

Foto: Adobe Stock/.shock

Beim Thema IT-Sicherheit ist meist die Software im Blick - die physische Grundlage der Daten sollte aber ebenfalls nicht außer Acht gelassen werden: „Fallen Rechenzentren aus oder lassen sie sich nicht an neue Anforderungen anpassen, gerät die Handlungsfähigkeit der Verwaltung unter Druck."

Rechenzentren

Angelpunkte digitaler Souveränität

Software, Cloud, Daten: Das alles macht Digitalisierung aus. Dazu kommt aber auch die physische Infrastruktur – Rechenzentren spielen eine wesentliche Rolle für die digitale Souveränität. Warum er Kommunen empfiehlt, hier neu zu denken, schlüsselt IT-Experte Georg Raiser auf.

Immer mehr Verwaltungsleistungen werden digital. Laut Branchenverband Bitkom sind inzwischen 349 von 579 Leistungen regional online verfügbar. Damit wächst die Abhängigkeit von der Infrastruktur, auf der diese Leistungen laufen: den Rechenzentren. Fallen sie aus oder lassen sie sich nicht an neue Anforderungen anpassen, gerät die Handlungsfähigkeit der Verwaltung unter Druck.

KONTROLLE IST ENTSCHEIDEND FÜR KOMMUNEN

Bei digitaler Souveränität stehen häufig Software, Cloud-Anbieter und Daten im Mittelpunkt. Doch jede digitale Verwaltungsleistung ist letztlich auf physische Infrastruktur angewiesen.

Digitale Souveränität heißt für Kommunen, wesentliche Entscheidungen über Daten und Systeme selbst treffen zu können: Wo werden Daten verarbeitet, wer kann zugreifen, welchem Rechtsraum unterliegen Vertragspartner? Lassen sich Anwendungen und Daten später übertragen?

Der US Cloud Act zeigt, warum der Speicherort allein noch keine Souveränität gewährleistet. Unter bestimmten Voraussetzungen können Unternehmen, die der US-Jurisdiktion unterliegen, im Rahmen rechtmäßiger Verfahren zur Herausgabe von Daten verpflichtet werden – auch wenn sie in Europa gespeichert sind. Entscheidend sind daher neben dem →

MEHR KAPAZITÄTEN

Die Nationale Rechenzentrumsstrategie wurde am 18. März 2026 vom Bundeskabinett veröffentlicht. Sie zielt laut Bundesministerium für Digitales und Staatsministerium darauf ab, die Rechenzentrumskapazitäten in Deutschland bis 2030 mindestens zu verdoppeln und die Rechenkapazitäten für High-Performance-Computing (HPC) und Künstliche Intelligenz (KI) mindestens zu vervierfachen. Die Strategie richte sich an Betreiber, Investoren, Ausrüster und Gestalter der digitalen Zukunft sowie die öffentliche Hand. Sie umfasst laut Ministerium drei zentrale Handlungsfelder:

- Energie und Nachhaltigkeit: Förderung nachhaltiger Rechenzentren mit erneuerbarem Strom und energieeffizienten Lösungen.
- Standort und Fläche: Beschleunigung von Planungs- und Genehmigungsverfahren sowie Ausweisung von Vorzugsflächen.
- Technologie und Souveränität: Aufbau hochleistungsfähiger KI-Rechenkapazitäten und Unterstützung der Ansiedlung einer europäischen KI-Gigafabrik in Deutschland.

Standort auch Kontrolle, Rechtsraum, Portabilität und Resilienz. Die Politik reagiert darauf mit Initiativen wie dem Cloud and AI Development Act und der Nationalen Rechenzentrumsstrategie.

WIE ZEIGT SICH RESILIENZ BEIM STROMAUSFALL?

Digitale Souveränität bemisst sich ebenso daran, ob kritische Services auch bei Stromausfällen, Cyberangriffen oder anderen Störungen verfügbar bleiben oder schnell wiederhergestellt werden. Geografisch getrennte Rechenzentren können die Resilienz erhöhen, wenn sie weit genug auseinanderliegen und dadurch unterschiedliche Risikoprofile aufweisen.

Kommunen sollten auch das Energieeffizienzgesetz (EnEfG) beachten. Eine zentrale Kennzahl ist die Power Usage Effectiveness (PUE), die Gesamtenergieverbrauch und IT-Verbrauch ins Verhältnis setzt. Bestandsrechenzentren dürfen ab 2027 höchstens eine PUE von 1,5 und ab 2030 von 1,3 aufweisen. Für Rechenzentren, die ab 1. Juli 2026 den Betrieb aufnehmen, gilt maximal 1,2.

Hinzu kommen Vorgaben etwa zur Abwärmenutzung. Das erhöht den Modernisierungsdruck auf Kommunen mit eigenen Rechenzentren.

Auch Künstliche Intelligenz (KI) verschärft die Anforderungen. Rechenintensive Anwendungen verlangen mehr von Stromversorgung, Leistungsdichte und Kühlung. Moderne Infrastruktur muss zudem Konnektivität und Anpassungsfähigkeit für sich verändernde Workloads bieten.

Wer heute Infrastruktur beschafft oder modernisiert, sollte deshalb Datenkontrolle, Resilienz, Effizienz und AI Readiness berücksichtigen und drei Infrastrukturoptionen abwägen: On-Premise, Cloud und Colocation. Das ist keine Entweder-Oder-Entscheidung – auch eine Mischung kann das Ergebnis sein.

ON-PREMISE

On-Premise heißt: Die Server befinden sich in eigenen Räumen oder Rechenzentren der Kommune oder ihres IT-Dienstleisters. Das bietet direkte Kontrolle. Gleichzeitig müssen Stromversorgung, Kühlung, Sicherheit und Konnektivität betrieben und modernisiert sowie qualifiziertes Fachpersonal vorgehalten werden. Entscheidend ist, ob die Kommune diese Infrastruktur personell, technisch und wirtschaftlich dauerhaft betreiben und etwa für KI und EnEfG weiterentwickeln kann.

CLOUD-SERVICES

Cloud-Services stehen schnell bereit und skalieren, während Gebäudeinfrastruktur und Hardware ausgelagert sind. Kommunen müssen jedoch Abhängigkeiten berücksichtigen. Proprietäre Technologien und große Datenmengen können einen späteren Anbieterwechsel erschweren oder verteuern. Datenübertragbarkeit und die Möglichkeit, einen Cloud-Service zu verlassen, sollten deshalb von Beginn an feste Beschaffungskriterien sein.

COLOCATION

Bei Colocation sind Gebäudeinfrastruktur und IT getrennt. Der Anbieter stellt Rechenzentrumsflächen samt Energieversorgung, Kühlung, Brandschutz, physischer Sicherheit und Konnektivität bereit. Die Kommune oder ihr IT-Dienstleister bleibt Eigentümer der Server und behält die Kontrolle über Betriebssysteme, Anwendungen und Daten. So lässt sich die komplexe physische Infrastruktur an einen spezialisierten Betreiber auslagern, ohne die direkte Kontrolle über die IT-Umgebung aufzugeben. Colocation kann damit Teil einer hybriden Strategie aus Kontrolle, Resilienz und Flexibilität sein.

Colocation wird für immer mehr Organisationen attraktiv. Laut Bitkom entfielen 2025 erstmals mehr als 50 Prozent der deutschen Rechenzentrumskapazität auf Colocation. Das Segment wuchs gegenüber dem Vorjahr um 17,5 Prozent.

WELCHE INFRASTRUKTUR PASST?

Keine der drei Infrastrukturoptionen schafft automatisch digitale Souveränität. Kritische Systeme können beispielsweise in Colocation laufen, standardisierte Anwendungen ohne sensible Daten in der Cloud und Back-ups im eigenen Rechenzentrum. Entscheidend ist, Datenkontrolle, Resilienz, Effizienz und AI Readiness gemeinsam zu betrachten und daraus abzuleiten, welche Infrastruktur für die jeweilige Anforderung am besten passt. Die Infrastrukturwahl wird damit zum Fundament kommunaler digitaler Souveränität. *Georg Raiser*



Foto: Adobe Stock/Zerofukuman

Entscheidend sollte sein: „Datenkontrolle, Resilienz, Effizienz und AI Readiness gemeinsam zu betrachten und daraus abzuleiten, welche Infrastruktur für die jeweilige Anforderung am besten passt."

DER AUTOR

Georg Raiser ist Managing Director DACH bei AtlasEdge.