Digitale Souveränität

Die Kontrolle behalten

[29.08.2024] Die Wahl des richtigen Cloudanbieters ist entscheidend, um die digitale Souveränität zu erhöhen. Darüber hinaus minimieren ein Multicloudansatz und Open Source Software die Abhängigkeit von einzelnen Anbietern.

Digitale Souveränität in öffentlichen Einrichtungen ist kein Luxus, sondern eine Notwendigkeit. Der Staat darf sich nicht von Akteuren abhängig machen, die im Grundgesetz nicht vorgesehen sind. So sind beispielsweise sensible personenbezogene Daten der Bürger in staatlicher Obhut nur dann wirksam vor unberechtigten Zugriffen geschützt, wenn der Staat seine digitale Infrastruktur kontrollieren kann.Eine zu große Nähe der IT staatlicher Institutionen zu Akteuren außerhalb der eigenen Jurisdiktion birgt die Gefahr einer Beeinträchtigung der digitalen Souveränität. So können beispielsweise US-Behörden aufgrund der Gesetze CLOUD Act und Foreign Intelligence Surveillance Act (FISA) häufig ohne richterliche Anordnung oder Widerspruchsmöglichkeit Daten von US-Providern anfordern, unabhängig davon, wo diese gespeichert sind. Ein weiterer Grund, warum digitale Souveränität für staatliche Institutionen ein Muss sein sollte, ist ein ganz pragmatischer: In politisch unsicheren Zeiten ist es wichtig, dass der Staat zeigen kann, dass er auch im digitalen Bereich souverän handeln kann, ohne erpressbar zu sein: Wer seine IT in die Hände US-amerikanischer Dienstleister gibt, macht sich im Spannungsfall von Anordnungen eines US-Präsidenten abhängig, die als Sanktionen unmittelbar auch außerhalb der USA wirken können. Zudem benötigt IT in US-Hand fast immer eine Verbindung zu Back Ends in den USA – typischerweise hergestellt über Tiefseekabel im Ozean und damit angreifbar. **Drei denkbare Lösungen** Damit die öffentliche Hand ein gesundes Maß an digitaler Souveränität erreichen kann, ohne dass die Kosten unkalkulierbar werden, bieten sich verschiedene technische Lösungen an. So gibt es beispielsweise das so genannte Air-Gapping in Rechenzentren der öffentlichen Hand, bei dem ein Computersystem oder ein Netzwerk physisch von anderen Netzwerken wie dem Internet isoliert wird. Hacker hätten so kaum Möglichkeiten, an Daten zu gelangen. Allerdings bringt eine solche Lösung auch neue Herausforderungen mit sich, etwa eine gewisse Einschränkung der Konnektivität und damit der uneingeschränkten Nutzbarkeit. Eine weitere Möglichkeit wäre ein Multicloudansatz, der die Abhängigkeit von einzelnen Anbietern minimiert. Dieser Ansatz sollte vorzugsweise auf Brokerage-Portalen basieren, die dafür sorgen, dass die beteiligten Clouddienstleister entsprechend kuratiert werden und geeignete Schnittstellen zur Verfügung stehen. Auf diese Weise kann die öffentliche Hand auf Clouddienste verschiedener Anbieter zugreifen und diese nutzen. Drittens ist Open Source Software zu nennen. Diese bietet den Nutzern mehr digitale Souveränität, da der öffentliche Code einsehbar ist und ein Vendor Lock-in vermieden werden kann. Open Source lebt von der Zusammenarbeit und sollte nicht von einem einzelnen Marktteilnehmer oder einem Staat dominiert werden. Open Code ermöglicht es Nutzern, Software zu modifizieren oder auf andere Systeme zu migrieren, wodurch Abhängigkeiten von einzelnen Anbietern vermieden werden. Die Verantwortlichen im öffentlichen Sektor müssen abwägen, ob der Einsatz sinnvoll ist, da sich die Mitarbeiter möglicherweise an neue Software gewöhnen müssen, was eine kulturelle Herausforderung darstellen kann.**Was der Anbieter leisten muss** Die Wahl des richtigen Cloudanbieters ist entscheidend für die Stärkung der digitalen Souveränität. Öffentliche Einrichtungen sollten bei der Auswahl darauf achten, dass der Anbieter ihre besondere Situation und ihre Einschränkungen versteht. Dazu gehören das föderale Prinzip der Bundesrepublik und die grundgesetzlichen Beschränkungen der Zusammenarbeit zwischen dem Bund und anderen föderalen Ebenen. Darüber hinaus sollte der Anbieter in der Lage sein, Fragen der Compliance

und des Datenschutzes angemessen zu berücksichtigen. Der Anbieter muss zudem ein Mindestangebot an Leistungen erbringen. Er muss loyal gegenüber dem Staat sein, für den er die Dienstleistung erbringt, und dort Steuern zahlen, wo das Geld verdient wird. Außerdem sollte er ein C5-Zertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI), eine Zertifizierung nach ISO 27001 und BSI IT-Grundschutz vorweisen können. Darüber hinaus ist es sinnvoll, wenn der Cloudanbieter über eine ausreichende Bonität für einen planbaren und nachhaltigen Service über einen längeren Zeitraum sowie über eine ausreichende Investitionskraft verfügt. Zu guter Letzt sollte er die Möglichkeit einer geografischen Redundanz für Speicherung, Back-up und Recovery nachweisen können. Das heißt, er sollte in der Lage sein, die Daten an mehreren geografisch voneinander getrennten Standorten zu speichern. **Souverän entscheiden** Es bleibt noch viel zu tun. In Deutschland beispielsweise müssten einige Artikel des Grundgesetzes behutsam geändert werden, damit die föderalen Ebenen besser zusammenarbeiten können. Darüber hinaus wäre es hilfreich, wenn eine souveräne digitale Infrastruktur die gleiche Aufmerksamkeit erhalten würde wie beispielsweise die Verkehrsinfrastruktur oder der Glasfaseranschluss. Souveränes Cloud Computing wird für die Daseinsvorsorge immer wichtiger, deshalb sollte die öffentliche Hand auch auf Cloudalternativen aus Deutschland und Europa vertrauen.

()

Dieser Beitrag ist in der Ausgabe August 2024 von Kommune21 im Schwerpunkt Cloud erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Cloud Computing, Digitale Souveränität, IONOS