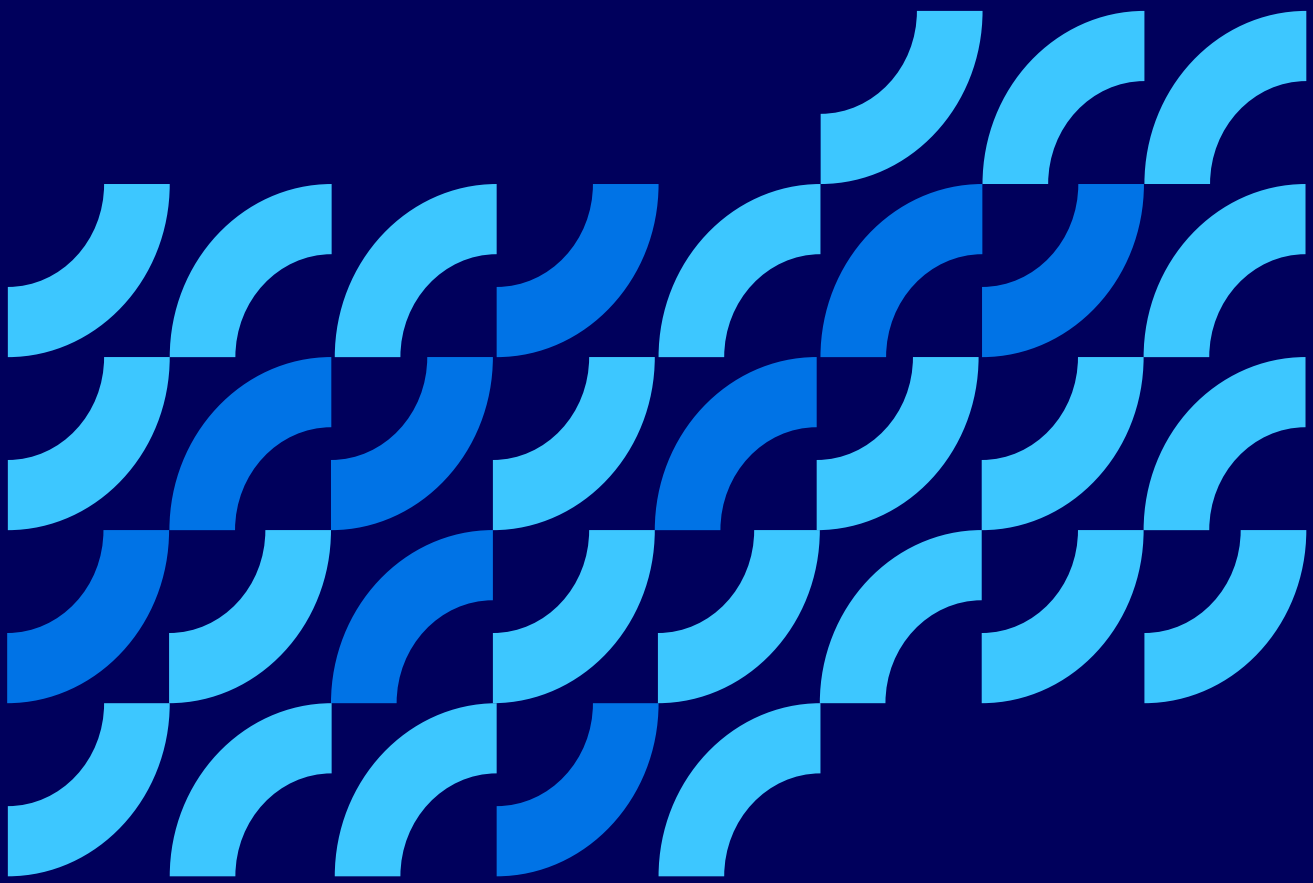
Kundenmagazin für den öffentlichen Sektor

Digitale Souveränität



Inhalt

Digitale Souveränität ist längst kein politisches Schlagwort mehr – sie ist zur strategischen Notwendigkeit geworden.

Als Verantwortlicher für Public Sector, Defense und Healthcare und Geschäftsführer bei Atos Deutschland erlebe ich täglich, wie nah Digitalisierung am Alltag der Bürgerinnen und Bürger ist – und wie deutlich ihre Erwartung nach mehr Geschwindigkeit geworden ist.

Gleichzeitig zeigen geopolitische Umbrüche und neue wirtschaftspolitische Weichenstellungen sehr deutlich: Digitale Abhängigkeiten sind kein abstraktes Thema mehr, sondern ein reales Risiko. Was lange effizient erschien, muss heute neu bewertet werden.

Für mich heißt das klar: Resilienz, Redundanz und digitale Handlungsfähigkeit sind keine technischen Detailfragen, sondern zentrale Voraussetzungen für staatliche und europäische Souveränität.

Digitale Souveränität heißt nicht Abschottung oder technologische Autarkie. Sie bedeutet nicht, jede Infrastruktur, jede Plattform und jede Anwendung selbst zu betreiben. Digitale Souveränität meint vielmehr, die Fähigkeit, technologische Entscheidungen bewusst zu treffen, Alternativen vorzuhalten und die Kontrolle über Daten, Prozesse und kritische Systeme zu behalten – auch dann, wenn sich politische, wirtschaftliche oder regulatorische Rahmenbedingungen abrupt verändern.

Martina Klement, CDO des Landes Berlin, formuliert es treffend: „Wir wollen wissen, was wir einsetzen. Und wir wollen Alternativen haben, wenn sich technische, wirtschaftliche oder politische Rahmenbedingungen ändern."

Souveränität wird damit zu einem architektonischen und strategischen Gestaltungsprinzip. Sie zeigt sich unter anderem in modularen, resilienten IT-Landschaften, die Flexibilität ermöglichen, Vendor-Lock-Ins vermeiden und staatliche Handlungsfähigkeit sichern – im Regelbetrieb wie im Krisenfall.

In unserem Kundenmagazin erfahren Sie, welche Fragen sich öffentliche Organisationen heute in Bezug auf Digitale Souveränität stellen sollten. Und wir zeigen exemplarisch und detailliert, was Digitale Souveränität für Fachthemen wie Künstliche Intelligenz oder Arbeitsbereiche wie Leitstellen bedeutet.

Ich wünsche Ihnen interessante Einblicke und viel Freude beim Lesen!

Ihr Boris Hecker

Geschäftsführer Atos Germany und Leiter Public Sector, Defense und Healthcare Deutschland

1 Souverän oder abhängig?

Fünf Fragen, die jede öffentliche Organisation heute beantworten sollte

Es ist Montagmorgen. Eine Fachanwendung fällt aus.

Die Daten liegen irgendwo – aber nicht dort, wo sie gebraucht werden.

Der Support sitzt im Ausland. Die Verträge sind komplex.

Und plötzlich stellt sich eine unbequeme Frage: Wer hat hier eigentlich die Kontrolle?

Digitale Souveränität ist längst kein abstraktes IT-Thema mehr.

Für den öffentlichen Sektor geht es um **Handlungsfähigkeit, Vertrauen und Verantwortung** gegenüber Bürgerinnen und Bürgern, Mitarbeitenden und dem Staat.

Doch bevor man über Lösungen spricht, braucht es etwas anderes:

Klarheit über den eigenen Status quo.

Digitale Souveränität ist kein Zustand. Sie ist eine bewusste Entscheidung und beginnt mit den richtigen Fragen.

1. Wissen wir, wo unsere Daten wirklich liegen und wer Zugriff hat?

Datenhoheit ist die Grundlage jeder souveränen Entscheidung.

Doch viele Organisationen haben historisch gewachsene Landschaften mit begrenzter Transparenz über Speicherorte, Zugriffsrechte und Abhängigkeiten von Dritten.

Souveränität beginnt mit Transparenz.

2. Wie unabhängig sind wir von einzelnen Anbietern oder Technologien?

Vendor-Lock-Ins entstehen selten bewusst, sie entwickeln sich schleichend.

Im Ernstfall entscheidet diese Abhängigkeit darüber, wie schnell eine Organisation reagieren oder umsteuern kann.

Wahlfreiheit ist kein Luxus, sondern Resilienz.

3. Entsprechen unsere digitalen Lösungen unseren regulatorischen und politischen Anforderungen?

Public Sector heißt: besondere Verantwortung.

Compliance, Datenschutz, nationale und europäische Vorgaben sind keine Randthemen. Sie definieren den Rahmen für jede digitale Entscheidung.

Souverän ist, wer Regeln nicht nur einhält, sondern aktiv gestaltet.

4. Haben wir die Fähigkeiten und Strukturen, um souverän zu handeln?

Technologie allein macht nicht souverän.

Es braucht Governance, klare Rollen, Entscheidungsmodelle und Menschen, die diese Verantwortung tragen können

Souveränität ist auch eine Organisations- und Kulturfrage.

5. Haben wir eine klare Zielvorstellung oder reagieren wir nur auf äußeren Druck?

Viele Initiativen entstehen aus Krisen, Audits oder politischen Vorgaben. Der Unterschied zwischen Reaktion und Strategie entscheidet darüber, ob Souveränität kurzfristig oder nachhaltig entsteht.

Wer das Ziel kennt, kann den Weg gestalten.

Diese fünf Fragen liefern keine Schulnoten. Aber sie liefern etwas Wertvolleres: Orientierung.

Scannen Sie den QR-Code, beantworten Sie wenige gezielte Fragen und erhalten Sie einen ersten Überblick über den Souveränitätsstatus Ihrer Organisation.

Ihre Vorteile auf einen Blick

- ☑ Eine klare Einschätzung Ihres aktuellen Status und der wichtigsten Risiken
- ☑ Sofort umsetzbare Empfehlungen für größere Unabhängigkeit und Einhaltung
- ☑ Aussagekräftige Visualisierungen für Management und Stakeholder
- ☑ Leitlinien, die auf Herausforderungen & Vorschriften abgestimmt sind
- ☑ Atos als Ihr vertrauenswürdiger Berater

Buchen Sie jetzt Ihren Termin und **gestalten Sie aktiv Ihre digitale Souveränität** mit Atos!

Marina Anderschitz

verantwortet bei Atos Consulting den Bereich Organizational Change Management.

**Scannen.
Reflektieren.
Klarer sehen.**

2 So wird digitale Souveränität Realität: Ein Überblick

Governance-Regeln, hybride/ Multi-Cloud-Modelle, zentrale Orchestrierung und FinOps greifen ineinander: Souveränität bedeutet gelebter Standard statt Einzelmaßnahmen.

Digitale Souveränität besteht aus drei grundlegenden Säulen

Digitale Souveränität ist die Fähigkeit einer Organisation, differenzierte, aktive, vorausschauende Kontrolle über ihre Daten und Technologien zu behalten, zu wissen, wo Ressourcen gehostet werden, wer darauf zugreifen kann und welche Vorschriften gelten.

Digitale Souveränität erfordert IT- und Cloud-Architekturen, die Sicherheit, Kontrolle und Flexibilität miteinander verbinden. Grundlage ist ein klar definiertes Zielbild aus einem Assessment, das Schutzbedarf, Kritikalität und regulatorische Anforderungen berücksichtigt.

Typische Bausteine souveräner Architekturen sind Private und EU-souveräne Cloud-Umgebungen für hochkritische Daten und Prozesse, Hybride und Multi-Cloud-Modelle, um Skalierbarkeit und Innovationsfähigkeit zu ermöglichen und klare Governance-Regeln, die festlegen, wo welche Workloads betrieben werden dürfen.

Eine zentrale Orchestrierung der unterschiedlichen Umgebungen reduziert Komplexität und stellt sicher, dass Organisationen auch bei veränderten politischen, rechtlichen oder sicherheitstechnischen Rahmenbedingungen steuerungs- und handlungsfähig bleiben.

Digitale Souveränität ist ohne wirksame Cybersecurity nicht realisierbar. Ein ganzheitlicher Ansatz umfasst Governance, Risk und Compliance, Identity und Access Management sowie operativen Schutz durch souveräne Sicherheitsbetriebsmodelle. Gleichzeitig schaffen FinOps-Methoden Transparenz über Kosten und Ressourcennutzung. So lassen sich IT- und Cloud-Umgebungen wirtschaftlich steuern und priorisieren. Digitale Souveränität wird damit nicht zum Selbstzweck, sondern zu einem dauerhaft tragfähigen Betriebsmodell – auch unter Budget und Haushaltsdruck.

Wie Atos unterstützt

Analyse und Zielbild —› Sovereign Assessment und Quick Check
Souveräne Architekturen —› Private, hybride, Multi Cloud und EU Cloud Modelle
Zentrale Steuerung —› Atos Cloud Platform zur Orchestrierung
Cybersecurity und Compliance —› Souveräne SOCs und klare Zugriffsmodelle
Kostenkontrolle —› FinOps für planbare, revisionssichere Cloud-Nutzung

Wie sichern Sie in Ihrer Organisation Kontrolle, Compliance und Zukunftsfähigkeit Ihrer IT?

Unser eBook liefert die Antworten:
https://atos.net/de/lp/digitale-souveraenitaet

Hätten Sie's gewusst?

48 % der Haushalte nutzen Smart-Home-Technologien und schaffen damit die Voraussetzung für die Abhängigkeit von Plattformen und Herstellern.
Quelle: Bitkom

Viele Smart Homes bestehen aus mehr als fünf vernetzten Geräten wie z.B. Sprachassistenten, Saugroboter und smarte Türschlösser.
Quelle: Bitkom

67 % der Deutschen erledigen ihre Bankgeschäfte online. **40 %** prüfen ihren Kontostand täglich, Bankgeschäfte sind damit vom gelegentlichen Vorgang zum digitalen Alltagsritual geworden.
Quelle: Destatis und Deloitte

3 Wo digitale Souveränität zum Tragen kommt: Vom Anspruch zur Umsetzung

Wo digitale Souveränität zur Praxis wird: Dieses Kapitel zeigt, wie digitale Handlungsfähigkeit konkret entsteht – im Digital Workplace, mit steuerbaren Cloud-Modellen und NIS2 als Führungsroutine. Dazu: Sovereign AI und kontrollierter Open Source Einsatz als Hebel für weniger Abhängigkeiten und mehr Resilienz.

Digital Workplace 2026

Komfort wie privat—Kontrolle wie gefordert. So wird der Arbeitsplatz produktiv, sicher und souverän

Auf einen Blick

1. Platzieren und steuern: Regeln für Private vs. Public Cloud festlegen; zentrale Orchestrierung, Zero Trust und Policies aktivieren.

2. Integrationen zuerst: Identity, UEM, Kollaboration, Monitoring verbinden – „geräuschlose" Administration sicherstellen.

3. Risikomanagement statt Abschottung: Kritische Assets differenziert absichern, Nutzung zentral kontrollieren, Exit Tests einplanen.

Vom effizienten Endgerätmanagement über spezialisierte Applikationen bis hin zu vernetzten Kollaborationsplattformen und dem begleitenden Support: Der Digital Workplace ist längst mehr als „E-Mail plus Kollaboration". Er ist der Ort, der für öffentliche Verwaltungen und Unternehmen gleichzeitig arbeitsfähig, sicher und compliant sein muss, und das bei steigenden geopolitischen, regulatorischen und technologischen Anforderungen. Die zentrale Leitfrage verschiebt sich: Stand früher die reine Funktionalität im Vordergrund, geht es heute zusätzlich darum, wie der Arbeitsplatz modern, anwenderfreundlich und barrierefrei bleibt – ohne die Kontrolle über Daten, Identitäten und Betriebsmodelle zu verlieren.

Genau hier trifft der Digital Workplace das Thema Digitale Souveränität.

Was Nutzer heute erwarten: „Consumer-Erlebnis" im Behörden- und Unternehmenskontext

Die Erwartungen sind hoch und konkret: Der digitale Arbeitsplatz soll einfach, intuitiv und schnell funktionieren – unabhängig von Endgerät und Arbeitsort. Gleichzeitig muss er stabil, effizient administrierbar und weitgehend störungsfrei sein. Der zunehmende Einsatz generativer KI verstärkt diese Anforderungen: Der moderne Arbeitsplatz soll die Nutzererfahrung privater Anwendungen bieten und zugleich strenge Vorgaben zu Sicherheit und digitaler Souveränität erfüllen.

Was IT und Security herausfordert: Komplexität, Abhängigkeiten, Regulierung

Während die Erwartungen an Nutzerkomfort konstant hoch bleiben, nehmen technologische und regulatorische Anforderungen deutlich zu:

Kritische Abhängigkeiten: Digitale Souveränität bedeutet, Abhängigkeiten – etwa bei Preisen, Updates, Support oder Datenzugriff – selbstbestimmt und proaktiv zu steuern. Ziel ist es, kritische Abhängigkeiten entlang des gesamten digitalen Arbeitsplatzes zu identifizieren, aktiv zu managen oder klare Exit-Strategien zu definieren.

Mehr Komponenten, mehr Schnittstellen: Ein souveräner digitaler Arbeitsplatz ist modular statt monolithisch aufgebaut. Die Entkopplung zentraler Bausteine wie Identitäten, Kollaboration, Endgeräte oder Monitoring schafft Kontrolle, erfordert jedoch höheres Integrations-Knowhow sowie einen Mehraufwand an Management und Kontrolle.

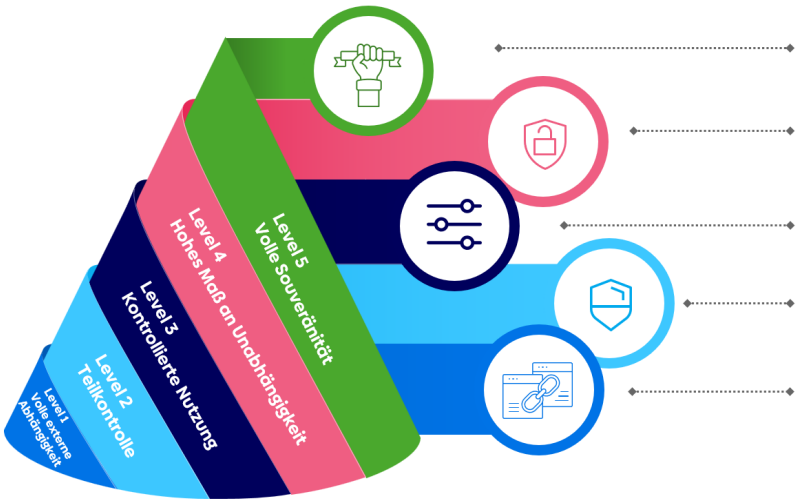
Regulatorischer Druck: Vorgaben wie NIS-2 verschärfen Anforderungen an Sicherheit, Datenschutz, KI-Einsatz und Rechtsdurchsetzung. Souveränität heißt hier, auch in geopolitischen Krisenszenarien die Kontrolle über den digitalen Arbeitsplatz zu behalten.

Souveränität als CIO-Priorität: Geopolitische Risiken rücken europäische Lösungen stärker in den Fokus. Souveränität entsteht durch das Zusammenspiel souveräner Cloud-Infrastrukturen, open-source-basierter Anwendungen und europäischer Service Partner.

Konsequenz: Es geht nicht um die Alternative „völlige Autarkie oder Vendor-Lock-In", sondern um ein ausgewogenes Kontinuum: Für jede Anforderung ist das passende Maß an Eigenständigkeit festzulegen, um Abhängigkeiten von außereuropäischen Anbietern gezielt zu reduzieren.

Digitale Souveränität im Workplace: kein „Abschotten", sondern Risikomanagement

Digitale Souveränität im digitalen Arbeitsplatz bedeutet nicht, sich technisch „abzuschotten". Entscheidend ist ein pragmatisches Risikomanagement: Geschäftskritische Assets werden differenziert abgesichert, ihre Nutzung steuerbar gemacht und zentral kontrolliert. Da es keine „absolute" Souveränität gibt, braucht es ein Kontinuum an Technologieoptionen – über Infrastruktur, Daten und Applikationen hinweg –, um Daten und Workloads je nach Schutzbedarf sinnvoll zu platzieren.



Das Atos Digital Sovereignty Framework im Überblick: Ein konsistentes Framework zur Bewertung und Steuerung digitaler Souveränität – von Device und Open Source bis Collaboration, Unified Endpoint Management und Monitoring.

Die Wahl des Betriebsmodells entscheidet heute maßgeblich über die langfristige Handlungsfähigkeit und die Vermeidung eines einseitigen Vendor-Lock-In. Dabei darf digitale Souveränität nicht als reine Abwehrreaktion oder technologische Isolation missverstanden werden Ein souveräner Digital Workplace ist nicht der, der am meisten verbietet – sondern der, der Nutzung ermöglicht, während Kontrolle, Resilienz und Nachvollziehbarkeit in den kritischen Schichten gewährleistet bleiben.

Aktuelle Entwicklung: Open Source als Souveränitätshebel

Open Source hat sich von der technologischen Nische zunehmend zur politischen und operativen Handlungsoption entwickelt, um digitale Abhängigkeiten zu reduzieren und Gestaltungsspielräume zu vergrößern. 73 % aller befragten Organisationen sehen Open-Source-Software ausdrücklich als das wichtigste Instrument zur Stärkung der digitalen Souveränität. (Quelle: Bitkom (2025), Open Source Monitor 2025.)

Gleichzeitig ist im aktuellen Diskurs klar: Open Source stärkt Souveränität nicht automatisch. Damit aus Software echte strategische Freiheit entsteht, muss der Fokus über den reinen Quellcode hinaus auf die Professionalisierung des Betriebs wandern: Entscheidend sind Strategie und Governance um "Wildwuchs" von Open Source Komponenten zu verhindern, die Nutzung technischer Industriestandards zur Sicherung der Interoperabilität, Kostenmanagement (insbesondere Lizenzmanagement) sowie professionelles Security-Tooling – von der Absicherung der Software-Lieferkette über Schwachstellenmanagement bis hin zu konsequentem Patchmanagement.

Um in komplexen IT-Strukturen die Übersicht zu behalten und dauerhaft kosteneffizient zu agieren, ist eine softwaregestützte Analyse der Applikationslandschaft essenziell. Atos nutzt hierfür ALOA – den Application Landscape Optimization Accelerator. Das Programm analysiert Nutzung, Performance, Abhängigkeiten und Lizenzen KI-gestützt sowie datenbasiert, um direkt umsetzbare Verbesserungsvorschläge zu liefern. Damit wird die IT-Landschaft von einem statischen Kostenfaktor zu einem dynamisch kontrollierbaren Asset, das kontinuierlich im Ganzen optimiert wird.

Konsequenz: Ein souveräner Digital Workplace ist nicht die Frage „Open Source ja oder nein", sondern: Open Source kontrolliert, sicher und beherrscht einsetzen.

„Gelungene Souveränität zeigt sich dort, wo die Kontrolle in der Tiefe die Handlungsfreiheit an der Oberfläche garantiert.“

Lars Voß

Architekt für Digital Workplace und digitale Souveränität.

Atos ist offizieller Reseller, Platinum Partner und Integrator von Nextcloud und bietet beispielsweise dem österreichischen Bundesministerium für Arbeit und Wirtschaft (BMAW) einen ganzheitlichen „End-to-End“-Service für Nextcloud-Instanzen – von Beratung und Architekturdesign über Implementierung bis hin zu Betrieb und kontinuierlicher Weiterentwicklung. Der Betrieb erfolgt in souveränen Rechenzentren in Österreich und wird durch lokale Experten aus Consulting, Implementierung und Operations verantwortet. So verbindet Atos technologische Exzellenz mit nationaler Datensouveränität und schafft eine sichere, skalierbare Kollaborationsplattform für die öffentliche Verwaltung.

Video ansehen:

Austrian Ministry of Economic Affairs – Schritte zur digitalen Souveränität: Austrian Ministry of Economic Affairs takes decisive steps towards digital sovereignty - YouTube

Hätten Sie’s gewusst?

Rund **40 %** der Beschäftigten in Deutschland arbeiten zumindest teilweise mobil, vor der Pandemie waren es nur rund 12 %. Quelle: Destatis

Der Anteil der Unternehmen, die Online-Meetings nutzen, stieg von **32 %** (2019) auf über **70 %** (2023). Quelle: Eurostat

In Deutschland ist der digitale Arbeitsplatz typischerweise eine Kombination aus Laptop oder PC plus Smartphone; Tablets kommen je nach Rolle zusätzlich dazu. Quelle: Bitkom

Mehr als jeder Dritte arbeitet im Homeoffice legerer als im Büro, rund ein Drittel der Beschäftigten gibt an, sich gezielt „videotauglich“ zu kleiden. Quelle: Owl Labs

Cloud-Strategien für den Staat: Zukunftssicherheit durch Souveränität und Steuerbarkeit

Auf einen Blick

1. Hybrid denken: Sensible Daten on-prem, skalierbare Dienste flexibel aus der Cloud – mit klarer Governance.

2. FinOps einsetzen: Transparenz über Kosten und Nutzen herstellen; Budget Forecast und Unit Costs überwachen.

3. Routinen verankern: Cloud-Steuerung, Security und Wirtschaftlichkeit als gemeinsame Führungsaufgabe etablieren.

Cloud-Technologien haben in der öffentlichen Verwaltung inzwischen eine zentrale Bedeutung: Sie ermöglichen moderne Fachverfahren, datengetriebene Innovation und den Einsatz von KI-gestützten Verwaltungsdiensten. Angesichts föderaler Strukturen, strenger deutscher und europäischer Datenschutzanforderungen sowie des Umgangs mit sensiblen Daten lassen sich Stabilität und Sicherheit jedoch nur gewährleisten, wenn die öffentliche Verwaltung nicht ausschließlich auf Public-Cloud-Lösungen setzt.

Deshalb gewinnen Hybrid- und Multi-Cloud-Architekturen an Bedeutung, in denen sensible Daten in sicheren bzw. europäischen Infrastrukturen verbleiben, während skalierbare Dienste flexibel aus der Cloud bezogen werden. Initiativen wie die Deutsche Verwaltungscloud (DVC) sollen den Weg zu sicheren europäischen Infrastrukturen ebnen und die Behörden technisch unabhängiger machen.

FinOps: Wirtschaftliche Steuerung als Teil staatlicher Souveränität

Mit wachsender Cloud-Nutzung steigt auch der Bedarf an ökonomischer Souveränität, denn der Einsatz von Cloud führt nicht automatisch zu Einsparungen.

Der Einsatz von FinOps, also des Managements der finanziellen Operationen rund um den Cloud-Einsatz, kann wesentlich dazu beitragen, Kosten, Nutzen und Auslastung transparent zu steuern. FinOps hilft Organisationen, Cloud-Ausgaben effektiv zu verwalten und zu optimieren und die volle finanzielle Kontrolle über die Cloud-Ressourcen zu erlangen, Transparenz zu schaffen und Technologieinvestitionen bestmöglich einzusetzen.

Für den öffentlichen Sektor bedeutet der Einsatz von FinOps die Offenlegung langfristiger wirtschaftlicher Abhängigkeiten, die bessere Vorhersagbarkeit von IT-Budgetentwicklungen und damit des Haushaltes und die klare Priorisierung zwischen Innovationsdruck und Kostenkontrolle.

FinOps ergänzt damit die technische digitale Souveränität durch eine finanzielle Perspektive.

In der Umsetzung ist Konsequenz essenziell

Deutschland verfügt über die Bausteine, um eine moderne, unabhängige und resiliente digitale Verwaltung aufzubauen: souveräne Cloud-Plattformen, hybride Architekturen und FinOps-Prozesse. Entscheidend ist jedoch ihre konsequente Anwendung – technisch, organisatorisch und wirtschaftlich.

„Nur wenn Cloud-Modelle, Sicherheitsanforderungen und wirtschaftliche Steuerung ineinandergreifen, kann die Verwaltung ihre digitale Handlungsfähigkeit dauerhaft sichern und flexibel auf neue Anforderungen reagieren.“

Markus Bähr

Senior Cloud-Advisor.

Hätten Sie’s gewusst?

Laut Bitkom sagen **62 %** der Unternehmen in Deutschland: Ohne Cloud-Dienste würde ihr Unternehmen stillstehen.

Unter den Cloud-nutzenden Unternehmen setzen **29 %** Hybrid-Cloud bereits ein, weitere **16 %** planen sie, und 12 % diskutieren den Einsatz.

Schon **41 %** der Cloud-nutzenden Unternehmen setzen Multi-Cloud ein. Weitere **14 %** planen, **10 %** diskutieren es.

Mehr als **50 %** der Menschen in Deutschland lagern ihre Erinnerungen in der Cloud, Fotos und Videos gehören zu den am häufigsten gespeicherten privaten Daten.

Quelle: Bitkom

NIS-2 im öffentlichen Sektor: Cybersicherheit als Basis digitaler Souveränität

Auf einen Blick

1. Führungsroutine: Quartalsweise Risikolage inkl. Lieferketten-Review bis Managementebene berichten.

2. 72-Stunden-Meldeübung und Notfallproben regelmäßig durchführen.

3. Compliance leben: BSI-Mindeststandards, Incident Response und Verantwortlichkeiten verbindlich verankern.

> *„Wir müssen als Staat vorangehen, resilient sein und insbesondere für Krisenzeiten vorbereitet sein.“*
>
> **Bundeskanzler Friedrich Merz 2025**
> auf der Pressekonferenz zur digitalen Souveränität Europas

Mit der Umsetzung der europäischen NIS-2-Richtlinie geht Deutschland einen großen Schritt in Richtung staatliche Resilienz. NIS-2 geht über reine IT-Sicherheit hinaus: Die Richtlinie legt verbindliche Vorgaben für Risikomanagement und Incident Response fest – und wird damit zur Grundlage digitaler Souveränität im Public Sector.

Von Technik zu Strategie

NIS-2 markiert einen Paradigmenwechsel: Cybersicherheit wird zur Steuerungsaufgabe und verpflichtet Behörden, Risiken systematisch zu analysieren, Sicherheitsmaßnahmen zu implementieren und Vorfälle strukturiert zu melden. Ziel: Eine belastbare und handlungsfähige IT-Struktur.

Resilienz statt Abhängigkeit

Digitale Souveränität braucht Transparenz und Krisenfestigkeit. NIS-2 fordert die Absicherung von IT-Dienstleistern, Lieferketten und kritischen Prozessen – nicht isoliert, sondern vernetzt.

NIS-2 stellt den öffentlichen Sektor vor klare Anforderungen. Risikomanagement, schnelle Vorfallmeldung und Compliance sind Pflicht – und stärken die digitale Widerstandsfähigkeit des Staates. NIS-2 markiert einen Paradigmenwechsel: Cybersicherheit wird zur Steuerungsaufgabe.

Mehr zum Thema in unserem Whitepaper *Sicher durch NIS 2*
Sicher durch NIS-2 - Atos

Souveräne KI – digitale Handlungsfreiheit neu definiert

Auf einen Blick

1.SLMs statt Monolithen: Domänenspezifische Small Language Modelle lokal betreiben und orchestrieren; sensible Daten verbleiben in eigener Umgebung.

2. Lifecycle sichern: Modell-/Daten- Schwachstellenanalyse, Versionierung, Monitoring, Akzeptanzkriterien als End-to-End-Pfad.

3. Governance verankern: Verschlüsselungshoheit, Zero-Trust-Identitäten, Policy Enforcement und vollständige Nachvollziehbarkeit jedes Agentenschritts.

Künstliche Intelligenz entwickelt sich rasant – doch mit dem wachsenden Einsatz steigt auch die Abhängigkeit von externen Plattformen, proprietären Modellen und intransparenten Datenflüssen. Atos versteht „Souveräne KI“ deshalb nicht als Schlagwort, sondern als klar strukturiertes Gestaltungsprinzip: Unternehmen und öffentliche Organisationen behalten jederzeit differenzierte, technisch durchsetzbare Kontrolle über Daten, Modelle und Infrastruktur. Dieses Prinzip bildet den Kern der Atos-Architektur für Sovereign AI.

Ausgangspunkt ist die Perspektive, dass Souveränität nur entsteht, wenn sie je nach Asset – ob Datensatz, Modell oder Workload – flexibel zugeschnitten werden kann. Atos adressiert dies durch ein Referenzarchitektur-Modell, das die gesamte Wertschöpfung von KI abbildet: von den Daten bis zum AI-Modell auf Basis souveräner Infrastrukturen. Und berücksichtigt dabei die gleichen Souveränitätsmaßstäbe von der Governance, Auditability bis hin Zero-Trust-Sicherheits-Mechanismen. Die Architektur ist bewusst als Meta-Modell gestaltet, denn Souveränität ist kein Produkt, sondern ein konfigurierbares Zusammenspiel aus Standards, Standardtechnologien und offenen Schnittstellen, die von anerkannten Sicherheitsprüfung von Anfang an bis End-to-End angewendet werden.

Open Source First als zentrales Element

Ein zentrales Element ist das Prinzip „Open Source First“. Offenheit und Unabhängigkeit ermöglichen Inspektionsfähigkeit, Reproduzierbarkeit und langfristige Unabhängigkeit von proprietären Plattformen – ein entscheidender Faktor, um regulatorische Vorgaben wie AI-Act, GDPR oder NIS-2 nicht nur zu erfüllen, sondern technisch sauber umzusetzen. Cybersecurity wird dabei nicht additiv verstanden, sondern durchgängig unter dem Fokus “Compliance-by-Design” innerhalb

der Souveränitätsbetrachtungen erst ermöglicht: Verschlüsselungshoheit, Zero-Trust-Identitäten, Policy-Enforcement und vollständige Nachvollziehbarkeit jedes Modells und Agentenschritts.

Souveräne KI bedeutet für Atos zudem Effizienz ohne Kontrollverlust. Statt monolithische, externe LLMs einzusetzen, setzt das Modell auf "Small Language Models (SLMs)" – spezialisierte Expertenmodelle, die lokal betrieben, orchestriert und domänenspezifisch feinjustiert werden können. Damit bleiben sensible Daten in der eigenen Umgebung, Betriebs- und Latenzkosten sinken, und durch orchestrierte Multi-Agent-Systeme lassen sich dennoch komplexe Aufgaben abdecken. Unternehmen behalten so die volle Kontrolle über Ausgangsmodell, Datenverarbeitung, Entscheidungsregeln und Betriebsumgebung – ein wesentlicher Unterschied zu generischen Cloud-LLM-Architekturen.

Souveräne Organisationen sind resilienter

Schließlich erweitert Atos das Verständnis von Souveränität um Resilienz. KI-Systeme müssen in realen Geschäftsprozessen zuverlässig und nachvollziehbar funktionieren. Daher umfasst die Architektur einen End-to-End-Lifecycle mit modell- und datenspezifischer Schwachstellenanalyse, operationalen Design-Domänen, kontinuierlichem Monitoring und klaren Qualitäts- und Akzeptanzkriterien. Damit wird Souveränität messbar und überprüfbar – nicht nur im Sinne regulatorischer Anforderungen, sondern auch als Grundlage vertrauenswürdiger Geschäftsprozesse- und Akzeptanzkriterien.

So definiert Atos souveräne KI: kontrolliert, auditierbar, offen, sicher und spezifisch auf die operative Realität europäischer Unternehmen zugeschnitten. Eine Souveränität, die echten Wert schafft, weil sie technologische Innovation mit verlässlicher Governance verbindet.

Marius Kiskemper

Lead Data Scientist, spezialisiert auf souveräne KI-Modelle.

Gerrit Viola

Chief Technical Officer der Business Line Data & AI Atos Germany.

Hätten Sie's gewusst?

67 % der Menschen in Deutschland nutzen bereits generative KI.

Laut Bitkom geben rund **11 %** der Menschen in Deutschland an, dass sie sich eine romantische Beziehung mit einer KI grundsätzlich vorstellen können.

Auch KI als „Therapeut" ist für viele kein Tabu mehr: Bereits rund **25 %** der Menschen in Deutschland können sich vorstellen, psychologische Unterstützung durch eine KI in Anspruch zu nehmen.

Quelle: Bitkom

4 Digitale Souveränität: Anwendungen im Fokus

Drei Einsatzfelder, ein Prinzip: Wie digitale Souveränität Transformationsprozesse in Leitstellen, Kliniken und der Bundeswehr absichert – und neue Handlungsräume eröffnet.

...in der Leitstelle

Wenn jede Sekunde zählt, darf Technik keine Schwachstelle sein. Leitstellen müssen auch dann handlungsfähig bleiben, wenn Cloud-Dienste, Internetverbindungen oder externe Kartenplattformen ausfallen. Souveräne Routing, Geodaten und Leitstellenarchitekturen sind der Schlüssel, um Einsatzführung, Disposition und Lagebild jederzeit unter Kontrolle zu behalten – gerade im Ernstfall.

Einsatzfähigkeit sichern – auch ohne Cloud, Netz oder externe Kartenplattformen

Wenn Leitstellen unter Hochlast arbeiten, zählt vor allem eines: jederzeit handlungsfähig zu sein und damit die KRITIS-Infrastruktur zu schützen. Deshalb gilt es zu vermeiden, dass Einsatzführung, Disposition und Lagebild von einzelnen externen APIs oder Internetverbindungen abhängig sind. Die Basis für die gewünschte Unabhängigkeit ist eine hochverfügbare Geodateninfrastruktur kombiniert mit modernen Geodaten- und Leitstellenarchitekturen, ein zentral verwaltetes Routing, Hochverfügbarkeit als Resilienzprinzip und Offline-Daten und -Karten für die maximale Datenhoheit im Betrieb.

Routing: Souveräne Disposition mit passender Einsatzlogik

Routing ist in Leitstellen mehr als die Festlegung einer Strecke von A nach B. Es geht um die bedarfsgerechte Disposition von Einsatzmitteln, die Berechnung von Erreichbarkeitszonen – inklusive individueller Spezialisierung auf Einsatzfahrzeuge und der Erweiterung für ein Blaulicht-Routing.

Ein entscheidender Souveränitätshebel ist deshalb der Aufbau einer eigenen Routing- und Kartenfunktion für den Leitstellenbetrieb, die behördliche Bedarfe abbildet,

statt Standardannahmen aus dem Consumer-Bereich zu übernehmen.

Dabei stärkt die Möglichkeit, das Routing auf Basis kommerzieller oder Open-Source-Daten aufzubauen, die Unabhängigkeit. So wird eine maximale Flexibilität und Anpassungsfähigkeit gewährleistet– ohne das Einsatzprinzip neu zu erfinden.

Hochverfügbarkeit: Resilienz als Souveränitätskriterium – autark, georedundant, krisenfest

Digitale Souveränität zeigt sich besonders dann, wenn etwas ausfällt. Eine souveräne Leitstellenarchitektur ist deshalb vollständig autark in eigener Infrastruktur betreibbar – und damit unabhängig von potenziell störungsanfälligen Cloudanbietern.

Kritisch ist zudem das Verhalten im Schadensfall: Selbst der Ausfall mehrerer Brandabschnitte darf den laufenden Betrieb nicht stoppen.

Für besonders hohe Anforderungen sehen wir deshalb georedundante Standorte vor, die – wenn nötig – vom Internet entkoppelt (air-gapped) betrieben werden können. Das reduziert Abhängigkeiten, senkt Angriffsflächen und erhöht die Krisenfestigkeit.

Offline-Daten und -Karten: Datenhoheit in der Leitstelle und in der Lage – auch ohne Internetzugriff

Karten sind die essenzielle Grundlage von Leitstellen, um schnell und souverän agieren zu können. Stets verfügbare Offline-Karten und Geodaten können, beispielsweise durch lokale Karten-Caches, verfügbare Hintergrundkarten und Informationen ohne Internetzugriff liefern.

Diese können individuelle Grundkarten für den Leitstellenkontext enthalten– inklusive Informationen, die nur bei bestimmten Einsatzarten benötigt werden – sowie eine einheitliche Symbolisierung für behördenübergreifendes Verständnis.

Noch weiter geht echte Datensouveränität: der Aufbau eines eigenständigen Geodatenbestands durch Integration neuer Daten und Migration von Alt- bzw. Bestandsdaten.

Ein individuelles Datenmodell vermeidet Abhängigkeiten von webbasierten Geodaten; die Zusammenführung reduziert Inkonsistenzen („Datenmodelle aus einer Hand“). Daten können eigenständig aufbereitet, gespeichert und gezielt angereichert werden. Durch den Aufbau eines eigenen Geocodierungsdienstes können die Suchanfragen von Adressdaten oder POIs individuell für den Leitstellenbetrieb optimiert werden, ohne externe Services nutzen zu müssen.

> *„Wer Routing, Verfügbarkeit und Geodaten selbst beherrscht, beherrscht im Ernstfall das Entscheidende: die Lage.“*
>
> **Josefine Kottke**

Jan Sniehota

Spezialist für hochverfügbare Geodateninfrastrukturen im öffentlichen Sektor.

Josefine Kottke

Spezialistin für Geodatenintegration und Infrastrukturentwicklung.

Hätten Sie's gewusst?

Ungefähr **230** Integrierte Leitstellen (ILS) der nichtpolizeilichen Gefahrenabwehr sind in Deutschland über 112 erreichbar.

Es gibt ca. **84.000.** Notrufe am Tag in Deutschland, das ist ca. ein Anruf pro Sekunde.

Zuständigkeit und Routing: Jeder Standort gehört genau einem **112**-Notrufursprungsbereich an, die Rufursprungsbereiche für die polizeiliche Gefahrenabwehr können davon abweichen.

Quelle: Bitkom

...in Kliniken

Zwischen Regulatorik, Cyberbedrohungen und Fachkräftemangel stehen Kliniken vor einer strategischen Weichenstellung: Wer künftig Daten, Systeme und digitale Prozesse kontrolliert, entscheidet über Versorgungssicherheit, Resilienz und Wettbewerbsfähigkeit im Gesundheitswesen. Digitale Souveränität wird zum Schlüssel.

Digitale Souveränität – strategischer Hebel für Kliniken

Kliniken stehen heute unter erheblichem Transformationsdruck. Als Teil der KRITIS-Infrastruktur unterliegen sie steigenden regulatorischen Anforderungen wie DSGVO und NIS-2, sie sind zunehmend Cyberangriffen ausgesetzt und von anhaltendem Fachkräftemangel betroffen. Gleichzeitig gibt es hohe Erwartungen an Effizienz, Qualität und Patientensicherheit. Parallel gewinnen datengetriebene Medizin, KI-gestützte Diagnostik und interoperable Versorgungsmodelle stark an Bedeutung und verändern den klinischen Alltag grundlegend.

In vielen Krankenhäusern treffen diese Entwicklungen jedoch auf historisch gewachsene IT-Strukturen: fragmentierte Systemlandschaften, eingeschränkte Interoperabilität und eine hohe Abhängigkeit von einzelnen Software- und Plattformanbietern. Bei begrenzten personellen und finanziellen Ressourcen wird die Einführung neuer Technologien dadurch zur besonderen Herausforderung. Genau in diesem Spannungsfeld rückt digitale Souveränität in den Fokus der Klinikleitungen.

Digitale Souveränität entscheidet darüber, ob Kliniken ihre Patienten und Versorgungsdaten strategisch nutzen, Innovation kontrolliert integrieren und ihre Prozesse selbstbestimmt steuern können – oder ob Abhängigkeiten von externen Infrastrukturen die Handlungsfähigkeit einschränken. Für Krankenhäuser bedeutet sie, die Kontrolle über Daten, Systeme und digitale Wertschöpfung zu behalten und gleichzeitig moderne Technologien wie Cloud-Lösungen und KI sicher, regelkonform und kosteneffizient einzusetzen.

Digitale Souveränität im Klinikalltag: Was gewinnen Krankenhäuser konkret?

Bessere Patientenversorgung

Sicherer, strukturierter Zugriff auf Gesundheitsdaten ermöglicht fundierte klinische Entscheidungen

Mehr IT Resilienz

Geringere Angriffsflächen und stabiler Klinikbetrieb trotz wachsender Cyberrisiken

Interoperabilität

Vernetzte Zusammenarbeit über Sektor und Ländergrenzen hinweg (z. B. mit FHIR)

Weniger Abhängigkeiten

Vermeidung von Anbieter-Lock-Ins durch bewusste Architekturentscheidungen

Höhere Effizienz

Standardisierte Datenflüsse reduzieren administrativen Aufwand

Gestärktes Vertrauen

Transparenter Umgang mit Daten stärkt Akzeptanz bei Patienten und Partnern

Technologisch basiert digitale Souveränität im Krankenhaus vor allem auf souveränen Cloud Modellen. Sie verbinden skalierbare Infrastrukturen mit klaren Governance-Strukturen und einem konsequenten Security-by-design-Ansatz. Ergänzt durch definierte Daten und Zugriffsmodelle, Verschlüsselung, Zero-Trust-Konzepte und kontinuierliches Sicherheitsmonitoring entsteht eine zukunftsfähige IT Architektur.

Für Klinikleitungen ist digitale Souveränität damit keine rein technische Fragestellung, sondern eine strategische Führungsaufgabe. Sie schafft die Grundlage, um moderne Medizin, wirtschaftliche Stabilität und regulatorische Sicherheit nachhaltig miteinander zu verbinden – und die Zukunft der klinischen Versorgung aktiv zu gestalten.

Willi Wöllner

Head of Consulting
Digital Health.

Hätten Sie's gewusst?

In Deutschland gibt es **472.851** Betten in 1.841 Krankenhäusern.

7,1 Tage beträgt die durchschnittliche Verweildauer je stationärem Aufenthalt.

Im Jahr 2024 gab es **17,9** Mio. stationäre Behandlungsfälle.

Im Laufe des Lebens verbringt ein Mensch in Deutschland ca. **17** Aufenthalte im Krankenhaus.

Quelle: Statistisches Bundesamt.

...in der Bundeswehr

Wenn Systeme ausfallen, Netzwerke angegriffen werden und Entscheidungen unter Zeitdruck getroffen werden müssen, zeigt sich, worauf es wirklich ankommt. Der Operationsplan Deutschland verdeutlicht, warum Verteidigungsfähigkeit heute untrennbar mit digitaler Souveränität verbunden ist – und weshalb Kontrolle über Daten, IT-Architekturen und digitale Schnittstellen im Ernstfall über Handlungsfähigkeit und Sicherheit entscheidet.

Warum Verteidigungsfähigkeit heute digital gedacht werden muss

Digitale Souveränität ist im Verteidigungsbereich kein abstraktes Konzept, sondern eine konkrete Voraussetzung für Handlungsfähigkeit. Das zeigt auch der Operationsplan Deutschland.

Der **Operationsplan Deutschland** (OPLAN DEU) beschreibt, wie Deutschland im Krisen- und Verteidigungsfall funktioniert – im Zusammenspiel von Bundeswehr, öffentlicher Verwaltung und Privatwirtschaft. Im Mittelpunkt stehen Logistik, Infrastruktur, Digitalisierung und Echtzeitdaten. Der Plan legt unter anderem fest, welche Verkehrswege genutzt werden, wie Transporte erfolgen und wie kritische Punkte geschützt werden. Ziel ist eine robuste und widerstandsfähige Gesamtarchitektur, die auf aktuelle Bedrohungen vorbereitet ist.

Geschwindigkeit, Koordination, Lagebild

Das Operative Führungskommando betont die Notwendigkeit, strategische Vorgaben schnell in konkretes Handeln zu übersetzen. Im Fokus stehen:

- Landes- und Bündnisverteidigung
- glaubhafte Abschreckung
- ein gesamtstaatliches Lagebild
- enge Abstimmung mit NATO-Partnern

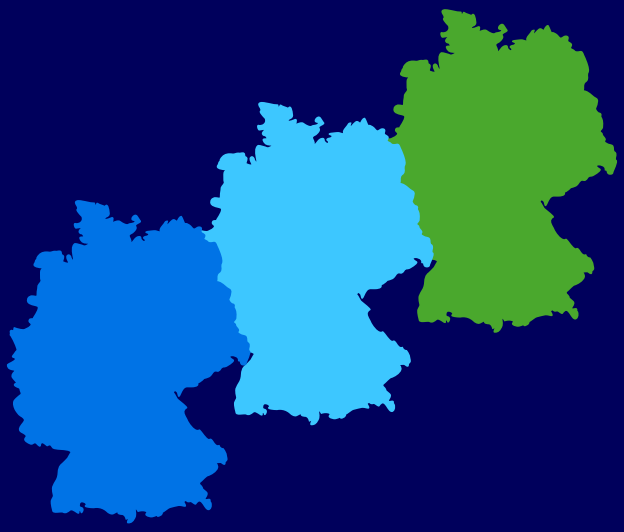
Dabei geht es nicht nur um militärische Informationen. Auch zivile Komponenten wie Infrastruktur, Energie, Transport und Kommunikation müssen in ein gemeinsames Lagebild integriert werden.

Gleichzeitig ist Deutschland hybriden Angriffen ausgesetzt. Beispiele dafür gibt es zuhauf: von Fake-News, Deepfakes und politische Einflussnahme über Sabotage, Cyberangriffe, verdeckte Operationen und Subversion bis hin zu wiederholten Lufthoheitsverletzungen. Diese „nicht-linearen“ Angriffe können in größere militärische Eskalationen münden.

Wo Digitale Souveränität ins Spiel kommt

Die Umsetzung des OPLAN DEU hängt maßgeblich von digitalen Strukturen ab: von sicheren Kommunikationsnetzen, geschützten IT- und OT-Systemen, belastbaren Datenplattformen und Echtzeit-Transparenz über Logistik und Infrastruktur.

Digitale Souveränität bedeutet in diesem Kontext die Kontrolle über eigene Daten und Systeme, Unabhängigkeit bei kritischen Technologien, resiliente Betriebsmodelle im Krisenfall und Schutz vor Manipulation und Ausfall.



Denn nur wenn digitale Infrastrukturen unter nationaler Kontrolle stehen und widerstandsfähig sind, kann ein gesamtstaatlicher Verteidigungsansatz funktionieren.

Zivil-militärische Zusammenarbeit als Schlüssel

Im Krisen- und Verteidigungsfall ist die Bundeswehr auf umfassende zivile Unterstützung angewiesen. Verkehrswege, Energieversorgung, Transportkapazitäten oder medizinische Einrichtungen werden Teil der Gesamtverteidigung. Damit entsteht ein eng vernetztes System aus staatlichen Stellen, Sicherheitsbehörden und privatwirtschaftlichen Akteuren. Digitale Souveränität wird hier zum verbindenden Element: Sie ermöglicht sichere Datenintegration, transparente Abläufe und abgestimmtes Handeln über Organisationsgrenzen hinweg.

Matthias Puschnig, Oberst im Generalstabsdienst, Sonderstab Ukraine im BMVg,
verdeutlicht die Wichtigkeit der IT-Architektur in Bezug auf den aktuellen Ukraine-Krieg:

„Der Schlüssel zum militärischen Überleben der Ukraine ist die Integration von Technologie in die militärische Praxis, und zwar nicht von einer Technologie wie Robotik, Space, Cyber oder AI. Es ist die Vernetzung all dieser Technologien mit den militärischen Strukturen buchstäblich bis zum letzten Mann, zum letzten Gerät. Also letztlich die IT-Architektur.“

Matthias Böhmer

verantwortet das Business Development für Discrete Manufacturing in Defense.

René Gimmler

Experte für Defense und Intelligence Operations.

Hätten Sie’s gewusst?

Rund **260.000** Menschen arbeiten für die Bundeswehr, über 81.000 davon sind zivile Beschäftigte.

Gebirge und Hochgebirge, große Höhenunterschiede, arktische Bedingungen, mangelnde Infrastruktur: Die **Gebirgsjäger** sind auf schwieriges bis extremes Gelände und extreme klimatische Bedingungen spezialisiert.

Die **Marine** schützt auch Daten: Unterseekabel transportieren einen Großteil des weltweiten Internetverkehrs und werden zunehmend strategisch geschützt.

Quelle: bundeswehr.de

5 Digitale Souveränität – was jetzt wirklich zählt

Im Interview ordnet Thomas Götz, CTO für Deutschland, Österreich und Zentraleuropa bei Atos, die größten Abhängigkeiten ein und erklärt, worauf es künftig ankommt: Transparenz, Priorisierung und messbare Fortschritte statt Schlagworte.

„Digitale Souveränität ist die Fähigkeit, kritische Abhängigkeiten systematisch und proaktiv zu managen.“

Thomas Götz,
CTO für Deutschland, Österreich und Zentraleuropa bei Atos.

Andrea Birkner (AB), Kundenmagazin: Welche Abhängigkeit macht den Staat heute am verletzlichsten? Daten, Plattformen, Lieferketten oder Kompetenzen?

TG: Kurz gesagt: Es trifft alle Felder. Bei Plattform-Abhängigkeiten sehen wir die fast alles beherrschende Rolle von Hyperscalern mit massiven „Lock-in-Effekten“ (z. B. bei Microsoft). Bezüglich der Daten sehen wir die schwierigen Auswirkungen lang gewachsener Beziehungen aufgrund von typischen Einsatzmustern und daraus folgenden sehr hohen Marktanteilen – bei der Nutzung von Datenbanken im öffentlichen Bereich liegen wir bei ca. 90 % Marktanteil von Oracle in Deutschland. Und bei KI Workloads hängen viele Verfahren an Stacks, die de facto nur auf wenigen Technologien basieren, zu denen es aktuell keine echte Alternative gibt (z. B. Nvidia mit CUDA). Der erste Schritt ist deshalb immer: Transparenz über Abhängigkeiten erzeugen, und diese dann differenziert betrachten – wo und wie stark sind wir wirklich abhängig und in welchem Umfang? Erschwerend kommen föderale Unterschiede und uneinheitliche Strategien im Umgang mit digitalen Plattformen dazu: Das Spektrum reicht von „strategische Verbindung“ (Bayern) bis „voll souveräner Kurs mit klarer Kante“ (Schleswig-Holstein). Wenn schon innerhalb Deutschlands über die Bundesländer hinweg diese Spannbreite vorliegt und wir unsere sehr knappen Expertenressourcen darüber dann verteilen, werden wir kaum vorankommen mit höherer Souveränität. Wir brauchen eine gemeinsame Haltung und wirksame Strategie für digitale Souveränität. Hier gibt es jetzt immerhin positive Signale.

AB: Welches Missverständnis begegnet Ihnen in Bezug auf digitale Souveränität am häufigsten?

TG: Das erste Missverständnis ist das Häufigste: Souveränität ist kein Zustand, kein Label oder Zertifikat, sondern eine Fähigkeit. Ein weiterer Irrglaube besteht darin, es sei eine Option, „alles in das eigene Rechenzentrum auf dezidierte Server zu verlagern“ - das ist keine Souveränität, sondern opfert Skalierbarkeit und Innovation für eine vermeintliche Unabhängigkeit.

Drittes Missverständnis: Es geht nicht nur um Technik Betriebs- und Liefermodelle, Vertragsgestaltung, Governance, Kriterien für Investitionen, Prozesse und Verantwortlichkeiten sind genauso entscheidend – und erfordern oft unbequemen organisatorischen Wandel und Change-Management nicht nur in der IT. Kurz gesagt: Souveränität ist Chefsache, und sollte nicht allein der IT überlassen werden.

AB: Welche Workloads priorisiert Atos für souveräne Umgebungen?

TG: Ganz pragmatisch: Wir starten damit zu bewerten, was wirklich zählt. Heißt: Wir legen alle digitalen Assets auf den Tisch – Applikationen mit ihren Workloads und KI-Komponenten, Datenbestände, Verträge/ Rechte und Fachkompetenzen (Personal), ausdrücklich inklusive Schlüsselpersonen und Zugänge zu tieferem Technologiewissen. Daraus filtern wir die „Kronjuwelen", also die Teile, die für Auftrag und Betrieb am kritischsten sind, und priorisieren diese Assets.
Dann nehmen wir jedes dieser priorisierten Assets einzeln unter die Lupe – entlang von vier Blickrichtungen:

Autonomie, Resilienz, Sicherheit und Kontrolle. Der Fokus variiert je nach Zweck: Im Bereich Intelligence oder Defence streben wir ein sehr hohes Autonomie Niveau an; im KRITIS-Umfeld hat Resilienz Vorrang, also Robustheit gegenüber Ausfällen und Schocks. Natürlich gibt es auch kombinierte Kriterien – jeder Zweck hat sein spezifisches Anforderungsmuster an Souveränität. Wir stellen auch immer die Frage: Sind wir bereit, eine kritische Abhängigkeit auch einmal zu akzeptieren, wenn der Nutzen der Lösung gegenüber den Risiken der Abhängigkeit überwiegt – und wenn wir dann auch geeignete „Wächter"-Funktionen implementieren und im Risiko-Management abrufbare Handlungsanweisungen für den Eventualfall vorsehen?

Wichtig dabei ist, dass Zielkonflikte offen benannt werden. Ein Beispiel aus dem Bereich Kontrolle: In Hyperscaler Stacks (z. B. Microsoft) werden Metadaten und Telemetriedaten genutzt, um Kapazitäten und Updates zu steuern. Gebe ich die Metadaten und Telemetriedaten aus Gründen meiner gewünschten strategischen Autonomie nicht heraus, bekomme ich keine (oder weniger) Updates. Das ist ein bewusster Trade off, den man sich spezifisch anschauen muss – nicht pauschal. Man muss bei diesem Beispiel dann die Frage stellen, ob es auch Alternativen gibt, bei denen ich Sicherheitsupdates und innovative neue Features auch bekomme, obwohl ich meine Metadaten und Telemetriedaten bei mir behalte. Spätestens dann wird man in die Liefer- und Betriebsmodelle und die dazugehörigen Verträge schauen müssen und herausfinden, welche Flexibilitäten noch vorhanden sind oder schon vor langer Zeit geopfert wurden – oder sogar unbewusst aufgegeben wurden.

Und wir fokussieren: Statt alles gleichzeitig zu optimieren, konzentrieren wir uns auf die obersten 10–20 % der Assets, diejenigen mit der höchsten zukünftigen Bedeutung für den Zweck der Organisation. Dabei arbeiten wir strikt nach der Design to Budget-Regel: Wir planen Maßnahmen so, dass sie in den vorgegebenen Budgetkorridor passen – und machen transparent, welche zusätzlichen Mittel welches Plus an Autonomie, Resilienz, Sicherheit oder Kontrolle bringen würden. Dann entscheidet am Schluss die Abwägung, was innerhalb des realistisch machbaren „Souveränitäts-Budgets" auch tatsächlich finanzierbar ist. Hierfür ist eine enge Diskussion zwischen IT- und Fachseite unbedingt notwendig.

Unterm Strich entsteht so eine überschaubare, realistische Roadmap von Transformationsmaßnahmen – Workload für Workload, Daten für Daten, Asset für Asset, mit klaren Prioritäten, offen gelegten Trade Offs und bewussten Abwägungsentscheidungen.

„Wir sprechen bei Souveränität immer über strategische Autonomie, Resilienz, Kontrolle und Sicherheit."

AB: Mit welchem belastbaren KPI können Verwaltungen bis Ende 2027 ihren Fortschritt bei digitaler Souveränität messen?

TG: Es gibt nicht den einen KPI. Gesteuert wird entlang der vier Dimensionen – strategische Autonomie, Resilienz, Sicherheit, Kontrolle. Bezüglich der Autonomie kann es z.B. der Anteil von Open Source im Infrastruktur-Stack sein, kombiniert mit einem Vendor-Konzentrationsindex. Für Sicherheit existieren etablierte Kennzahlen, z. B. das CVS-System; für Resilienz liefern geprüfte, standardisierte Business Continuity Frameworks geeignete KPIs, z.B. RTO/RPO. In der Kontrolle zählen u. a. Asset Transparenz, Lizenz-Transparenz, Policy Compliance Rate und End of Life Indikatoren. Wichtig ist ein übersichtliches Set – typischerweise 4 bis 8 KPIs – aber auch hier spezifisch je nach Zweck. Wenn man das systematisch anpacken möchte, empfehlen wir den Einsatz eines Sovereignty Level Modells, wie z.B. das der EU, mit den SEAL-Level 0-4 für Cloud Sovereignty. Bei Atos haben wir ein darüber hinausgehendes Framework entwickelt, das auch die IT außerhalb der Cloud-Thematik vollständig miteinbezieht, und das EU-Modell zu hundert Prozent abbildet. Dieses setzten wir auch in unseren Souveränitäts-Assessment-Werkzeugen ein.

„Wir dürfen auf keinen Fall vorhandene Abhängigkeiten weiter zementieren und unsere zukünftigen Optionen immer mehr einschränken.“

AB: Letzte Frage: Was wäre Ihr Souveränitäts-versprechen an Bürgerinnen und Bürger für die nächsten 24 Monate?

TG: Ich drehe den Spieß mal um: Bund und Länder sollten ein klares Versprechen abgeben, Steuermittel so einzusetzen, dass weniger kritische Abhängigkeiten entstehen und mehr Handlungsspielraum geöffnet wird – mit mehr Unabhängigkeit, Resilienz, mehr Sicherheit und mehr Kontrolle – auch basierend darauf, dass man wieder über echte Optionen verfügen kann. Statt Abhängigkeiten von wenigen Anbietern außerhalb unseres Rechtsraums zu zementieren, sollten gezielt Alternativen aufgebaut werden und die eigene Steuerungsfähigkeit gestärkt werden. Parallel sollte systematisch in eigene Kompetenzen hierzulande investiert werden: Von solider MINT-Bildung über technisch/wissenschaftliche Studiengänge mit modernem Curriculum bis hin zu einer Vergabepolitik und Ausschreibungspraxis, die nicht Abhängigkeiten verstärkt, sondern unsere eigenen Fähigkeiten aufbaut und nutzt. Dazu gehört dann im großen Bild auch die weitere Schaffung eines echten EU-Binnenmarktes für digitale Angebote und ein harmonisiertes und leistungsfähigeres Wagniskapitalregime. Warum sollten unsere Top-Software- und KI-Ingenieure fast alle zu den Top-US-Brands gehen (wie sie es heute tun), und unsere innovativen Startups nur aus den USA finanziert werden? Es ist eben nicht „Neuland für uns alle“ - wir wissen schon, was zu tun ist. Also mein Appell: Wir richten IT-Investitionen konsequent auf mehr Souveränität aus – konstruktiv, zukunftsorientiert und zum Nutzen aller Bürgerinnen und Bürger!

Jetzt konkret werden

Mehr Souveränität.

Weniger Abhängigkeit.

Kompakte Schritte, Praxisbeispiele, Werkzeuge: – jetzt loslegen: https://atos.net/de/lp/digitale-souveraenitaet

Scan me

Ihre Ansprechpartnerin

Andrea Birkner

Marktkommunikation & Business Development Manager
Public Sector Atos Germany

andrea.birkner@atos.net

Über die 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 den Bereichen Cybersicherheit und Cloud arbeitet die Atos Gruppe für eine sichere und dekarbonisierte Zukunft und bietet maßgeschneiderte KI-gestützte End-to-End Lösungen für alle Branchen. Atos Group ist die Marke, unter der Atos SE (Societas Europaea) tätig ist. Atos SE ist an der Euronext Paris notiert.

Folgen Sie uns

1107575 - SB+HC - Design Support for Customer Magazine