



Quelle: Depositphotos

Europäische IT-Souveränität: Chancen und Grenzen

Know-how Praktikable souveräne Lösungen für Storage und Security existieren zwar, bei KI und SaaS bleibt die Abhängigkeit von den USA indes bestehen, wenn man auf Innovationsgeschwindigkeit und Integrationstiefe nicht verzichten will.

Von Marc Zimmermann

Die EU will im Rahmen der «Digital Decade 2030» erreichen, dass bis 2030 rund 75 Prozent der Unternehmen Cloud, Big Data und KI produktiv nutzen – ein Ziel, das den Druck auf souveräne Infrastrukturen erhöht. Gleichzeitig dominieren die US-Hyperscaler AWS, Microsoft Azure und Google Cloud nach wie vor den europäischen Cloud-Markt, was die Abhängigkeit von aussereuropäischen Plattformen unterstreicht.

Für die Schweiz ist der Datacenter-Markt stark wachstumsgetrieben: Das Volumen lag gemäss den Marktforschern von Imap 2025 bei rund 435 Millionen US-Dollar und soll sich bis 2034 auf 900 Millionen fast verdreifachen, getrieben durch Cloud-Services, digitale Transformation und Investitionen globaler Tech-Konzerne. In Zürich konzentrieren sich über 60 Prozent der Datacenter-Kapazitäten, mit einem hybriden Ökosystem von Colocation und Hyperscaler-Anbietern. Diese Entwicklung spiegeln auch die Voraussagen für den Cloud-Services-Markt wider: Einer Studie von Digital Realty zufolge soll der Schweizer Markt für Infrastruktur-, Plattformen, Software und andere Cloud-Services (IaaS, PaaS, SaaS, etc.) bis 2032 um jährlich 13 Prozent auf knapp 15 Milliarden Dollar wachsen. Gemäss IDC wiederum sollen bereits dieses Jahr Public-Cloud-Dienste ein Volumen von 11 Milliarden Franken erreichen. Hyperscaler werden demnach auch in Zukunft souveräne Schweizer Anbieter bei weitem übertreffen.

Was bedeutet europäische IT?

Unter digitaler Souveränität wird in der europäischen Debatte in der Regel verstanden, dass Staaten, Unternehmen und Individuen ihre Daten, Systeme und Wertschöpfungsketten so steuern können, dass sie nicht von fremden Rechtsräumen und Monopolstrukturen abhängig sind. Dazu gehören technische, rechtliche und organisatorische Elemente wie Datenlokalität, Verschlüsselung, offene Standards, aber eben auch die Kontrolle über Lieferketten und Schlüsseltechnologien wie Chips oder künstliche Intelligenz.

Projekte wie Gaia-X (siehe Kasten Seite 30) sollen eine interoperable, föderierte Daten- und Cloud-Infrastruktur etablieren, die europäischen Werten, Datenschutz und der Abwehr extraterritorialer Gesetzgebung verpflichtet ist. Parallel dazu wird versucht, mit dem European Chips Act, Europas Anteil an der weltweiten Halbleiterproduktion bis

2030 auf 20 Prozent zu erhöhen. Es versteht sich von selbst, dass mit diesem bereits ambitionierten Ziel Abhängigkeiten bei Hardware und kritischen Komponenten nicht verhindert, sondern lediglich verringert werden können.

Wo europäische IT heute praktikabel ist

Dennoch lassen sich in einigen Bereichen für Schweizer Unternehmen bereits heute konsistente, weitgehend europäische IT-Landschaften umsetzen, ohne gravierende Abstriche bei Funktionalität und Wirtschaftlichkeit machen zu müssen.

Für Infrastruktur-Cloud und Hosting betreiben europäische Anbieter wie nationale Telcos, spezialisierte Cloud- und Colocation-Anbieter Datacenter in der Schweiz und der EU mit klar definierten Datenresidenz- und Compliance-Konzepten. Über Gaia-X-konforme Angebote und EU-Cloud-Codes-of-Conduct kön-

INHALT

Europäische IT-Souveränität: Chancen und Grenzen	29
Souveränitäts-Washing bei Cloud-Diensten	32
Warum digitale Souveränität lokale Provider braucht	34
Die richtige Balance zählt	36
Open Source als Schlüssel zur digitalen Souveränität	38
Wie die Schweiz mit Open Source ihre Unabhängigkeit zurückgewinnt	42
Marktübersicht: IT made in Europe – mehr als nur Nachzügler	43

nen so insbesondere für regulierte Branchen Workloads gezielt auf souveräne, mit externen Audits geprüfte Umgebungen gelegt werden.

Was Storage, Backup und Archivierung angeht, so sind Lösungen mit Hosting in der Schweiz oder der EU mit Schweizer respektive EU-Vertragsrecht am Markt etabliert. Sie erlauben es, sensible Daten vom Zugriff fremder Rechtsräume abzuschirmen. Wenn eine hochskalierende, globale Content-Verteilung nicht zwingend ist, dann erlauben Objekt-Storage-Services europäischer und Schweizer Anbieter, die Gaia-X-konform mit Fokus auf Schweizer Datenschutz und DSGVO sind, eine Alternative zu (Amazon)-S3-kompatiblen US-Angeboten.

Security-Produkte wie Firewalls, IDS/IPS, Lösungen für E-Mail-Sicherheit oder Identity- und Access-Management gibt es von europäischen Herstellern oder als Open-Source-basierte Lösungen, die in europäischen Rechenzentren betrieben werden können.

Sonderfall Open Source

Open-Source-Stacks (Linux, Kubernetes, Sovereign Cloud Stack etc.) erlauben es, europäische Kontroll- und Governance-Anforderungen umzusetzen, selbst wenn einzelne Komponenten weltweit entwickelt wurden. Solche Sammlungen modularer, quelloffener Softwarekomponenten (z.B. OpenStack), die zusammen ähnlich wie die grossen Public-Cloud-Anbieter eine komplette Cloud-Infrastruktur bilden, erlauben eine vollständige Kontrolle über die eigene Hardware und Daten, da der Code einsehbar, veränderbar und frei nutzbar ist.

So können private oder hybride Clouds aufgebaut und virtuelle Maschinen, Speicher und Netzwerke verwaltet werden, die zum Beispiel für Big-Data-Anwendungen und KI skalierbar sind. Dabei sind oft Komponenten wie Kubernetes und Software Defined Storage wie etwa Ceph bereits integriert.

Branchen- und Fachanwendungen

In gewissen Bereichen wie Finanz-Backoffice, Gesundheitsinformationssysteme oder Systeme für öffentliche Verwaltungen existieren spezialisierte europäische oder schweizerische Software-Häuser, die Anwendungen nach

lokalen Regulatorien (FINMA, Datenschutz, E-Health) entwickeln. Hier überwiegen oft Domänenwissen, Supportnähe und das Erfüllen von Regulatorien den Vorteil globaler Plattform-Ökosysteme.

Wo ohne Nicht-EU-Anbieter wenig geht

Es gibt jedoch Segmente, in denen europäische Angebote aktuell nicht mit den führenden US- oder asiatischen Playern mithalten können. Die dominierenden Hyperscaler setzen durch enorme Investitionen, globale Regionen, proprietäre PaaS-Dienste und künstliche Intelligenz (KI) den De-facto-Standard für moderne Cloud-Architekturen. Viele innovative Services – von Managed-Kubernetes-Ökosystemen über Serverless-Plattformen bis hin zu voll integrierten KI-Stacks – sind in dieser Form bei rein europäischen Anbietern nicht oder nur mit funktionalen Lücken verfügbar.

Generative KI-Plattformen und Foundation-Modelle stammen überwiegend aus den USA, mit integrierter Tooling-Landschaft, Ökosystemen und globalen Marktplätzen. Europäische und selbst Schweizer KI-Ansätze existieren, sind jedoch meist spezialisierter und skalierten bisher nicht in vergleichbarer Geschwindigkeit und Breite, was Integrationen und Entwickler-Communities

betrifft. Die Schweizer ChatGPT-Alternative Apertus von ETH und EPFL ist zwar das grösste Modell, das als Ergebnis der Swiss AI Initiative die Compliance-Anforderungen des EU AI Act erfüllt. Ein eigenes Webportal wie es ChatGPT anbietet, betreibt die ETH aber nicht. Sie stellt das «Gehirn» von Apertus als Open-Source-Software zur Verfügung. Forscher und Firmen können dieses Modell herunterladen und auf eigenen Servern nutzen. Auch die KI-Alternative des Bundes für öffentliche Verwaltungen steckt noch in sehr kleinen Kinderschuhen (Gov-GPT).

In Bereichen wie Office-Anwendungen, Kollaboration, CRM, Marketing-Automation oder Produktivitäts-Tools dominieren US-Anbieter mit etablierten Ökosystemen, App-Marktplätzen und globaler Verbreitung. Zwar gibt es europäische, Schweizer und auch Open-Source-Alternativen. Aber die Integrationstiefe zu Drittservices, Verfügbarkeit von Fachkräften und die Innovationsgeschwindigkeit sind geringer, was die Total Cost of Ownership relativiert.

Hinzu kommt, dass Europa rund 20 Prozent der globalen Halbleiter verbraucht, aber nur einen wesentlich kleineren Anteil selbst produziert. Dies verdeutlicht die enorme Abhängigkeit von asiatischen und US-Lieferanten. Selbst bei souveränen Software- und

GAIA-X: DIE EUROPÄISCHE INITIATIVE FÜR SOUVERÄNE DATENINFRASTRUKTUR

Gaia-X ist eine europäische Initiative für eine föderierte, sichere und souveräne Dateninfrastruktur, die die Abhängigkeit von US- und chinesischen IT-Grosskonzernen verringern und Europas digitale Souveränität stärken soll. Sie schafft einen standardisierten Rahmen für vertrauenswürdige Cloud-Dienste und Datenaustausch, damit Daten in Europa bleiben, der Datenschutz-Grundverordnung der EU (DS-GVO) unterliegen und Unternehmen die Kontrolle behalten, mit Fokus auf Offenheit, Interoperabilität und Transparenz.

Zentrale Ziele sind die digitale Souveränität durch geringere Abhängigkeit von internationalen Hyperscalern, Datensouveränität durch volle Kontrolle der Dateninhaber sowie mehr Vertrauen und Sicherheit mittels Zertifizierungen und Sicherheitsstandards. Zudem soll Interoperabilität sicherstellen, dass unterschiedliche Cloud-Dienste und Datenquellen nahtlos zusammenarbeiten, während Offenheit und Transparenz durch den Einsatz von Open-Source-Technologien gefördert werden.

Gaia-X funktioniert als dezentrales Netzwerk europäischer Anbieter, das gemeinsame Regeln und Standards befolgt, statt als einzelner Cloud-Provider aufzutreten. Ein Katalog zertifizierter Dienste erleichtert es Nutzern, sichere und interoperable Angebote – etwa für Datenanalyse oder KI – zu finden, während sogenannte Datenräume den geschützten Datenaustausch über Unternehmens- und Branchengrenzen hinweg ermöglichen.

Für Europa hat Gaia-X besondere Bedeutung, weil es Innovation fördert und Unternehmen den Zugang zu moderner digitaler Infrastruktur bietet, ohne europäische Werte und Vorschriften, insbesondere hohe Datenschutzerfordernisse, zu kompromittieren.

Cloud-Architekturen bleibt bei der Hardware-Ebene eine strukturelle Abhängigkeit.

Grenzen europäischer IT: Preis, Skalierung, Ökosystem

Digitale Souveränität ist kein Selbstzweck. Sie muss sich im Spannungsfeld von Wirtschaftlichkeit, Innovationsfähigkeit und Compliance behaupten. Hyperscaler und globale SaaS-Anbieter profitieren von massiven Skaleneffekten, standardisierten Baukästen und global ausgerollten Services, was die Stückkosten pro Serviceeinheit senkt. Europäische Anbieter können diese Preise bei vergleichbarer Funktionalität in der Regel nicht erreichen, insbesondere bei hochskalierenden, global verteilten Workloads.

Hinzu kommt, dass Entwickler, Integratoren und Berater stark auf die dominanten Plattformen spezialisiert sind. So sinken Implementierungskosten und Risiken, wenn auf etablierte US-Plattformen gesetzt wird. Für viele europäische Lösungen existiert hingegen ein deutlich kleineres Partner-Ökosystem, was Projekte in der Schweiz komplexer, teurer und risikoreicher machen kann. Eine strikt europäische IT-Landschaft bedeutet demzufolge häufig Multi-Provider-Modelle mit unterschiedlicher Technologie-Basis und Fertigungstiefe. Das wiederum macht Governance, Monitoring, Security und Betriebsprozesse für Unternehmen anspruchsvoller. Ohne klare Architekturrichtlinien drohen indes Schatten-IT, Datensilos und Integrationsbrüche, also genau jene Risiken, die man mit grossen Plattformen eigentlich vermeiden will.

Entscheidungs-Framework für Schweizer Unternehmen

Für IT-Entscheider in der Schweiz bietet sich ein pragmatisches Framework an, das Souveränität und Marktrealitäten verbindet:

- Daten- und Prozesskritikalität klassifizieren
- Kategorien wie «strategisch-kritisch», «reguliert», «vertraulich» und «unkritisch» helfen zu definieren, welche Daten zwingend in europäischen oder Schweizer Infrastrukturen verbleiben müssen.
- Für strategisch-kritische und regulierte Daten sollte primär auf Schweizer oder

EU-basierte Provider mit klarer Abgrenzung von extraterritorialem Recht gesetzt werden.

- Rechts- und Risikoanalyse müssen verankert werden.
- Prüfen, inwiefern Cloud Act, andere extraterritoriale Regelungen oder Exportkontrollen den gewählten Dienst betreffen und wie technische und organisatorische Massnahmen (Verschlüsselung, Schlüsselhaltung in CH/EU, Pseudonymisierung) Risiken abmildern.
- Regulatorische Anforderungen wie zum Beispiel FINMA-Rundschreiben oder branchenspezifische Vorgaben direkt mit IT-Architektur-Entscheiden verknüpfen, statt sie erst nachträglich überzustülpen.
- Grundsatz: Basis-Infrastruktur, Kern-Datenhaltung und sicherheitskritische Dienste möglichst bei europäischen respektive Schweizer Providern beziehen, ergänzt um global führende Plattformen dort, wo Innovation, Skalierung oder Ökosysteme entscheidend sind.
- Technische Entkopplung über API-first-Ansätze, Containerisierung und offene Standards reduziert Vendor-Lock-in, auch wenn ein Hyperscaler genutzt wird.
- Kennzahlen wie Anteil der Workloads auf europäischen Plattformen, Anteil der kritischen Daten in der Schweiz und der EU, Anzahl unabhängiger Alternativen pro kritischem Dienst oder Abhängigkeit von einzelnen Rechtsräumen helfen, digitale Souveränität quantifizierbar zu machen.
- Regelmässige Reviews (z.B. im Rahmen des Risk- oder Compliance-Reportings) stellen sicher, dass sich die IT-Landschaft mit geopolitischen und regulatorischen Veränderungen weiterentwickelt.
- Investitionen in Know-how zu europäischen Cloud-Plattformen, Open-Source-Stacks und Datenschutz-Engineering sind notwendig, um souveräne Optionen überhaupt realistisch betreiben zu können.
- Darüber hinaus stärken Kooperationen mit lokalen Anbietern, Hochschulen und Branchennetzwerken in der Schweiz das Ökosystem und reduzieren die Abhängigkeit von globalen Monokulturen.

Kein Entweder-oder

Eine rein europäische oder Schweizer IT-Landschaft ist dort sinnvoll, wo Datenhoheit, regulatorische Sicherheit und strategische Unabhängigkeit für das Geschäftsmodell kritisch sind – etwa bei sensiblen Behörden-, Gesundheits- oder Finanzdaten. Dabei gilt es zu beachten, dass man zwar beispielsweise für Cloud-Dienste eines Hyperscalers den Vertrag mit einem Schweizer Infrastrukturanbieter schliessen kann, aber dennoch die Geschäftsbedingungen und des US-Anbieters akzeptieren muss. In vielen Bereichen wie Hyperscale-Cloud, KI-Plattformen oder globalen SaaS-Ökosystemen lassen sich aber US- und andere Nicht-EU-Angebote faktisch kaum umgehen, wenn Skalierung, Innovationsgeschwindigkeit, Integrationstiefe und Preis-Leistung im Vordergrund stehen.

Für Schweizer IT-Entscheider gibt es also kein Entweder-oder zwischen rein europäischer beziehungsweise Schweizer IT und globalen Plattformen, sondern eine bewusst gesteuerte Balance, in der digitale Souveränität dort maximiert wird, wo sie geschäftskritisch ist – ohne auf die Innovationsdynamik und Skaleneffekte der internationalen Cloud- und SaaS-Welt zu verzichten. ■

DER AUTOR

Marc Zimmermann, Head of Business Development bei UMB, ist Cloud-Experte mit über 15 Jahren Erfahrung und seit 2022 bei UMB, zunächst als Head of Cloud Services, seit 2026



neu als Head of Business Development. Er ist spezialisiert auf Multi-Cloud (AWS, Azure) und führte UMB zu ISG-Leader-Auszeichnungen und AWS «Rising Star 2023».