secunet

Datensouveränität in Europa und Deutschland

Wie Open Source den Kampf um digitale Kontrolle prägt und herausfordert

secunet.com

Executive Summary: Digitale Souveränität durch Open-Source-Cloud-Lösungen

In einer Zeit, in der internationale Anbieter den Cloud-Markt dominieren, sehen sich deutsche Behörden und Unternehmen immer häufiger gezwungen, kritische Daten außerhalb ihrer Kontrolle zu speichern.

Neben Skalierbarkeit und Effizienz rückt dabei die Datensouveränität in den Mittelpunkt. Europäische Organisationen müssen angesichts internationaler Gesetze wie dem US CLOUD Act ihre Daten sicher verwalten, ohne die Anforderungen der DSGVO zu gefährden.

Immer mehr Organisationen setzen dabei auf Open-Source-Technologien, die Flexibilität und Unabhängigkeit garantieren. Der Sovereign Cloud Stack (SCS), entwickelt im Rahmen der GAIA-X-Initiative, bietet eine offene Cloud-Infrastruktur, die höchsten Anforderungen an Sicherheit und Datenschutz gerecht wird und zugleich die Souveränität der Daten garantiert.

Darüber hinaus spielen in Deutschland regulatorische Maßnahmen wie die EVB-IT Cloud und der C5-Standard des BSI eine zentrale Rolle. Sie sorgen für klare rechtliche Rahmenbedingungen und IT-Sicherheitsstandards, die gewährleisten, dass öffentliche Institutionen und Unternehmen souveräne und sichere Cloud-Dienste nutzen können.

Neben den technologischen Herausforderungen proprietärer Cloud-Lösungen wie dem Vendor Lock-in gewinnt auch die politische Einflussnahme von internationalen Technologiekonzernen an Bedeutung. US-Hyperscaler versuchen durch umfangreiche Lobbyarbeit europäische Datenschutzbestimmungen zu beeinflussen, was für europäische Organisationen zusätzliche Risiken mit sich bringt. Die Entscheidung für Open-Source-Lösungen ist daher nicht nur eine Frage der technologischen Unabhängigkeit, sondern auch eine notwendige Maßnahme, um sich vor politischer Einflussnahme und externen Interessen zu schützen.

Diese Entwicklungen sind ein entscheidender Schritt, um die digitale Souveränität Europas und Deutschlands zu stärken und gleichzeitig den sicheren und flexiblen Betrieb von Cloud-Infrastrukturen zu ermöglichen.

Souveräne Cloud-Infrastrukturen für Europa und Deutschland

Die rasante Entwicklung und Nutzung von Cloud-Diensten hat die Art und Weise verändert, wie Unternehmen und Behörden ihre Daten verwalten. Gleichzeitig stellt die Frage der Datensouveränität – also die Kontrolle über die eigenen Daten – eine immer größere Herausforderung dar, insbesondere für europäische Organisationen. Im Rahmen der Datenschutz-Grundverordnung (DSGVO) ist die Einhaltung strenger Datenschutzvorgaben verpflichtend, was viele Unternehmen und Behörden dazu veranlasst, nach Cloud-Lösungen zu suchen, die nicht nur flexibel und kosteneffizient sind, sondern auch die Souveränität über ihre Daten garantieren.

Studien zeigen, dass etwa 92 % der großen Unternehmen in Europa bereits auf Cloud-Dienste angewiesen sind. Dennoch äußern mehr als 60 % dieser Unternehmen Bedenken hinsichtlich der Datensicherheit und Souveränität, was auf den zunehmenden Druck hinweist, sichere und souveräne Cloud-Lösungen zu wählen (Eurostat, 2022). Diese Bedenken verschärfen sich durch den US CLOUD Act, der es US-Behörden ermöglicht, auf Daten zuzugreifen, die von US-Unternehmen verarbeitet werden, selbst wenn diese Daten in Europa gespeichert sind.

Open-Source-Technologien bieten Flexibilität und reduzieren Abhängigkeiten von proprietären Systemen. Weitere Details zu den Vorteilen und Risiken dieser Technologien finden sich im Abschnitt „Vorteile und Kriterien von Open-Source-Lösungen“. Der Einsatz von Open Source minimiert das Risiko eines „Lock-in“-Effekts, bei dem Organisationen an spezifische Anbieter gebunden sind, und sorgt gleichzeitig für die höchste Sicherheit und Anpassungsfähigkeit.

Europäische Cloud-Strategie: Souveränität und Sicherheit in der EU

Die europäische Cloud-Strategie spielt eine zentrale Rolle bei den Bemühungen, die digitale Souveränität in der EU zu gewährleisten. Um die Abhängigkeit von internationalen Cloud-Anbietern zu verringern, setzt Europa auf Initiativen, die für Open-Source-Technologien und europäische Sicherheitsstandards eintreten.

Ein herausragendes Beispiel ist der Sovereign Cloud Stack (SCS), der von der Open Source Business Alliance (OSBA) entwickelt und unterstützt wird. Der SCS stellt eine offene, standardisierte und vollständig auf Open-Source-Technologien basierende Cloud-Infrastruktur dar. Sein Ziel ist es, eine europäische Cloud-Lösung zu schaffen, die höchsten Anforderungen an Sicherheit, Skalierbarkeit und Transparenz gerecht wird, während sie die Souveränität ihrer Nutzer garantiert. Der SCS wird im Rahmen der GAIA-X-Initiative gefördert, die darauf abzielt, ein föderiertes Cloud-Ökosystem aufzubauen, das europäische Datenschutz- und Sicherheitsanforderungen erfüllt. Diese Architektur erlaubt es Unternehmen und öffentlichen Institutionen, eine Cloud-Lösung zu nutzen, die vollständig unter ihrer Kontrolle steht.

Auf EU-Ebene spielt auch das European Cloud Security Scheme (EUCSS) eine wichtige Rolle. Diese Initiative der ENISA (Agentur der Europäischen Union für Cybersicherheit) hat das Ziel, die Sicherheitsanforderungen für Cloud-Dienste innerhalb der EU zu harmonisieren und ein einheitliches Zertifizierungsverfahren zu schaffen. Das EUCSS stärkt das Vertrauen in europäische Cloud-Anbieter und gewährleistet, dass sie die höchsten Sicherheits- und Datenschutzstandards einhalten.

Deutsche Cloud-Strategie: Souveräne Cloud und regulatorische Unterstützung

Auch in Deutschland haben sich wichtige regulatorische Rahmenbedingungen und Standards entwickelt, die die Beschaffung und Nutzung sicherer Cloud-Lösungen vorantreiben. Eine zentrale Rolle spielt hierbei die EVB-IT Cloud, eine Einkaufsrichtlinie, die den rechtlichen Rahmen für die Beschaffung von Cloud-Diensten durch die öffentliche Hand definiert. Diese Richtlinie stellt sicher, dass Cloud-Dienste den hohen Anforderungen an Datenschutz und Verfügbarkeit entsprechen. Insbesondere werden Regelungen zur Datensicherheit, zur Vertragsgestaltung und zur Haftung festgelegt, die sicherstellen, dass öffentliche Institutionen ihre Souveränität über ihre Daten bewahren.

Zusätzlich ist der C5-Standard (Cloud Computing Compliance Controls Catalogue) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ein wichtiger Sicherheitsstandard. Er bietet Cloud-Anbietern eine Anleitung, wie sie ihre Dienste im Einklang mit den IT-Grundschutzvorgaben des BSI sichern können. Der C5-Standard umfasst Maßnahmen zur Datenverschlüsselung, zum Schutz vor Cyberangriffen und zur Sicherstellung der Datenverfügbarkeit und -integrität.

Diese regulatorischen Maßnahmen und Sicherheitsstandards tragen maßgeblich dazu bei, dass deutsche Unternehmen und öffentliche Institutionen eine souveräne Cloud-Infrastruktur nutzen können, die sowohl sicher als auch datenschutzkonform ist.

Zusammengefasst:

Souveräne Cloud-Infrastrukturen für Europa und Deutschland

Initiativen wie der Sovereign Cloud Stack, die EVB-IT Cloud, der C5-Standard und das EUCSS bilden zusammen eine solide Grundlage für eine sichere und transparente Cloud-Strategie in Europa und Deutschland. Sie ermöglichen es Unternehmen und Institutionen, die Kontrolle über ihre Daten zu behalten, Abhängigkeiten von internationalen Anbietern zu vermeiden und eine zukunftssichere Cloud-Infrastruktur aufzubauen. Sowohl auf europäischer als auch auf nationaler Ebene fördern diese Initiativen die digitale Souveränität und sorgen für eine nachhaltige, sichere und flexible Nutzung von Cloud-Diensten.

Die Herausforderungen von proprietären Cloud-Lösungen

Proprietäre Cloud-Anbieter, vor allem die großen US-basierten Unternehmen wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud, dominieren den globalen Cloud-Markt. Diese Unternehmen bieten umfassende Services, die technologisch ausgereift sind und eine Vielzahl an Funktionalitäten bieten. Doch diese Marktdominanz bringt einige erhebliche Risiken mit sich.

Wichtige Prinzipien für echte Cloud Souveränität

Um diese Herausforderungen zu meistern, müssen Cloud-Lösungen bestimmte Kernprinzipien erfüllen, die die Grundlage für echt Datensouveränität bilden. Diese Prinzipien umfassen:

- **Betriebshoheit:**
  Unternehmen und Organisationen müssen jederzeit volle Transparenz und Kontrolle über die betrieblichen Abläufe der genutzten Cloud-Lösung haben. Dies bedeutet, dass Kunden detaillierten Einblick in die Sicherheitsprotokolle, den Betrieb und die Infrastruktur haben und notwendige Änderungen eigenständig initiieren können. Eine Einschränkung dieser Kontrolle durch externe Anbieter oder Drittparteien muss ausgeschlossen sein. Im Vergleich zu US-Lösungen, bei denen der Zugriff oft eingeschränkt ist, bieten souveräne Cloud-Lösungen diese Transparenz und Kontrollmöglichkeiten von Beginn an.

- **Technologische Souveränität:**
  Eine wirklich souveräne Cloud-Lösung bietet Unternehmen die Möglichkeit, ihre technologische Basis selbst zu verwalten und zu kontrollieren. Dabei sollte die Wahl der genutzten Technologien offen und flexibel sein, sodass Organisationen nicht in Abhängigkeit von bestimmten Anbietern geraten. Offene Standards und Open-Source-Lösungen spielen hier eine zentrale Rolle, da sie sicherstellen, dass Systeme anpassbar und interoperabel bleiben. Dies schützt vor langfristigen Kostenfallen und technischen „Lock-ins“, die bei proprietären Systemen oft auftreten.

- **Datenhoheit:**
  Organisationen müssen sicherstellen, dass ihre Daten stets den rechtlichen Rahmenbedingungen ihres Heimatlandes unterliegen. Dies bedeutet, dass die Speicherung und Verarbeitung von Daten in Übereinstimmung mit der DSGVO und anderen lokalen Gesetzen erfolgen muss. Die Einhaltung dieser Gesetze ist nur garantiert, wenn Daten nicht durch ausländische Gesetzgebung, wie den US CLOUD Act, bedroht werden. Eine souveräne Cloud-Lösung ist daher vollständig in Europa verankert und gewährleistet, dass Daten in europäischen Rechenzentren verarbeitet werden.

- **Wirtschaftliche Unabhängigkeit:**
  Die Nutzung von Open-Source-Technologien ermöglicht Unternehmen, sich von marktbeherrschenden Cloud-Anbietern zu lösen und teure Lizenzgebühren zu vermeiden. Dadurch bleiben Investitionen und technologische Kompetenzen im eigenen Land, was die lokale Innovationskraft stärkt und neue Arbeitsplätze schafft. Zudem bietet Open Source Planungssicherheit, da Unternehmen und Organisationen nicht von plötzlichen Änderungen im Lizenzmodell proprietärer Anbieter betroffen sind. Diese Unabhängigkeit unterstützt eine stabile, langfristig planbare digitale Infrastruktur und stärkt gleichzeitig die wirtschaftliche Widerstandsfähigkeit und nationale Souveränität.

Die souveräne Cloud: Kriterien für digitale Souveränität und Sicherheit

Digitale Souveränität ist für Deutschland und die EU von zentraler Bedeutung. Eine „souveräne Cloud“ zeichnet sich dadurch aus, dass sie den strengen Anforderungen an Datenschutz, Datensicherheit und die vollständige Kontrolle über die Datenverarbeitung gerecht wird. In Deutschland wurden dafür klare Anforderungen definiert, die durch das Positionspapier der Datenschutzkonferenz (DSK) der Länder und des Bundes gestützt werden. Diese Kriterien sind in MUSS- und SOLL-Kriterien unterteilt.

Die MUSS-Kriterien stellen sicher, dass:

- eine klare Dokumentation vor Vertragsschluss vorliegt und Anbieter nur auf Weisung des Kunden Daten verarbeiten.
- keine Daten in Drittländer ohne ausreichenden Schutz übertragen werden.
- alle Datenverarbeitungen klar getrennt und nachvollziehbar sind.

Die **SOLL**-Kriterien bieten zusätzliche Empfehlungen, um eine souveräne Cloud noch transparenter zu gestalten. Sie beinhalten unter anderem die Nutzung von Open-Source-Technologien, die Unterstützung offener Standards und die Möglichkeit zur Kombinierbarkeit verschiedener Cloud-Dienste.

Diese Anforderungen bilden die Grundlage dafür, dass europäische Unternehmen und Behörden ihre Daten unter vollständiger Kontrolle behalten und eine maximale Transparenz und Sicherheit gewährleisten.

Vorteile und Kriterien von Open-Source-Lösungen für Datensouveränität

Open-Source-Lösungen bieten zahlreiche Vorteile, die für die Sicherstellung der Datensouveränität entscheidend sind. Sie ermöglichen es Unternehmen und öffentlichen Institutionen, die Kontrolle über ihre Daten zu behalten, ohne von proprietären Anbietern abhängig zu sein. Gleichzeitig erfüllen sie wichtige Kriterien, die für eine souveräne Cloud-Lösung notwendig sind.

1. Flexibilität und Unabhängigkeit

Open-Source-Technologien ermöglichen es Organisationen, ihre Cloud-Infrastruktur individuell anzupassen und weiterzuentwickeln, ohne von einem bestimmten Anbieter abhängig zu sein. Durch den Einsatz von offenen Standards wird die Gefahr des Vendor-Lock-ins minimiert, was die langfristige Planungssicherheit erhöht.

2. Transparenz und Sicherheit

Ein zentraler Vorteil von Open-Source-Lösungen ist die vollständige Transparenz. Da der Quellcode offen einsehbar ist, können Sicherheitslücken frühzeitig erkannt und geschlossen werden. Zudem ermöglichen Open-Source-Technologien unabhängige Prüfungen, was die Vertrauenswürdigkeit erhöht. Diese Transparenz steht im Einklang mit den Anforderungen der Datenschutz-Grundverordnung (DSGVO), die eine sorgfältige Kontrolle und Verarbeitung von Daten verlangt.

3. Wirtschaftliche Unabhängigkeit und Kosteneffizienz

Durch den Verzicht auf Lizenzgebühren und proprietäre Technologien können Unternehmen Kosten einsparen und ihre Ressourcen besser nutzen. Gleichzeitig fördert die Verwendung von Open-Source-Lösungen den Aufbau technologischer Kompetenz im eigenen Land, was die wirtschaftliche Unabhängigkeit und die Stärkung der nationalen Innovationskraft unterstützt.

4. Kriterien für Souveränität und Sicherheit

Für eine souveräne Cloud-Lösung müssen bestimmte Kriterien erfüllt werden, die über die technologischen Vorteile hinausgehen. Dazu zählen die Möglichkeit der Datenhoheit, die Einhaltung von DSGVO-Vorgaben, der Schutz vor Zugriffen durch Dritte und die Sicherstellung der Datenverarbeitung innerhalb der EU. Open-Source-Lösungen erfüllen diese Anforderungen, da sie eine unabhängige Kontrolle und Anpassbarkeit ermöglichen.

5. Nachhaltigkeit und Zukunftsfähigkeit

Ein weiterer wichtiger Aspekt von Open-Source-Lösungen ist die Nachhaltigkeit. Da sie auf offenen Standards basieren, sind sie zukunftssicher und anpassbar an neue Technologien und Anforderungen. Dies ermöglicht eine langfristige Weiterentwicklung der Infrastruktur, ohne dass teure Migrationsprozesse erforderlich werden.

Sicherheitslösungen in Open-Source-Clouds

Open-Source-Technologien bieten eine Vielzahl von Sicherheitslösungen, die den Schutz von Daten in der Cloud gewährleisten. Durch Georedundanz wird sichergestellt, dass Daten in mehreren Rechenzentren innerhalb der EU verteilt und geschützt werden. Dies erhöht die Verfügbarkeit und sichert die Daten auch bei regionalen Ausfällen. Zudem ermöglicht Confidential Computing die Verschlüsselung von Daten während der Verarbeitung, wodurch ein durchgängiger Schutz von sensiblen Informationen gewährleistet wird. Open Source bietet damit ein hohes Maß an Transparenz und Kontrolle über die implementierten Sicherheitsprotokolle.

Exit-Strategien: Sicherer Anbieterwechsel ohne Hindernisse

Ein zentraler Aspekt der digitalen Souveränität ist die Fähigkeit, jederzeit und ohne große Hindernisse die Kontrolle über Daten und IT-Infrastrukturen zu behalten. Um dies zu gewährleisten, müssen Exit-Strategien von Beginn an in die Cloud-Strategie einbezogen werden. Dies ist besonders wichtig, um auf geänderte Rahmenbedingungen oder Leistungsdefizite des Cloud-Anbieters flexibel reagieren zu können, ohne von einem einzelnen Anbieter abhängig zu sein – eine Herausforderung, die mit proprietären Lösungen oft schwer zu bewältigen ist.

Die Nutzung von Open-Source-Technologien und offenen Standards spielt eine entscheidende Rolle dabei, langfristige Unabhängigkeit zu garantieren. Offene Schnittstellen und standardisierte Datenformate ermöglichen einen einfachen Wechsel des Cloud-Anbieters, ohne dass hohe Kosten oder technische Hürden entstehen. Damit können Behörden und Unternehmen sicherstellen, dass sie ihre digitale Souveränität auch bei einem Anbieterwechsel bewahren.

Mögliche Gründe für einen Wechsel des Cloud-Anbieters können sein:

- Nichterfüllung neuer Compliance-Anforderungen durch den Anbieter
- Unverhältnismäßige Kostensteigerungen ohne nachvollziehbare Begründung
- Sicherheitsmängel, wie z. B. fehlende Datensicherheit oder unzureichende Verschlüsselungstechnologien
- Technologische Rückständigkeit, die zu Inkompatibilitäten mit neuen Anforderungen führt
- Eingeschränkte Datenverfügbarkeit oder wiederholte Serviceausfälle

Indem Open-Source-Lösungen in die Cloud-Strategie integriert werden, schaffen Unternehmen und Behörden die Grundlage für eine zukunftssichere und flexible IT-Landschaft. Diese Technologien bieten nicht nur die Möglichkeit, jederzeit einen Wechsel des Anbieters vorzunehmen, sondern auch volle Transparenz und Kontrolle über die Datenverarbeitung. Standardisierte Datenformate und -schnittstellen erleichtern dabei den Anbieterwechsel erheblich und stellen sicher, dass die Datensouveränität auch im Übergang erhalten bleibt.

Handlungsempfehlungen: Schritte zur Einführung von Open-Source-Cloud-Lösungen

Die Einführung von Open-Source-Cloud-Lösungen erfordert eine umfassende Planung und einen strukturierten Ansatz, um sicherzustellen, dass Unternehmen und Behörden alle Vorteile der Datensouveränität nutzen können. Die folgenden Schritte bieten einen umfassenden Leitfaden, wie der Umstieg zu einer souveränen Cloud-Umgebung erfolgreich umgesetzt werden kann:

1. Analyse der bestehenden Cloud-Infrastruktur

Bevor ein Wechsel zu einer Open-Source-Cloud erfolgt, ist eine vollständige Analyse der aktuellen IT- und Cloud-Infrastruktur erforderlich. Diese umfasst:

- Bewertung der aktuellen Abhängigkeiten von proprietären Anbietern: Systeme oder Anwendungen, die stark auf spezifische Cloud-Anbieter angewiesen sind, sollten identifiziert werden.
- Überprüfung der Sicherheits- und Compliance-Anforderungen: Sicherzustellen ist, dass die neue Infrastruktur alle regulatorischen Anforderungen erfüllt, insbesondere die DSGVO. Diese Analyse hilft, potenzielle Schwachstellen und Herausforderungen frühzeitig zu erkennen.
- Risikomanagement: Eine Strategie zur Risikominimierung während des Übergangs ist entscheidend, um die Auswirkungen auf betriebswichtige Prozesse zu reduzieren.

2. Auswahl der geeigneten Open-Source-Technologien

Open-Source-Technologien wie Kubernetes, OpenStack oder Ceph bieten eine Vielzahl von Möglichkeiten zur Implementierung souveräner Cloud-Lösungen. Die passende Lösung für die jeweilige Organisation wird durch folgende Maßnahmen bestimmt:

- Definieren technischer Anforderungen: Die gewählte Technologie muss die spezifischen Anforderungen der Anwendungen und Arbeitslasten erfüllen.
- Sicherstellung von Kombinierbarkeit und Modularität: Modularität der Open-Source-Lösungen ermöglicht eine flexible Integration und Anpassung an zukünftige Entwicklungen.

3. Durchführung eines Pilotprojekts

Vor dem umfassenden Einsatz ist die Durchführung eines Pilotprojekts ratsam, um die Open-Source-Technologien im kleineren Rahmen zu testen. Ein solches Pilotprojekt bietet Vorteile wie:

- Testen der Migrationsstrategie: Die technischen und betrieblichen Herausforderungen der Migration zu Open-Source-Technologien können präziser bewertet werden.
- Evaluierung von Performance und Sicherheit: Die Leistung, Skalierbarkeit und Sicherheit der Lösung wird unter realen Bedingungen geprüft.
- Schulung der IT-Teams: Diese Phase dient der Vorbereitung der IT-Teams auf den Betrieb der neuen Umgebung, inklusive Schulungen und Trainings für die Verwaltung und Nutzung von Open-Source-Technologien.

4. Schrittweise Migration und Übergang

Eine schrittweise Migration von proprietären Cloud-Lösungen zu Open-Source-Technologien minimiert Risiken und reduziert Betriebsstörungen. Dabei sind folgende Punkte zu beachten:

- Priorisierung der Anwendungen: Der Übergang sollte mit weniger kritischen Anwendungen beginnen, basierend auf den Erkenntnissen aus dem Pilotprojekt.
- Datenmigration und -sicherung: Eine robuste Strategie für die Datenmigration sowie Backup-Lösungen sind notwendig, um Datenverlust zu vermeiden.
- Anpassung der Governance-Prozesse: Die bestehenden Governance- und Kontrollprozesse sind an die Anforderungen der Open-Source-Umgebung anzupassen, um gesetzliche und sicherheitsrelevante Vorgaben langfristig einzuhalten.

5. Sicherstellung von Sicherheit und Compliance

Durch Open-Source-Lösungen besteht die Möglichkeit, Sicherheitsmaßnahmen flexibel anzupassen. Dabei ist zu beachten:

- Regelmäßige Sicherheitsüberprüfungen: Kontinuierliche Penetrationstests und Sicherheitsanalysen tragen dazu bei, Schwachstellen frühzeitig zu identifizieren und zu beheben.
- Einsatz von Verschlüsselungstechnologien: Verschlüsselung von Daten während der Übertragung und im Ruhezustand ist essenziell. Technologien wie Confidential Computing bieten eine zusätzliche Sicherheitsebene.
- Überwachung und Reporting: Monitoring- und Reporting-Mechanismen gewährleisten, dass alle Aktivitäten innerhalb der Open-Source-Infrastruktur jederzeit nachvollziehbar und sicher bleiben.

6. Entwicklung einer langfristigen IT-Strategie

Der Wechsel zu Open-Source-Technologien ist als langfristige Strategie zu verstehen, die Flexibilität, Sicherheit und Unabhängigkeit von Anbietern sicherstellt. Dies umfasst:

- Entwicklung einer klaren Roadmap: Eine Roadmap dient der schrittweisen Migration und dem Ausbau der Open-Source-Infrastruktur.
- Partnerschaften mit Open-Source-Communities: Die Vorteile der Open-Source-Communitys fördern Innovation und Weiterentwicklung; eine aktive Beteiligung an der Open-Source-Entwicklung wird in Erwägung gezogen.
- Sicherstellung der Zukunftsfähigkeit: Die kontinuierliche Anpassung und Weiterentwicklung der Open-Source-Infrastruktur sichert die Zukunftsfähigkeit der IT-Landschaft.

7. Zusammenarbeit mit externen Dienstleistern

Für komplexe Implementierungen kann die Zusammenarbeit mit spezialisierten externen Dienstleistern von Vorteil sein. Diese bieten:

- Kommerzielle Unterstützung: Professioneller Support durch Dienstleister, die auf Open-Source-Technologien spezialisiert sind, kann den Umstellungsprozess vereinfachen.
- Beratung und Expertise: Externe Berater unterstützen bei der Auswahl der besten Lösungen und steigern die Effizienz der Implementierung.

8. Planung einer Exit-Strategie für langfristige digitale Souveränität

Zur Sicherung der digitalen Souveränität wird eine Exit-Strategie empfohlen. Open-Source-Technologien erleichtern durch ihre Flexibilität den Wechsel zu einem anderen Cloud-Anbieter, ohne hohe Kosten oder technische Hürden. Zu berücksichtigen sind:

- **Gründe für einen Anbieterwechsel:** Steigende Kosten, fehlende Compliance, Sicherheitsmängel oder technologischer Rückstand könnten einen Wechsel notwendig machen.
- **Einsatz offener Standards:** Offene Datenformate und Schnittstellen in Open-Source-Lösungen vereinfachen den Anbieterwechsel und minimieren potenzielle Ausfallzeiten.
- **Vertragliche Absicherung:** Klare Regelungen für Datenexport, -rückgabe und -löschung in den Verträgen gewährleisten einen reibungslosen Übergang zu einem neuen Anbieter.

Maßnahmen und Zeitschiene

Dieser Plan beschreibt die kurz-, mittel- und langfristigen Maßnahmen zur Migration und Implementierung von Open-Source-Cloud-Lösungen. Ziel ist es, eine flexible, sichere und nachhaltige Cloud-Infrastruktur zu schaffen, die den Anforderungen der Organisation gerecht wird.

Kurzfristige Maßnahmen (0–6 Monate)

Diese Phase konzentriert sich auf die Vorbereitung der IT-Landschaft für die Migration zu Open-Source-Cloud-Lösungen.

Maßnahme	Dauer	Beschreibung
Analyse der bestehenden Cloud-Infrastruktur	1–2 Monate	Analysieren Sie die vorhandene IT- und Cloud-Infrastruktur, um Abhängigkeiten und Compliance-Standards zu identifizieren. Sicherheits- und Compliance-Prüfungen sowie Risikomanagement sind eingeschlossen.
Auswahl geeigneter Open-Source-Technologien	2–3 Monate	Bestimmen Sie passende Open-Source-Lösungen (z. B. Kubernetes, OpenStack), die den Anforderungen der Organisation entsprechen. Die Auswahl sollte auf der Analyse der Infrastruktur basieren.
Erstellung eines Pilotprojekts	1–2 Monate (nach Technologiewahl)	Definieren Sie ein Pilotprojekt mit klaren Zielen, um die Migration zu Open-Source-Technologien im kleinen Maßstab zu evaluieren und das IT-Team vorzubereiten.

Mittelfristige Maßnahmen (6–12 Monate)

Diese Phase umfasst die ersten Schritte der Migration zu Open-Source-Cloud-Lösungen und die Sicherstellung der Governance.

Maßnahme	Dauer	Beschreibung
Schrittweise Migration und Übergang	6–12 Monate	Migrieren Sie weniger kritische Anwendungen, um Risiken zu minimieren. Implementieren Sie Backup-Lösungen und Datenmigrationsstrategien, um Datenverluste zu vermeiden.
Anpassung der Governance-Prozesse	3–4 Monate	Entwickeln Sie Governance-Prozesse, die auf die Anforderungen der Open-Source-Cloud-Lösung abgestimmt sind, um Datenschutzkonformität sicherzustellen.
Sicherstellung von Sicherheit und Compliance	Ab Monat 6, kontinuierlich	Führen Sie Penetrationstests und Sicherheitsüberprüfungen durch. Nutzen Sie Verschlüsselung und Monitoring zur Sicherung der Infrastruktur.

Langfristige Maßnahmen (ab 12 Monaten)

Diese Maßnahmen stellen sicher, dass die Open-Source-Cloud-Lösung nachhaltig bleibt und zukünftigen Anforderungen gerecht wird.

Maßnahme	Dauer	Beschreibung
Entwicklung einer langfristigen IT-Strategie	12–18 Monate	Erarbeiten Sie eine Roadmap für den Ausbau der Cloud-Umgebung. Diese Strategie sollte eine regelmäßige Überprüfung der IT-Landschaft vorsehen, um Flexibilität und Sicherheit zu gewährleisten.
Partnerschaften mit Open-Source-Communities	Ab 12 Monaten, kontinuierlich	Arbeiten Sie mit Open-Source-Communities zusammen, um die Weiterentwicklung der Cloud-Lösungen zu unterstützen und das technische Know-how des IT-Teams zu fördern.
Planung einer Exit-Strategie	Ab 12 Monaten	Implementieren Sie eine Exit-Strategie zur Sicherstellung der Flexibilität für Anbieterwechsel, einschließlich offener Standards und Schnittstellen für nahtlosen Datenexport.

Do‘s and Don‘ts für eine erfolgreiche Migration

Um die Migration zu einer Open-Source-Cloud erfolgreich zu gestalten, sollten bestimmte bewährte Praktiken beachtet und häufige Fehler vermieden werden. Nachfolgend finden Sie eine Liste der wichtigsten Do‘s and Don‘ts für eine schrittweise und sichere Umsetzung:

Do‘s:

- Schrittweise vorgehen: Beginnen Sie mit weniger kritischen Anwendungen, um Risiken zu minimieren.
- Regelmäßige Tests durchführen: Führen Sie kontinuierliche Tests während der Migration durch, um Probleme frühzeitig zu identifizieren.
- Transparente Kommunikation: Informieren Sie alle Beteiligten (IT-Teams, Management, Endnutzer) über die geplanten Schritte und mögliche Auswirkungen.
- Daten sicher migrieren: Implementieren Sie robuste Backup-Strategien, um sicherzustellen, dass keine Daten verloren gehen.
- Fachwissen nutzen: Ziehen Sie externe Experten hinzu, wenn interne Kenntnisse nicht ausreichen, um die Migration erfolgreich umzusetzen.

Don‘ts:

- Alle Anwendungen auf einmal migrieren: Vermeiden Sie die gleichzeitige Migration aller Anwendungen, um unvorhersehbare Risiken und Störungen zu minimieren.
- Unzureichende Sicherheitsmaßnahmen: Verzichten Sie nicht auf regelmäßige Sicherheitsprüfungen und Penetrationstests während der Migration.
- Fehlende Dokumentation: Vermeiden Sie es, die Migration und die Anpassungen nicht ausreichend zu dokumentieren – dies erschwert spätere Anpassungen und Fehlerbehebungen.
- Komplexität unterschätzen: Die Migration von Cloud-Lösungen ist ein komplexer Prozess. Vermeiden Sie eine unzureichende Planung und Risikobewertung.
- Unklare Verantwortlichkeiten: Sorgen Sie dafür, dass Verantwortlichkeiten klar definiert sind, um Verzögerungen und Missverständnisse zu vermeiden.

Erfolgsfaktoren und Best Practices

Phasenweise Migration zur Risikominimierung

Viele europäische Unternehmen und Behörden betonen, dass die phasenweise Migration zu einer souveränen Cloud-Lösung wesentlich zur Risikominimierung beiträgt. Ein stufenweiser Übergang ermöglicht es, während des Prozesses flexibel zu bleiben und bei Komplikationen Anpassungen vorzunehmen. Zudem wird immer wieder auf die Wichtigkeit einer hybriden Infrastruktur hingewiesen, bei der bestehende Systeme und neue Cloud-Komponenten parallel betrieben werden. Diese Kombination bietet die Möglichkeit, Risiken zu minimieren und neue Lösungen unter realen Bedingungen zu testen, bevor eine vollständige Migration erfolgt.

Sicherstellung der Datensouveränität

Ein zentraler Aspekt der Cloud-Migration in Europa ist die Sicherstellung der Datensouveränität. Viele Organisationen setzen auf Maßnahmen zur Risikominderung, indem sie zusätzliche Sicherheitsprotokolle implementieren, die speziell auf europäische Anforderungen und die DSGVO abgestimmt sind. Die Gewährleistung der Sicherheit und Compliance während und nach der Migration ist entscheidend, um die volle Kontrolle über die Datenverarbeitung zu behalten.

Change Management als Erfolgsfaktor

Zusätzlich betonen Entscheidungsträger die Relevanz von Change Management als kritischen Erfolgsfaktor. Um Widerstände zu minimieren und eine reibungslose Übernahme der neuen Infrastruktur zu gewährleisten, sind Schulungsmaßnahmen für Mitarbeiter und die klare Kommunikation der Vorteile von entscheidender Bedeutung. Durch das Einbeziehen der Mitarbeitenden kann sichergestellt werden, dass die gesamte Organisation bereit ist, die neuen Technologien zu adaptieren und zu nutzen. Diese Erfahrungen aus erfolgreichen Migrationsprojekten unterstreichen die Bedeutung einer strategischen Planung, die sowohl technische als auch organisatorische Aspekte berücksichtigt.

Rechtliche Rahmenbedingungen und regulatorische Anforderungen bei Cloud-Diensten

Die Nutzung von Cloud-Diensten in Europa unterliegt strengen Anforderungen, insbesondere im Bereich Datensouveränität und Datenschutz. Unternehmen und Behörden müssen sicherstellen, dass ihre Cloud-Infrastruktur den nationalen und EU-weiten Regularien entspricht. Die wichtigsten Rahmenbedingungen sind die Datenschutz-Grundverordnung (DSGVO), die EVB-IT Cloud sowie der C5-Standard des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Anwendungsbereiche der Regulierungen

- **DSGVO:** Gilt für alle Organisationen, die personenbezogene Daten von EU-Bürgern verarbeiten. Sie stellt sicher, dass Daten innerhalb der EU verarbeitet werden und der Datenschutz durch klare Richtlinien gewährleistet ist.
- **EVB-IT Cloud:** Regelt die Beschaffung von Cloud-Diensten durch öffentliche Institutionen und stellt sicher, dass Anforderungen an Datenschutz, Verfügbarkeit und rechtliche Sicherheit erfüllt sind.
- **C5-Standard des BSI:** Bietet Cloud-Anbietern Orientierung für IT-Sicherheit, einschließlich Maßnahmen zur Verschlüsselung, Schutz vor Cyberangriffen und Sicherstellung der Datenverfügbarkeit.

Übersichtstabelle der rechtlichen Anforderungen

Regulierungen	Anwendungsbereich	Hauptanforderungen	Gilt für
DSGVO	Datenschutz personenbezogener Daten	Verarbeitung innerhalb der EU, klare Richtlinien zur Datenverarbeitung	Alle Organisationen
EVB-IT Cloud	Öffentliche Verwaltung	Anforderungen an Datenschutz, Verfügbarkeit und rechtliche Sicherheit	Öffentliche Institutionen
C5-Standard (BSI)	IT-Sicherheit von Cloud-Diensten	Maßnahmen zur Verschlüsselung, Schutz vor Cyberangriffen, Sicherstellung der Datenverfügbarkeit	Cloud-Anbieter (für alle Nutzer)

Checkliste für rechtliche Compliance

- **DSGVO-Konformität:**
  - Werden personenbezogene Daten nur innerhalb der EU verarbeitet?
  - Gibt es eine Dokumentation vor Vertragsabschluss?
- **EVB-IT Cloud:**
  - Sind vertragliche Verpflichtungen zu Datensicherheit und Verfügbarkeit klar definiert?
- **C5-Standard:**
  - Werden alle relevanten Sicherheitsmaßnahmen umgesetzt?

Risiken und Sanktionen bei Nichteinhaltung

Die Nichteinhaltung der Anforderungen, insbesondere der DSGVO, kann erhebliche Konsequenzen nach sich ziehen. Unternehmen drohen hohe Geldstrafen von bis zu 4 % des Jahresumsatzes. Zudem kann die Missachtung des C5-Standards dazu führen, dass Cloud-Dienste als unsicher gelten und das Vertrauen der Kunden verloren geht.

Praxisnahe Fallstudien: Erfolgreicher Einsatz von Open-Source-Cloud-Lösungen

In diesem Abschnitt werden konkrete Beispiele aus der Praxis präsentiert, die den erfolgreichen Einsatz von Open-Source-Cloud-Lösungen veranschaulichen. Dabei wird gezeigt, wie Organisationen durch den Einsatz dieser Technologien ihre Datensouveränität und Sicherheit erhöht haben.

1. Europäische Kommission und OpenStack

Die Europäische Kommission hat OpenStack genutzt, um ihre digitale Transformation zu beschleunigen und die Abhängigkeit von proprietären Cloud-Anbietern zu verringern. Durch die Implementierung von OpenStack konnte die Kommission eine private Cloud entwickeln, die unter ihrer vollständigen Kontrolle steht und gleichzeitig den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entspricht. Diese Lösung half der Kommission, ihre IT-Kosten zu senken und gleichzeitig Effizienz und Skalierbarkeit zu verbessern.
Quelle: OpenStack User Story – European Commission

2. CERN und Kubernetes

Das CERN, eine der größten Forschungsorganisationen in Europa, setzt eine Kombination aus Kubernetes und OpenStack ein, um die enormen Datenmengen aus der Teilchenphysik zu verwalten. Diese Infrastruktur ermöglicht es den Forschern, flexibel zwischen Cloud- und On-Premise-Lösungen zu wechseln. Diese Technologie stellt sicher, dass die Daten souverän verwaltet werden und die europäischen Datenschutzrichtlinien eingehalten werden.
Quelle: Kubernetes at CERN - CNCF Case Study

3. Deutsche Telekom und die Open Telekom Cloud

Die Deutsche Telekom hat mit der Open Telekom Cloud eine eigene Cloud-Plattform entwickelt, die auf Open-Source-Technologien basiert, insbesondere OpenStack. Diese Cloud-Plattform richtet sich an europäische Unternehmen und erfüllt die Anforderungen der DSGVO. Ein wesentlicher Vorteil besteht darin, dass die Cloud vollständig in Europa gehostet wird, was Unternehmen vor dem Zugriff durch außereuropäische Behörden schützt und die Abhängigkeit von internationalen Cloud-Anbietern reduziert.
Quelle: Deutsche Telekom – Open Telekom Cloud

4. ING Bank und Open Source

Die ING Bank nutzt Open-Source-Technologien wie Kubernetes und Docker, um ihre digitale Infrastruktur zu modernisieren und flexibler auf Marktveränderungen zu reagieren. Die Bank konnte ihre Abhängigkeit von proprietären Cloud-Anbietern verringern und eine DSGVO-konforme Lösung implementieren, die die Sicherheit und den Datenschutz ihrer Kunden gewährleistet.
Quelle: ING Kubernetes Case Study – CNCF

5. BBC und OpenStack

Die BBC hat OpenStack implementiert, um ihre digitale Medienplattform für Streaming-Dienste zu betreiben. Durch die Nutzung dieser flexiblen und skalierbaren Lösung konnte die BBC ihre Abhängigkeit von kommerziellen Cloud-Anbietern reduzieren und die volle Kontrolle über ihre Inhalte und Daten behalten. Diese Infrastruktur erfüllt die Anforderungen an Datenschutz und Souveränität.
Quelle: OpenStack BBC Case Study

6. GAIA-X: Europas Antwort auf digitale Souveränität

Das GAIA-X-Projekt, initiiert von Deutschland und Frankreich, zielt darauf ab, eine föderierte Cloud-Infrastruktur aufzubauen, die europäische Standards für Datensouveränität, Interoperabilität und Sicherheit gewährleistet. GAIA-X ist ein entscheidender Schritt, um europäische Unternehmen vor der Abhängigkeit von großen US-Cloud-Anbietern zu schützen und eine offene, transparente Cloud-Umgebung zu schaffen.
Quelle: Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study

7. CloudFerro und CREODIAS: Souveräne Cloud für Erdbeobachtungsdaten

CloudFerro betreibt die Plattform CREODIAS, die von der Europäischen Weltraumorganisation (ESA) und der Europäischen Kommission genutzt wird. CREODIAS basiert auf Open-Source-Technologien und bietet eine souveräne Cloud-Umgebung, die innerhalb Europas gehostet wird, um Daten aus der Erdbeobachtung sicher zu verarbeiten und zu speichern. Diese Plattform ermöglicht es Dritten, eigene Anwendungen zu entwickeln und die Datensouveränität zu gewährleisten.
Quelle: CloudFerro's CREODIAS platform

Fazit: Open Source als Schlüssel zur europäischen Datensouveränität

Die Zukunft der Cloud für europäische Organisationen liegt in Open-Source-Technologien. Sie bieten die notwendige Flexibilität, Unabhängigkeit und Sicherheit, die Unternehmen und Behörden benötigen, um in einer zunehmend digitalisierten Welt zu bestehen. Open Source ermöglicht nicht nur den Schutz der Daten vor externem Zugriff, sondern bietet auch langfristige wirtschaftliche und technologische Vorteile. Durch den Verzicht auf proprietäre Systeme und die Nutzung offener Standards können Organisationen sicherstellen, dass sie die volle Kontrolle über ihre Daten und Systeme behalten – ein entscheidender Faktor für echte Datensouveränität in Europa.

Cloud-Lösungen auf Basis von Open Source sind daher nicht nur eine kosteneffiziente Alternative zu proprietären Anbietern, sondern auch die ideale Lösung für alle Organisationen, die langfristige Kontrolle und Flexibilität in einer sicheren digitalen Umgebung suchen.

Mit secunet zur digitalen Souveränität: Unabhängige und sichere Cloud-Lösungen

Die Sicherstellung der Datensouveränität ist essenziell für die langfristige digitale Unabhängigkeit Ihres Unternehmens oder Ihrer Institution. Mit Open-Source-Technologien und einem klaren Fokus auf flexible, transparente und sichere Cloud-Lösungen schaffen Sie eine nachhaltige IT-Infrastruktur, die den Anforderungen der DSGVO und weiterer europäischer Datenschutzbestimmungen gerecht wird.

Als secunet sind wir seit über 25 Jahren IT-Sicherheitspartner der Bundesrepublik Deutschland. Unsere Erfahrung in der digitalen Sicherheit und unsere enge Zusammenarbeit mit staatlichen Institutionen garantieren Ihnen höchste Sicherheitsstandards und maßgeschneiderte Lösungen. Mit secunet als Partner profitieren Sie von unserer Expertise in der Entwicklung und Implementierung von souveränen Cloud-Lösungen, die speziell auf die Anforderungen von Behörden und kritischen Infrastrukturen zugeschnitten sind.

Jetzt ist der richtige Zeitpunkt, gemeinsam mit einem erfahrenen Partner wie secunet Maßnahmen zu ergreifen und die ersten Schritte in Richtung einer souveränen Cloud-Infrastruktur zu unternehmen.

Wir beraten Sie gerne über die Vorteile von Open-Source-Lösungen und unsere bewährten Sicherheitsstrategien. Gemeinsam gestalten wir Ihre souveräne und sichere Cloud-Zukunft.
info@secunet.com

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

secunet