Lünendonk im Interview mit TechniData

Wer die Daten kontrolliert, gewinnt – Souveränität als Zukunftswährung

Digitale Souveränität ist längst zur strategischen Überlebensfrage geworden und erfordert klare Entscheidungen darüber, wer die Kontrolle über Daten, Systeme und KI-Modelle behält. Peter Jung, CEO der TechniData IT AG, erläutert, wie Unternehmen sich aus Abhängigkeiten lösen, ohne Innovationskraft einzubüßen, und warum hybride IT-Modelle zum neuen Standard werden. Er macht deutlich: Souveränität bedeutet heute nicht Abschottung, sondern professionelle Governance, transparente Partner und die konsequente Sicherung von Wechsel- und Handlungsfähigkeit.

Peter Jung
CEO
TechniData

Herr Jung, die TechniData IT-Gruppe ist ein deutscher IT-Service- und -Solution-Provider. Was bedeutet digitale Souveränität für Sie und welche Rolle nimmt TechniData dabei ein?

Peter Jung: Digitale Souveränität heißt für mich, bewusst zu entscheiden, welche Technologien wir einsetzen, wo unsere Daten liegen, wer im Ernstfall darauf zugreifen darf und unter welchen rechtlichen Rahmenbedingungen das geschieht. Es geht um Wettbewerbsfähigkeit, um Resilienz und Regulierung. Wer die Hoheit über Daten und Systeme verliert, verliert langfristig seinen Handlungsspielraum.

Wir sehen TechniData in der Rolle des Architekten und Sparringspartners. Wir bauen und betreiben IT-Infrastrukturen, organisatorisch, prozess- und sicherheitstechnisch. Ob in unserem, mit Blauem Engel und ISO 27000 zertifizierten Rechenzentrum am deutschen Standort, im lokalen Rechenzentrum des Kunden oder in der Cloud. Entscheidend ist, dass die Lösungen für den Kunden passend sind und nachhaltig seine digitale Souveränität stärken. Am Ende sollen unsere Kunden sagen können: Wir wissen was wir tun und wir behalten die Kontrolle..

Zu Ihren Kunden zählen Konzerne wie auch der Mittelstand. Welche Besonderheiten zeigt aus ihrer Sicht de Mittelstand im Vergleich zu Konzernen in Sachen Souveränität?

Peter Jung: In Bezug auf die Anforderungen sehen wir kaum Unterschiede zwischen Konzernen, Mittelstand oder öffentlicher Verwaltung. Die Ziele sind weitgehend identisch: unabhängig werden, Risiken beherrschen, Innovation ermöglichen.

Oft sind die Wege dorthin aber unterschiedlich. Je internationaler ein Unternehmen agiert, umso komplexer sind die technischen, juristischen und regulatorischen Anforderungen. Für viele global tätige Unternehmen führt deshalb Stand heute kein Weg an den großen amerikanisch dominierten Hyperscalern vorbei. An diesem Zustand wird sich auch kurzfristig kaum etwas ändern.

Was sich aber generell verändert hat: das Bewusstsein für Abhängigkeiten wächst spürbar. Wer kontrolliert die Plattform? In welchem Rechtsraum bewegen wir uns? Der Mittelstand denkt heute strategischer als noch vor einigen Jahren.

Wir haben davon gesprochen, dass der Mittelstand auch weiterhin IT-Services in eigenen Rechenzentren betreibt. Einerseits sind externe Abhängigkeiten somit eher gering, gleichzeitig kämpft der Mittelstand mit der digitalen Transformation, dem Fachkräftemangel und einer globalen Wettbewerbssituation. Sind die zunehmenden Souveränitätsanforderungen nun ein Treiber dafür, die IT-Strategie zu überdenken und neue Wege zu gehen?

Peter Jung: Ganz klar: ja. Wir erleben gerade so etwas wie eine strategische Standortbestimmung. Viele Unternehmen fragen sich sehr nüchtern: Was können und wollen wir selbst betreiben? Wo überfordern wir uns personell oder technologisch?

Das eigene Rechenzentrum galt lange als Inbegriff von Kontrolle. Heute sehen wir: Security, Compliance und ein 24/7-Betrieb sind in Zeiten des Fachkräftemangels nur schwer wirtschaftlich abzubilden. Für viele Mittelständler ist es sinnvoller, auf zertifizierte Rechenzentren von lokalen Dienstleistern oder Managed Services zu setzen. Nicht als Kontrollverlust, sondern als bewusste Arbeitsteilung. Souveränität entsteht durch professionelle Sicherheits- und Betriebsstandards, nicht allein durch den Standort.

Hybride Modelle spielen dabei eine große Rolle. Kritische Systeme bleiben in einer souveränen Umgebung, andere Workloads laufen flexibel in der Cloud. Digitale Souveränität wird so zum Kompass: Was gehört strategisch ins eigene Haus? Was in ein Datacenter „Made in Germany"? Wo nutze ich bewusst internationale Plattformen? Diese Differenzierung schafft Stabilität und Machbarkeit, ohne Innovationskraft einzubüßen.

89 Prozent der Studienteilnehmer geben an, dass Datensouveränität eine sehr hohe Relevanz für Ihr Unternehmen hat. Hinterfragen Kunden heute stärker, wo ihre Daten liegen und wie sicher sie sind?

Peter Jung: Absolut! Die Frage nach dem Datenstandort ist kein reines IT-Thema mehr. Auch endet sie nicht bei der Geografie. Es geht um Zugriffsmöglichkeiten, um Rechtsräume, um Transparenz. Gesetze wie die DSGVO oder internationale Regelwerke wie der Cloud Act haben das Bewusstsein geschärft. Auch wenn viele Unternehmen über die europäischen Datenschutzregeln schimpfen, so wollen doch die allermeisten von diesen Regeln profitieren.

Unternehmen wollen wissen: Wer kann im Zweifel auf Daten zugreifen? Wie sind Zugriffe dokumentiert? Wie sehen Backup- und Recovery-Konzepte aus? Insbesondere im Gesundheitswesen, in der Industrie oder bei kritischen Infrastrukturen ist das existenziell. Dort geht es um Patientendaten, um geistiges Eigentum oder um Versorgungs- und Produktionsfähigkeit.

Datensouveränität bedeutet deshalb nicht Abschottung oder komplette Rückkehr zu On-Premises-Lösungen, sondern Professionalität und Lösungswillen.

Unternehmen suchen Partner, die transparent, zertifiziert und nachvollziehbar arbeiten. Datensouveränität ist kein Hemmschuh für Innovation, sie ist ihre Voraussetzung und schafft Mut für weitere Digitalisierungsschritte.

Ebenso zeigt die Studie auf, dass komplexe IT-Landschaften die Förderung von digitaler Souveränität stark beeinträchtigen, da historisch gewachsene Systeme nur mit großem Aufwand anpassbar sind und die Betriebsfähigkeit dadurch gefährdet wird. An welchen Stellen ist digitale Souveränität überhaupt sinnvoll und realisierbar?

Peter Jung: Tatsächlich ist die Ablösung von gewachsenen IT-Systemen, unabhängig vom Betriebsmodell, für alle Unternehmen eine riesige Herausforderung. Digitale Souveränität kann auch verloren gehen, wenn wir zu lange an Systemen oder Technologien festhalten, deren Support und Wartung immer schwieriger wird. Dies trifft besonders stark auf eigenentwickelte Systeme zu.

"Datensouveränität ist kein Hemmschuh für Innovation, sie ist ihre Voraussetzung."

Peter Jung
TechniData

Solche Systeme bremsen nicht nur Transformation, sondern schaffen zudem Abhängigkeiten von Einzelpersonen oder spezialisiertem Know-how und gefährden damit langfristig Souveränität. Gleichzeitig haben sich Cloud-Lösungen vor allem im Bereich Collaboration und Arbeitsplatzsysteme in den vergangenen Jahren stärker durchgesetzt, weil sie skalierbar und effizient sind. Es muss daher immer eine bewusste Entscheidung sein, welche Systeme in die Cloud migriert werden und welche Systeme unbedingt lokal betrieben werden müssen. Die Zukunft liegt hier ganz klar in hybriden Systemlandschaften, die je nach Anforderung die Vorteile von Cloud und On-Premises sinnvoll kombinieren.

Kritische Workloads können im eigenen Rechenzentrum oder in einer souveränen Cloud betrieben werden, während weniger sensible Anwendungen in flexiblen, skalierbaren Public-Cloud-Umgebungen laufen.

Mit dem Vormarsch generativer KI verschieben sich Datenflüsse und Abhängigkeiten erneut. Wie verändert der Einsatz von KI aus Ihrer Sicht die Anforderungen an digitale Souveränität. Welche Leitplanken empfehlen Sie Unternehmen konkret, bevor sie sensible Prozesse oder Daten an KI-Plattformen koppeln?

Peter Jung: KI ist keine Entscheidung für oder gegen ein Toolset, sondern ein Technologiesprung, dessen Anfänge wir gerade erst erleben. Aber hier gelten im Grund die gleichen Fragen wie bei der Auslagerung von Daten an dritte Anbieter. Welche Daten dürfen das eigene Haus verlassen und welche nicht?

Generative KI schafft eine neue Qualität der Abhängigkeit. Dabei werden nicht nur Daten verarbeitet. Modelle, die mit Unternehmenswissen angereichert sind, erzeugen neue Inhalte und Entscheidungsgrundlagen. Damit entsteht eine zusätzliche Ebene der Souveränität: die Kontrolle über Wissensableitung und Modellverhalten.

In sensiblen Bereichen kann eine generative KI-Lösung in einer On-Premises-Architektur sinnvoll sein. In anderen Szenarien bieten Plattformlösungen enorme Innovationsgeschwindigkeit. Entscheidend ist, dass Architektur, Governance und Compliance sauber definiert sind. Dazu gehören eine verbindliche Prompt-Governance, die Protokollierung von Interaktionen sowie gezielte Schulungen für Mitarbeitende, um unbeabsichtigte Datenabflüsse zu vermeiden.

Letztendlich geht es auch bei KI darum, dass ein Unternehmen die Kontrolle über die genutzten Modelle, Datenquellen und Zugriffsrechte behält. Souveränität setzt voraus, Modelle oder Plattformen bei Bedarf wechseln zu können. Architekturentscheidungen sollten daher konsequent auf Portabilität und Exit-Fähigkeit ausgelegt sein.

Wenn ein Unternehmen digitale Souveränität ernsthaft angehen will: Wie sieht aus Ihrer Sicht ein professioneller Einstieg aus – von der Risikoanalyse bis zu einer tragfähigen Souveränitätsstrategie?

Peter Jung: Ein professioneller Einstieg beginnt immer mit einem Perspektivwechsel. Digitale Souveränität ist weit mehr als nur die Frage, wo Daten gespeichert werden. Es geht zuallererst um den aktiven Schutz der digitalen Identität eines Unternehmens, seiner Systeme und seiner gesamten Geschäftsprozesse.

Wir starten deshalb immer mit einer strukturierten Vorgehensweise. Wo werden sensible Daten verarbeitet? Welche Abhängigkeiten bestehen? Welche rechtlichen und technischen Risiken ergeben sich? Darauf aufbauend erfolgt eine Bestandsaufnahme der kompletten IT-Landschaft.

Auf dieser Basis entwickeln wir eine Sicherheitsarchitektur und bewerten den Reifegrad entlang von Infrastruktur, Applikationen, Daten und internem Know-how. Regulatorische Anforderungen wie DSGVO oder NIS-2 werden integriert. Die Datenhaltung und -verarbeitung sollte idealerweise im rechtssicheren EU-Raum erfolgen, vorzugsweise in einem zertifizierten deutschen Rechenzentrum.

"Digitale Souveränität ist weit mehr als nur die Frage, wo Daten gespeichert werden. Es geht zuallererst um den aktiven Schutz der digitalen Identität eines Unternehmens, seiner Systeme und seiner gesamten Geschäftsprozesse."

Peter Jung
TechniData

Daraus entsteht eine tragfähige Souveränitätsstrategie, mit definierten Zielen, priorisierten Handlungsfeldern und konkreten Projekten. Entscheidend ist jedoch: Digitale Souveränität ist kein einmaliges Projekt, sondern ein laufender Steuerungsprozess mit regelmäßigen Reviews. Genau deshalb gehört sie ins Board und nicht isoliert in die IT. Die Verantwortung sollte organisatorisch klar auf C-Level organisiert sein, denn sie beeinflusst unmittelbar Geschäftsmodell, Risikoprofil und Wettbewerbsfähigkeit. Wird sie so verstanden, wachsen unternehmerische Handlungsfähigkeit, Resilienz und Wettbewerbsvorteile.

Digitale Souveränität erfordert eine sichere und verlässliche IT. Die TechniData IT-Gruppe entwickelt und betreibt IT-Infrastrukturen für Mittelstand, Konzerne und öffentliche Einrichtungen und schafft damit eine stabile, zukunftsfähige Basis für Geschäftsprozesse. Unser Anspruch ist es, IT so zu gestalten, dass Transparenz, Kontrolle und langfristige Handlungsfähigkeit gewährleistet sind.

Wir begleiten unsere Kunden ganzheitlich, von der Beratung über die Konzeption moderner IT-Architekturen bis zu Implementierung, Betrieb und kontinuierlicher Weiterentwicklung. Unser Service Desk gewährleistet stabile IT-Prozesse im Tagesgeschäft.

IT verstehen wir als integralen Bestandteil des Geschäftsmodells. Technologien entfalten ihren Wert erst dann, wenn sie sicher, wirtschaftlich und nachhaltig eingesetzt werden. Ein zentraler Pfeiler digitaler Souveränität ist unsere eigene Datacenter-Infrastruktur: Im Raum Stuttgart betreiben wir ein hochsicheres, hochverfügbares Rechenzentrum, ergänzt durch zwei georedundante Standorte im Raum Frankfurt. Dort stellen wir mit der „Flex Cloud" eine souveräne Cloud bereit, die volle Transparenz über Speicherung und Verarbeitung der Daten bietet. Unser eigenes Security Operations Center (SOC) sorgt durch kontinuierliches Monitoring, strukturierte Prozesse und klare Verantwortlichkeiten für hohe Sicherheit und digitale Resilienz.

Mit unseren spezialisierten und eigenständigen Gesellschaften decken wir ein breites Portfolio ab: von Netzwerk- und IT-Security über Cloud- und Managed Services bis zu Open-Source-Technologien. Besonders in KRITIS-Bereichen verfügen wir über langjährige Erfahrung und tiefgehende Expertise.

Seit 2005 entwickeln wir uns kontinuierlich weiter. Heute beschäftigt die TechniData IT-Gruppe über 360 Mitarbeitende. Unser Handeln basiert auf Vertrauen, Verantwortung und langfristigen Partnerschaften. Firmensitz der TechniData IT AG, Holding der Gruppe, ist Karlsruhe.

UNTERNEHMENSPROFIL

TECHNI DATA
it-gruppe

KONTAKT

Petra Moggioli
Leiterin Unternehmenskommunikation
E-Mail: petra.moggioli@technidata-it.com

Dennis Pudeck
Leiter Marketing & Produktmanagement
E-Mail: dennis.pudeck@technidata-it.com

TechniData IT AG
Albert-Nestler-Str. 28, 76131 Karlsruhe
Website: https://www.technidata.de/