Souveränitätsaspekte und Compliance Automation: Cloud-Einsatz im Blickwinkel der Regulatorik

Know-how to go

12.06.2025

Heiko Müller

"Der Einsatz von Cloud Services wird aktuell mehr hinterfragt denn je. Viele Fragen sind dabei sinnvoll und berechtigt, aber das notwendige Compliance- und Souveränitätsniveau ist nicht für jeden Anwendungsfall gleich.

Außerdem findet man viele unterschiedliche Ansätze zur Definition und Messung des richtigen Niveaus. Welche Ansätze sind also für die eigene Organisation am sinnvollsten einsetzbar?"

Heiko Müller – Senior Manager
DevOps & Cloud Transformation

Agenda

1. Souveränitätsaspekte in der Cloud
2. Ansätze zur Automatisierung von Compliance

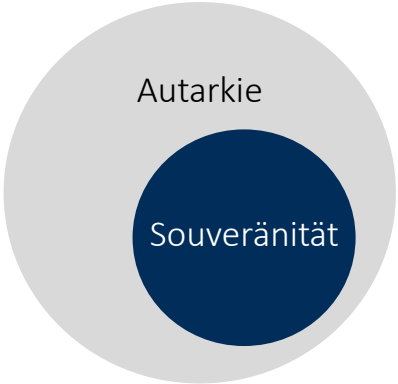
Was unterscheidet Souveränität von Compliance?

Im Unterschied zu Compliance-Standards gibt es für Souveränität **keine allgemeingültige Definition** und somit auch keine Standards anhand derer festgestellt werden kann, ob ein **Mindestniveau** an Souveränität vorliegt.

Das gewünschte Niveau muss also **selbst definiert und überprüft** werden.

Abgrenzung: Autarkie und Souveränität

Autarkie bezeichnet den Zustand der Unabhängigkeit oder Selbstversorgung einer Organisation. Ein autarkes System ist in der Lage, seinen eigenen Bedarf an Gütern und Dienstleistungen ohne externe Unterstützung oder Importe zu decken.



Souveränität bezieht sich auf die Fähigkeit eines Staates oder einer Organisation, unabhängig und selbstbestimmt Entscheidungen zu treffen und zu handeln, ohne von externen Einflüssen abhängig zu sein.

> *„In der Tat ist Autarkie nicht die einzige Möglichkeit, Souveränität zu erlangen.“*
>
> Claudia Plattner, BSI-Präsidentin, März 2025

Ein autarkes System ist somit immer auch souverän, der **Umkehrschluss** gilt jedoch nicht. In der öffentlichen Diskussion scheint dieser Umstand häufig verwechselt oder nicht beachtet zu werden.

Was kennzeichnet das Umfeld, in dem wir uns bewegen?

Stichwort: Cyber Dominance

- Cyber Dominance beschreibt die Situation, in der eine **Einflussnahme** einer Organisation gegenüber anderen Organisationen oder Individuen existiert – häufig betrifft dies auch digitale „Alltagsprodukte“.
- Dies kann sowohl **positive** als auch **negative** Aspekte haben:
  - Kontrolle über SW-Updates kann Geräte unerwartet unbrauchbar machen.
  - Im Fall eines Diebstahls kann das erwünscht sein.
- Ziel muss es sein, trotz Cyber Dominance eine **souveräne** und **sichere Nutzung** von **Digitaltechnologien** zu ermöglichen.

In Anlehnung: Positionierung des BSI zu Digitaler Souveränität in Zeiten von Cyber Dominance, Claudia Plattner, BSI-Präsidentin, März 2025

Wie ist der Stand der Dinge am Markt?

This quadrant evaluates service providers offering **IaaS solutions** that comply with the **Gaia-X framework** for sovereignty. The majority of the providers in this category are of **European origin** and ensure **data residency** within the EU.

Meenakshi Srivastava

Welche Parameter bestimmen ein Souveränitätsniveau in der Cloud?

Kontrolle über…
- Datenspeicherorte
- Verschlüsselung (int./ext. Key-Store/Nitro & Conf. Computing)
- Zugriffe & Identitätsmgmt.
- Transparenz und unbeeinflussbare Berichtsfunktionen
- Update-Kanäle
- Resilienzfunktionalitäten

Umgang mit…
- (vertraglichen) Zusicherungen der Anbieter
- gesellschaftsrechtlichen Aspekten
- Updates & Service-Identität
- Meta-Daten
- staatlichen Eingriffsmöglichkeiten
- Kosten- und Abrechnungsmodellen
- Komplexität

Wie unterscheiden sich die „besonders“ souveränen Angebote der Hyperscaler und wo liegen Gemeinsamkeiten?

	MSSC MS / Delos*	AWS ESC*	Google - local partnerships
Datensouveränität	in Deutschland gespeichert	wählbar, in Deutschland gespeichert	wählbar (Assured Workloads)
Verschlüsselung	<Keine Angaben>	Nitro-Architektur, int./ext. KMS (selbst/lok. Partner)	int./ext. KMS (beim lokalen Partner)
Meta-Daten	Datendoide „vom BSI kontrolliert“	eigene Abrechnung, eigenes IAM	Admin-Zugriff eingeschränkt
Krisenfall-Autarkie	mittlere Resilienz (2 DC), läuft ohne MS-Konzernmutter (Betrieb & Update)	hohe Resilienz (multi DC), läuft ohne AWS-Konzernmutter (Betrieb & Update)	hohe Resilienz (multi DC), läuft nur in der GCP
Gesellschaftsrecht	eigene Gesellschaft, deutsche Konzernmutter, „unabhängig“ von MS	eigene Gesellschaft, amerikanische Konzernmutter, „unabhängig“ von AWS-weltweit	<Keine Angaben> (ggf. ext. Partner)
Betriebsteam	sicherheitsüberprüftes Personal	EU-Personal, eigenes SOC	kriterienbasiert (Assured Workloads Support)
Services/Updates	identisches Service-Subset, „auditierte und behördenkontrollierte Updates“	identisches Service-Subset inkl. Kontroll-dienste, signierte und automatisierte Updates	alle Services, Assured Workloads-Monitoring
Kundengruppe	öffentliche Verwaltung	alle Kunden/Workloads mit besonders hohen Souveränitätsanforderungen	alle Kunden mit besonders hohen Souveränitätsanforderungen
Weitere Infos	2 DC in D, Anbindung an Behörden-netz, lt. BMI: Übergangslösung M365	eigenständige Ergänzung zur AWS Cloud, 7,8 Mrd. EUR Invest in die ESC, eigene Trust Certificate Gesellschaft	Distributed Cloud (Air-Gapped-Konfiguration); SW Sovereignty via Google Workspace

*) Stand der Planung, tw. vereinfachte Darstellung

Welche Chancen und Risiken werden aktuell am häufigsten diskutiert?

Risiken

Chancen

Datenabfluss
(außerhalb des gewählten Speicherorts)

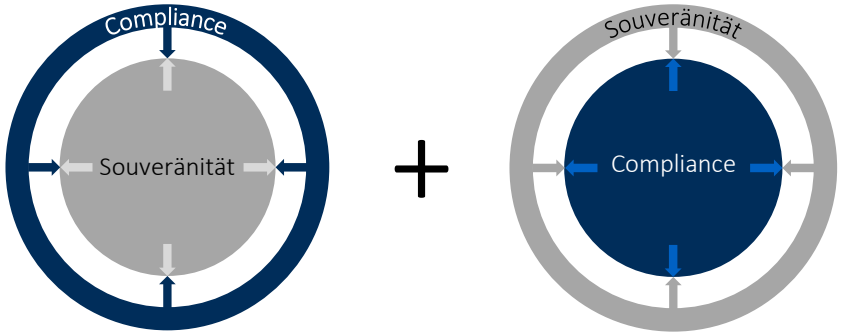
Antwort auf Fachkräftemangel
(Shared Responsibility und in Verbindung mit KI)

Einfluss auf die Betriebsfähigkeit
(Abschalten von Services)

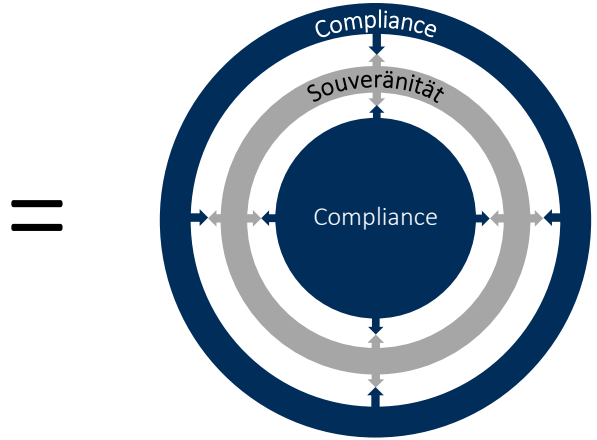
Antwort auf Innovationsdruck
(Fokussierung aufs Wesentliche)

Was verbindet Souveränität und Compliance?

Allgemein: Während **Souveränität Autonomie ermöglicht**, stellt **Compliance** sicher, dass diese Autonomie innerhalb der akzeptierten **rechtlichen, technischen und ethischen Grenzen** ausgeübt wird.



Cloud Computing: Compliance-Standards beinhalten oft Regelungen, die (unter anderem) ein **Mindestmaß an Souveränität** garantieren sollen (z. B. wenn der Compliance-Standard vorschreibt Multi-Cloud-Ansätze zu verfolgen).



Welche Chancen ergeben sich für Compliance-Nachweise in der Cloud?

- **Zeit- und Aufwandsvorteil:** Automatisierung von Compliance-Prozessen
- **Qualitätsvorteil:** Echtzeit-Überwachung (nicht stichtagbezogen) und Reporting (ggf. auch Verhinderung oder automatisierte Gegenmaßnahmen)
- **Auswertung der Überwachungsdaten:** Neben der Erfüllung der Compliance-Anforderungen können weitere Erkenntnisse zu technischen, prozessualen oder organisatorischen Optimierungspotenzialen gewonnen werden.

Wie könnte die Zukunft von Audits angesichts der Automatisierungspotenziale aussehen?

- **Transparenzpotenzial:** Anstatt periodischer Prüfungen könnte die Automatisierung ermöglichen, Audits kontinuierlich und in Echtzeit durchzuführen.
- **Vertrauenspotenzial:** Automatisierung bietet die Möglichkeit zur lückenlosen Nachverfolgung und Protokollierung von Audit-Aktivitäten, was das Vertrauen in die Ergebnisse stärkt.
- **Verbesserungspotenzial:** KI-gestützte Systeme könnten bei der Erkennung von Anomalien, bei der Prognose zukünftiger Risiken und beim Vorschlagen von Korrekturmaßnahmen helfen.
- **Vorbereitungsnotwendigkeit:** Geplante Umstellungen sollten mit den Auditoren frühzeitig besprochen und ggf.
  Nachweise zur Unveränderbarkeit der Protokolle bereitgehalten werden.

Was hilft voranzukommen?

- Die richtigen **Anforderungen** an das **Souveränitätslevel selbst ermitteln** – …„under no circumstances…“ ist nicht immer das richtige, teilweise sogar das unmögliche Level.
- Bei der **Exit-Strategie** den finanziellen Nachteil durch „**abgeschnittene Innovationsspitzen**“ gegen das **Ausfallrisiko** halten.
- Bewertung des **Gesamtrisikos** einer Cloud-Implementierung im Vergleich zu anderen, **nicht cloud-bezogenen Risiken** (z. B. durch Shared Responsibility) durchführen.
- Bedenken, dass auch **Wettbewerbsnachteile** die **Souveränität einschränken** können, weil bestimmte **wirtschaftliche Optionen** dann **nicht** mehr **infrage kommen.**
- Das **Automatisierungspotenzial** für **Compliance-Nachweise** nutzen.

Quelle: AWS Summit 2025 Hamburg 06.06.2025

Ein einfaches Beispiel – hinreichend souverän und compliant

- Fachverfahren zur Verwaltung von Asylunterkünften in einem Landkreis
  - ersetzt mehrere XLS-Lösungen (Versions-problematik) und eine MS Access-DB (Zugriffsproblematik)
  - hilft die knappen Personalressourcen besser auf alle Themen zu verteilen (auch durch direkte Beteiligung der Bürger und Asylantragstellende)
  - Einbindung des Datenschutzbeauftragten von Anfang an
  - Potenzial zur Nutzung in weiteren Landkreisen (weitgehend identische Fachverfahren)

Quellenangaben

- Positionierung des BSI zu Digitaler Souveränität in Zeiten von Cyber Dominance; https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/Digitale_Souveraenitaet_250319.html
- Warum konzentriert sich das BSI nicht auf nationale oder europäische Cloud-Anbieter; https://www.linkedin.com/posts/bsibund_hyperscaler-cloud-activity-7309817999195082753-sjDZ?utm_source=share&utm_medium=member_desktop&rcm=ACoAAA0AWiMBQmvPZ2XD8zXDEWMkB0ZjYkSojzc
- AWS European Sovereign Cloud & AWS Sovereignty Pledge; https://aws.amazon.com/de/compliance/europe-digital-sovereignty/
- https://www.deloscloud.de/index.html - Gemeinsam souverän, die Cloud für den öffentlichen Dienst
- Google Sovereign Cloud, https://cloud.google.com/sovereign-cloud?hl=de
- Studie: Sovereign Cloud 2024, https://www.t-systems.com/de/de/cloud-services/gated-content/studie-sovereign-cloud?wt_mc=ss.de-de.go.MKT_2025_Paid_SEA_Always_On_Cloud.701J5000000946nIAA.Whitepaper-leads.cl.studie-sovereign-cloud-de-tsys_DE_Generic_Cloud_and_Infrastructure-Always-on
- Mit Microsoft in die digitale Abhängigkeit, https://netzpolitik.org/2024/delos-cloud-mit-microsoft-in-die-digitale-abhaengigkeit/
- ISG Provider Lens – Multi Public Cloud Services / Quadrant Report, December 2024
- Built, operated, controlled, and secured in Europe: AWS unveils new sovereign controls and governance structure for the AWS European Sovereign Cloud; AWS 03.06.2025; https://www.aboutamazon.eu/news/aws/built-operated-controlled-and-secured-in-europe-aws-unveils-new-sovereign-controls-and-governance-structure-for-the-aws-european-sovereign-cloud

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com