

Die Basis muss stimmen

Georg Raiser

Digitale Souveränität hängt auch von der IT-Infrastruktur ab. Kommunen müssen deshalb abwägen, wie sie Kontrolle, Resilienz, Skalierbarkeit und Wirtschaftlichkeit verbinden. On-Premise, Cloud und Colocation bieten dafür unterschiedliche Ansätze.

Laut dem Hightech-Verband Bitkom werden inzwischen 349 von 579 Verwaltungsleistungen digital angeboten. Und auch intern wird immer mehr digitalisiert. Digitalisierung schafft aber nur dann Mehrwert, wenn sie zuverlässig funktioniert – sprich: Services müssen verfügbar bleiben. Damit wird die IT-Infrastruktur zu einem strategischen Faktor. Sie bestimmt entscheidend mit, wie digital souverän eine Kommune sein kann.



Chorut/stock.adobe.com

Eine souveräne IT-Infrastruktur bildet das Fundament erfolgreicher Digitalisierung.

Digitale Souveränität bedeutet die Fähigkeit, IT selbstbestimmt und sicher zu nutzen und dabei die Kontrolle über wesentliche Entscheidungen zu Daten und Systemen zu behalten. Die vergangenen Jahre haben gezeigt, dass der Zugriff auf Daten von rechtlichen Rahmenbedingungen abhängig ist, die außerhalb von Europa gesetzt werden. So verpflichtet der US CLOUD Act Anbieter unter US-Jurisdiktion dazu, auf Anfrage Daten bereitzustellen, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden – unabhängig davon, wo diese Daten gespeichert sind. Für Kommunen ist die Frage, welchen Jurisdiktionen ihre Anbieter unterliegen, daher wichtig für die Entscheidung, wo und wie Daten verarbeitet werden.

Dieser Aspekt rückt auch regulatorisch in den Fokus. So soll der 2026 vorgeschlagene Cloud and AI Development Act den Ausbau von Rechen-, Cloud- und KI-Kapazitäten unterstützen und einen gemeinsamen Rahmen schaffen, mit dem sich die Souveränität entsprechender Angebote besser bewerten lässt. Für öffentliche Auftraggeber könnte damit transparenter werden, welche rechtlichen, technischen und organisatorischen Abhängigkeiten mit einem Angebot verbunden sind. Auch die im März 2026 veröffentlichte Nationale Rechenzentrumsstrategie soll die technologische Souveränität stärken.

Eine Kommune bleibt nur handlungsfähig, wenn kritische Services

und Daten auch bei Stromausfällen, Cyber-Angriffen oder technischen Defekten verfügbar bleiben oder innerhalb eines vertretbaren Zeitraums wiederhergestellt werden können. Resilienz ist deshalb ein wesentlicher Bestandteil von Souveränität. Für kritische Services kann eine geografisch getrennte Infrastruktur sinnvoll sein. Wird ein zweiter Standort unabhängig vom ersten betrieben – mit separater Stromversorgung und Konnektivität sowie einem anderen lokalen Risikoprofil –, reduziert dies das Risiko, dass ein einzelner Vorfall beide betrifft.

Für Organisationen, die langfristige Infrastrukturentscheidungen treffen, werden Energieeffizienz

und der Zugang zu nachhaltiger Energie neben Resilienz, Sicherheit und Kosten zu wichtigen Kriterien. Ein zentraler Kennwert der Energieeffizienz von Rechenzentren ist die Power Usage Effectiveness (PUE). Je näher der PUE-Wert an 1,0 liegt, desto effizienter arbeitet das Rechenzentrum. Das Energieeffizienzgesetz (EnEfG) verschärft hier die Anforderungen. Bestandsrechenzentren müssen ab 2027 einen PUE-Wert von höchstens 1,5 und ab 2030 von höchstens 1,3 erreichen. Für Anlagen, die ab Juli 2026 in Betrieb gehen, gilt grundsätzlich ein Höchstwert von 1,2. Das EnEfG betrifft auch Rechenzentren der öffentlichen Hand.

Modernisierungsdruck entsteht jedoch nicht allein durch das EnEfG. KI- und andere High-Density-Workloads erhöhen die Leistungsdichte pro Rack und stellen neue Anforderungen an Rechenzentren. Das kann leistungsfähigere Kühlkonzepte, höhere Anforderungen an die Stromverteilung und mitunter auch an Bodenlasten und Statik erforderlich machen.

Vor diesem Hintergrund sind Kommunen gut beraten, drei grundlegende IT-Infrastrukturoptionen zu betrachten: On-Premise, Cloud und Colocation. On-Premise bedeutet, dass die Server in eigenen Räumen oder Rechenzentren der Kommune oder ihres IT-Dienstleisters laufen. Die Kommune behält dabei die Kontrolle über Hardware, Netzwerke, Zugänge und Datenhaltung. Diese unmittelbare Kontrolle kann für besonders schützenswerte Systeme ein wichtiger Vorteil sein.

Sie kommt aber zum Preis hoher Kosten, denn ein Rechenzentrum

umfasst weit mehr als Server. Von der Stromversorgung über Kühlung, Brandschutz, physische Sicherheit und Konnektivität bis hin zu Back-ups und Hardware: All das kostet Geld und erfordert qualifiziertes Fachpersonal. Daher kann ein veraltetes eigenes Rechenzentrum die Souveränität eher einschränken als stärken. Eigentümer der Infrastruktur zu sein, garantiert somit noch keine digitale Souveränität.

Cloud-Services wiederum bieten flexiblen Zugriff auf Speicher, Rechenkapazität, Plattformen und Anwendungen und ermöglichen eine schnelle Skalierung, ohne dass Kommunen die zugrunde liegende Infrastruktur selbst besitzen müssen. Für viele Workloads kann das erhebliche operative und wirtschaftliche Vorteile bieten. Gleichzeitig müssen Organisationen Abhängigkeiten, die mit einzelnen Cloud-Plattformen einhergehen können, aktiv managen. Ein Vendor-Lock-in kann entstehen, wenn eine Anwendung proprietäre Datenbanken, Schnittstellen oder Funktionen nutzt, die nur ein bestimmter Cloud-Anbieter bereitstellt. Soll dann später ein Wechsel zu einem anderen Anbieter erfolgen, kann das erhebliche Probleme und Kosten verursachen.

Bei großen Datenbeständen kommen mögliche Egress-Kosten hinzu. Diese entstehen, wenn Daten aus einer Cloud-Umgebung zu einem anderen Anbieter oder Standort übertragen werden. Für Kommunen ist deshalb entscheidend, bereits bei der Beschaffung zu klären, wie Daten und Anwendungen exportiert werden können, wie aufwendig ein Wechsel wäre und welche Kosten dabei entstehen.

Colocation schließlich trennt die Gebäudeinfrastruktur von der IT. Der Colocation-Anbieter stellt Rechenzentrumsflächen einschließlich Energieversorgung, Kühlung, Brandschutz, physischer Sicherheit und Konnektivität bereit. Die Kommune oder ihr IT-Dienstleister bleibt als Eigentümer der Server für Betriebssysteme, Anwendungen und Daten verantwortlich. Diese Arbeitsteilung wird für immer mehr Organisationen attraktiv. Im vergangenen Jahr entfiel laut Bitkom erstmals mehr als die Hälfte der deutschen Rechenzentrumskapazität auf Colocation; die Kapazität dieses Segments wuchs gegenüber dem Vorjahr um 17,5 Prozent.

Digitale Souveränität wird nicht dadurch bestimmt, ob Infrastruktur On-Premise, in der Cloud oder in Colocation betrieben wird. Sie entsteht durch bewusste Entscheidungen darüber, wo Daten und Anwendungen liegen, wer sie kontrolliert, wie resilient sie sind und wie einfach sie verlagert werden können. Extrem kritische Systeme können beispielsweise in Colocation laufen, während standardisierte Anwendungen ohne sensible Daten in der Cloud betrieben werden und Back-ups in einem eigenen Rechenzentrum liegen.

Eine solche hybride Architektur ermöglicht es Organisationen, bewusste Entscheidungen zwischen Kontrolle, Skalierbarkeit, Resilienz und Wirtschaftlichkeit zu treffen. Die Wahl der richtigen IT-Infrastruktur bildet das Fundament digitaler Souveränität.

Georg Raiser ist Managing Director der AtlasEdge DACH-Region.