheit bewahren, irreversible Abhängigkeiten begrenzen und geistiges Eigentum schützen, gewinnen Sie die Freiheit zurück, mit Zuversicht zu innovieren, zu verändern und zu transformieren.

Aus all diesen Gründen **ist digitale Souveränität nicht optional**. Sie darf weder als nachgelagerte Überlegung behandelt werden, noch ausschließlich einzelnen Fachbereichen überlassen werden. Vielmehr muss sie zu einem zentralen Bestandteil der digitalen Unternehmensstrategie werden – als strategischer Treiber für Resilienz, Differenzierung und nachhaltiges Wachstum. Gleichzeitig erfordert sie einen unternehmensweiten Ansatz mit abgestuften Kontrollmechanismen auf Daten- und Workload-Ebene.

2. Keine einfachen Antworten – und schon gar keine binären

Die erste Herausforderung der digitalen Souveränität ist es, sie zu definieren. Für die einen bedeutet Souveränität in erster Linie Datenresidenz. Andere verbinden damit nationale Cloud-Anbieter, rechtliche Immunität, operative Autonomie oder Cyberresilienz. Vorstände betrachten das Thema vor allem unter dem Gesichtspunkt von Risiko und Verantwortung. IT-Architekten übersetzen es in Architekturentscheidungen. Rechtsabteilungen konzentrieren sich auf Fragen der Jurisdiktion. Security-Teams stellen Zugriffs- und Kontrollmechanismen in den Mittelpunkt, während Einkaufsorganisationen häufig auf Anbieterbezeichnungen und Zertifizierungen achten. Zuständigkeit und rechtliche Absicherung bleiben

häufig unklar, bis sie juristisch geprüft oder gerichtlich geklärt werden. Solche Verfahren sind langwierig, länderspezifisch und bieten selten unmittelbaren operativen Schutz, wenn der Druck steigt. Daher sollten sie nicht als primäre Verteidigungslinie betrachtet werden.

Was Unternehmen hingegen bereits heute aktiv beeinflussen können, sind die konkreten Steuerungsmechanismen innerhalb ihrer digitalen Umgebung – also ihre Daten, ihre Technologien und ihre Betriebsprozesse. Führungskräfte sollten deshalb drei grundlegende Fragen beantworten:

Wo werden meine Daten und Modelle gespeichert und verarbeitet – und wie werden sie verschlüsselt?

Dies ist die sichtbarste Dimension digitaler Souveränität, weil sie unmittelbar die rechtliche Zuständigkeit und mögliche Zugriffsrechte widerspiegelt. Der Speicherort allein reicht jedoch nicht aus. Tatsächliche Kontrolle entsteht erst durch wirksame Sicherheitsmechanismen. Dazu gehören insbesondere souveräne Verschlüsselungskonzepte, bei denen kryptografische Schlüssel im Eigentum und unter der Kontrolle des Unternehmens verbleiben und durch souveräne Schlüsselmanagement-Lösungen sowie Confidential Computing zusätzlich geschützt werden.

Wer kann auf meine Systeme und meine Daten zugreifen, sie betreiben und letztlich kontrollieren?

Diese Frage umfasst zwei Dimensionen. Zum einen müssen Anbieter nachweisen, wie Zugriffe innerhalb ihres Betriebsmodells geregelt sind, insbesondere im Hinblick auf privilegierte Benutzerrollen und grenzüberschreitende Zugriffsmöglichkeiten. Zum anderen müssen Kunden auf den von ihnen verantworteten Ebenen – beispielsweise der Datenebene bei SaaS oder der Anwendungs- und Konfigurationsebene bei PaaS – die tatsächliche Kontrolle behalten.

Digitale Souveränität setzt voraus, dass Zugriffsrechte über Identitäten, Berechtigungen und Betriebsabläufe hinweg eindeutig vergeben und wieder entzogen werden können. Die zugrunde liegenden Kontrollmechanismen müssen technisch durchsetzbar und jederzeit überprüfbar sein.

Wie widerstandsfähig und robust sind meine Technologie und meine Abläufe im Falle von Störungen, Abhängigkeiten oder Eskalationen?

Resilienz, die Aufrechterhaltung des Geschäftsbetriebs und die Fähigkeit, selbst unter außergewöhnlichen Bedingungen handlungsfähig zu bleiben, sind strategisch ebenso wichtig wie der Ort, an dem Daten verarbeitet oder gespeichert werden. Dazu gehört auch, die eigene Entscheidungsfreiheit langfristig zu erhalten: durch glaubwürdige Alternativen zu kritischen Abhängigkeiten, eine möglichst geringe Bindung an einzelne Anbieter oder Plattformen sowie Architekturen auf Basis offener Standards und Open-Source-Komponenten, die einen Weiterbetrieb – gegebenenfalls im eingeschränkten Modus – eine Migration oder eine Rekonfiguration ermöglichen, wenn sich Rahmenbedingungen ändern oder ein Kill Switch aktiviert werden muss.



Die Beantwortung dieser Fragen erfordert, dass Unternehmen einen Schritt zurücktreten und das gesamte Zusammenspiel der Technologien und digitalen Fähigkeiten betrachten, auf denen ihre Geschäftstätigkeit basiert. Die strategische Bedeutung einzelner Workloads unterscheidet sich innerhalb eines Unternehmens erheblich, und nicht jede Ebene des IT-Stacks trägt gleichermaßen zum Souveränitätsrisiko bei. Pauschale Ansätze oder Durchschnittsbetrachtungen greifen daher zu kurz. Digitale Souveränität erfordert eine bewusste und differenzierte Herangehensweise.

Diese Bewertung darf sich nicht auf die technischen Ebenen allein beschränken. Ebenso entscheidend sind die Betriebs- und Bereitstellungsmodelle – etwa Software as a Service (SaaS) – die Lieferketten von Anbietern und Software, Governance-Mechanismen sowie die tatsächliche Durchsetzbarkeit rechtlicher Kontrollmöglichkeiten über verschiedene Rechtsräume hinweg.

Obwohl die zentralen Fragen der digitalen Souveränität häufig auf die Wahl eines Cloud- oder Infrastrukturproviders reduziert werden, greift diese Sichtweise zu kurz. Tatsächlich handelt es sich um ein komplexes und mehrdimensionales Thema. Unternehmen müssen Entscheidungen zur Risikominimierung auf einer sehr granularen Ebene treffen und den jeweiligen Anforderungen entsprechend unterschiedliche Schutz- und Kontrollmechanismen für einzelne Workloads implementieren.

In der Praxis wird digitale Souveränität durch eine Vielzahl technischer und operativer Kontrollpunkte sichergestellt, die tief in den einzelnen Schichten des IT-Stacks und an deren Schnittstellen verankert sind. Dazu gehören unter anderem die Isolation des Datenzugriffs, Verschlüsselung und Eigentum an kryptografischen Schlüsseln, das Management von Identitäten und Berechtigungen, Protokollierung und Auditierbarkeit, regionalisierte Backup- und Wiederherstellungskonzepte, kontrollierte Software-Lieferketten, Einschränkungen des administrativen Zugriffs sowie Resilienzmechanismen gegenüber Abhängigkeiten und Störungen.

Keiner dieser Kontrollmechanismen ist für sich allein ausreichend. Digitale Souveränität entsteht erst durch das Zusammenspiel aller Maßnahmen, ihre konsistente Governance und ihren zuverlässigen Betrieb über die gesamte Lebensdauer der IT-Landschaft hinweg. Dies erfordert grundlegende Architekturprinzipien, die sicherstellen, dass sich die einzelnen Kontrollen gegenseitig ergänzen, anstatt als voneinander isolierte Maßnahmen zu wirken.

Diese Prinzipien müssen über alle Dimensionen der digitalen Souveränität hinweg angewendet werden.



Über den gesamten IT-Stack hinweg

Digitale Souveränität muss von den grundlegenden Infrastrukturebenen – Netzwerke, Cloud- und Infrastrukturplattformen sowie Cybersecurity – bis hin zu den geschäftsnahen Ebenen wie Anwendungen, Endgeräten, Künstlicher Intelligenz und Analytik bewertet und umgesetzt werden. Jede dieser Ebenen bringt eigene Angriffspunkte, Steuerungsmöglichkeiten und Abhängigkeiten mit sich.



Nach Workloads und Anwendungsfällen

Nicht jeder Workload weist dieselbe Sensibilität oder strategische Bedeutung auf. Kernsysteme, geschäftskritische Anwendungen oder besonders sensible Workloads einer Branche können deutlich strengere Anforderungen an die digitale Souveränität stellen als weniger kritische Systeme. Unternehmen müssen daher ihre Risiken und geschäftlichen Prioritäten genau analysieren und die jeweils passenden Leitplanken für den betreffenden Workload definieren.



Nach Geografie und Zuständigkeit

Auch die Anforderungen an die digitale Souveränität unterscheiden sich erheblich zwischen Ländern und Regionen. Ausschlaggebend sind nationale und branchenspezifische Vorschriften, unterschiedliche Rechtsordnungen, geopolitische Rahmenbedingungen sowie die jeweilige Regulierungspraxis. Architekturentscheidungen, Betriebsmodelle und die Auswahl von Partnern müssen deshalb an die jeweiligen lokalen Gegebenheiten angepasst werden, anstatt von weltweit einheitlichen Rahmenbedingungen auszugehen.

Diese Komplexität wird durch eine unvermeidliche Realität noch verstärkt: Souveränität ist mit Investitionen verbunden. Erweiterte Souveränitätskontrollen können mit höheren Kosten, eingeschränktem Zugang zu bestimmten Innovationen und Abwägungen bei der Time-to-Market einhergehen. Diese Trade-offs müssen explizit, bewusst und geschäftsbezogen bewertet werden. Wie Cybersecurity ist auch Souveränität im Kern eine Entscheidung über Risikobereitschaft. Es gibt keine universell richtige Antwort: Das angemessene Maß an Kontrolle hängt davon ab, welche Exposition eine Organisation bereit ist zu akzeptieren, und wie Abhängigkeiten sowie potenzielle Störungen gegen

Kosten, Geschwindigkeit und Zugang zu Innovation abgewogen werden. Dadurch ist die Formulierung der Entscheidung genauso wichtig wie die Entscheidung selbst. Ohne einen strukturierten, faktenbasierten Ansatz laufen Souveränitätsentscheidungen Gefahr, von Wahrnehmung oder Politik bestimmt zu werden, statt von messbarem Risiko und geschäftlicher Priorität. Effektive digitale Souveränität bedeutet deshalb nicht, überall das maximale Maß an Kontrolle anzustreben. Entscheidend ist vielmehr, für jeden Anwendungsfall die richtige Balance zwischen den verfügbaren Kontrollmechanismen und den damit verbundenen Zielkonflikten zu finden.

In der Praxis orientieren sich Souveränitätsstrategien an vier zentralen Zielsetzungen: Autonomie, Resilienz, Kontrolle und Sicherheit. Innerhalb der verfügbaren Investitionsmittel müssen Unternehmen ihre Maßnahmen zwischen diesen vier Dimensionen ausbalancieren. Dies setzt eine enge Abstimmung zwischen Fachbereichen und IT voraus, um geschäftskritische Workloads zu identifizieren, Abhängigkeiten zu bewerten und für jeden Anwendungsfall das angemessene Maß an digitaler Souveränität einschließlich der erforderlichen Investitionen festzulegen.

Diese Zielkonflikte dürfen jedoch nicht zum Hemmnis werden. Zum einen können die Kosten mangelnder digitaler Souveränität erheblich höher ausfallen als die Investitionen in geeignete Schutzmaßnahmen. Zum anderen bedeutet digitale Souveränität nicht zwangsläufig höhere Kosten. Durch bewusste Architekturentscheidungen, den Einsatz offener Standards, Open-Source-Komponenten, modularer Architekturen und diversifizierter Partnerökosysteme können Unternehmen ihre Kontrolle stärken und gleichzeitig Innovationsfähigkeit sowie Wirtschaftlichkeit erhalten.

Agentische KI verschiebt dieses Verhältnis zusätzlich. Werden Durchsetzung, Überwachung und automatisierte Gegenmaßnahmen innerhalb souveräner IT-Umgebungen durch intelligente Agenten übernommen, sinken die operativen Aufwände für die Einhaltung hoher Kontrollstandards erheblich. Was bislang häufig als Zielkonflikt zwischen Kosten und Innovation galt, kann so zu einem skalierbaren Betriebsmodell werden.

Die Frage der digitalen Souveränität gewinnt zusätzlich an Bedeutung, wenn IT-Betriebsmodelle zunehmend automatisiert werden und KI-Agenten eigenständig Aufgaben übernehmen. Sobald Künstliche Intelligenz Workflows initiieren und systemübergreifend Entscheidungen treffen kann, müssen die Leitplanken der digitalen Souveränität auch für diese Agenten gelten. Dazu gehören ihre Identität, ihre Berechtigungen, die Durchsetzung von Richtlinien, Protokollierung, definierte Eskalationspfade, Kill-Switch-Mechanismen sowie Kontrollmöglichkeiten über die zugrunde liegenden KI-Modelle.

Gleichzeitig eröffnet eine auf digitale Souveränität ausgerichtete IT-Transformation die Möglichkeit, agentenbasierte Betriebsmodelle über Infrastruktur, Cybersecurity und IT-Operations hinweg einzuführen. Automatisierte Kontrollen, die kontinuierliche Durchsetzung von Richtlinien sowie KI-gestützte Überwachungs- und Remediationsmechanismen werden dabei direkt in die technische Plattform integriert. Auf diese Weise können Unternehmen ihre digitale Souveränität stärken und gleichzeitig Effizienz und Kostendisziplin verbessern.



3. Überzeugungen aus unserer operativen Erfahrung

Atos – mit Eviden als zentralem Baustein für digitale Souveränität – unterstützt seit Jahrzehnten Unternehmen und Organisationen beim Aufbau und Betrieb hochkritischer digitaler Systeme. Unsere Arbeit umfasst einige der anspruchsvollsten IT-Umgebungen weltweit: historisch gewachsene Systemlandschaften, Mainframe-nahe Architekturen, stark regulierte Branchen, geschäftskritische Betriebsumgebungen sowie souveräne Infrastrukturen, die dauerhaft höchsten Anforderungen an die Cybersicherheit unterliegen.

Hierzu zählen auch Umgebungen mit militärischen Sicherheitsstandards, in denen Zuverlässigkeit, Sicherheit, Resilienz, Vertrauen und vollständige Nachvollziehbarkeit unverzichtbar sind. Solche Systeme müssen auch bei Ausfällen, Cyberangriffen, eingeschränkten Betriebszuständen und unter extremen operativen Rahmenbedingungen zuverlässig funktionieren. Software muss selbst im Fehlerfall kontrolliert reagieren, Führungs- und Kontrollfunktionen erhalten und jederzeit einer kontinuierlichen Prüfung durch interne und externe Aufsichtsinstanzen standhalten.

Das Vertrauen unserer Kunden hat uns im Laufe der Jahre ein tiefes Verständnis dafür vermittelt, wie komplexe digitale Betriebsumgebungen in der Realität funktionieren. Es handelt sich selten um neu entwickelte Idealarchitekturen. Vielmehr sind sie das Ergebnis vieler Jahre technologischer, regulatorischer und organisatorischer Entscheidungen. Sie bestehen aus zahlreichen Ebenen, vielfältigen Abhängigkeiten und eng miteinander verknüpften Systemen.

Jede Ebene des IT-Stacks führt ihre eigenen Parameter, Abhängigkeiten und Einschränkungen ein. Diese Komplexität schafft Risiken, Exposition und blinde Flecken. Kontrolle kann in Datenströmen, im operativen Zugriff, in vererbten Abhängigkeiten oder in den Lücken zwischen Systemen, Anbietern und Teams verloren gehen. Je kritischer das Umfeld, desto wichtiger sind diese Schwachstellen.

Die Kernaufgabe von Atos ist es, diese Komplexität und diese Abhängigkeiten mit Vertrauen zu steuern. Unsere Aufgabe ist es, End-to-End-Umgebungen zu orchestrieren, Risiken vorherzusehen und zu managen, bevor sie sich materialisieren, und Transparenz in Systeme zu bringen, die über die Zeit kontrollierbar, auditierbar und widerstandsfähig bleiben müssen. Wir entwerfen, betreiben und verwalten souveräne digitale Umgebungen konsistent über den gesamten IT-Stack hinweg – einschließlich der Erweiterung von KI-Modellen, fein abgestimmten LLMs sowie agentischen Geschäftsplattformen und Anwendungen, die das grundlegende geschäftskritische Wissen und die Geschäftsgeheimnisse von Organisationen enthalten. Für uns ist digitale Souveränität ein zentrales Designprinzip, das von Anfang an in Architekturen, Betriebsmodelle sowie Technologie- und Anbieterentscheidungen integriert und dann kontinuierlich im Betrieb bewiesen wird.

In der Praxis erfordert dies eine einheitliche Kontroll- und Orchestrierungsebene, um Souveränitätsziele mit durchsetzbaren Richtlinien über Vermögenswerte, Daten, Workloads und Sicherheitsdomänen hinweg zu verknüpfen und sicherzustellen, dass Governance-Regeln konsistent über Umgebungen hinweg überwacht und implementiert werden. Ohne diese Ebene riskieren Multistack-Architekturen, sich in isolierte Kontrollinseln zu fragmentieren, wo die schwächste Komponente letztlich das effektive Maß der Souveränität bestimmt.



Dieses Erbe beruht auf einer Reihe klarer Überzeugungen

Erstens: Digitale Souveränität ist weder absolut noch monolithisch. Digitale Souveränität bedeutet nicht Autarkie und auch nicht den Aufbau einer vollständig abgeschotteten IT-Umgebung. Obwohl sie häufig als Entweder-oder-Entscheidung dargestellt wird, versteht Atos digitale Souveränität als ein Kontinuum unterschiedlicher Kontrollstufen. Je nach Schutzbedarf können verschiedene Steuerungs- und Kontrollmechanismen kombiniert werden. Im Cloud-Umfeld unterscheidet Atos beispielsweise verschiedene Souveränitätsmodelle – von Native über Controlled und Trusted bis hin zu Disconnected. Jedes dieser Modelle umfasst spezifische Kontrollmechanismen und adressiert unterschiedliche Anforderungen hinsichtlich Kritikalität und Schutzbedarf einzelner Workloads. Tatsächliche digitale Souveränität entsteht daher durch das Zusammenspiel von Entscheidungen in den Bereichen Daten, Technologien, Betriebsmodelle und rechtliche Rahmenbedingungen.

Zweitens: Zertifizierungen und Gütesiegel sind keine Garantie für digitale Souveränität. Zertifizierungen, regulatorische Labels und Compliance-Nachweise sind wertvolle Orientierungshilfen. Insbesondere zu Beginn eines Transformationsvorhabens oder beim Nachweis regulatorischer Anforderungen liefern sie wichtige Anhaltspunkte. Sie schaffen jedoch keine digitale Souveränität. Diese entsteht vielmehr durch fundierte Architekturentscheidungen, den Einsatz offener Standards und Open-Source-Komponenten, geeignete Betriebsmodelle, wirksame Governance-Strukturen sowie durch technisch durchgesetzte Kontrollmechanismen im täglichen Betrieb. Erst deren Zusammenspiel schafft Transparenz, reduziert Abhängigkeiten und ermöglicht tatsächliche Kontrolle.

Drittens: Organisationen sind nur so souverän wie ihr schwächstes Glied. Die Lokalisierung von Daten und die Wahl eines geeigneten Cloud-Anbieters sind notwendige Voraussetzungen, reichen jedoch allein nicht aus. Digitale Souveränität muss ganzheitlich gedacht werden. Sie muss den gesamten IT-Stack sowie den vollständigen Lebenszyklus digitaler Systeme umfassen. Cybersecurity bildet dabei die grundlegende Durchsetzungsebene. Alle Schutzmaßnahmen müssen konsistent aufeinander abgestimmt sein und gemeinsam das angestrebte Souveränitätsniveau unterstützen.

Viertens: Digitale Souveränität ist niemals dauerhaft erreicht. Sie muss kontinuierlich überprüft, überwacht und an neue Rahmenbedingungen angepasst werden. Dies erfordert belastbare Governance-Strukturen, eine fortlaufende Steuerung sowie die Fähigkeit, auf regulatorische Änderungen, technologische Entwicklungen oder geopolitische Ereignisse flexibel zu reagieren.

Kurz gesagt, für uns bedeutet digitale Souveränität, kritische Abhängigkeiten aktiv zu steuern – durch Transparenz, wirksame Kontrolle und den Erhalt der eigenen Wahlfreiheit.

Unser Ansatz:

Digitale Souveränität als gelebte Betriebspraxis für unsere Kunden

Für CxOs und ihre Teams macht Atos Souveränität zu einer operativen Fähigkeit, die auf Transparenz, Entscheidungsfreiheit und Kontrolle basiert. Wir machen Abhängigkeiten sichtbar, setzen Kontrollen konsequent durch und halten Optionen über die Zeit hinweg offen. So wird Souveränität im großen Maßstab handhabbar, anstatt zu einer ständigen Quelle von Unsicherheit und Reibung zu werden.

Atos agiert als Berater und Orchestrator und steuert die Komplexität der Souveränitätsanforderungen ihrer Kunden sicher, effizient und transparent im Rahmen eines End-to-End-Ansatzes. Das beginnt mit einem tiefen Verständnis für den Geschäftskontext unserer Kunden, ihre IT-Umgebungen, ihre operativen Realitäten und die

kritischen Fragen, die sie bewältigen müssen. Atos hilft Organisationen, ihre Schwachstellen zu identifizieren, ihre Souveränitätsbedürfnisse zu klären und zu bestimmen, welche Workloads welches Maß an souveränen Kontrollen erfordern. Wir strukturieren konkrete Optionen und Transformationsszenarien: Wir definieren, was so bleiben kann, was verstärkt werden muss und was sich im Laufe der Zeit weiterentwickeln sollte. Unsere Kunden erhalten fundierte Architekturentscheidungen, realistische Migrationspfade sowie eine transparente Darstellung der jeweiligen Zielkonflikte. Ergänzend etablieren wir Governance-Modelle, mit denen sich digitale Souveränität langfristig steuern und kontinuierlich weiterentwickeln lässt.

Darauf aufbauend entwickeln, implementieren und betreiben die Teams von Atos, Atos Amplify und Eviden geeignete souveräne Zielarchitekturen. Dabei greifen wir auf ein breit aufgestelltes Netzwerk zertifizierter Partner in unterschiedlichen Regionen zurück. Digitale Souveränität wird nicht allein über Cloud- und Infrastrukturentscheidungen hergestellt, sondern konsequent über Anwendungen, Daten, Künstliche Intelligenz, Cybersecurity und Betriebsprozesse hinweg umgesetzt. Unterstützt wird dies durch klare Governance- und Managementstrukturen.

Im laufenden Betrieb sorgt Atos dafür, dass Daten, Technologien und Betriebsmodelle dauerhaft mit dem jeweils erforderlichen Souveränitätsniveau in Einklang bleiben und rechtliche Risiken jederzeit transparent bewertet werden können. Treten neue Herausforderungen auf, unterstützen wir unsere Kunden dabei, den Betrieb schnell zu stabilisieren und geeignete Schutzmaßnahmen zu implementieren, um zukünftige Risiken nachhaltig zu reduzieren.

Praxisbeispiel | Souveräne agentische KI

Souveräne agentische KI lässt sich nicht durch eine einfache zusätzliche Schicht über bestehenden KI-Modellen erreichen. Die Herausforderungen der digitalen Souveränität im Umfeld agentischer KI sind reale und konkrete Fehlerszenarien, mit denen Unternehmen konfrontiert werden, sobald sie den Schritt von Pilotprojekten in den produktiven Betrieb vollziehen. Die Atos Lösungen für Sovereign Agentic AI wurden entwickelt, um genau diese Herausforderungen durch geeignete Architekturen, belastbare Betriebsmodelle und technisch durchsetzbare Kontrollmechanismen zu adressieren.

Identitäten, Zugang, Kontrolle und menschliche Aufsicht

KI-Agenten arbeiten unter expliziten, nicht geteilten Identitäten mit streng definierten Berechtigungen. Der Zugang zu Tools und Systemen wird durch Zero-Trust-Prinzipien geregelt, zentral durchgesetzt, mit Just-in-Time-Zugriff, wo angemessen, und der Möglichkeit, den Zugriff in Echtzeit zu widerrufen. Privilegierte Berechtigungen und Eskalationspfade sind kontrolliert und vollständig audittierbar. Dadurch wird verhindert, dass Agenten ihre Befugnisse mit zunehmendem Autonomiegrad unbemerkt erweitern. Gleichzeitig können Aktionen mit hoher Auswirkung gezielt auf autorisierte Identitäten und definierte Genehmigungsprozesse beschränkt werden. Ziele, Absichten und Handlungsgrenzen der Agenten werden eindeutig definiert und kontinuierlich überwacht. Änderungen an Zielvorgaben unterliegen grundsätzlich einer menschlichen Freigabe. Zusätzlich sorgen vertrauensbasierte Eskalationsmechanismen dafür, dass sich Agenten nicht schleichend vom ursprünglich vorgesehenen Geschäftszweck entfernen.

Datenqualität und Souveränität von Anfang an

KI-Agenten arbeiten ausschließlich mit kuratierten, verwalteten und vertrauenswürdigen Datenbeständen, für die Eigentumsverhältnisse und Lebenszyklen eindeutig geregelt sind. Bereits vor der Inbetriebnahme werden Datenqualität, Herkunft, Anforderungen an die digitale Souveränität sowie Datenschutzvorgaben bewertet und anschließend kontinuierlich überwacht. Dadurch wird verhindert, dass autonome Systeme inkonsistente, veraltete oder nicht vertrauenswürdige Informationen weiterverarbeiten oder verstärken.

Orchestrierung und Architektur für den produktiven Einsatz

Atos stellt eine dedizierte Orchestrierungsebene sowie Referenzarchitekturen bereit, einschließlich sicherer Multi-Context-Protocol-(MCP)-Server auf Basis eines Zero-Trust-Ansatzes. Diese koordinieren die Zusammenarbeit zwischen KI-Agenten, IT-Systemen und Menschen. Zustandsinformationen, Übergaben zwischen Agenten, Eskalationslogiken und Wiederherstellungsmechanismen werden explizit entworfen und implementiert. Dazu gehören deterministische Rollback-Verfahren, Kill-Switch-Funktionen sowie kontrollierte Neustarts einzelner Agenten und Workflows. Auf diese Weise werden fragile Punkt-zu-Punkt-Integrationen vermieden und ein vorhersehbares Verhalten auch in großem Maßstab sichergestellt.

Durchgängige Sicherheit über den gesamten Workflow

Atos entwickelt agentenbasierte Workflows als verteilte Systeme mit klar definierten Mechanismen für Orchestrierung, Zustandsverwaltung und Fehlerbehandlung. Sicherheitsmaßnahmen wie Schutz vor Prompt Injection, Validierung von Eingaben, Isolation von Arbeitsspeichern und Einschränkungen bei der Nutzung von Tools werden nicht ausschließlich auf Modellebene umgesetzt, sondern über den gesamten Workflow hinweg.

Dies umfasst die vollständige Verarbeitungskette – von Eingaben über Retrieval, Speicher und Koordination bis hin zur Nutzung externer Tools. Geeignete Architekturmechanismen sorgen dafür, dass Fehler isoliert bleiben und sich Sicherheitslücken nicht auf weitere Agenten oder Systeme ausbreiten können.

Dazu gehört auch die Absicherung der agentenbasierten Lieferkette selbst. Drittanbieter-Agenten, Partnerkomponenten, Modellabhängigkeiten und externe Tools werden wie produktive Softwarekomponenten geprüft, versioniert und kontrolliert. Kontinuierliche Integritätsprüfungen verhindern, dass kompromittierte Komponenten in produktive Workflows gelangen.

Nachvollziehbarkeit, Auditierbarkeit und Reaktionsfähigkeit

Jede Aktion eines KI-Agenten ist vollständig nachvollziehbar. Entscheidungen, Tool-Nutzung, Datenzugriffe und Ergebnisse werden so protokolliert, dass sie sowohl operative Analysen als auch regulatorische Nachweise und sicherheitsrelevante Untersuchungen unterstützen. Diese lückenlose Nachvollziehbarkeit schafft die Grundlage für eine schnelle Reaktion auf Vorfälle. Anomalien, Richtlinienverstöße oder Fehlfunktionen können rasch untersucht, kontrolliert zurückgesetzt und gezielt behoben werden.

Kostenkontrolle und wertorientierte Skalierung

Bereits ab dem ersten Tag werden AgentOps- und FinOps-Prinzipien etabliert. Die Betriebskosten von KI-Agenten werden mit geschäftlichen Kennzahlen wie Durchlaufzeiten, Cost-to-Serve, Durchsatz und Qualitätskennzahlen verknüpft und kontinuierlich überwacht, während der Grad der Automatisierung zunimmt. Echtzeitüberwachung und geeignete Steuerungsmechanismen stehen bereits vor einer breiten Skalierung zur Verfügung. Dadurch können Budgets gezielt auf Funktionen, Workflows, Projekte, Programme oder ganze Geschäftsbereiche verteilt sowie Ausgaben bei Bedarf begrenzt oder gestoppt werden.

Wiederverwendbare und zentral verwaltete KI-Agenten werden in einer kontrollierten Bibliothek bereitgestellt. Dadurch wird Wiederverwendung gegenüber redundanter Entwicklung bevorzugt, eine unkontrollierte Vermehrung von Agenten verhindert und gleichzeitig die Wertschöpfung beschleunigt. Unternehmen behalten so die Kontrolle über Token-Verbrauch, Werkzeugaufrufe, Wiederholungen und Ausführungsschleifen, ohne ihre Wahlfreiheit einzuschränken oder neue Herstellerabhängigkeiten entstehen zu lassen.

Schutz des geistigen Eigentums durch souveräne Modell- und Lieferentscheidungen

Wenn KI in Kernabläufe eingebettet wird, fließen proprietäres Wissen, Prozesse und Trainingsdaten durch Modelle und Orchestrierungsschichten, die möglicherweise außerhalb Ihrer Kontrolle liegen. Atos adressiert dies durch bewusste Modellauswahl, einschließlich privater, offener oder speziell entwickelter Modelle von vertrauenswürdigen Partnern, kombiniert mit Bereitstellungsarchitekturen (Private Cloud, Hybrid, Air-Gapped) und spezifischen Souveränitätsrichtlinien, die proprietäre Daten und Modellausgaben innerhalb kontrollierter Grenzen halten. Confidential Computing bietet dabei einen zusätzlichen Schutz, indem Daten selbst während ihrer Verarbeitung verschlüsselt bleiben. Ziel ist es, sicherzustellen, dass das geistige Eigentum und die Wettbewerbsvorteile eines Unternehmens weder unbeabsichtigt in Trainingsprozesse Dritter einfließen noch Zugriffsansprüchen anderer Rechtsräume ausgesetzt werden.

Atos versteht digitale Souveränität nicht als linearen Weg zu einem einzigen Zielzustand, sondern als eine Abfolge bewusster Entscheidungen, die sich an den jeweiligen geschäftlichen Prioritäten orientieren.

In der Praxis beginnen die meisten Organisationen mit einem klar abgegrenzten Anwendungsbereich – beispielsweise mit ausgewählten geschäftskritischen Workloads, sensiblen Datenbereichen oder besonders exponierten Abhängigkeiten. Auf diese Weise entsteht ein erster, pragmatischer Grad an digitaler Souveränität, der den Beginn einer Transformation ermöglicht, ohne Risiken oder Kosten unnötig zu erhöhen.

Da jede Organisation ein individuelles Souveränitätsprofil besitzt, verankert Atos entsprechende Gestaltungsprinzipien über das gesamte Leistungsportfolio hinweg. Dadurch können Transformations- und Betriebsleistungen gezielt auf einzelne Workloads und über den gesamten IT-Stack hinweg ausgerichtet werden. Das Portfolio reicht von Beratungsleistungen und Frameworks für souveräne Cloud-Architekturen über Cybersecurity-Lösungen – einschließlich souveräner Produkte von Eviden – bis hin zu KI-Lösungen für regulierte Umgebungen. Dabei stehen der Erhalt der Wahlfreiheit und die Vermeidung unumkehrbarer Lieferantenabhängigkeiten stets im Mittelpunkt.

Digitale Souveränität wird so vom einschränkenden Rahmen zu einem Enabler für Innovation.

Über die Konzeption und den Betrieb souveräner Architekturen hinaus unterstützt Atos seine Kunden dabei, dauerhaft eigene Kompetenzen im Bereich der digitalen Souveränität aufzubauen. Gemeinsam mit Fachbereichen sowie IT-, Sicherheits- und Risikoteams entwickeln wir das notwendige Know-how, geeignete Entscheidungsstrukturen und die organisatorischen Fähigkeiten, die Organisationen benötigen, um ihre digitale Souveränität langfristig eigenständig zu steuern und weiterzuentwickeln.



Für die Zukunft:

Digitale Souveränität wird in den kommenden Jahren ein prägendes Thema für Vorstände und Führungsteams bleiben.

Atos wird diesen Dialog in den kommenden Monaten weiterführen und das Angebot an branchenspezifischen Anwendungsfällen, Partnerschaften und regionalen Initiativen kontinuierlich ausbauen.

Digitale Souveränität ist und bleibt ein strategisches Kernanliegen von Atos.



Lassen Sie uns ins Gespräch kommen!

Wir möchten verstehen, welche Bedeutung digitale Souveränität für Ihre Organisation hat – und gemeinsam mit Ihnen die nächsten Schritte entwickeln.

Unabhängig davon, an welchem Punkt Ihrer Transformation Sie sich befinden, unterstützen wir Sie dabei:

- **Bewerten Sie**, was digitale Souveränität für Ihre Organisation bedeutet – und vergleichen Sie Ihre aktuelle Lage über Daten, Workloads und Abhängigkeiten hinweg, damit Sie sich zuerst **auf die wichtigsten Herausforderungen konzentrieren können**.
- **Erstellen Sie** eine Souveränitätsstrategie und eine pragmatische Roadmap, die auf Ihre Geschäftsprioritäten, Ihre Risikobereitschaft und Ihre regionalen Anforderungen abgestimmt sind.
- **Ergreifen Sie** konkrete Schritte, um Kontrolle, Resilienz und Transparenz in Ihrem digitalen Stack zu stärken, damit Sie Ihre digitale Souveränitätsposition kontinuierlich gestalten und verbessern können.

Nehmen Sie Kontakt auf unter
digitalsovereignty@atos.ai

Die Tech-Ambition der Atos Group

Die Strategie der Atos Group basiert auf drei eng miteinander verknüpften Prioritäten: Agentic AI für Mission-Critical-Umgebungen, digitaler Souveränität und Security. Gemeinsam schaffen sie die Voraussetzungen dafür, dass Organisationen mit Zuversicht innovieren, die Kontrolle über ihre kritischen digitalen Assets bewahren und in einer zunehmend komplexen Welt sicher agieren können. Getragen wird dieser Anspruch durch die komplementären Stärken von Atos, Atos Amplify und Eviden.

Atos

Atos ist die Marke der Atos Group für KI-gestützte, sichere und ganzheitliche digitale Services. Atos entwirft, entwickelt und betreibt kritische digitale Umgebungen, die Leistungsfähigkeit, Ausfallsicherheit und Souveränität fördern. So unterstützt Atos öffentliche und private Organisationen weltweit dabei, die Kontrolle über ihre Daten und IT-Infrastrukturen zu bewahren und gleichzeitig regulatorische Anforderungen zu erfüllen.

Atos unterstützt Kunden bei der Modernisierung ihrer zentralen IT-Systeme, der Beschleunigung ihrer Cloud- und Datentransformation, der Stärkung ihrer Cybersicherheit sowie der Bereitstellung sicherer digitaler Arbeitsplatzlösungen.

Als vertrauenswürdiger Partner beim Betrieb komplexer und geschäftskritischer Umgebungen unterstützt Atos Organisationen in stark regulierten und souveränen Kontexten.

atos.ai

Atos Amplify

Atos Amplify ist die auf KI ausgerichtete Consulting- und Advisory-Einheit der Atos Group. Sie unterstützt Organisationen dabei, strategisch wichtige Entscheidungen zu treffen und diese in messbare Geschäftsergebnisse zu überführen.

Durch die Verbindung von tiefem Branchenwissen, unternehmerischem Verständnis und KI-getriebener Innovation arbeitet Atos Amplify gemeinsam mit seinen Kunden daran, Transformationsstrategien zu entwickeln, die Einführung neuer Technologien zu beschleunigen und Mehrwert aus Daten, KI und digitalen Plattformen zu erschließen. Der Consult-to-Build-Ansatz verbindet Strategie und Umsetzung und unterstützt Organisationen dabei, Komplexität zu bewältigen, digitale Souveränität zu stärken, ihre Resilienz zu erhöhen und nachhaltiges Wachstum zu fördern.

Auf Grundlage menschenzentrierter Werte und verantwortungsvoller KI-Prinzipien ermöglicht Atos Amplify Organisationen, Transformation mit Vertrauen, Transparenz und Verantwortlichkeit zu gestalten.

atos.ai/atos-amplify

EVIDEN

Eviden ist die Marke der Atos Group mit Schwerpunkt auf Cybersecurity-Produkten, Mission-Critical Systemen und Vision AI.

Als vertrauenswürdiger Partner für Organisationen im öffentlichen und privaten Sektor setzt Eviden fortschrittliche Analysefähigkeiten ein und unterstützt seine Kunden dabei, die Widerstandsfähigkeit, Kontinuität und Resilienz ihrer Betriebsabläufe sicherzustellen.

Das Portfolio kombiniert fortschrittliche Cybersecurity-Technologien, Lösungen für digitale Identitäten, Fähigkeiten zum Schutz von Daten sowie Mission-Critical Systeme für besonders anspruchsvolle Einsatzumgebungen mit KI-gestützten Echtzeit-Monitoring- und Analysefähigkeiten.

Mit mehr als 2.200 Expertinnen und Experten sowie über 720 Patenten trägt Eviden dazu bei, Menschen, Daten und kritische Infrastrukturen weltweit zu schützen – an der Schnittstelle von Intelligenz, Souveränität und Vertrauen.

eviden.com

Über Atos Group

Die [Atos Group](#) ist ein weltweit führender Anbieter im Bereich der digitalen Transformation. Mit ca. 56.000 Mitarbeitenden und einem Jahresumsatz von ca. 7,2 Mrd. EUR (auf Basis des künftigen Unternehmenszuschnitts) agiert das Unternehmen in 54 Ländern unter zwei Marken: Atos für Services und Eviden für Produkte und Systeme. Als europäische Nummer eins in der Cybersicherheit und führend im Bereich Cloud arbeitet die Atos Group für eine sichere und dekarbonisierte Zukunft und bietet maßgeschneiderte KI-gestützte End-to-End Lösungen für alle Branchen. Atos Group ist an der Euronext Paris notiert.

Erfahren Sie mehr über uns
[atos.ai](#)

Beginnen Sie das Gespräch mit uns



Atos Group ist eine eingetragene Marke der Atos Group. © Atos Group. Vertrauliche Informationen, die der Atos Group gehören und nur vom Empfänger verwendet werden dürfen. Dieses Dokument oder ein Teil davon darf ohne vorherige schriftliche Genehmigung der Atos Group nicht reproduziert, kopiert, verbreitet und/oder verteilt oder zitiert werden.

107924 - EM + HC - SOVEREIGNTY

The Atos logo is displayed in a large, bold, blue font. The letters 'A', 't', 'o', and 's' are connected, with the 't' and 'o' having a unique, stylized design.