Zentrum Digitale Souveränität

Digitale Souveränität als Staatsaufgabe

Bausteine einer souveränen Digitalstrategie | 02/2025

Politischer Handlungsbedarf

Die deutsche Verwaltung ist in hohem Maße abhängig von proprietären, US-amerikanischen IT-Lösungen. 96% der Verwaltungsangestellten arbeiten täglich mit Microsoft-Produkten. 80% der Verwaltungsdaten werden in Datenbanken des US-Anbieters Oracle gespeichert und 75% der Virtualisierungslösungen kommen von VMWare.

In der Vergangenheit führte dies „nur“ zur Abhängigkeit von einzelnen Herstellern und deren Preisdiktat. Heute hingegen führt sie dazu, dass die **Trump-Administration** einen Hebel hat, um:

a) sich **auf jedem beliebigen Politikfeld** die Unterstützung Deutschlands zu sichern, da andernfalls die Abschaltung, Beeinträchtigung oder Kompromittierung der verwendeten Technologien angedroht werden kann und

b) **desinformierend und destabilisierend** zu wirken, indem z. B. vorhandene Sicherheitslücken der verwendeten Technologien nicht geschlossen werden oder Leistungen für Bürger:innen – bis hin zu demokratischen Wahlen – nicht mehr störungsfrei angeboten werden können.

Nur ein digital souveräner Staat ist handlungsfähig

Der deutsche Staat kann seine Kernaufgaben – **Sicherung der wirtschaftlichen Stabilität, Nachhaltigkeit, innere Sicherheit, Bildung, Daseinsvorsorge, Gewährleistung demokratischer Prozesse** – nur dann erfüllen, wenn er die Verfügbarkeit, Sicherheit und Funktionsweise der dafür eingesetzten IT-Lösungen sicherstellen kann. Digitale Souveränität muss daher als **Teil der nationalen und europäischen Sicherheitsarchitektur** verstanden und priorisiert werden.

Eine Strategie für digitale Souveränität

Verwaltungshandeln muss unabhängig gemacht werden von proprietären IT-Lösungen, die der Kontrolle von Drittstaaten unterliegen. Dazu braucht es eine klare **Strategie**, die die **digitale Souveränität als Staatsaufgabe** versteht, priorisiert und mit konkreten Maßnahmen untermauert. Kern dieser Strategie muss der konsequente **Umstieg von proprietären Lösungen auf Open-Source-Software** sein. So können bestehende Abhängigkeiten gelöst und es kann verhindert werden, dass in neuen Bereichen – beispielsweise KI – neue Abhängigkeiten entstehen.

Digital souveräne Lösungen sind Open Source

Nur Open-Source-Lösungen, offene Standards und Schnittstellen geben dem Staat die Kontrolle über seine IT-Infrastruktur zurück: **Transparenz** über Systeme, die Möglichkeit, **Anbieter zu wechseln** sowie **Einfluss** auf Funktionen, Logiken und den Betrieb von Software zu nehmen.

Open-Source-Prinzipien schaffen Resilienz

Offener Code und dezentral-föderierte kollaborative Strukturen – die entscheidenden Prinzipien von Open Source – schaffen **Resilienz gegenüber Cyberangriffen** und **sichern kritische Infrastrukturen** gegen externe Schocks.

Was getan werden muss

Marktanreize schaffen und die Einkaufsmacht des Staates nutzen

Es müssen schnell **Marktanreize** geschaffen werden, damit die Wirtschaft digital souveräne Lösungen bereitstellt, weiterentwickelt und betreibt. Der deutsche und europäische Markt – v. a. KMUs – ist in der Lage, **konkurrenzfähige Lösungen** zu liefern, wenn das Innovations- und Effizienz-Potential von Open-Source-Entwicklung gehoben wird. Dafür braucht es eine klare politische Zielsetzung, und der Staat muss seine **Einkaufsmacht strategisch nutzen** und gezielt in souveräne Lösungen investieren.

Digitale Souveränität europäisch vorantreiben

Ganz Europa steht vor denselben Herausforderungen. Wir müssen begrenzte Ressourcen bündeln und mit innovativen Ansätzen eine **gemeinsame europäische Souveränitätsinfrastruktur** schaffen. Open Source ermöglicht es, in grenzüberschreitenden Projekten smarte und leichtgewichtige Lösungen zu entwickeln. Ansätze wir der „EuroStack“ weisen in die richtige Richtung. Diese Tätigkeiten müssen auf europäischer Ebene koordiniert werden – das ZenDiS ist dafür der prädestinierte Akteur.

Drei zentrale Maßnahmen

1. Ein schrittweise steigender, verpflichtender **Open-Source-Mindestanteil** bei Beschaffungs-vorgängen und Rahmenverträgen der ÖV: Startend in dieser Legislatur mit einer Höhe von 20% - mit dem Ziel, bis 2035 die vollständige Umstellung in der Beschaffung vollzogen zu haben.
2. Investitionen in die öffentliche IT abhängig machen von einem verpflichtenden, vorgeschalteten **Souveränitätscheck**. Dieser Check wird IT-Lösungen, Anbieter, Lizenzen und Verträge überprüfbar machen und als Ergebnis einen **Souveränitätsindex** liefern: Wie digital souverän ist eine Behörde bzw. die Verwaltung zu einem bestimmten Zeitpunkt. Auf dieser Basis wird ein **Lagebild zur Digitalen Souveränität** erstellt und kontinuierlich fortgeführt.
3. Mit dem **ZenDiS** steht der Öffentlichen Verwaltung ein etablierter Partner zur Seite, der sie berät, befähigt und einen niedrigschwelligen Zugang zu souveränen IT-Lösungen bereit-stellt. Damit das ZenDiS seinem Auftrag gerecht werden kann, benötigt es **Investitionen in den weiteren Aufbau sowie eine überjährige Absicherung**. Nur so kann es seiner zentralen Rolle als Partner für Bund, Länder und Kommunen sowie seiner Vorreiterrolle auf europäischer Ebene gerecht werden.