Digitale Souveränität

Ist die Schmerzgrenze erreicht?

[02.07.2025] Auf dem Zukunftskongress Staat & Verwaltung diskutierten Experten in der vergangenen Woche den aktuellen Stand bei der digitalen Souveränität. Diese ist durch geopolitische Verschiebungen wieder ins Blickfeld der Politik geraten. Ob die Marktdominanz von US-Konzernen bei Netzen und Software in der öffentlichen Verwaltung überwunden werden kann, erscheint indes weiter ungewiss.

Die aktuellen geopolitischen Entwicklungen – Stichworte: Ukrainekrieg und Regierung Trump – lassen digitale Souveränität wieder ins Visier der Politik geraten. Dabei gehört deren Stärkung nicht zu den Lieblingsthemen hiesiger Entscheider. Sie haben sich immer wieder dem Einfluss und der Marktdominanz amerikanischer Tech-Konzerne, namentlich Microsoft, gebeugt, anstatt eine konsequente Open-Source-Strategie zu entwickeln. Einzig das Bundesland Schleswig-Holstein geht einen entschlossen anderen Weg. Dort steht den Mitarbeitern der Verwaltung ein Open-Source-Arbeitsplatz zur Verfügung und momentan wird nach einer Testphase das Videokonferenzsystem OpenTalk ausgerollt (wir berichteten).

Kommunaler Vorreiter der Open-Source-Bewegung war die Stadt München, die ab 2003 mit LiMux ein Open-Source-Paket in der Verwaltung einsetzte (wir berichteten). Durch geschickten Lobbyismus hat sich dann Microsoft im Jahr 2017, als die deutsche Konzernzentrale nach München verlegt wurde, wieder ins Spiel gebracht.

Sorgen vor politischer Einflussnahme

Digitale Souveränität erscheint unter verschiedenen Gesichtspunkten entscheidend. Vor allem mit der Regierung Trump haben sich Sorgen vor politischer Einflussnahme bewahrheitet. Die teils opportunistischen Reaktionen einzelner Technologiekonzerne – etwa hinsichtlich Diversität – zeigen, wie wirkmächtig die disruptive Agenda der derzeitigen amerikanischen Regierung ist. Infolgedessen haben digitale Souveränität und technologische Resilienz in Europa einen neuen Stellenwert erhalten. Seitens des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) heißt es, dass technologische Abhängigkeiten ein strategisches Risiko darstellten. Deutschland müsse mehr Eigenständigkeit und Sicherheit durch europäische Kooperationen und Investitionen in Schlüsseltechnologien vorantreiben. Dies gilt nicht nur für die Verwaltungsdigitalisierung. Der gesamte Bereich Kritischer Infrastrukturen und Datenhoheit in Clouddiensten, Netzwerktechnik und Betriebssystemen ist davon betroffen.

Datenabfluss in die USA

Bedenken gab es schon zuvor. Im Jahr 2019 hatte die niederländische Regierung im Zuge einer Risikofolgenabschätzung den Verstoß von Microsoft-Produkten gegen die europäische Datenschutz-Grundverordnung (DSGVO) nachweisen können. Zumindest die Telemetriedaten der Anwender fließen aus Microsofts cloudbetriebenen Office-Anwendungen in Richtung Vereinigte Staaten. Der US-Konzern will sein internationales Cloudgeschäft weiter ausbauen und bietet als vertrauensschaffende Maßnahme inzwischen DSGVO-konforme Rechenzentren auf europäischem Territorium (EU Data Boundary) an – so wie etwa auch Amazon mit seiner AWS-Cloud mit Standorten in Europa wirbt. Angesichts des US-Cloud-

Acts jedoch, der US-Unternehmen auf Geheiß von Strafverfolgungsbehörden verpflichten kann, auf im Ausland gespeicherte Daten zuzugreifen, ließen sich entsprechende Bedenken nie ganz zerstreuen.

Welche Strategien und Technologien sind nun notwendig, um die digitale Souveränität zu stärken und die Infrastrukturabhängigkeit der deutschen Verwaltung zu reduzieren? Diese Fragen stellten sich Experten auf dem 11. Zukunftskongress Staat & Verwaltung Ende Juni 2025 in Berlin. Als ausgemacht gilt, dass eine technologische Unabhängigkeit von den großen US-Playern weder wünschenswert noch aussichtsreich sei. Zwar „beweisen der deutsche Mittelstand und seine Hidden Champions, dass Innovationen auch ohne die Mega-Unternehmen möglich sind“, sagte die Leiterin des Bundesrechenzentrums ITZBund, Frauke Greven, „eine Autarkie ist jedoch nicht möglich“. Die IT-Dienstleister müssten funktionierende Fachverfahren anbieten und seien dadurch notgedrungen marktabhängig. Für Jörg Kremer, Abteilungsleiter föderales IT-Architekturmanagement bei der FITKO, müssen IT-Architekturen definiert werden, die auf offenen Protokollen und gut definierten Standards und Schnittstellen basieren. Kremer sprach sich für eine Angebotsorientierung aus, Gesetze und Rechtsvorschriften seien der falsche Weg: „Wir müssen gute Angebote schaffen, die alle nutzen wollen.“

Standards statt Insellösungen

Auch Johann Bizer, Vorstandsvorsitzender von Dataport und maßgeblich für die Open-Source-Entwicklungen in seinem Haus verantwortlich, sprach sich nicht mehr ausschließlich für Open Source aus: „Nur auf Open Source zu setzen, reicht nicht aus.“ Vielmehr seien Standards notwendig, die Open Source unterstützen (Open Source supported) und damit gewährleisten, dass auch andere öffentliche IT-Dienstleister erreicht werden können. Die Häuser müssten stärker zusammenarbeiten, anstatt Insellösungen zu schaffen. Gerade hinsichtlich staatlicher Resilienz sei ein föderales Zusammenarbeiten notwendig. „Dies hat die Bundesregierung nicht im Blick“, so Bizer. Er wies auch darauf hin, dass die im Digitalbereich stark vertretenen Beratungsunternehmen transnational denken und agieren und insofern einer nationalen Resilienz entgegenstehen.

Mehr auf Open Source setzen

Für John Reyels, Beauftragter für Digitalisierung, Cyberabwehr und Digital- und Datenpolitik im Auswärtigen Amt, kam das Thema digitale Souveränität bislang nie so recht voran. Trotz besseren Wissens gebe es nach wie vor eine große Abhängigkeit von US-Netzen und Hardware aus China. Souveränität bedeutet in seinen Augen vor allem Datensouveränität, die das Auswärtige Amt dadurch erreicht, dass es bestimmte Daten nicht in einer Cloud lagert. Reyels bezeichnete dieses etwas exklusiv erscheinende Vorgehen, das sicherlich nicht zum Maßstab erhoben werden kann, als „Resilienz by default“. Zugleich drückte er die Hoffnung aus, dass mit der neuen politischen Großwetterlage eine Schmerzgrenze erreicht sei und künftig in Deutschland mehr auf Open Source gesetzt werde.

Der Beauftragte für die Netze des Bundes, Tessen Freund, hob den besonderen Stellenwert der Kritischen Infrastrukturen hervor, die bei Konflikten sowohl physische Ziele darstellen als auch vermehrt ins Visier von Cyberattacken geraten. Er sprach sich für doppelte und ausfallsichere Netze aus. Die aktuellen Netze des Bundes stammten noch aus einer Zeit der Zentralisierung. Künftige neue Netze hingegen müssten disloziert und auf mehrere Standorte verteilt werden, damit sie resilient sind und nie komplett ausfallen. Für Frauke Greven ist es Aufgabe des Staates zu definieren, welche Daten wo gelagert und geschützt werden – notfalls auch On-Premises, also außerhalb einer Cloud. Und auch Jörg Kremer verwies darauf, dass

beim Projekt Deutsche Verwaltungscloud (DVC) zwar nicht auf Privatanbieter verzichtet werden könne. Allerdings müsse ein Regelwerk bestimmen, welche Daten besonders schützenswert sind und unabhängig vorgehalten werden sollen.

Argument Wirtschaftlichkeit

Ob sich aus diesen Erkenntnissen nun allerdings eine Handlungskonsequenz ergibt, ist ungewiss. Und ob eine Schmerzgrenze tatsächlich zu einem Umschwenken hin zu mehr Open-Source-Produkten führt ebenfalls. Das schlagende Argument ist häufig eine größere Wirtschaftlichkeit: Im Cloudbereich können die so genannten Hyperscaler andere Preise anbieten als die deutsche Konkurrenz.

Johann Bizer lässt dieses Argument zumindest für Open-Source-Software nicht gelten und verweist darauf, dass die Produkte des Zentrums für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) günstiger seien als Microsoft-Lizenzen. Außerdem sei die Entscheidung für Open Source und damit größerer digitaler Souveränität letztlich vor allem „eine Frage des politischen Mutes“.

()

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