

Sovereign Cloud als strategische Notwendigkeit

Warum digitale Souveränität zur Voraussetzung für Sicherheit,
Resilienz und Marktzugang wird

INHALT

Table of Contents

1. WARUM SOUVERÄNE CLOUD JETZT ENTSCHEIDEND IST	3
2. VON DER FORDERUNG ZUR LÖSUNG - DIE SMARTE BÜNDELUNG AUS TECHNOLOGIE UND BETRIEB	4
<i>Ivanti Neurons for MDM als technologisches Fundament</i>	4
<i>sector27 als souveräner Betreiber</i>	5
EINORDNUNG IM KONTEXT DES EU CLOUD SOVEREIGNTY FRAMEWORKS.....	7
3. EINORDNUNG DURCH DAS CYBERINTELLIGENCE INSTITUTE.....	8
5. JURISTISCHE BEWERTUNG DER LÖSUNG.....	9
<i>Einordnung durch Prof. Dr. Dennis Kenji Kipker</i>	9
<i>Extraterritoriales Recht als strukturelles Risiko</i>	9
<i>Grenzen semi-souveräner Cloud Modelle</i>	9
<i>Bedeutung für Regulierung und Marktzugang</i>	9
<i>Zukunftssicherheit als strategischer Vorteil</i>	10
6. ZIELGRUPPEN UND EINSATZSZENARIEN.....	10
<i>Öffentliche Verwaltung und staatliche Einrichtungen</i>	10
<i>Kritische Infrastrukturen und regulierte Industrien</i>	11
<i>Unternehmen mit hohen Compliance Anforderungen</i>	11
<i>Cloud Late Adopter und sicherheitsbewusste Organisationen</i>	11
7. FAZIT	12
QUELLENVERZEICHNIS.....	12

1. Warum souveräne Cloud jetzt entscheidend ist

Digitale Souveränität ist längst kein politisches Modewort mehr. Sie ist zu einer handfesten wirtschaftlichen Notwendigkeit geworden. Die Welt ist unsicherer, fragmentierter und konfliktgeladener als noch vor wenigen Jahren. Handelskonflikte, geopolitische Machtverschiebungen und wachsende politische Spannungen wirken heute direkt in digitale Infrastrukturen hinein. Cloud Computing ist davon nicht ausgenommen. Unternehmen und Behörden stehen damit vor einer unbequemen Realität: Wer heute Cloud nutzt, entscheidet nicht nur über Technologie. Er entscheidet über Recht, Abhängigkeiten und Risiken. Jede Cloud Architektur transportiert ein Rechtsregime, eine politische Ordnung und eine Frage der Kontrolle gleich mit. Oft unbemerkt. Oft unterschätzt.

Was früher als Effizienzfrage galt, ist heute eine Frage der Resilienz. Globale Cloud Modelle versprechen Skalierung und Innovation, bringen aber zugleich neue Verwundbarkeiten mit sich. Extraterritoriale Gesetze, staatliche Zugriffsrechte und geopolitische Interessen treffen auf hochsensible Daten, kritische Geschäftsprozesse und staatliche Aufgaben. Spätestens seit der Verschärfung internationaler Konflikte ist klar: Digitale Abhängigkeiten sind reale Abhängigkeiten.

Cloud-Technologie als strategische Infrastruktur

Europa reagiert darauf nicht aus Protektionismus, sondern aus Notwendigkeit. Die Debatte um digitale Souveränität ist Ausdruck eines Lernprozesses. Sie folgt der Erkenntnis, dass wirtschaftliche Handlungsfähigkeit ohne rechtliche und technologische Kontrolle nicht dauerhaft zu sichern ist. Cloud wird damit zur strategischen Infrastruktur. Und Souveränität zur Voraussetzung für Vertrauen, Sicherheit und Zukunftsfähigkeit.

Die geopolitische Lage hat diese Abhängigkeiten sichtbar gemacht. Globale Machtverschiebungen, Handelskonflikte und extraterritoriale Gesetzgebung wirken längst direkt in europäische IT-Infrastrukturen hinein. Der US CLOUD Act erlaubt US-Behörden den Zugriff auf Daten von US-Unternehmen unabhängig vom physischen Speicherort. Ergänzt wird dies durch Regelwerke wie den Foreign Intelligence Surveillance Act. Damit wird klar: Serverstandorte allein schaffen keine Souveränität. Entscheidend ist, welchem Recht ein Anbieter unterliegt.

Europas notwendiger Weg: digitale Souveränität führt zu Resilienz

Der Branchenverband Bitkom ordnet diese Entwicklung eindeutig ein. Europa müsse digitale Souveränität als Fähigkeit zur selbstbestimmten Nutzung digitaler Technologien verstehen. Im Mittelpunkt stünden Kontrolle über Daten, Infrastrukturen und Entscheidungsprozesse, nicht die bloße Herkunft einzelner Anbieter. Digitale Souveränität werde damit zum Standortfaktor und zur Voraussetzung für Innovationsfähigkeit, Wettbewerbsfähigkeit und Vertrauen in digitale Dienste.

Diese Einschätzung deckt sich mit der zunehmenden regulatorischen Dynamik auf europäischer Ebene. Mit NIS2, DORA und dem geplanten European Cybersecurity Certification Scheme werden verbindliche Anforderungen an Sicherheit, Resilienz und

Nachweisbarkeit definiert. Cloud Modelle, die diese Anforderungen nicht erfüllen, verlieren künftig ihre Marktfähigkeit. Nicht aus politischen Gründen, sondern aus rechtlichen.

Souveräne Cloud ist damit keine Frage der Ideologie. Sie ist eine Frage der Haftung, der Zukunftsfähigkeit und der unternehmerischen Verantwortung.

Ivanti hat die Lösung Ivanti Neurons for MDM - Sovereign Edition - EU entwickelt, um Unternehmen und öffentlichen Einrichtungen einen rechtssicheren Zugang zu moderner Cloud Technologie zu ermöglichen. Das erklärte Ziel: Innovation und Automatisierung nicht gegen regulatorische Anforderungen auszuspielen, sondern beides konsequent zusammenzuführen. Die Lösung ist eine Antwort auf steigende geopolitische Risiken und europäische Regulierung und schafft die Grundlage für sichere, zukunftsfähige Cloud Nutzung im europäischen Markt.

2. Von der Forderung zur Lösung - Die smarte Bündelung aus Technologie und Betrieb

Viele Anbieter reagieren auf die Entwicklungen mit rein kosmetischen Anpassungen. Meistens werden dann die Server einfach in die EU verlagert. Verträge werden ergänzt. Der rechtliche Kern bleibt unangetastet. Genau hier scheitern sogenannte „semi souveräne Cloud Modelle“.

Echte Souveränität entsteht erst, wenn Technik, Betrieb und Recht zusammengedacht werden. Die Ivanti Sovereign Cloud folgt genau diesem Ansatz: Sie bündelt die technologische Leistungsfähigkeit von Ivanti Neurons for MDM mit der operativen und regulatorischen Expertise von sector27 als vollständig unabhängigem europäischem Betreiber. Souveräne Cloud entsteht nicht durch ein einzelnes Sicherheitsmerkmal. Sie entsteht durch das Zusammenspiel technischer, organisatorischer und rechtlicher Maßnahmen. Erst diese Kombination macht digitale Souveränität belastbar und überprüfbar.

Ivanti Neurons for MDM als technologisches Fundament

Als Grundlage für die souveräne Cloud Lösung fungiert eine Ivanti-Technologie: Ivanti Neurons for MDM ist eine cloudbasierte Unified Endpoint Management Lösung zur sicheren Verwaltung, Absicherung und Automatisierung aller Endgeräte im Everywhere Workplace. Sie unterstützt iOS, Android, macOS, Windows, ChromeOS sowie spezialisierte und industrielle Endgeräte. Die Plattform bietet zentrale Steuerung von Gerätekonfigurationen, Sicherheitsrichtlinien, Compliance Maßnahmen, Applikationsmanagement und Zero Trust Zugriffen.

Zu den zentralen Sicherheits und Managementfunktionen zählen:

- Automatisiertes Onboarding und Lifecycle Management von Endgeräten
- Durchsetzung von Sicherheits und Compliance Richtlinien in Echtzeit
- Trennung von privaten und geschäftlichen Daten auf Endgeräten
- Verschlüsselte Kommunikation und kontrollierter Applikationszugriff
- Integration von Zero Sign On, Multi Faktor Authentifizierung
- Zentrale Richtliniensteuerung für alle Endgeräte und Betriebssysteme
- Durchgängige Verschlüsselung von Daten im Ruhezustand und während der Übertragung
- Trennung von geschäftlichen und privaten Daten auf Endgeräten

Die Architektur ist hochverfügbar, skalierbar und für regulierte Umgebungen ausgelegt. Ivanti Neurons for MDM erfüllt anerkannte Sicherheitsstandards und verfügt unter anderem über SOC 2 Type II und CSA STAR Zertifizierungen. Ivantis Verpflichtung zu den ‚Secure by Design‘-Prinzipien der CISA ist dabei weit mehr als ein US-Standard. Sie bildet das technologische Fundament, das Kunden dabei unterstützt, europäische Anforderungen wie die NIS2-Richtlinie und den kommenden EU Cyber Resilience Act (CRA) zu erfüllen. Durch die proaktive Härtung der Cloud-Infrastruktur und eine maximale Transparenz in der Software-Lieferkette stellt Ivanti sicher, dass Kunden in Deutschland und Europa eine Lösung einsetzen, die bereits heute die regulatorischen Sicherheitsanforderungen von morgen erfüllt.

Ivanti Neurons for MDM validiert kontinuierlich Geräte, Nutzer und Kontexte, bevor Zugriff auf Unternehmensressourcen gewährt wird. Damit wird ein adaptives Sicherheitsmodell umgesetzt, das nicht auf Vertrauen, sondern auf überprüfbaren Zuständen basiert.

sector27 als souveräner Betreiber

Was die Lösung jedoch erst souverän macht, ist das Betriebsmodell und dessen sicherheitstechnischer Ausgestaltung. Die Sovereign Cloud Instanz wird vollständig durch sector27 betrieben. Der Betrieb erfolgt auf einer dedizierten, ausschließlich im europäischen Rechtsraum angesiedelten Infrastruktur. Hosting und Plattformbetrieb liegen vollständig in der Verantwortung des europäischen Betreibers. Administrative Hoheit, Systemsteuerung und Betriebsverantwortung sind klar getrennt vom Softwarehersteller und organisatorisch wie technisch abgesichert.

Die technische Umgebung orientiert sich an den Anforderungen des BSI-IT-Grundschutzes. Das eingesetzte Rechenzentrum ist entsprechend zertifiziert. Das heißt nicht nur das Rechenzentrum, sondern insbesondere die Prozesse zum Betrieb von Cloud-Lösungen sind geprüft. Die sector27 GmbH plant, betreibt und stellt im Kundenauftrag eine standardisierte Basisplattform für fachspezifische Anwendungen bereit. Die fachspezifische Anwendung wird entweder durch die Kunden eigenverantwortlich administriert oder auf Wunsch Partner. Die Basisplattform besteht aus IT-Systemen mit ihren erforderlichen Betriebssystemen, der Netzwerkinfrastruktur sowie den erforderlichen Management- und Überwachungssystemen. Die Systeme werden in einer sicheren infrastrukturellen Umgebung des Auftraggebers betrieben. Der Zertifizierungsumfang umfasst weiterhin den Betrieb

von IT-Grundschutz konformen EMM-Systemen (Enterprise Mobility Management Lösung), die auf der Basisplattform aufsetzen.

Sicherheitsrelevante Prozesse folgen somit einem strukturierten Informationssicherheitsmanagementsystem. Dazu zählen

- rollenbasierte Administrationskonzepte
- Prinzip der minimalen Rechtevergabe
- dokumentierte Zugriffspfade
- durchgängige Protokollierung
- Überwachung sicherheitskritischer Aktivitäten.

Maßnahmen zur Verfügbarkeit, Integrität und Vertraulichkeit der Systeme sind systematisch umgesetzt und regelmäßig überprüft.

Maximaler Schutz – auch beim Personal

Auch die personelle Sicherheit ist integraler Bestandteil des Betriebsmodells. Damit erfüllt die Lösung zentrale Voraussetzungen für den Einsatz in sicherheitskritischen und regulierten Umgebungen und adressiert zugleich die Anforderungen, die im Rahmen des European Cybersecurity Certification Scheme für Cloud Services insbesondere auf dem hohen Vertrauensniveau definiert werden.

Ivanti selbst hat keinen operativen Zugriff auf produktive Daten. Herstellerseitiger Support erfolgt ausschließlich anonymisiert und verschlüsselt auf Third Level Ebene. Ivanti hat auch auf Third Level Ebene keinen Zugriff auf die Daten - es sei denn sector27 (bzw. der Partner) übermittelt diese aktiv und verschlüsselt nach einer Anonymisierung an Ivanti. Damit wird eine klare organisatorische und technische Trennung zwischen Produktentwicklung und Cloud Betrieb sichergestellt.

Bereitstellung und Verantwortlichkeiten: Das Ivanti Sovereign Cloud Modell

Das Fundament dieser Initiative ist Ivanti Neurons for MDM - Sovereign Edition - EU. Während Ivanti als Hersteller für die kontinuierliche Produktentwicklung, die Bereitstellung von Updates und die technologische Roadmap verantwortlich bleibt, erfolgt der physische Betrieb und das Hosting der Infrastruktur exklusiv durch den spezialisierten Partner sector27 in einem hochsicheren, europäischen Rechenzentrum.

Für den Marktzugang stehen zwei Modelle (Routes to Market) zur Verfügung:

1. **Direktbezugsmodell:** Die Lösung wird direkt über den Hosting-Partner sector27 bezogen, der neben dem Betrieb auch den Vertrieb und den umfassenden Service verantwortet.
2. **Erweitertes Partnermodell:** Jeder autorisierte Ivanti-Partner kann die Sovereign Cloud Lösung vertreiben und die Kundenbeziehung führen, sofern er den qualifizierten First- und Second-Level-Support sicherstellt.

Diese klare Struktur garantiert, dass Kunden unabhängig vom gewählten Vertriebsweg immer ein identisches, herstellergeprüftes Ivanti-Produkt auf einer souveränen, durch sector27 betriebenen Infrastruktur nutzen. Zudem erhalten Kunden damit die Wahlfreiheit, ihre bestehenden, vertrauten Partnerbeziehungen zu nutzen, ohne auf eine souveräne Infrastruktur verzichten zu müssen.

Einordnung im Kontext des EU Cloud Sovereignty Frameworks

Die Ivanti Sovereign Cloud in der durch sector27 betriebenen Ausprägung wurde entlang des Cloud Sovereignty Frameworks der Europäischen Kommission vom renommierten Cyberintelligenz Institut bewertet. Maßgeblich sind dabei die acht definierten Souveränitätsziele sowie die jeweiligen SEAL-Level von 0 bis 4.

Die Lösung erreicht in zentralen Dimensionen das Niveau der Digitalen Resilienz (SEAL-3). Dies betrifft insbesondere:

- Strategische Souveränität (SOV-1)
- Sicherheits- und Compliance-Souveränität (SOV-7)

Hier bestätigt das Gutachten eine substanzielle europäische Kontrolle über Betrieb, Governance, Entscheidungsstrukturen und Sicherheitsorganisation

In weiteren Kernbereichen – insbesondere rechtliche Einordnung, operative Steuerung, Lieferkette und technologische Weiterentwicklung – wird eine starke europäische Verankerung festgestellt, allerdings unter verbleibenden strukturellen Herstellerabhängigkeiten. Diese betreffen primär die vorgelagerte Produktentwicklung und globale Lieferkette, nicht jedoch die operative Diensthoheit des konkreten Cloud-Dienstes.

Das Gutachten kommt daher zu dem Ergebnis, dass die Lösung insgesamt dem SEAL-2-Niveau („Datensouveränität“) mit deutlicher Annäherung an SEAL-3 („Datenresilienz“) zuzuordnen ist

Die verbleibenden nicht-europäischen Abhängigkeiten liegen nicht im Bereich des operativen Betriebs, der Datenkontrolle oder der Sicherheitsorganisation, sondern in der Produktentwicklung des Herstellers. Für einen internationalen Softwareanbieter ist dies strukturell unvermeidbar.

Damit positioniert sich das Ivanti Sovereign Cloud Modell im oberen Spektrum dessen, was für eine globale Softwarelösung unter europäischer Betriebsführung realistisch erreichbar ist.

3. Einordnung durch das Cyberintelligence Institute

Souveränität lässt sich nicht nur beschreiben, sie lässt sich messen. Genau an diesem Punkt setzt das Cyberintelligence Institute (CII) an. Das Institut ist ein unabhängiges, interdisziplinäres Forschungs- und Analysezentrum mit Schwerpunkt auf Cybersecurity, digitale Souveränität und geopolitische Risikobewertung digitaler Infrastrukturen. Es arbeitet an der Schnittstelle von Technik, Recht und Politik und berät öffentliche Institutionen, Unternehmen sowie sicherheitsrelevante Organisationen. Ziel des CII ist es, komplexe digitale Abhängigkeiten sichtbar, vergleichbar und bewertbar zu machen.

Das Cyberintelligence Institute bewertet Cloud-Souveränität nicht politisch, sondern strukturell. Maßgeblich ist die Frage, ob europäische Kontrolle in strategischer, operativer und sicherheitsorganisatorischer Hinsicht substantiell ausgeprägt ist und ob verbleibende Drittstaatenbezüge kritisch oder lediglich strukturell vorgelagert sind.

Im Gutachten wird bestätigt:

- Die operative Hoheit über Infrastruktur, Betrieb und Support liegt vollständig in europäischer Jurisdiktion.
- Sicherheitsmanagement, Compliance-Strukturen und Incident Response erfüllen das Niveau der Digitalen Resilienz.
- Die unmittelbare Datenverarbeitung erfolgt ausschließlich innerhalb der EU.

In der Gesamtwürdigung stellt das Gutachten fest, dass materielle nicht-europäische Abhängigkeiten in der Software- und Lieferkette verbleiben, diese jedoch nicht die operative Steuerung des Dienstes dominieren.

Gerade diese Differenzierung ist zentral. Das Framework verlangt für SEAL-4 eine vollständige technologische Autonomie einschließlich Produktentwicklung und Lieferkette. Für internationale Hersteller ist dieses Niveau faktisch nur durch vollständige europäische Neuentwicklung erreichbar.

Vor diesem Hintergrund ist die Kombination aus:

- europäischem Betreiber
- klarer juristischer Trennung zwischen Hersteller und Cloud-Betrieb
- BSI-konformer Infrastruktur
- europäischer Sicherheitsorganisation

der strukturell wirksamste Weg, ein Höchstmaß an Souveränität innerhalb eines globalen Softwaremodells zu erreichen.

Die Cloud Risiko Matrix des Cyberintelligence Institute bestätigt, dass echte Souveränität nicht durch Datenlokalisierung allein entsteht, sondern durch überprüfbare europäische Kontrollstrukturen. Genau diese sind im vorliegenden Modell ausgeprägt.

5. Juristische Bewertung der Lösung

Einordnung durch Prof. Dr. Dennis Kenji Kipker

Digitale Souveränität ist keine technische Komfortfrage. Sie ist eine rechtliche Notwendigkeit. Prof. Dr. Dennis Kenji Kipker, einer der anerkanntesten Experten für IT Sicherheits-, Daten- und Plattformrecht in Deutschland, weist seit Jahren darauf hin, dass Cloud Entscheidungen zunehmend über Rechtskonformität, Marktzugang und Haftung entscheiden.



Extraterritoriales Recht als strukturelles Risiko

Im Zentrum der juristischen Debatte steht die Frage nach anwendbarem Recht. Prof. Kipker macht deutlich, dass insbesondere US-amerikanische Regelwerke wie der CLOUD Act und der Foreign Intelligence Surveillance Act ein dauerhaftes Risiko für europäische Cloud Nutzer darstellen. Diese Gesetze ermöglichen staatlichen Zugriff auf Daten von US-Unternehmen unabhängig vom Speicherort. Damit wird die physische Lokalisierung von Daten rechtlich entwertet.

Nach Einschätzung von Prof. Kipker sind Cloud Modelle, bei denen der Betrieb weiterhin unter der rechtlichen Kontrolle eines Drittstaates steht, langfristig nicht mit europäischen Datenschutz- und Sicherheitsanforderungen vereinbar. Dies betreffe insbesondere öffentliche Auftraggeber, kritische Infrastrukturen und regulierte Industrien.

Grenzen semi-souveräner Cloud Modelle

Prof. Kipker übt deutliche Kritik an sogenannten semi souveränen Cloud Ansätzen. Dazu zählen Modelle, bei denen zwar Rechenzentren in der EU betrieben werden, die rechtliche Kontrolle jedoch beim ausländischen Mutterkonzern verbleibt. Aus juristischer Sicht reiche dies nicht aus, um digitale Souveränität herzustellen.

Er betont, dass europäische Aufsichtsbehörden und Gesetzgeber zunehmend zwischen formaler Compliance und tatsächlicher Kontrollfähigkeit unterscheiden. Cloud Angebote, die lediglich auf Vertragsklauseln oder technische Zusatzmaßnahmen setzen, ohne die rechtliche Zugriffsmacht zu eliminieren, seien nicht zukunftsfähig.

Bedeutung für Regulierung und Marktzugang

Mit Blick auf kommende Regulierungen sieht Prof. Kipker eine klare Entwicklung: NIS2, DORA und das European Cybersecurity Certification Scheme aus dem CSA verschärfen nicht nur Anforderungen an Sicherheit, sondern auch an Nachweisbarkeit und Governance. Cloud Modelle, die keine rechtlich souveräne Betriebsstruktur vorweisen können, riskieren den Ausschluss aus sensiblen Anwendungsfeldern.

Besonders relevant ist dies für den öffentlichen Sektor und für Unternehmen, die Teil kritischer Lieferketten sind. Hier werde Cloud Souveränität zur Voraussetzung für Ausschreibungsfähigkeit. Prof. Kipker spricht in diesem Zusammenhang von einer neuen Markteintrittsschwelle für Cloud Anbieter.

Zukunftssicherheit als strategischer Vorteil

Prof. Kipker weist ferner darauf hin, dass Cloud Souveränität nicht nur Risiken minimiert, sondern strategische Vorteile schafft. Unternehmen, die heute in rechtlich belastbare Cloud Architekturen investieren, sichern sich regulatorische Handlungsfreiheit, Planungssicherheit und Vertrauen bei Kunden und Partnern.

Juristische Resilienz wird damit zu einem Wettbewerbsfaktor. Nicht als abstraktes Prinzip, sondern als konkrete Voraussetzung für Wachstum in regulierten Märkten.

6. Zielgruppen und Einsatzszenarien

Souveräne Cloud ist längst kein Nischenthema für Spezialfälle oder besonders sicherheitskritische Organisationen. Sie betrifft zunehmend alle Unternehmen und Institutionen, deren Geschäftsmodell auf Vertrauen, Verfügbarkeit und rechtlicher Belastbarkeit beruht. In einer digitalisierten Wirtschaft ist das keine Ausnahme mehr, sondern der Regelfall.

Mit wachsender regulatorischer Dichte verschiebt sich der Maßstab. Cloud Entscheidungen werden nicht mehr allein nach Funktionalität, Kosten oder Skalierbarkeit getroffen. Sie werden zum Bestandteil von Risiko, Compliance und Unternehmensführung. NIS2, DORA, der EU AI Act und kommende Zertifizierungsregime wie EUCS machen deutlich, dass digitale Infrastrukturen künftig denselben Anforderungen unterliegen wie klassische kritische Geschäftsprozesse.

Damit erweitert sich der Kreis der betroffenen Organisationen stetig. Was heute noch als Spezialanforderung des öffentlichen Sektors gilt, wird morgen zum Standard für regulierte Industrien und übermorgen zum Erwartungshorizont von Kunden, Partnern und Aufsichtsbehörden. Souveräne Cloud wird so von der Option zur Voraussetzung.

Öffentliche Verwaltung und staatliche Einrichtungen

Für Behörden auf kommunaler, Landes und Bundesebene ist Cloud Souveränität bereits heute ein zentrales Vergabekriterium. Datenschutz, Geheimschutz und rechtliche Zugriffsfreiheit sind nicht verhandelbar. Modelle mit extraterritorialem Risiko scheiden faktisch aus.

Die hier beschriebene Lösung adressiert diese Anforderungen direkt durch:

- rechtlich unabhängigen EU-Betrieb
- BSI zertifizierte Infrastruktur
- auditierbare Prozesse und klare Verantwortlichkeiten

Damit erfüllt sie die Voraussetzungen für den Einsatz in besonders sensiblen Verwaltungsumgebungen.

Kritische Infrastrukturen und regulierte Industrien

Energieversorgung, Gesundheitswesen, Finanzdienstleister, Transport und Telekommunikation stehen unter wachsendem regulatorischem Druck. NIS2 und DORA verlangen nicht nur technische Sicherheit, sondern auch belastbare Governance und Resilienzkonzepte. Cloud Modelle, die rechtliche Unsicherheiten enthalten, erhöhen das operationelle Risiko. Das Cyberintelligence Institute weist ausdrücklich darauf hin, dass solche Risiken künftig nicht mehr akzeptabel sein werden.

Die Kombination aus Ivanti Neurons for MDM und sector27 ermöglicht:

- sichere Verwaltung heterogener Endgeräte
- klare Trennung von Betrieb und Hersteller
- stabile Betriebsmodelle auch im Krisenfall

Unternehmen mit hohen Compliance Anforderungen

Auch jenseits klassischer KRITIS Branchen wächst der Bedarf an souveränen Cloud Lösungen. Unternehmen mit internationaler Präsenz, sensiblen Daten oder hohen Compliance Anforderungen müssen regulatorische Entwicklungen antizipieren.

Gartner prognostiziert, dass bis 2027 ein Großteil multinationaler Organisationen eine explizite Sovereign Cloud Strategie implementieren wird. Souveränität beeinflusst zunehmend die Anbieterwahl.

Für diese Unternehmen bietet die Lösung Planungssicherheit, ohne auf moderne Cloud Funktionalitäten verzichten zu müssen.

Cloud Late Adopter und sicherheitsbewusste Organisationen

Nicht zuletzt richtet sich die Lösung an Organisationen, die Cloud bislang bewusst zurückhaltend eingesetzt haben. Für sie ist Souveränität oft die Eintrittskarte in die Cloud Nutzung.

Ein rechtlich belastbares, auditierbares und transparentes Betriebsmodell senkt die Einstiegshürden und schafft Vertrauen. Gerade im Bereich Endgeräte Management ist dies ein entscheidender Faktor, da mobile Endpunkte häufig sensible Zugänge zu Unternehmensdaten darstellen.

7. Fazit

Digitale Souveränität lässt sich nicht nachrüsten. Sie muss von Anfang an Teil der Architektur sein. Wer Cloud nur als Infrastruktur betrachtet, verkennet ihre rechtliche und strategische Dimension.

Die Lösung Ivanti Neurons for MDM - Sovereign Edition - EU zeigt, wie echte Souveränität in der Praxis umgesetzt werden kann. Nicht durch Marketingbegriffe, sondern durch klare Strukturen. Technik, Betrieb und Recht greifen ineinander.

Die Bündelung aus Ivanti Neurons for MDM als technologisches Fundament und sector27 als unabhängiger europäischer Betreiber erfüllt die Anforderungen heutiger und zukünftiger Regulierungen. Sie adressieren die zentralen Risiken extraterritorialer Abhängigkeiten und schaffen eine belastbare Grundlage für Sicherheit, Resilienz und Vertrauen.

Für Unternehmen und öffentliche Einrichtungen bedeutet das:

- rechtliche Planungssicherheit
- regulatorische Zukunftsfähigkeit
- Schutz sensibler Daten und Prozesse
- Wettbewerbsvorteile in regulierten Märkten

Souveräne Cloud ist kein politisches Statement. Sie ist eine strategische Entscheidung. Wer sie heute trifft, bleibt morgen handlungsfähig.

Quellenverzeichnis

- Bitkom e.V.: Europas Weg zur digitalen Souveränität, Presseinformation, 2024.
- Cyberintelligence Institute: Requirements for National and European Cloud Sovereignty, Prof. Dr. Dennis-Kenji Kipker, 18.05.2025.
- Cyberintelligence Institute: Cloud Risiko Matrix und Souveränitätsbewertung, 2026.
- Ivanti: Ivanti Neurons for MDM Data Sheet, 2023.
- Gartner: Sovereign Cloud Strategy Market Forecast, zitiert nach Ivanti Marktübersicht.