

Digitale Souveränität beginnt mit Transparenz

Die Rückkehr der Geopolitik sowie Abhängigkeiten von Technologiekonzernen, Cloud-Diensten und KI rücken die digitale Souveränität auf die Agenda von Unternehmen und Behörden. Am Swiss EA Connect Day 2026 diskutierten Fachleute, wie sich digitale Handlungsfreiheit zurückerobern lässt – und was sie kostet. Autor: Joël Orizet



Podiumsdiskussion am Swiss EA Connect Day 2026: Hélène Mourgue d'Algue, CIO, Stadt Biel; Syrian Hadad, CTO, Adesso Schweiz, und BFH-Professor Matthias Stürmer (v. l.).

Wer digitale Dienste nutzt, begibt sich zwangsläufig in Abhängigkeiten. Lange galten diese höchstens als technisches oder wirtschaftliches Problem. Doch mit den zunehmenden geopolitischen Spannungen, der erratischen Wirtschaftspolitik der US-Regierung und dem Vordringen künstlicher Intelligenz in immer mehr Geschäftsprozesse stellen sich neue Fragen: Wer kontrolliert die Daten? Wer bestimmt die Regeln? Wie riskant wird es, wenn kritische Systeme an wenigen Anbietern hängen? Und wie lässt sich digitale Handlungsfreiheit zurückgewinnen?

Über diese Fragen diskutierten Fachleute am Swiss EA Connect Day 2026 an der FFHS in Zürich. Organisiert wurde der Anlass von BOC Schweiz und Adesso Schweiz. Im Zentrum stand dabei ein Begriff, der vor wenigen Jahren noch vor allem in Fachkreisen kursierte: digitale Souveränität.

Wenn Abhängigkeit politisch wird

Lock-in-Effekte seien in der Wirtschaft nichts Neues, sagte Matthias Stürmer, Professor an der Berner Fachhochschule und Leiter des Instituts Public Sector Transformation, zum Auftakt der Veranstaltung. Man kennt es auch von Druckerherstellern mit ihren Tintenpatronen oder von diesen Kapselkaffeemaschinen: Hersteller versuchen seit jeher, Kundschaft an ihre Produkte, Schnittstellen und

Lizenzmodelle zu binden. Neu ist aber die politische Schärfe der Debatte.

Stürmer verwies auf steigende Lizenzkosten, freihändige Vergaben und die Marktmacht grosser Anbieter. Solange solche Abhängigkeiten vor allem Preis- und Beschaffungsfragen betrafen, liessen sie sich als betriebswirtschaftliches Ärgernis behandeln. Inzwischen gehe es jedoch auch um Datenzugriff, Verfügbarkeit und Vertrauen. Der US CLOUD Act, politischer Druck und Debatten

um mögliche Abschaltungen von Diensten hätten die Risikobetrachtung verändert.

Aus dieser Diagnose leitete Stürmer sein Verständnis von digitaler Souveränität ab. Sie soll Organisationen nicht von der Welt abschotten, sondern ihre Handlungsfähigkeit stärken. Niemand könne und solle sämtliche Technologie selbst bauen. Entscheidend seien Wahlmöglichkeiten: Organisationen müssten Alternativen kennen, Anbieter wechseln und kritische Systeme kontrollieren können. Es geht also nicht um Unabhängigkeit um jeden Preis, sondern um Handlungsfähigkeit durch Wahlfreiheit.

Open Source als Mittelweg

Für Stürmer spielt Open Source dabei eine zentrale Rolle. Nicht, weil offene Software grundsätzlich kostenlos wäre, sondern weil sie Wettbewerb und Wechselmöglichkeiten schafft. Während proprietäre Lösungen Organisationen direkt an einzelne Hersteller binden, entsteht rund um Open-Source-Produkte oft ein Markt aus verschiedenen Dienstleistern.

Als Beispiel nannte Stürmer Deutschland. Dort investiert die öffentliche Hand seit einigen Jahren gezielt in offene Alternativen zu Microsoft 365 und bündelt bestehende Open-Source-Lösungen auf gemeinsamen Plattformen.



Solche Projekte seien zwar nicht gratis, könnten sich aber langfristig rechnen. Vor allem aber würden sie den Wettbewerb stärken und Alternativen zu etablierten Anbietern schaffen.

Auch in der Schweiz gewinnt das Thema politisch an Gewicht. Seit 2017 gab es hierzulande auf allen Staatsebenen mehr als 40 Vorstösse zur digitalen Souveränität. Zuletzt nahm der Ständerat eine Motion von Heidi Z'graggen (Mitte/UR) für ein «Impulsprogramm zur Stärkung der digitalen Souveränität der Schweiz» an – ein Entscheid, mit dem Stürmer nach eigenen Angaben nicht gerechnet hatte.

Entscheidend sei nun, die politischen Absichtserklärungen in konkrete Projekte zu übersetzen. An einem solchen wirkt Stürmer selbst mit: Das im Juli 2025 gegründete «Netzwerk SDS – Souveräne Digitale Schweiz» zählt nach seinen Angaben bereits mehr als 200 Unternehmen, Behörden und weitere Organisationen. Ziel sei es, Akteure zu vernetzen und vorhandenes Know-how zu bündeln.

Seine Botschaft fiel entsprechend pragmatisch aus: Die Schweiz verfüge sowohl über die Nachfrage als auch über die technischen Kompetenzen. Entscheidend sei nun, die Kräfte besser zu koordinieren.

Wenn die Produktion nicht stillstehen darf

Wie digitale Souveränität im Unternehmensalltag aussieht, zeigte anschliessend Emmi. Für den Luzerner Milchverarbeiter steht vor allem die Betriebssicherheit im Vordergrund – die Produktion darf nicht stillstehen, wie Aiko Frank, Enterprise Architect bei Emmi Schweiz, deutlich machte. Entsprechend beurteilt das Unternehmen Technologien primär danach, wie zuverlässig und robust sie den Betrieb unterstützen.

Kritische Produktionssysteme betreibt Emmi weiterhin in eigenen Rechenzentren und möglichst nahe an den Werken. Andere Anwendungen können durchaus in die Cloud wandern. Ausschlaggebend sei letztlich die Kritikalität einer Anwendung – nicht eine grundsätzliche Präferenz für oder gegen bestimmte Technologien.

Um solche Entscheidungen treffen zu können, setzt Emmi auf Transparenz. Das Unternehmen verwaltet mehr als 500 Applikationen und bewertet diese nach Kriterien wie Verfügbarkeit, Vertraulichkeit und geschäftlicher Relevanz. Digitale Souveränität entsteht aus Sicht von Emmi deshalb vor allem durch Übersicht und Priorisierung.

Transparenz vor Transformation

Daran knüpften die Beiträge von Adesso Schweiz und BOC Schweiz an. Matthew Turnbull, Head of Advisory bei Adesso Schweiz, betonte, dass digitale Souveränität für jede Organisation etwas anderes bedeute. Eine Bank, eine Behörde oder ein Industriebetrieb hätten unterschiedliche Risiken und Anforderungen. Eine Patentlösung gebe es daher nicht.

Felix Meentken, Managing Director von BOC Schweiz, argumentierte, dass digitale Souveränität zunächst sichtbar gemacht werden müsse. Wer nicht weiss, welche Anwendungen, Datenbestände und Abhängigkeiten im Unternehmen existieren, kann Risiken weder bewerten noch reduzieren.

Enterprise Architecture Management (EAM) soll diese Transparenz schaffen. Es dokumentiert Prozesse, Anwendungen, Daten und Infrastruktur und macht sichtbar, wo kritische Abhängigkeiten bestehen. Erst auf dieser Grundlage lassen sich Fragen beantworten wie: Welche sensiblen Daten liegen bei welchem Anbieter? Wo fehlen Alternativen? Und welche Systeme würden bei einem Ausfall besonders stark ins Gewicht fallen?

Wechseln können, statt alles selbst betreiben

Hélène Mourgue d'Algue, CIO der Stadt Biel, betonte in der Podiumsdiskussion die Bedeutung von Transparenz über die eigene IT-Landschaft. Biel habe inzwischen rund 95 Prozent seiner Systeme und Schnittstellen modelliert. Digitale Souveränität bedeute für sie jedoch nicht, alles selbst zu betreiben. Entscheidend sei vielmehr die Fähigkeit, Anbieter wechseln zu können. Ob eine Lösung aus der Schweiz oder dem Ausland komme, sei zweitrangig, solange sie die definierten Anforderungen erfülle.

Einen anderen Akzent setzte Syrian Hadad, CTO von Adesso Schweiz und früherer CTO des Kantons Aargau. Er widersprach der verbreiteten Annahme, die Public Cloud sei automatisch günstiger als eigene Infrastrukturen. Mit Open-Source-Technologien, Automatisierung und entsprechendem Know-how liessen sich auch eigene Plattformen effizient betreiben. Viele Organisationen hätten jedoch über die Jahre technologische Kompetenzen abgebaut.

Trotz unterschiedlicher Perspektiven zeichnete sich ein Konsens ab: Digitale Souveränität bedeutet weder Abschottung noch Autarkie. Wer digitale Handlungsfreiheit gewinnen will, muss zuerst die eigenen Systeme, Daten und Abhängigkeiten kennen. Oder, wie sich durch viele Beiträge des Tages zog: Digitale Souveränität beginnt mit Transparenz.

Der Swiss EA Connect Day 2026 fand an der FFHS in Zürich statt.



Den vollständigen Artikel finden Sie online
it-markt.ch