Digitale Souveränität als Staatsaufgabe

Wie Abhängigkeiten unsere Demokratie gefährden

Jutta Horstmann, Vorsitzende der Geschäftsführung, Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS)

© Thomas von der Heiden

von Jutta Horstmann

Während ich diesen Artikel schreibe, wird Donald Trump gerade vereidigt. Und schon wirft seine zweite Amtszeit Schatten voraus. Die Missachtung der staatlichen Souveränität anderer – man denke an Kanada, Grönland oder Panama – oder der Aufbau einer Oligarchie der Big-Tech-Milliardäre: Schwer zu sagen, was mehr Sorge bereiten sollte.

Wie wird die Welt aussehen, wenn Sie diesen Text lesen? Die Mischung aus atemberaubender Irrationalität und demokratieverachtendem Eigennutz, die der neue US-Präsident an den Tag legt, macht eine Prognose schwierig.

Ich möchte mit einer Worst-Case-Betrachtung starten. Trump ist ein radikaler Machtpolitiker, der jede Schwäche anderer zu seinen Gunsten ausnutzen wird. Deutschland und Europa wiederum haben viele offene Flanken – und wir müssen davon ausgehen, dass er sich jeder einzelnen davon bedienen wird, um seine Agenda durchzusetzen.

Technologische Abhängigkeiten als offene Flanke

Eine dieser Flanken ist die Abhängigkeit unseres Staates von US-Technologien.

96 Prozent der Verwaltungsangestellten im Bund arbeiten täglich mit Microsoft-Produkten. 80 Prozent der Verwaltungsdaten werden in Datenbanken des US-Anbieters Oracle gespeichert und 75 Prozent der Virtualisierungslösungen kommen von VMWare, ebenfalls aus den USA. Nicht so schlimm, solange die Verwaltung funktioniert? Und immerhin sprechen wir hier schon von digitalisierten Arbeitsweisen und Prozessen. Das ist doch eine tolle Sache. Oder?

Leider ist es nicht so einfach. Ein Staat, der seine Kernaufgaben – Sicherung der wirtschaftlichen Stabilität, Nachhaltigkeit, innere Sicherheit, Bildung, Daseinsvorsorge, Gewährleistung demokratischer Prozesse – nur mit Hilfe von IT-Lösungen erfüllen kann, deren Verfügbarkeit, Sicherheit und Funktionsweise er nicht unter Kontrolle hat, ist seiner Souveränität beraubt.

Dennoch ist genau das in Deutschland seit Jahrzehnten gelebte Praxis. Eine Praxis, die mit jeder Beschaffung und Rahmenvertragsverlängerung zugunsten der bisherigen Anbieter weiter zementiert wird.

Kostenexplosion und Kontrollverlust

Bislang wurde dieser Umstand – wenn überhaupt – vor allem unter dem Aspekt explodierender Kosten adressiert: Allein der Bund gab 2023 mehr als 1 Milliarde Euro für Software-Lizenzen aus, 57 Prozent mehr als im Vorjahr. Der Rahmenvertrag der Bundesregierung mit Oracle beläuft sich auf 4,6 Mrd. Euro. VMWare diktierte Ende 2023 Preissteigerungen um bis das Zwölffache.

Auch der Kontrollverlust der Verwaltung über ihre eigene IT wurde in diesem Zusammenhang beklagt: Offene Standards konnten nicht eingefordert werden, die Durchsetzung von Datenschutzregeln war nicht mehr möglich. Stattdessen wird die Verwaltung mit immer mehr Anwendungen in die Cloud des jeweiligen Anbieters gezwungen.

Eine neue Dimension der Abhängigkeit

Mit der Machtübernahme Trumps in den USA bekommt die Abhängigkeit der öffentlichen Verwaltung nun eine weitere, verheerende Dimension. Jetzt geht es nicht mehr „nur“ um das Diktat von Konditionen durch Hersteller. Jetzt geht es um Eingriffe in alle Bereiche staatlichen Handelns.

Im Worst Case müssen wir uns auf Folgendes einstellen: Unterstützt der digital abhängige Staat Trumps Politik nicht, werden Cloud-Angebote abgeschaltet, Updates nicht mehr bereitgestellt, Sicherheitslücken nicht mehr gepatcht. Wenn es den Zielen des neuen US-Präsidenten oder seiner Oligarchen dient, werden Datenströme und Datenbanken kompromittiert, mitgelesen, verändert. Destabilisierung, Desinformation und Handlungsunfähigkeit des Staates sind die Folgen. Unsere Demokratie ist in Gefahr.

Digitale Souveränität als Staatsaufgabe

Verwaltungshandeln muss unabhängig gemacht werden von IT-Lösungen, die der Kontrolle von Drittstaaten unterliegen. Um dieses Ziel zu erreichen, 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, kritische Abhängigkeiten gelöst und es kann verhindert werden, dass in neuen Bereichen – beispielsweise KI – weitere entstehen.

> Verwaltungshandeln muss unabhängig gemacht werden von IT-Lösungen, die der Kontrolle von Drittstaaten unterliegen.

Durch den Einsatz von Open-Source-Lösungen und die Nutzung offener Standards und Schnittstellen gewinnt der 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. Und er wird resilienter gegenüber Cyberangriffen. Anstatt auf wichtige Patches der Hersteller warten zu müssen, können bei Open-Source-Software jederzeit Expert:innen damit beauftragt werden, Schwachstellen schnell und wirksam zu schließen.

Dazu tragen die Prinzipien von Open Source – allen voran Offenheit, Dezentralität und Kollaboration – wesentlich bei. Sie sorgen dafür, dass Lösungen unter Stress oder bei Angriffen immer besser werden, anstatt auszufallen oder in ihrer Performance nachzulassen. Und stärken so letztlich die geopolitische Resilienz.

Der Einstieg in den Umstieg

Um schnell die Handlungsfähigkeit zurückzugewinnen, braucht es ein klares Signal zum Einstieg in den Umstieg – angelehnt an andere große Transformationsvorhaben wie den Kohle- oder den Atomausstieg: Ein ab 2025 schrittweise steigender, verpflichtender Open-Source-Mindestanteil bei Beschaffungsvorgängen und Rahmenverträgen der Öffentlichen Hand – mit dem Ziel, bis 2035 die vollständige Umstellung auf Open Source in der Beschaffung vollzogen zu haben.

Das bietet allen Beteiligten die nötige Planungssicherheit: der Verwaltung für die damit verbundenen Präzisierungen im Vergaberecht, für die Umstellung der Ausschreibungs- und Vergabepraxis, für den Aufbau von spezifischem Open-Source-Wissen und das Auslaufen von Rahmenverträgen über proprietäre Lösungen. Und auch die Wirtschaft erhält Klarheit: Anbieter, die heute noch auf proprietäre Software setzen, können ihre Geschäftsmodelle sukzessive in Richtung Open Source umbauen und ihr Geschäft damit langfristig absichern.

Zusätzlich müssen ab sofort alle Investitionen in die öffentliche IT von einem verpflichtenden, vorgeschalteten Souveränitätscheck abhängig gemacht werden. Damit vermeiden wir von vornherein die Beschaffung von Lösungen, die unsere staatliche Souveränität gefährden. Und: Auf diese Weise können wir den Umbau zu einem digital souveränen Staat kostenneutral gestalten. Dazu braucht es kein zusätzliches Geld – ein strategisches Umschichten vorhandener Mittel reicht aus.

Ein Souveränitätspaket für die Öffentliche Verwaltung

Die Dringlichkeit der Lage und die notwendigen Maßnahmen liegen also auf der Hand. Klar ist aber auch: Es fehlt in der Verwaltung noch an strategischer und ganz praktischer Umsetzungskompetenz, um die nächsten Schritte zu gehen.

Viele Einrichtungen sind heute noch unerfahren im Umgang mit Open Source und den damit einhergehenden Lizenzmodellen. Das gilt für die Nachnutzung bestehender Lösungen ebenso wie für die Beauftragung neuer Entwicklungsprojekte.

Eine Schlüsselrolle in dieser Transformation kommt daher dem Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) zu. Das ZenDiS bietet ein umfassendes Souveränitätspaket: Es berät die Verwaltung und bietet Zugang zu souveränen Lösungen. Außerdem stellt das ZenDiS die zentrale Plattform bereit, auf der staatliche Einrichtungen gemeinsam und föderal übergreifend an Open-Source-Projekten arbeiten und Wissen aufbauen können und die zunehmend zur Basis für eine sichere Softwarelieferkette ausgebaut wird.

Diese Arbeit ist wichtiger denn je. Sie zahlt direkt auf die Handlungsfähigkeit und Souveränität unseres Staates ein. Die kommende Bundesregierung muss diese Bedeutung verstehen und das ZenDiS noch stärker als bislang strategisch verankern und ausbauen.

America first? Europe united!

Die offene Flanke der digitalen Abhängigkeiten betrifft jedoch nicht nur den deutschen Staat und unsere Verwaltung. Ganz Europa steht vor dieser Herausforderung.

Digitale Souveränität muss daher immer über nationale Grenzen hinaus gedacht und gelebt werden. Nur im Zusammenspiel mit unseren europäischen Partnern können wir dem kompromisslosen „America first“ und den daraus erwachsenden Risiken eine wirksame Antwort entgegensetzen.

Auch hier ist Open Source der entscheidende Hebel. Es ermöglicht die grenzüberschreitende Zusammenarbeit zur Stärkung der Digitalen Souveränität. Das ZenDiS spielt dabei eine entscheidende Rolle, indem wir schon heute in internationalen Projekten aktiv sind und zudem unser Vorgehen als Blaupause mit unseren europäischen Partnern teilen.

Zusammen verfolgen wir ein großes Ziel: eine gemeinsame europäische Souveränitätsinfrastruktur – für ein handlungsfähiges Europa. ■