

Souveränitäts-Washing bei Clouddiensten

[02.09.2025] Ist eine Cloud souverän, nur weil die Server in Europa stehen? Auf diese Frage geht ein neues Whitepaper des Zentrums für Digitale Souveränität (ZenDiS) ein. Es erklärt die Problematik des sogenannten Souveränitäts-Washing und gibt Kriterien für tatsächlich souveräne Lösungen an die Hand.

Souveränitäts-Washing bei Cloud-Diensten erkennen: Unter diesem Titel hat jetzt das Zentrum für Digitale Souveränität ([ZenDiS](#)) ein [Whitepaper](#) veröffentlicht. Das Dokument gibt Kriterien für souveräne Clouds an die Hand und soll bei der Bewertung bestehender Angebote helfen. „Mit ihrer Größe und Marktmacht haben vor allem die US-amerikanischen Hyperscaler in den vergangenen Jahren faktisch ein Oligopol geschaffen“, heißt es in der Einleitung des Papers. Diese Stellung wollen die Konzerne nicht aufgeben. „Ihre Reaktion auf das europäische Streben nach mehr Digitaler Souveränität sind neue Produkte, die Souveränität versprechen – aber faktisch nicht liefern“, schreiben die Verfasser der ZenDiS-Veröffentlichung. Beispielsweise verweisen die Konzerne auf europäische Rechenzentren, Datengrenzen oder Partnerschaften mit hiesigen Unternehmen. Allerdings habe dieses Souveränitätsversprechen „in technischer, rechtlicher und operativer Hinsicht keinen Bestand“. Diese „neue Verpackung altbekannter Abhängigkeiten“ wird als Souveränitäts-Washing bezeichnet.

Hinzu komme, dass Interessenvertreter der Konzerne die Digitale Souveränität als nicht definiert darstellen und versuchen, sie in ihrem Sinne umzudeuten. Auch diesen Aspekt berücksichtigt das Whitepaper. „Es bringt in Erinnerung, wie Politik und Verwaltung in Deutschland Digitale Souveränität definieren, gibt klare, sachliche Kriterien an die Hand und zeigt auf, warum sich Digitale Souveränität nicht allein an Rechenzentrumsstandorten oder Betriebsmodellen festmachen lässt“, heißt es in der Publikation. Dazu wird unter anderem aufgezeigt, warum proprietäre Cloud-Infrastrukturen strukturell unsouverän bleiben. Zum einen führen hier Update-Zyklen zur Betriebsabhängigkeit. Zum anderen bestehe ein strukturbedingter Plattform-Lock-in. Zwar werben die meisten Anbieter mit der Unterstützung offener Standards. Da der Aufwand eines Plattformwechsels aber in technischer, organisatorischer und finanzieller Hinsicht zu hoch sei, sei die Portabilität von Daten und Workloads quasi nur auf dem Papier gegeben.

Nicht zuletzt geht das Paper auf juristische Risiken ein und hält rechtliche Entwicklungen und politische Beobachtungen fest.

Die Publikation stützt sich laut ZenDiS auf Vorarbeiten und Positionen unter anderem der Datenschutzkonferenz (DSK), der Digitalministerkonferenz sowie des Bundesministeriums des Innern (BMI) und der Föderalen IT-Kooperation (FITKO). Zudem blickt sie auf den Koalitionsvertrag der aktuellen Regierung und auf die Regelungen des EU Data Acts.

(ve)