Lünendonk im Interview mit Materna

Von der Abhängigkeit zur Handlungsfähigkeit: Der Weg zur digitalen Souveränität

Digitale Souveränität ist längst kein politisches Schlagwort mehr, sondern entwickelt sich für Unternehmen und Behörden zur strategischen Überlebensfrage. Timon Schmotz von Materna zeigt im Interview, wie geopolitische Unsicherheiten, strenge Regulierung und der Wunsch nach technologischer Unabhängigkeit neue Maßstäbe für Cloud-Architekturen, KI-Einsatz und Sicherheitsstrategien setzen. Er macht deutlich, wo heute die größten blinden Flecken liegen – von intransparenten Service-Ketten bis hin zu proprietären Lock-ins – und warum echte Souveränität nur durch klare Kontrolle über Daten, Betreiberstrukturen und Prozesse entsteht.

Timon Schmotz
Business Development Manager
Materna

MATERNA

Viele Unternehmen sehen digitale Souveränität zunehmend als geschäftskritische Fähigkeit. Was ist aus Ihrer Sicht der wichtigste Treiber: geopolitische Unsicherheiten, regulatorischer Druck oder der Wunsch nach mehr technologischer Gestaltungsfreiheit?

Timon Schmotz: Aus unserer Arbeit mit Kunden sehen wir, dass sich alle drei Treiber gegenseitig verstärken. Im öffentlichen Sektor ist der regulatorische Druck zweifellos der dominierende Faktor, denn hier müssen Vorgaben zu Datenschutz, Datenlokalisierung, IT-Sicherheit und Compliance zwingend eingehalten werden. Gleichzeitig wirken geopolitische Unsicherheiten als Katalysator, weil extraterritoriale Gesetze oder politische Spannungen Abhängigkeiten von globalen IT-Anbietern plötzlich zu strategischen Risiken machen können. In Industrien wie Automotive, Manufacturing oder Finance erleben wir häufiger, dass der Wunsch nach technologischer Gestaltungsfreiheit im Vordergrund steht – etwa um Innovation selbstbestimmter zu steuern oder proprietäre Lock-ins zu vermeiden. Übergreifend zeigt sich jedoch: Digitale Souveränität ist heute ein strategisches Thema der Resilienz und Zukunftsfähigkeit, nicht nur ein technisches oder politisches.

Digitale Souveränität bedeutet im ersten Schritt, bestehende Abhängigkeiten sichtbar zu machen. Wo erleben Sie heute die größten „Blind Spots" in IT-Architekturen und Service-Beziehungen?

Timon Schmotz: Die größten blinden Flecken entstehen dort, wo Transparenz über Herkunft, Kontrolle und Betriebswege digitaler Dienste fehlt. Viele Organisationen verfügen nicht über eine vollständige Sicht darauf, welche Unterauftragnehmer in ihren Service-Ketten beteiligt sind, welche Softwarekomponenten tatsächlich eingesetzt werden oder wie Daten zwischen Systemen fließen. Besonders im Public Sector stoßen wir häufig auf unklare Betreiberstrukturen bei Cloud-Diensten, in denen Verantwortlichkeiten schwer zuzuordnen sind. Hinzu kommt, dass ein großer Teil der bestehenden IT-Landschaften auf proprietären Anwendungen basiert, deren Funktionsweise und Risiken mangels Quellcode-Transparenz nur eingeschränkt nachvollziehbar sind. Diese Kombination aus technischer Komplexität und fehlender Einsicht ist einer der zentralen Gründe, warum viele Organisationen ihren Abhängigkeitsgrad unterschätzen.

"Digitale Souveränität ist heute ein strategisches Thema der Resilienz und Zukunftsfähigkeit, nicht nur ein technisches oder politisches."

Timon Schmotz
Materna

Die Cloud bleibt der zentrale Baustein moderner IT-Landschaften. Wie verändern souveräne Cloud-Modelle Ihrer Beobachtung nach die Architektur- und Sourcing-Entscheidungen von Unternehmen und Behörden?

Timon Schmotz: Wir beobachten eine deutliche Verschiebung hin zu differenzierten, mehrstufigen Cloud-Strategien. Statt einer generischen Cloud-First-Logik entscheiden Kunden heute viel stärker anhand der Kritikalität ihrer Daten, wo und wie Workloads betrieben werden sollen. Sensible oder besonders schützenswerte Informationen werden zunehmend in souveräne Betriebsmodelle überführt,

die entweder von europäischen beziehungsweise deutschen Anbietern stammen oder in speziellen Hyperscaler-Modellen mit EU-Betreiberstrukturen realisiert werden. Gleichzeitig behalten Standard-Public-Clouds eine wichtige Rolle, jedoch meist ergänzt durch zusätzliche Sicherheits- und Kontrollmechanismen. Multi-Cloud-Architekturen werden zur Normalität, und Exit-Fähigkeit entwickelt sich zu einer Grundanforderung im Sourcing. Dadurch entstehen hybride, hochsegmentierte Architekturen, die regulatorische Sicherheit und technologische Innovationsfähigkeit miteinander verbinden sollen.

Viele Anbieter positionieren sich mit „souveränen" Lösungen. Wie unterscheiden Sie echte Souveränitätsmerkmale von Marketingversprechen, und welche Kriterien sollten Unternehmen dafür heranziehen?

Timon Schmotz: Der zentrale Maßstab ist immer die tatsächliche Kontrolle über Daten, Prozesse und Betreiberstrukturen. Eine souveräne Lösung zeichnet sich dadurch aus, dass klar erkennbar ist, welchem Rechtsraum sie unterliegt, welche Organisation letztlich Betreiber ist und welche technischen Mechanismen dem Kunden die tatsächliche Hoheit über seine Daten geben. Dazu gehören eigene Schlüsselhoheit, transparente Rollen- und Berechtigungskonzepte, Auditierbarkeit aller Betriebsprozesse und eine nachvollziehbare Exit-Strategie. Wenn Anbieter hingegen vor allem mit geografischen Hosting-Standorten argumentieren oder Souveränität als reine „Label-Eigenschaft" verwenden, ohne diese Kontrollpunkte abzubilden, handelt es sich eher um Marketing. Unternehmen sollten daher konsequent nachweisen lassen, wie sich Betreiberstrukturen, Verantwortlichkeiten und technische Kontrollen tatsächlich darstellen.

Mit Blick auf AI-Plattformen, generative Modelle und Datenräume entstehen völlig neue Abhängigkeiten. Wie müssen Unternehmen ihre Souveränitätsstrategie anpassen, wenn KI künftig tief in Kernprozesse eingreift?

Timon Schmotz: Sobald KI ein integraler Bestandteil der Wertschöpfung wird, verschiebt sich auch die Diskussion über Souveränität. Die eigentlichen Abhängigkeiten entstehen dann weniger bei Infrastruktur-Themen, sondern bei Modellen, Trainingsdaten, Update-Mechanismen und dem Zugriff auf spezialisierte Hardware. Unternehmen sollten ihre Strategien daher um den Aspekt der KI-Souveränität erweitern. Dazu gehört, Modelle und Datenflüsse klar zu kontrollieren, Trainingsprozesse transparent zu gestalten, europäische oder offene Modelle als Alternative zu prüfen und Governance-Strukturen zu etablieren, die den Umgang mit KI-Risiken nachvollziehbar regeln. Besonders Behörden verlangen zunehmend KI-Lösungen, die auditierbar, rechtskonform und sicher betreibbar sind – und zwar auch dann, wenn die Technologie selbst hochdynamisch ist. Wer diese Perspektive früh berücksichtigt, reduziert langfristige Abhängigkeiten und sichert seine Handlungsfähigkeit.

Wenn Sie auf Ihre Kunden blicken: Woran erkennt man, dass ein Unternehmen tatsächlich souveräner werden möchte – und nicht nur das Vokabular der politischen Debatte übernimmt?

Timon Schmotz: Man erkennt es daran, dass aus der Diskussion echte Maßnahmen werden. Organisationen, die souveräner werden wollen, definieren Verantwortlichkeiten, schaffen Governance-Strukturen, klassifizieren ihre Daten systematisch und führen Risikoanalysen für ihre Cloud- und Softwarelieferketten durch. Sie investieren in Transparenz über ihre Architekturen, schärfen ihre Sicherheitsmechanismen und etablieren Prozesse, die einen Anbieterwechsel tatsächlich möglich machen.

Unternehmen, die hingegen nur den Begriff in strategische Dokumente aufnehmen, jedoch weder Architekturen anpassen noch Budgets bereitstellen, sind meist eher im diskursiven als im operativen Modus. Souveränität zeigt sich daher nicht im Wording, sondern in der Konsequenz technischer und organisatorischer Entscheidungen.

"Organisationen, die souveräner werden wollen, definieren Verantwortlichkeiten, schaffen Governance-Strukturen, klassifizieren ihre Daten systematisch und führen Risikoanalysen für ihre Cloud- und Softwarelieferketten durch."

Timon Schmotz
Materna

Was bedeuten all diese Entwicklungen für Materna? Was erwarten Ihre Kunden von Ihnen, um souveräne IT-Ökosysteme erfolgreich aufzubauen und zu betreiben?

Timon Schmotz: Für Materna bedeutet dies eine deutliche Erweiterung unserer Rolle. Wir werden zunehmend als vertrauenswürdiger Partner gesucht, der technologische Expertise, regulatorisches Verständnis und architektonische Weitsicht miteinander verbindet. Unsere Kunden erwarten, dass wir sie ganzheitlich begleiten – von der Entwicklung einer souveränen Cloud- und Datenarchitektur über die Umsetzung von Governance-Modellen bis hin zu Sicherheit, Data-Management, KI-Strategien und Open-Source-Integration. Dabei geht es nicht nur um technische Implementierung, sondern immer häufiger auch um die Befähigung der Organisation selbst. Viele Kundinnen und Kunden möchten langfristig unabhängiger werden und benötigen Partner, die ihnen helfen, diese Eigenständigkeit strukturiert aufzubauen. Genau hier sehen wir unseren Auftrag: Souveränität nicht nur technisch, sondern auch organisatorisch zu ermöglichen.

Wenn wir drei Jahre vorspulen: Wie wird sich digitale Souveränität aus Ihrer Sicht weiterentwickeln? Welche Fortschritte erwarten Sie – und welche Herausforderungen werden Unternehmen und Behörden weiterhin begleiten?

Timon Schmotz: Digitale Souveränität wird deutlich stärker verankert sein – sowohl in Vergaben und regulatorischen Anforderungen als auch in Architekturentscheidungen. Souveräne Cloud-Modelle werden gereifter und funktional umfassender sein. Europäische Anbieter werden an Bedeutung gewinnen, auch wenn die Hyperscaler in vielen technologischen Segmenten weiterhin führend bleiben. Gleichzeitig wird der Bedarf an Nachweisen und Zertifizierungen steigen: Stakeholder möchten zunehmend sehen, wie Organisationen Souveränität tatsächlich umsetzen. Die größte Herausforderung wird allerdings in der Komplexität hybrider Architekturen liegen. Unternehmen und Behörden müssen lernen, regulatorische Sicherheit, Innovationsgeschwindigkeit und wirtschaftliche Effizienz miteinander auszubalancieren. Wer hier früh auf transparente und robuste Architekturen setzt, wird langfristig klar im Vorteil sein – und genau das ist die Entwicklung, die wir in den kommenden Jahren erwarten.