swissICT

SWISSICT MAGAZIN

OFFIZIELLES PUBLIKATIONSORGAN VON SWISSICT
AUSGABE 1/2026

DIGITALE SOUVERÄNITÄT

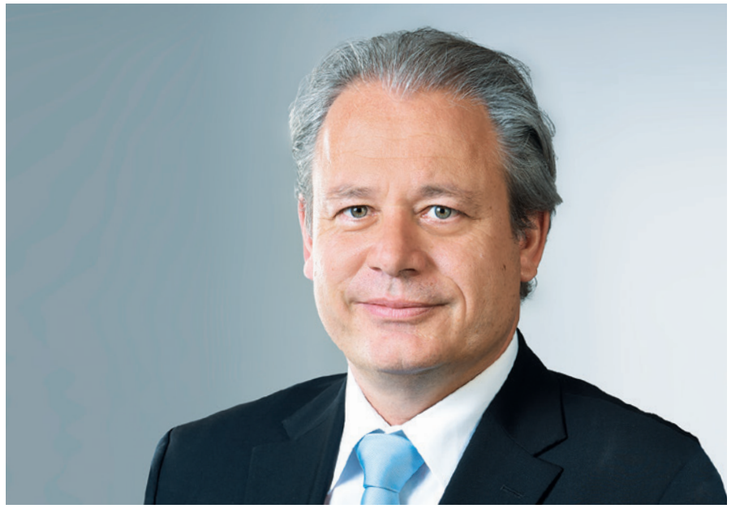
OPEN SOURCE & MICROSOFT
ZWEI PERSPEKTIVEN

CYBERSECURITY

DIE SCHWEIZ IM DIGITALEN ZEITALTER ZWISCHEN RESILIENZ UND KOOPERATION

Foto: Adobe Stock

DIGITALE SOUVERÄNITÄT
KARTOFFELN, CLOUDS & KONTROLLVERLUST



«Souverän ist, wer in jeder Situation über Alternativen verfügt.» Der Satz von Florian Schütz ist so nüchtern wie entlarvend: Souveränität zeigt sich nicht im Schönwetterbetrieb, sondern dann, wenn etwas ausfällt.

Ich musste beim Lesen unweigerlich an meine Kolumne von 2022 denken. Dort habe ich die digitale Souveränität als «Anbauschlacht des 21. Jahrhunderts» bezeichnet – in Anlehnung an den *Plan Wahlen*, mit dem die Schweiz im Zweiten Weltkrieg ihre Ernährungssouveränität sicherte. Kartoffeln statt Rasenflächen, Selbstversorgung statt Abhängigkeit. Heute sind die Felder digital: Chips, Clouds, Datenräume. Und die Abhängigkeiten sind mindestens so real wie damals.

Die Frage ist nur: Kämpfen wir die richtigen Schlachten?

Digitale Souveränität ist zum Lieblingswort der Digitalpolitik geworden. Kaum ein Strategiepapier, Panel oder Förderprogramm ohne. Gleichzeitig bleibt der Begriff erstaunlich elastisch. Für den Staat geht es um Kontrolle kritischer Aufgaben. Für Unternehmen – etwas bodenständiger formuliert – darum, den eigenen Laden im Griff zu haben: Daten kennen, Risiken steuern, Abhängigkeiten bewusst wählen.

Und genau hier beginnt die Realität jenseits der Buzzwords. Denn Souveränität bedeutet heute nicht mehr Unabhängigkeit. Sie bedeutet gestaltete Abhängigkeit. Kein Schweizer Unternehmen baut seine eigene Cloud, kein Staat seine eigenen Chips, kein KMU sein eigenes KI-Modell. Aber alle müssen verstehen, worauf sie sich einlassen – technisch, rechtlich und geopolitisch. Vendor-Lock-in ist kein Betriebsunfall mehr, sondern eine strategische Entscheidung.

Was mich nach über 20 Jahren Präsidium immer wieder fasziniert: Die Schweiz diskutiert digitale Souveränität oft wie eine ideologische Frage, obwohl sie in der Praxis eine Architektur- und Managementfrage ist. Wer Alternativen hat, bleibt handlungsfähig. Wer keine hat, nicht.

Die Beiträge in diesem Magazin zeigen genau diese Spannbreite: von souveränen Cloud-Stacks über Open-Source-Strategien bis zu Cyberresilienz und Governance. Und sie zeigen auch etwas sehr Schweizerisches: Souveränität entsteht hier nicht durch Abschottung, sondern Kooperation mit starken Institutionen, Partnern und Kompetenz. Vielleicht ist das unsere eigentliche Stärke als Kleinstaat: Wir waren nie autark, sondern immer vernetzt. Unsere Souveränität entstand historisch nicht aus Grösse, sondern aus Fähigkeit zur Kooperation, Innovation und klugen Priorisierung.

Digitale Souveränität ist Teil einer grösseren Frage: In welchen Bereichen wollen wir als Schweiz handlungsfähig bleiben? Energie, Forschung, Versorgung, Technologie, Sicherheit oder eben digital.

Meine Überzeugung hat sich seit 2022 nicht geändert: Wir führen tatsächlich eine Anbauschlacht des 21. Jahrhunderts. Nur wachsen heute keine Kartoffeln, sondern Kompetenzen, Infrastrukturen und Ökosysteme. Und wie damals gilt: Man muss entscheiden, was man selbst anbaut und was man bewusst importiert.

Mit diesem Editorial verabschiede ich mich nach 22 Jahren als Präsident von swissICT. Es war mir eine grosse Freude und Ehre, die Entwicklung der Schweizer ICT-Landschaft so lange begleiten zu dürfen.

Die Branche ist heute stärker, selbstbewusster und strategischer denn je. Wenn sie weiterhin so denkt und handelt wie in dieser Ausgabe sichtbar, dann mache ich mir um die digitale Souveränität der Schweiz wenig Sorgen.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre. Es lohnt sich – wie immer.

Herzlichst

Ihr Thomas Flatt
Präsident swissICT, Unternehmer, Berater und Verwaltungsrat

Bild: Adobe Stock

DIGITALE SOUVERÄNITÄT
HERRSCHAFTSBEGRIFF ODER MODEWORT?

Souveränität gilt als Grundpfeiler des schweizerischen Staatsverständnisses, doch die digitale Realität verschiebt ihre Koordinaten. Staatliche Aufgaben werden heute über internationale Lieferketten, Cloud-Dienste und vernetzte Systeme erfüllt. Muss im digitalen Zeitalter der Begriff der Souveränität neu definiert werden? Eine Reflexion zum bundesrätlichen Bericht «Digitale Souveränität der Schweiz».

AUTOR: MATTHIAS MICHEL

Wenn aktuell die Souveränität diskutiert wird, geschieht dies meist im Licht deren Gefährdung: Ist die Schweiz als global vernetztes und von internationalen Entwicklungen abhängiges Land noch souverän? Mit der Entwicklung zur digitalen Gesellschaft, die mit der künstlichen Intelligenz noch eine neue Dimension erhält, steht die Frage nach Abhängigkeiten und nach dem richtigen Mass an Unabhängigkeit mit verstärkter Dringlichkeit im Raum.

Spätes Erwachen der Politik

Noch im Jahr 2019 blieb die Forderung nach einer Strategie für digitale Souveränität[1] ohne Resonanz, obwohl der Bundesrat kurz zuvor selber kritische Abhängigkeiten der Bundesverwaltung von IT-Lieferant:innen feststellte[2]. Im Januar 2022 forderte swissICT-Präsident Thomas Flatt die nationale Sicherheit zu garantieren, systemrelevante Infrastrukturen zu schützen und die Handlungsfähigkeit der Wirtschaft im Digitalbereich zu erhalten. Dabei seien europäische Interessen über den Freihandel zu stellen und es brauche «unpopuläre Prioritäten», was er als «Anbauschlacht des 21. Jahrhunderts» bezeichnete. Als hätte er damit die Politik aufgeweckt: Im Februar 2022 folgte ein Postulat[3], das zum bundesrätlichen Bericht *Digitale Souveränität der Schweiz* vom November 2025 führte.

Handlungsfähig statt unabhängig

Definitiv erwacht ist das Parlament im letzten Jahr mit 21 parlamentarischen Vorstössen zum Thema. Digitale Souveränität dient dabei ab und zu als schlagwortartiger Lockvogel. So wird der Begriff überstrapaziert, wenn er auch für den privatwirtschaftlichen Digitalbereich verwendet wird; hier befindet man sich im Feld der digitalen Selbstbestimmung privater Akteur:innen. Oft wird Souveränität mit Unabhängigkeit gleichgesetzt, was zu kurz gegriffen ist. Treffend ist die bundesrätliche Definition: «Die mit staatlichen Aufgaben betrauten Akteur:innen in der Schweiz verfügen über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum, um die Erfüllung der ihnen übertragenen staatlichen Aufgaben sicherzustellen». Zur Stärkung der Handlungsfähigkeit kann ein Arbeiten im EU-Verbund geradezu geboten sein, was der Nationalrat mit Annahme einer entsprechenden Motion[4] zum Ausdruck brachte. Der hergebrachte Souveränitätsbegriff hat nicht ausgedient. Der Bundesrat fokussiert richtigerweise auf den verfassungsmässigen Begriff der Souveränität und auf Akteur:innen, die staatliche Aufgaben mit digitalen Ressourcen erfüllen. Das bundesrätliche Denkmodell macht handlungsfähig, da die Kompetenzordnung gewahrt bleibt.

koordiniert sein und auch die Ebene der kantonalen Aufgaben mitumfassen. Fragen stellen sich auch in Bezug auf die neu zu bildende interdepartementale *Arbeitsgruppe Digitale Souveränität*. Sie wird zwar dem Querschnittcharakter der Aufgabenstellung gerecht, es fragt sich aber, wie diese Arbeitsgruppe in die bestehenden Prozesse des Risikomanagements eingebunden wird.

Strategische Planung grundlegender Infrastrukturen

Digitalpolitik kann zusätzlich vorausschauende Investitionen in grundlegende Infrastrukturen notwendig machen. Es lohnt sich, Rechenleistung im eigenen Land zu sichern. Für grundlegende Infrastrukturen kann das Prinzip der Offenheit wichtig werden. Die strategische Planung muss anderen Regeln gehorchen als der tägliche Einkaufszettel der Verwaltung. Die Schweiz hat bereits heute eine hohe Dichte an Rechenzentren. Mit dem Swiss National Supercomputing Centre im Tessin ist die Schweiz vorne mit dabei. Zusätzlich hat sie die ETH und die EPFL als starke Forschungsinstitutionen mit fortschrittlicher Aufstellung in Sachen Künstliche Intelligenz. Mit ihrer Neutralität und ihrem hohen Bildungsniveau hat die Schweiz einen grossen Wert in der Hand. Sie sollte ihn ausbauen.

Menschen statt Technik

Im bundesrätlichen Bericht geht es nicht um Digitaltechnik. Vielmehr werden Ziele definiert, die an Akteur:innen und somit an Menschen und deren Kontroll- und Handlungsfähigkeit anknüpfen. Ohne das Handeln der adressierten Akteur:innen bliebe die Strategie toter Buchstabe. Der Bundesrat lässt aber die Frage offen, wie die Menschen befähigt werden, anhand der vorgegebenen Kriterien die richtigen Entscheidungen zu treffen. Hier könnte an die bestehenden Arbeiten der Akademien der Wissenschaften Schweiz angeknüpft und die unverzichtbare Data Literacy gefördert werden.

Priorisierung und prozessuale Einbindung der Massnahmen

Eine Grundfrage bleibt im bundesrätlichen Bericht unbeantwortet: Wie bedeutend ist die Erfüllung einer staatlichen Aufgabe für das Gemeinwesen? Eine Priorisierung wird möglich, wenn der Diskurs auch die systemische bzw. institutionelle Dimension einbezieht (so gemäss dem Whitepaper «Digitale Souveränität» der Swiss Data Alliance, 2024). Die Risikopolitik und das Inventar der kritischen, für die Schweiz besonders bedeutenden Infrastrukturen sollten im Lichte der Gesamtstrategie bereits Spuren gelegt, zum Beispiel mit der Förderung offener Standards und Schnittstellen. Die Verwaltung sollte sie nun aktiv verfolgen. Allerdings verhindert das auf verteilte Macht getrimmte Staatssystem nach wie vor, unser System wirklich zukunftsfähig und resilient zu gestalten. Damit ist die Ebene der Verfassung adressiert, die ja auch die grundlegenden souveränitätspolitischen Weichen stellen sollte. Diese Verfassungsebene wird mit parlamentarischen Vorstössen thematisiert[5/6/7]. Der Bundesrat verweist in seinen diesbezüglichen Antworten auf die Arbeiten der Digitalen Verwaltung Schweiz (DVS), die einen Digitalisierungsartikel in der Bundesverfassung anstrebt. Damit bekäme auch die digitale Souveränität eine verfassungsrechtliche Basis, welche die digitale Handlungsfähigkeit der Schweiz stärken wird.

Digitale Souveränität als Verfassungsfrage

Das Rad der Digitalisierung dreht schnell und immer schneller. Wie bleibt die Schweiz in dieser Dynamik souverän? Auf Gesetzesebene wurden mit dem EMBAG

1) Motion 19.3884 Derder «Eine Strategie für die digitale Souveränität der Schweiz»
2) Bericht des Bundesrats in Erfüllung des Postulats 16.3515 Weibel «Abhängigkeit von Herstellern und Wege zur Risikominderung bei IT-Beschaffungen»
3) Postulat 22.4411 Z'graggen «Strategie Digitale Souveränität der Schweiz»
4) Postulat 25.3197 Marti «Künstliche Intelligenz. Europäischen Effort und Zusammenarbeit stärken»
5) Postulat 23.3050 Die Mitte-Fraktion «Verbindliche Standards für die digitale Verwaltungslandschaft der Schweiz. Braucht es einen Digitalisierungsartikel in der Bundesverfassung?»
6) Motion 24.4045 Würth «Die Verfassung braucht einen Digitalisierungsartikel»
7) Motion 26.3005 SPK-S «Die Verfassung braucht einen Digitalisierungsartikel»

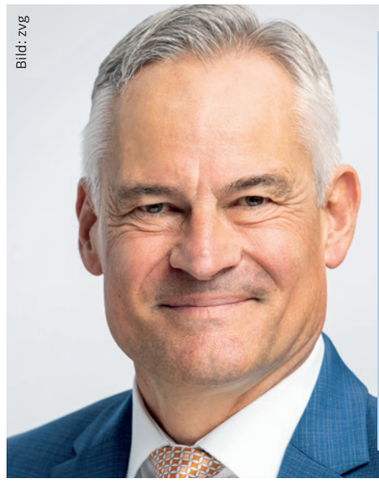


Bild: zvg

MATTHIAS MICHEL

Dr. Matthias Michel (FDP) vertritt den Kanton Zug im Ständerat und präsidiert dort die Kommission für Wissenschaft, Bildung und Kultur. Vorher war er – nach mehrjähriger Tätigkeit als Rechtsanwalt – während sechzehn Jahren als Regierungsrat im Kanton Zug tätig. Matthias Michel ist Mitglied der swissICT-Politikkommission.

MARC HOLITSCHER ZWEI PERSPEKTIVEN MATTHIAS STÜRMER

Bilder: Adobe Stock (mitte), zvg (links u. rechts)

Was bedeutet Digitale Souveränität konkret und welche Rolle spielen Open Source, internationale Cloud-Provider und staatliche Steuerung? Matthias Stürmer (Berner Fachhochschule BFH) und Marc Holitscher (Microsoft Schweiz) ordnen ein. Die Antworten wurden für das Magazin gekürzt. Die vollständigen Interviews finden Sie auf dem swissICT-Blog.

INTERVIEW: PHILIPP BINAGHI

Marc und Matthias, was verstehen Sie unter digitaler Souveränität?
Marc: Digitale Souveränität bedeutet, selbstbestimmt an digitaler Wertschöpfung teilhaben zu können. Entscheidend ist: Unternehmen und staatliche Stellen behalten die Kontrolle über Ort, Zugriff und Schutz der Daten. Dies umfasst die Fähigkeit, relevante Schlüsseltechnologien nutzen und weiterentwickeln zu können. Sicherheit bildet die Grundlage: Ohne Resilienz und Schutz vor Bedrohungen ist digitale Handlungsfähigkeit unmöglich. Wichtig ist eine faktenbasierte Debatte. Der Begriff wird häufig emotional oder politisch aufgeladen.

MARC HOLITSCHER

Marc Holitscher ist National Technology Officer bei Microsoft Schweiz. In dieser Funktion beaufsichtigt er die Entwicklung von Microsofts Technologievision und -strategie und übersetzt innovative Technologien in wirtschaftliche Effekte und Ergebnisse für Kund:innen und andere Stakeholder.

Für Lösungen braucht es eine realistische Betrachtung von Risiken und Fähigkeiten.
Matthias: Heute sind viele Bereiche der IT durch ausländische Tech-Konzerne kontrolliert. Sie steuern Software, Daten, KI-Lösungen und bestimmen, unter welchen Datenschutzregeln und Lizenzkosten wir damit arbeiten. Digitale Souveränität bedeutet, Alternativen zu schaffen, Abhängigkeiten zu reduzieren und Handlungsspielräume zu sichern – etwa durch Open Source Software, offene Standards und interoperable Technologien. Für den starken Schweizer IT-Sektor bietet dieser Ansatz grosse Chancen, mehr Wertschöpfung im Land zu behalten. Das stärkt Wettbewerb und Innovationskraft.

Eigenleistung oder bewusste Abhängigkeit: Wo sollte der Staat kontrollieren?
Matthias: In der Vergangenheit wurden oft attraktive Produkte von Providern wie Microsoft, Oracle oder SAP eingeführt. Das geistige Eigentum blieb beim Provider, der so über die letzten 20 Jahre hinweg seinen Einfluss auf die Verwaltung ausbauen konnte. Entsprechend kontrolliert der Staat heute den wesentlichen Teil der digitalen Infrastruktur nicht selbst, er ist fremdgesteuert. Das schwächt die digitale Souveränität und den heimischen IT-Sektor. Offene Ausschreibungen und technologieoffene Beschaffungen erhöhen die langfristige Handlungsfähigkeit des Staates.
Marc: Die Antwort bedarf einer strukturierten Risikoanalyse. Entscheidend sind Kritikalität und Kontrollmechanismen einer Technologie für staatliche Kernaufgaben. Relevant ist, wie die Zusammenarbeit gestaltet und abgesichert wird. Risiken lassen sich technisch, organisatorisch oder vertraglich steuern. Gleichzeitig braucht es technologische Grundkompetenz, um Lösungen fundiert beurteilen zu können. Digitale Souveränität bedeutet nicht zwingend Eigenproduktion, sondern bewusste, informierte Entscheidungen über Architektur, Schutzbedarf und Partnerwahl. Die Schweiz verfügt über ein vielfältiges Technologie-Ökosystem. Ebendiese Vielfalt stärkt die Handlungsfähigkeit.

Cloud-Technologien: Wie lassen sich Innovation und Kontrolle verbinden?
Marc: Cloud-Technologien sind zentral für Skalierbarkeit und Innovationsfähigkeit. Gleichzeitig stellen sie Anforderungen an Datenschutz, Transparenz und Sicherheit. Moderne Architekturen erlauben es, Daten abhängig vom Schutzbedarf unterschiedlich zu betreiben – in der Cloud, hybrid oder isoliert. Sicherheitsmechanismen ermöglichen gezielte Risikosteuerung. Entscheidend ist: Je höher die Kritikalität, desto mehr Schutz wird benötigt. Viele regulierte Branchen in der Schweiz zeigen, dass Wettbewerbsfähigkeit und kontrollierte Cloud-Nutzung kein Widerspruch sind.
Matthias: Auch bei Cloud-Services gilt: Je stärker proprietäre Dienste genutzt werden, desto schwieriger ein späterer Wechsel. Open-Source-Infrastrukturen bleiben vergleichsweise flexibel, während proprietäre Software- oder KI-Dienste Daten, Prozesse und Geschäftslogik an einen Provider binden (Vendor-Lock-in). Wichtig sind bewusste Architekturentscheidungen und kritische Fragen: Was bleibt austauschbar? Wo entstehen langfristige Bindungen? Wettbewerbsfähigkeit und Kontrolle lassen sich verbinden, wenn Interoperabilität und Wechseloptionen systematisch berücksichtigt werden.

Welche Rolle spielt Open Source für die digitale Souveränität?
Matthias: Open Source ist ein zentraler Hebel digitaler Souveränität. Offene Lizenzen schaffen Transparenz und ermöglichen Weiterentwicklung durch mehrere Akteur:innen. Vor einem Jahr war es noch undenkbar, dass eine US IT-Firma die politischen Interessen ihrer Regierung durchsetzt und beispielsweise den Datenzugriff von Mitarbeitenden eines internationalen Strafgerichtshofs sperrt. Die heutige Realität zeigt: Wenn es hart auf hart kommt, sind ausländische Unternehmen ihrem Ursprungsland stärker verpflichtet als ihren Schweizer Kund:innen. Mit gesetzlichen Grundlagen wie dem EMBAG, das die Veröffentlichung von Behörden-Software unter Open-Source-Lizenzen vorsieht, sind wichtige Schritte eingeleitet. Eine stärkere Förderung von Open Source ist wirtschaftlich und geopolitisch sinnvoll.
Marc: Open Source und proprietäre Modelle sind keine Gegensätze, sondern ergänzen sich. Microsoft engagiert sich seit Jahrzehnten im Open-Source-Umfeld und zählt weltweit zu den führenden Mitwirkenden. Für die digitale Souveränität entscheidend sind nicht Ideologien, sondern offene Standards, Interoperabilität und Datenportabilität. Wenn Daten in gängigen Formaten exportiert und Systeme flexibel kombiniert werden können, bleibt technologische Handlungsfähigkeit gewahrt. Souveränität entsteht dort, wo Wahlfreiheit besteht und Risiken steuerbar bleiben.

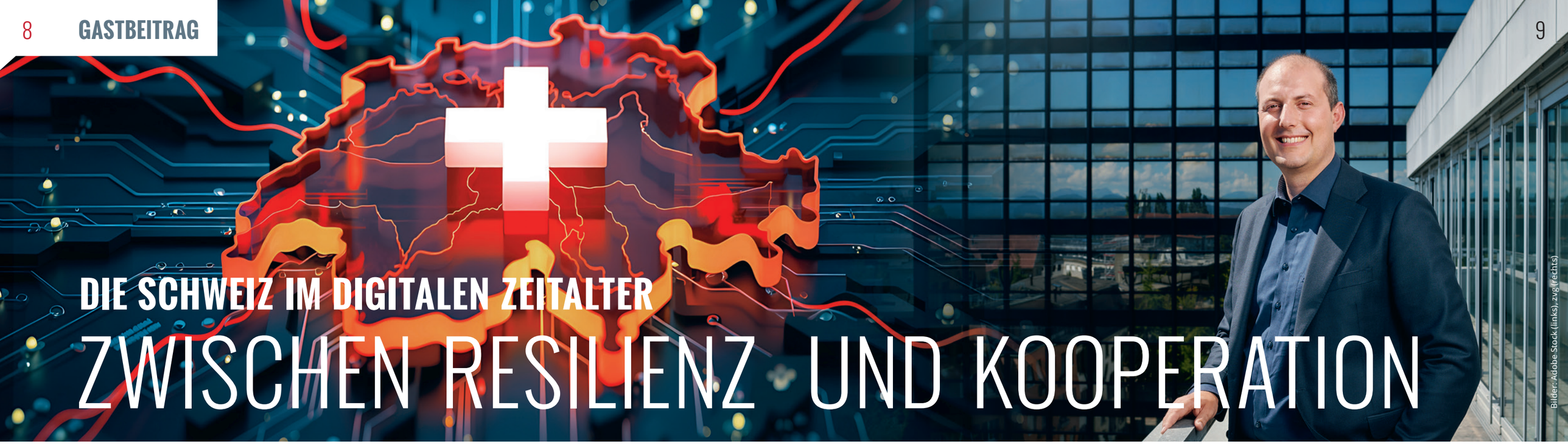
Woran erkennen wir in fünf Jahren, dass die Schweiz auf dem richtigen Weg ist?
Marc: Erfolg zeigt sich, wenn die Schweiz faktenbasiert entscheidet, technologische Entwicklungen aktiv gestaltet und Risiken realistisch bewertet. Konkret: Sie stärkt Sicherheit, Innovationskraft und Wettbewerbsfähigkeit. Eine konstruktive, sachliche Debatte ist dabei zentral. Digitale Souveränität ist die Fähigkeit, digitale Risiken zu steuern und Wahlfreiheit auch im Krisenfall zu sichern.
Matthias: Das zeigt sich, wenn die Schweiz ihre technologischen Abhängigkeiten effektiv reduziert, offene Standards stärkt und digitale Kompetenzen im Inland ausbaut. Dazu gehören eine Beschaffungspraxis, welche digitale Souveränität und mehr Wettbewerb im IT-Markt fördert. Dazu braucht es mehr IT-Kompetenz beim Staat, wofür es ein nationales Zentrum für digitale Souveränität braucht. Wenn wir weitermachen wie bisher und immer neue Updates von den proprietären Produkten vornehmen, die wir heute bereits installiert haben, verpassen wir eine Chance. Veränderung erfordert bewusste Entscheidungen – heute.

DAS GANZE INTERVIEW LESEN SIE AUF DEM SWISSICT-BLOG.

SWISSICT.CH/DIGITALE-SOUVERAENITAET-PERSPEKTIVEN-MICROSOFT-OPEN-SOURCE

MATTHIAS STÜRMER

Matthias Stürmer ist Professor und Leiter des Instituts Public Sector Transformation an der Berner Fachhochschule (BFH) sowie Dozent am Institut für Informatik der Universität Bern. Zu seinen Schwerpunkten zählen Open Source Software, KI, Open Data, Open Government und öffentliche Beschaffung.



Bilder: Adobe Stock (links), zvg (rechts)

DIE SCHWEIZ IM DIGITALEN ZEITALTER

ZWISCHEN RESILIENZ UND KOOPERATION

In einer zunehmend digitalisierten Welt ist Cybersicherheit weit mehr als eine technische Herausforderung. Die jüngsten geopolitischen Entwicklungen verdeutlichen, dass Cybersicherheit ein politisch-strategisches Schlüsselthema ist. Sie ist eine zentrale Voraussetzung für die digitale Souveränität von Staat, Wirtschaft und Gesellschaft.

AUTOR: FLORIAN SCHÜTZ

Häufig wird digitale Souveränität als technologische Autarkie missverstanden, also als vollständige Unabhängigkeit von ausländischen Produkten oder Diensten. Tatsächlich geht es aber nicht um Isolation, sondern um Handlungsfähigkeit in global verflochtenen digitalen Ökosystemen. Digitale Souveränität umfasst die Fähigkeit eines Staates oder einer Organisation, im digitalen Raum handlungsfähig zu bleiben, Risiken zu erkennen und auf sie zu reagieren – unabhängig davon, ob Daten, Infrastrukturen oder digitale Dienste im Inland oder international verortet sind. Dies hat der Bundesrat kürzlich in seinem Bericht *Digitale Souveränität der Schweiz*[1] dargelegt. Souverän ist, wer in jeder Situation über Alternativen verfügt und auf Ausfälle und Störungen rasch reagieren kann – ungeachtet dessen, ob diese durch technische Probleme, wirtschaftliche Lieferengpässe oder politische Druckversuche verursacht sind.

Bedeutung von Cyberresilienz

Die Vorbereitung auf Situationen, in denen die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen beeinträchtigt ist, gehört zu den Kernaufgaben der Cybersicherheit. Cyberresilienz bezeichnet hingegen die Fähigkeit, digitale Sicherheit zu gewährleisten und auch bei eingeschränkter Verfügbarkeit digitaler Produkte und Dienstleistungen handlungsfähig zu bleiben. Eine gestärkte Cyberresilienz von Wirtschaft und Behörden bildet die Grundlage für souveräne Entscheidungen im digitalen Raum. Unternehmen müssen digitale Risiken aktiv managen, Kompetenzen in Cyber- und Informationssicherheit ausbauen und technologische Optionen prüfen, um ihre Wettbewerbs- und Handlungsfähigkeit zu sichern. Dies ist keine einfache Aufgabe und erfordert daher einen engen Wissensaustausch zwischen allen Beteiligten. Insbesondere der Dialog mit der Forschung sollte gefördert werden, da sie eine Schlüsselrolle bei der Entwicklung neuer Technologien, Sicherheitstechniken und Standards spielt, die Vertrauen schaffen und zugleich Abhängigkeiten reduzieren.

Die Behörden wiederum tragen die Verantwortung, rechtliche Rahmenbedingungen zu schaffen, kritische Infrastrukturen beim Schutz vor Cyberbedrohungen zu unterstützen und durch strategische Planung und internationale Kooperation die Cyberresilienz zu stärken. Nötig sind dafür aus der Sicht der Cybersicherheit offene Standards, transparente Technologien und die Förderung von Open-Source-Lösungen.

Was tut die Schweiz?

Die Schweiz reagiert auf die zunehmende Bedeutung der Cyberresilienz strategisch und operativ. *In der Sicherheitspolitischen Strategie der Schweiz 2026 (Vernehmlassungsentwurf)*[2] ist die Stärkung der Cybersicherheit als Massnahme zur Stärkung der Resilienz definiert und somit klar als wichtiger Pfeiler der Sicherheitspolitik der Schweiz ausgewiesen. Die digitale Souveränität zählt zudem zu den zentralen Fokusthemen der *Strategie Digitale Schweiz*[3]. Konkrete Massnahmen für die Verbesserung der Cyberresilienz legt dann wiederum die *Nationale Cyberstrategie*[4] fest, welche vom Bundesrat 2023 verabschiedet wurde.

Zur operativen Stärkung der Cyberresilienz hat das Parlament im Dezember beschlossen, die Mittel des Bundesamts für Cybersicherheit ab 2026 um 10 Mio. CHF und ab 2027 um weitere 5 Mio. CHF zu erhöhen[5]. Dadurch kann der Schutz vor Cyberbedrohungen weiter ausgebaut und die Fähigkeiten für Prävention und Risikoanalyse erhöht werden.

Die internationale Zusammenarbeit bleibt dabei unabdingbar, um die Cybersicherheit zu stärken und die digitale Souveränität zu sichern. Die Schweiz arbeitet im Bereich Cybersicherheit eng mit verschiedenen internationalen Partnern zusammen. Diese Zusammenarbeit konzentriert sich auf mehrere Schlüsselfelder, darunter die Mitwirkung an internationalen Normierungs- und Standardisierungsprozessen, der Austausch und die Vertrauensbildung in multilateralen Foren, bilaterale Kooperationen im Cyber- und Sicherheitsbereich sowie der gemeinsame Schutz kritischer Infrastrukturen und der Umgang mit Cybervorfällen.

FLORIAN SCHÜTZ

Florian Schütz ist Direktor des Bundesamts für Cybersicherheit (BACS) der Schweiz. Zuvor leitete er das Nationale Zentrum für Cybersicherheit (NCSC). Er verantwortet die Umsetzung der nationalen Cyberstrategie und vertritt die Schweiz in internationalen Cyber-Gremien.

Zunehmende Bedeutung von digitaler Souveränität

Weltweit stellen technologische Dominanz und geopolitische Spannungen Staaten vor grosse Herausforderungen. Deutlich wird das mit Blick auf Europa, welches mittels Regulierung, Standardisierung und Innovationsförderung seine digitale Souveränität stärken und Abhängigkeiten von globaldominanten Technologieunternehmen reduzieren will.

International wird digitale Souveränität deshalb in naher Zukunft noch stärker als Sicherheitsfrage verstanden werden. Organisationen wie die NATO betonen bereits heute, dass Daten-, Betriebs- und Technologie-Souveränität essenziell für die Sicherheit moderner Staaten und ihrer militärischen wie zivilen Systeme ist. Dies unterstreicht den globalen Trend Cybersicherheit und digitale Handlungsfähigkeit als integrale Bestandteile nationaler Sicherheitspolitik.

Für die Schweiz stellen sich die gleichen Herausforderungen wie für alle europäischen Staaten. Als neutraler, hoch vernetzter Standort mit einer starken Wirtschaft und Forschungslandschaft sowie langfristig ausgerichteten Unternehmen, darunter zahlreiche Familienunternehmen, verfügt die Schweiz über gute Voraussetzungen, gezielt Nischenkompetenzen, wie beispielsweise in Kryptografie, vertrauenswürdigen Infrastrukturen und Sicherheitstechnologien auszubauen. Sie sollte dabei bewusst eine kooperative Rolle einnehmen, um als Brückenbauerin in internationalen Technologie- und Sicherheitsfragen zu wirken, ohne einseitige Abhängigkeiten zu schaffen.

Fazit

Digitale Souveränität ist kein statisches Ziel, sondern ein dynamischer, strategischer Prozess. Die Schweiz muss ihre Cyberresilienz kontinuierlich stärken, Risiken frühzeitig erkennen und Massnahmen laufend anpassen. Die erfolgreiche Umsetzung hängt von der engen Zusammenarbeit aller Akteur:innen und einem verantwortungsvollen Umgang mit neuen Technologien ab. Cybersicherheit bleibt damit eine langfristige, gemeinsame Aufgabe, die politische, technologische und gesellschaftliche Dimensionen umfasst. Strategisch gestaltete Abhängigkeiten, vorausschauendes Risikomanagement und internationale Kooperationen bilden die Grundlage, um die digitale Handlungsfähigkeit der Schweiz nachhaltig zu sichern.

1) www.news.admin.ch/de/newsb/2VPWG78YrVs4eAVeiklQx
2) www.sepos.admin.ch/dam/de/sd-web/bc4PAN7CoEsS/Sicherheitspolitische%20Strategie%20der%20Schweiz%202026.pdf
3) www.digital.swiss/de
4) www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html
5) Motion 25.3191 Salzmann «Ausreichende Mittel für die zivile Cybersicherheit»

«MUT IST, IDEEN ANZUGEHEN, AUCH WENN SIE NICHT PERFEKT SIND»

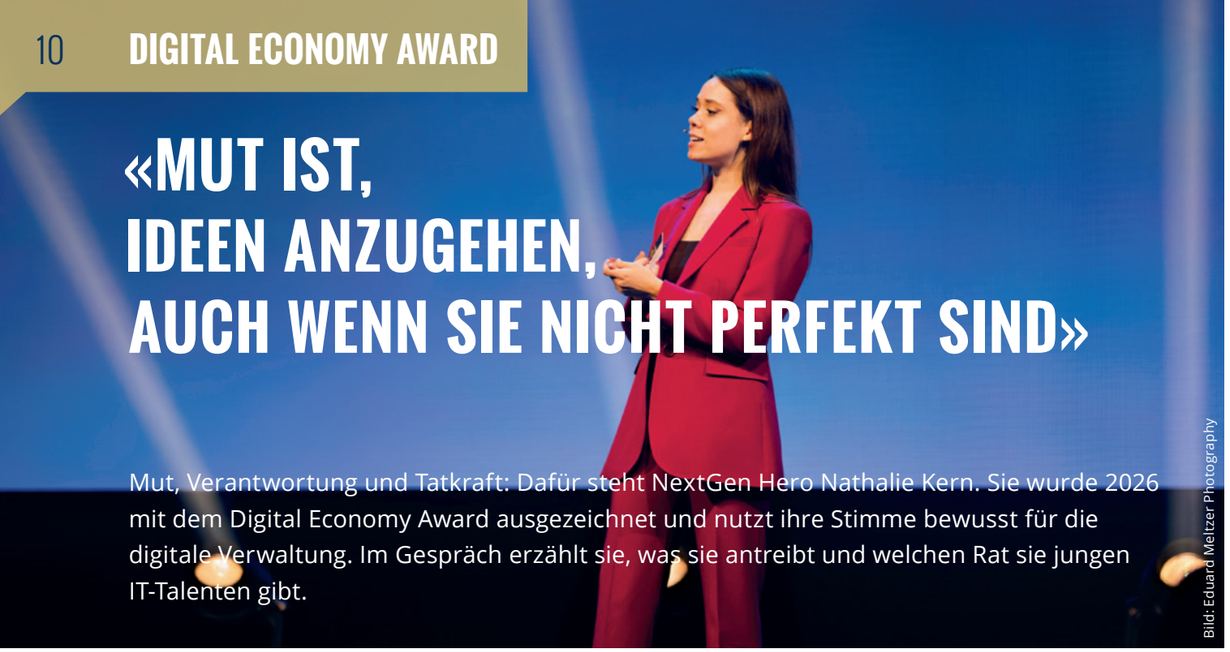


Bild: Eduard Meltzer Photography

Mut, Verantwortung und Tatkraft: Dafür steht NextGen Hero Nathalie Kern. Sie wurde 2026 mit dem Digital Economy Award ausgezeichnet und nutzt ihre Stimme bewusst für die digitale Verwaltung. Im Gespräch erzählt sie, was sie antreibt und welchen Rat sie jungen IT-Talenten gibt.

INTERVIEW: ROMANA BLEISCH

Herzliche Gratulation zum Digital Economy Award. Was ging dir durch den Kopf, als du deinen Namen gehört hast?
Herzlichen Dank! Bei der Verkündung stand ich noch voller Adrenalin vom Pitch. Als plötzlich mein Name aus den Lautsprechern kam, blieb für einen kurzen Moment alles stehen. Ich brauchte ein paar Sekunden, um zu realisieren, dass wirklich ich gemeint bin. Michael Jakob, mein Mitbewerber, musste mich sogar darauf aufmerksam machen.

Du hast als NextGen Hero auf der Bühne überzeugt. Wie kriegt man den perfekten Pitch in 90 Sekunden hin?
Ein entscheidender Faktor war das Training mit Stephan Lendi. Zu sehen, was dabei Schritt für Schritt bei allen Finalist:innen entstanden ist, war beeindruckend. Danach folgte der Feinschliff: Feedbacks einholen, Inhalte vereinfachen und eine punktgenaue Landung auf 90 Sekunden Pitch-Dauer zu üben.

Wenn du auf die Zeit vor dem Award zurückblickst, was ist hängen geblieben?
Ich konnte mir in der Casting-Phase kaum vorstellen, was mich erwartet, und war anfangs auch etwas überfordert: Was macht mich aus? Was will ich überhaupt erzählen? Als ich erfuhr, dass ich im Finale stehe, war die Freude riesig. Erst während der Vorbereitung wurde mir langsam klar, welche Dimension dieser Award hat und was es bedeutet, auf einer so grossen Bühne zu stehen. Meine Familie, meine Freunde und die Mitfinalist:innen haben mich durchgehend unterstützt und motiviert. Sie waren zugleich meine grösste Inspiration.

Hat sich seitdem beruflich etwas verändert oder haben sich neue Möglichkeiten ergeben?
Ich bin weiterhin begeisterte Enterprise Architektin und Projektleiterin bei eGovernment St. Gallen digital. Der Award hat mir jedoch neue Türen geöffnet. Ich bin neu in der *Arbeitsgruppe Architektur* der Digitalen Verwaltung Schweiz sowie in der *swissICT-Fachgruppe Future Experts* vertreten. Der Austausch und die Vernetzung in diesen Gremien sind enorm wertvoll.

Du widmest dich der Harmonisierung von IT-Systemen im föderalen Umfeld. Was sind deine grössten Herausforderungen?
Mein Ansatz ist, zuerst Transparenz mittels einer ganzheitlichen Übersicht der Systeme, Abhängigkeiten und Prozesse zu schaffen. Gleichzeitig ist ein tiefes Verständnis für die Verwaltungsrealität notwendig, da nahezu alle Bereiche betroffen sind – von Sozialversicherungen bis zu Baubewilligungen. Struktur, Klarheit und Dialog sind für mich die zentralen Erfolgsfaktoren, um Veränderungen nachhaltig umzusetzen.

Wo siehst du die grössten Chancen und Risiken, wenn kantonale oder staatliche Systeme digitalisiert werden?
Die grössten Chancen sehe ich in effizienteren Prozessen und mehr Transparenz für Bevölkerung und Wirtschaft. Wenn ich heute online einen Heimatausweis bestelle und diesen morgen im Postfach habe, ist End-to-End-Digitalisierung erreicht. Die grössten Risiken entstehen dort, wo Akzeptanz fehlt. Digitalisierung im staatlichen Umfeld bedeutet, unterschiedliche Bedürfnisse mitzudenken und niemanden auszuschliessen. Die Balance zwischen technologischem Fortschritt und gesellschaftlicher Verantwortung entscheidet über Erfolg.

Welchen Rat gibst du jungen IT-Aspirant:innen mit auf den Weg?
Habt den Mut, Ideen anzugehen, auch wenn sie noch nicht perfekt sind und zögert nicht, bis andere den ersten Schritt machen. Der Digital Economy Award bietet die Möglichkeit, sich selbst herauszufordern, dazuzulernen und Teil eines inspirierenden Netzwerks zu werden. Es geht weniger ums Gewinnen als darum, an sich zu glauben.

DIGITAL ECONOMY AWARD

Alle Informationen zum Digital Economy Award, Erfolgsstorys der vergangenen Jahre und regelmässige Updates finden Sie auf unserer Webseite.

DIGITALECONOMY-AWARD.CH

«CYBER-SICHERHEIT IST KEIN NISCHENTHEMA, SIE IST FÜHRUNGSFRAGE»

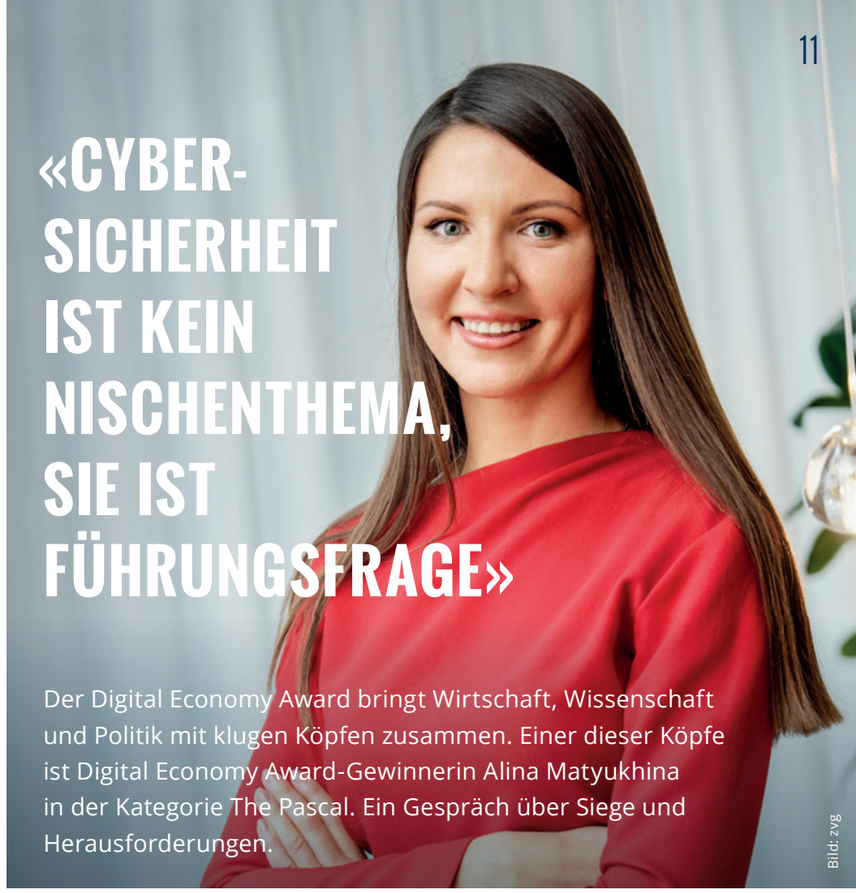


Bild: zvg

Der Digital Economy Award bringt Wirtschaft, Wissenschaft und Politik mit klugen Köpfen zusammen. Einer dieser Köpfe ist Digital Economy Award-Gewinnerin Alina Matyukhina in der Kategorie The Pascal. Ein Gespräch über Siege und Herausforderungen.

INTERVIEW: ROMANA BLEISCH

Liebe Alina, herzliche Gratulation! Was bedeutet die Auszeichnung für dich?
Für mich bedeutet sie vor allem grosse Dankbarkeit. Cybersicherheit ist nie Einzelleistung, sondern Teamarbeit und gemeinsames Lernen. Die Auszeichnung gilt deshalb auch meinen Mentor:innen, Kolleg:innen, Studierenden und Partner, die meinen Weg geprägt haben.

Was sagt die Auszeichnung über die Bedeutung von IT-Security heute aus?
Wir sprechen noch immer über Cybersicherheit, als handle es sich vor allem um eine Frage technischer Hygiene. Mein Sieg zeigt, dass Cybersicherheit kein Nischenthema mehr ist, sondern ein Thema von Governance, Führung, Risikomanagement und Unternehmenskultur. Cybersicherheit ist nicht nur eine IT-Verantwortung, sondern gehört weit oben auf die Strategie-Agenda.

Was reizt dich an einem Feld, das sich ständig mit Risiken und Bedrohungen beschäftigt?
Meine ursprüngliche Leidenschaft galt der Mathematik. Im Studium wurde mir klar, dass meine mathematische Forschung womöglich erst langfristig Wirkung entfalten würde – vielleicht sogar erst postmortem. Ich wollte jedoch an Themen mit unmittelbarem Impact arbeiten und wechselte deshalb in die Informatik. IT verbindet analytisches Denken mit konkretem gesellschaftlichem Nutzen. Dieses Zusammenspiel von Sinn und Verantwortung treibt mich bis heute an.

Welche Entwicklungen in der Cybersicherheit werden uns technisch und gesellschaftlich in naher Zukunft am stärksten herausfordern?
KI verändert die Cybersicherheit auf beiden Seiten: Die Verteidigung reagiert schneller, Angreifende skalieren Phishing, Deepfakes und Schwachstellensuche. Das Tempo steigt deutlich und neben Technologie braucht es klare Governance. Quantencomputing ist kurzfristig keine Bedrohung, wird aber langfristig die Kryptografie verändern und erfordert vorausschauende Planung. Und gesellschaftlich geht es vor allem um Vertrauen – in Informationen, Infrastrukturen und digitale Entscheidungen.

Wie lassen sich Schutz und digitale Souveränität in der Cybersicherheit vereinen?
Es braucht Kontrolle in kritischen Bereichen und Kooperation dort, wo sie stärkt. Vollständige digitale Unabhängigkeit ist angesichts verflochtener Technologien und Lieferketten unrealistisch. Entscheidend ist Transparenz über Daten, Systeme und Verantwortung, sonst bleibt digitale Souveränität theoretisch.

Gleichzeitig ist Cybersicherheit kooperativ. Informationsaustausch, gemeinsame Standards und internationale Zusammenarbeit erhöhen die Schutzwirkung erheblich.

Jetzt bist du IT-Persönlichkeit des Jahres 2025. Wie waren die letzten Monate?
2025 war ein intensives Jahr mit internationalen Dialogen zu Cybersicherheit und Post-Quantum-Themen. Um zwei Highlights zu nennen: Als Visiting Professor im Bereich Cybersecurity Leadership bereite ich MBA- und EMBA-Studierende auf strategische Führungsaufgaben vor. Mit dem *CYBERLEAD Hub* und einer Masterclass für Business Leaders habe ich zudem Bildungsangebote aufgebaut, die Entscheidungsträger:innen befähigen, Cyberrisiken fundiert zu steuern.

Dein Rat an die nächste Generation von ICT-Fachkräften – insbesondere jungen Frauen mit ähnlichen Ambitionen?
Bleibt neugierig, baut eure Expertise konsequent aus und zögert nicht, einen Platz am Tisch einzunehmen. Das kann sich anfangs ungewohnt anfühlen, aber eure Perspektive zählt! Fortschritt beginnt mit Einzelnen, die den Schritt nach vorne wagen und ihre Kompetenz sprechen lassen. So entsteht Wandel.

ALINA MATYUKHINA

Alina ist CSO und Global Head of Cybersecurity Business Unit bei Siemens. Sie wurde mit dem Digital Economy Award *The Pascal* als IT-Persönlichkeit des Jahres ausgezeichnet – als erste Frau überhaupt.
Sie setzt sich aktiv für mehr Diversität sowie die Nachwuchsförderung ein und leistet damit einen wichtigen Beitrag für die Branche.

Bild: Adobe Stock

PRINZIP ESTLAND

VERTRAUEN ALS VERTEIDIGUNGSSTRAT EGIE

Digitale Souveränität beginnt mit Vertrauen. Estland zeigt, wie ein demokratischer Staat im KI-Zeitalter durch Rechtsstaatlichkeit, Cybersicherheit und konsequente Datenhoheit der Bürger:innen Resilienz schafft. Ein Kommentar von Liisa Pakosta, Ministerin für Justiz und digitale Angelegenheiten in Estland.

AUTORIN: LIISA PAKOSTA

Estland ist weltweit eines der fortschrittlichsten Länder in Sachen Digitalisierung und setzt einen besonderen Fokus auf grundlegende Voraussetzungen für das KI-Zeitalter: öffentliches Vertrauen, Cybersicherheit und die Kontrolle der Bevölkerung über persönliche Daten. Diese Elemente sind untrennbar miteinander verbunden. Sie bilden die staatliche und gesellschaftliche Grundlage, auf der digitale Regierungsführung nachhaltig funktionieren kann.

Für Estland ist digitale Resilienz keine rein technologische Frage. Die geopolitische Realität neben Russland hat gezeigt, dass Widerstandsfähigkeit letztlich auf Vertrauen beruht – Vertrauen in Institutionen, in rechtliche Schutzmechanismen und in die Beziehung zwischen Staat und Bevölkerung. Beispielsweise setzen autoritäre Systeme KI oft als Instrument zur Überwachung ein, während demokratische Staaten eine grundsätzlich andere Logik verfolgen: KI soll die Handlungsfähigkeit der Einzelnen stärken. Denn im digitalen Zeitalter entsteht Stabilität durch eine vertrauensbasierte Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft.

Die Schweiz ist für Estland eine wertvolle Partnerin. Als langjährige Demokratie mit starker Tradition in Föderalismus und technologischer Exzellenz verbindet sie Stabilität mit Innovationsführerschaft. Im Jahr 2025 feierten Estland und die Schweiz 100 Jahre Handelsbeziehungen. Bei einem Besuch in der Schweiz anlässlich des Jubiläums wurde deutlich, dass die Zusammenarbeit nicht nur auf einer gemeinsamen Geschichte gründet, sondern sich zunehmend an einer gemeinsamen Zukunft orientiert.

Der Staat als Wegbereiter

Das Ziel ist es, ein System zu stärken, in dem die Bürger:innen die Kontrolle über ihre Daten und Entscheidungsprozesse haben. Estland versucht nicht, den Markt zu steuern oder private Initiativen zu ersetzen. Stattdessen werden fördernde Rahmenbedingungen geschaffen. Estland hat früh ein sicheres digitales Identitätssystem (eID) und eine Datenaustausch-Plattform (X-Road) aufgebaut. So entstand die Basis für gemeinsame digitale Lösungen von Staat und Unternehmen.

Heute sind in Estland fast alle öffentlichen Dienstleistungen online zugänglich. Mehr noch: Das Modell ist wirtschaftlich messbar. Dank eingesparter Arbeitszeit in der Administration erfolgt eine Steigerung des BIP um 2%. Eine Effizienzsteigerung, die Zeit für Unternehmertum, Gesellschaft und Innovation schafft.

Lehren aus Wikipedia

An der Universität Zürich habe ich eine Vorlesung von Wikipedia-Gründer Jimmy Wales über die «Sieben Regeln des Vertrauens» besucht. Das Prinzip und der Erfolg von Wikipedia verdeutlichen: Systeme, die ihren Nutzer:innen vertrauen, gewinnen mit höherer Wahrscheinlichkeit auch deren Vertrauen.

Für Estland ist dieses Prinzip keine reine Theorie. In einem geopolitischen Umfeld, in dem digitale Einmischung ein konkretes Risiko darstellt, ist digitale Souveränität eng mit der nationalen Sicherheit verbunden. Ein demokratischer Digitalstaat kann sich jedoch nicht allein auf technische Sicherheitsvorkehrungen verlassen. Entscheidend ist die demokratische Legitimität, die aus Transparenz, Rechtsstaatlichkeit und gesellschaftlicher Akzeptanz entsteht.

Wenn Bürger:innen dem Umgang des Staates mit ihren Daten vertrauen, nutzen sie digitale Dienste freiwillig und tragen aktiv zu deren Verbesserung bei. Estland steht derzeit kurz vor der landesweiten Einführung eines obligatorischen Daten-Trackers. Dieses System erlaubt es jeder Person nachzuvollziehen, welche Behörde wann und zu welchem Zweck auf ihre Daten zugegriffen hat.

IT-Sicherheit als öffentlich-private Verantwortung

Cyberabwehr wird nicht als ausschliessliche Aufgabe des Militärs oder der Nachrichtendienste verstanden, sondern als gemeinsame Verantwortung von Staat und Privatwirtschaft.

Private Unternehmen stellen dabei die erste Verteidigungslinie dar. Estland betreibt offene Kanäle für den Austausch von Bedrohungsinformationen und betrachtet private Akteur:innen als strategische Partner, statt als Risikofaktoren. IT-Fachexpert:innen aus dem Privatsektor bringen damit ihre Expertise aktiv in die nationale IT-Sicherheit ein. Das estnische Modell ähnelt in dieser Hinsicht dem milizbasierten Sicherheitsansatz der Schweiz, bei dem ziviles Engagement nationale Resilienz stärkt.

Souveräne KI und strategische Partnerschaft Estland-Schweiz

Mit der zunehmenden Integration von KI-Systemen in die öffentliche Verwaltung wird der Schutz der Souveränität zur strategischen Priorität. Digitale Souveränität bedeutet, Abhängigkeiten von externen Providern zu vermeiden und Kerninfrastrukturen demokratisch zu kontrollieren. Die Kooperation zwischen Estland und der Schweiz spielt in diesem Zusammenhang eine wichtige Rolle. Der Austausch mit Schweizer Forschungsinstitutionen, darunter die ETH Zürich sowie Partnerschaften mit verschiedenen Schweizer Unternehmen, unterstreichen die Bedeutung einer Zusammenarbeit in den Bereichen Deep Tech, Cybersicherheit und Biotechnologie. Estlands Mitgliedschaft bei der CERN und die akademischen Verbindungen zwischen estnischen und Schweizer Universitäten stärken dieses Netzwerk.

Mit der Einführung von generativer KI in der öffentlichen Verwaltung setzt Estland auf das Prinzip der «Sovereign AI». Das bedeutet, dass Systeme nach europäischem Recht arbeiten, die Grundrechte respektieren und dafür sorgen, dass die Bevölkerung die Kontrolle über ihre Daten und Entscheidungen behalten.

Estlands 20-jährige Erfahrung mit elektronischen Wahlen zeigt, dass digitale Lösungen, die auf Transparenz und Rechtssicherheit basieren, breite gesellschaftliche Akzeptanz erreichen können. Cybersicherheit und wertebasierte rechtliche Grundlagen bilden dabei die zentralen Bausteine für demokratische Wahlen.

Fazit

Estland und die Schweiz beginnen ein neues Kapitel ihrer Partnerschaft. Beide Länder müssen zeigen, dass Demokratien nicht nur ethisch besser dastehen, sondern auch strukturell und wirtschaftlich resilienter sind als autoritäre Systeme.

Estlands Ansatz bei digitaler Verwaltung und KI folgt einem einfachen Prinzip: Technologie soll den Menschen helfen, nicht über sie entscheiden. Im digitalen Zeitalter ist Vertrauen der wichtigste Schutz.

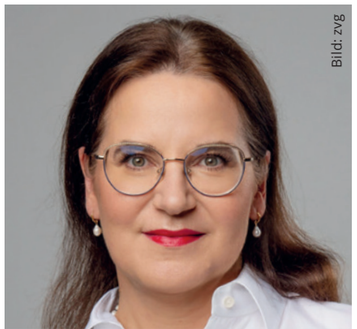


Bild: zvg

LIISA PAKOSTA

Liisa Pakosta ist Ministerin für Justiz und Digitale Angelegenheiten für Estland. Sie setzt sich für einen digitalen Staat ein, der auf Rechtsstaatlichkeit, individuellen Freiheitsrechten und einer innovationsgetriebenen Wirtschaft basiert. Liisa Pakosta war Ehrengast und Laudatorin am Digital Economy Award 2025.

DREI REALITÄTEN STAATSZIEL, MANAGEMENTAUFGABE, GESCHÄFTSMODELL

Bild: Adobe Stock

Für den Staat ein Gebot zur Sicherung der Handlungsfähigkeit, für Unternehmen eine Frage der Selbstbestimmung. Längst ist die Debatte um digitale Souveränität auch ein Handlungsfeld für IT-Provider, die mit gezielten Lösungen auf neue Marktbedürfnisse reagieren und die Diskussion aktiv mitgestalten.

AUTOREN: MATTHIAS EBNETER, ALEXANDER HOFMANN, SVEN KOHLMEIER

Sicht des Staates: Kontrolle als Kernaufgabe

Der Begriff digitale Souveränität ist in der politischen Debatte allgegenwärtig, doch sein Inhalt bleibt oft diffus. Während staatliche Souveränität territorial klar begrenzt ist, fehlt im digitalen Raum diese Abgrenzung. Daten kennen keine Grenzen. Um Orientierung zu schaffen, hat die Schweizer Bundesverwaltung eine klare Position formuliert: «Digitale Souveränität bedeutet, als Staat über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung staatlicher Aufgaben sicherzustellen.»

Der Bundesrat betont, dass der Begriff international unterschiedlich verwendet wird. Auch in der Schweiz existieren verschiedene Interpretationen, je nach Interessenlage von Staat, Wirtschaft oder Zivilgesellschaft.

Private Sicht: Den Laden im Griff haben

Für Unternehmen lässt sich digitale Souveränität einfach übersetzen: Man muss seinen Laden im Griff haben. In der digitalen Welt heisst das, Kontrolle über Daten und geschäftskritische Prozesse zu behalten. Treffender als digitale Souveränität ist dabei der Begriff digitale Selbstbestimmung, also die Fähigkeit, im digitalen Raum frei, sicher und eigenverantwortlich zu handeln.

In der Praxis bedeutet das, zu jeder Zeit zu wissen: Wer greift auf unsere Daten zu und wie wird damit gearbeitet? Kontrollfähigkeit ist entscheidend und nicht der physische Speicherort, der oft überbewertet wird. Auch beim Einsatz ausländischer Cloud-Provider zählt primär das Verständnis und Management der eigenen Risiken. Diese Risikokompetenz ist Kern unternehmerischer Sorgfaltspflicht und gewinnt angesichts geopolitischer Spannungen an Bedeutung. Fragen zu Vendor-Lock-in, Exit-Strategien und Resilienz werden zur Managementaufgabe.

Vollständige Autarkie – eigene Infrastruktur, Software und Betrieb – ist teuer, meist unrealistisch und auch nicht erstrebenswert. Die grössten Abhängigkeiten bestehen in Cloud-Ökosystemen mit globalen Rechtsregimen und Lieferkettenrisiken.

Die Antwort des Marktes: Das Geschäftsmodell «Sovereign Cloud»

Die politische und mediale Fokussierung auf digitale Souveränität hat auch im IT-Markt Spuren hinterlassen. Provider entwickeln neue Lösungen unter Labels wie «Sovereign Cloud», zugeschnitten auf öffentliche Stellen und Betreiber kritischer Infrastrukturen. Diese versprechen rechtliche Kontrolle durch inländische Datenhaltung, Einhaltung lokaler Regulierungen und vertrauensbildende Transparenz über Betrieb und Eigentum. Teilweise übernehmen lokal ansässige, sicherheitsgeprüfte Teams den Betrieb, was einem gezielten Schutz gegen extraterritoriale Rechtszugriffe gleichkommt.

Solche Modelle tragen nicht nur zur Datensicherheit, sondern auch zur lokalen Wertschöpfung bei. Je stärker Behörden und Firmen digitale Souveränität fordern, desto mehr investieren Provider in regional verankerte Cloud- oder On-Premise-Angebote mit Schweizer Rechtsrahmen. Wer sich als Kund:in für solche Lösungen entscheidet, stärkt Innovation und digitale Eigenständigkeit des Standorts. Digitale Souveränität wird damit vom politischen Ziel zum realen Standortvorteil.

Auch privatwirtschaftliche Akteure profitieren: Wer in seiner IT-Architektur souveräne Lösungen integriert, positioniert sich glaubwürdig als Partner für öffentliche Auftraggebende und schafft einen Wettbewerbsvorteil. So wird digitale Souveränität nicht nur zu einer Frage der Compliance, sondern zur Treiberin neuer Geschäftsmodelle im Technologiesektor.

Konklusion: Ein Begriff, drei Realitäten

Eine einheitliche digitale Souveränität gibt es nicht. Vielmehr bestehen drei Realitäten, abhängig von Rolle und Verantwortung:

- Für den Staat ist sie funktionale Notwendigkeit zur Sicherung seiner Kernaufgaben.
- Für Unternehmen bedeutet sie unter dem Begriff digitaler Selbstbestimmung Kontrolle, Resilienz und Risikobewusstsein.
- Für IT-Provider ist sie ein Markttrend, der spezialisierte Angebote und Innovation vorantreibt.

Der Schlüssel liegt im bewussten, differenzierten Umgang mit dem Thema. Digitale Souveränität entsteht, wenn Entscheidungen faktenbasiert, risikobewusst und verantwortungsvoll getroffen werden.

Ausblick: Souveränität als Frage der Resilienz

Die kommenden Jahre werden zeigen, ob digitale Souveränität in Europa mehr als ein politisches Ideal ist. Künftige Abhängigkeiten von globalen Technologieblöcken – sei es bei KI-Modellen, Speicherarchitekturen oder Quantencomputing – werden zur Nagelprobe staatlicher und wirtschaftlicher Handlungsfähigkeit. Wer heute in lokale Kompetenzen, Standards und partnerschaftliche Ökosysteme investiert, sichert sich morgen technologische und ökonomische Unabhängigkeit. Digitale Souveränität wird damit zum strategischen Prüfstein einer resilienten und gestaltbaren Zukunft.

Was bedeutet das für KMU?

Für viele KMU wird digitale Souveränität insbesondere dann geschäftlich relevant, wenn Kund:innen aus regulierten Bereichen bspw. aufgrund der Kritikalität oder Sensibilität der verarbeiteten Daten spezifische Anforderungen stellen. Dabei muss kein KMU in Aktionismus verfallen und unnötig überlegen, sich aus der Public Cloud zu verabschieden. Eine regelmässige Überprüfung der digitalen Selbstbestimmung, etwa durch eine Bewertung technischer und organisatorischer Abhängigkeiten, die Definition von Auswahlkriterien für vertrauenswürdige Provider, eine klare Datenklassifizierung sowie wiederkehrende Risikoanalysen und Exit-Strategien, lohnt sich indes allemal. Diese Schritte reduzieren Abhängigkeiten, erhöhen Transparenz und Resilienz, und sichern die langfristige Steuerbarkeit digitaler Systeme.

RECHTS-KOMMISSION

Das Autorenteam aus Rechtsanwälten und einem Unternehmensjurist sind aktive Mitglieder der swissICT-Rechtskommission. Das Ziel der Rechtskommission ist, Provider und Nutzer:innen von IT-Leistungen für juristische Themen und Probleme zu sensibilisieren und rechtliche Fragestellungen mit Relevanz für die IT-Industrie praxisgerecht aufzubereiten.

Bild: zvg

SUCCESS STORY: PRAXISBERICHT AUS DER ICT-SALÄRSTUDIE

Ende 2024 erforderte die Geschäftsaufgabe eines Dienstleisters die kurzfristige Migration der ICT-Salärstudie. Was als Notfall begann, erwies sich als Praxisbeispiel für digitale Souveränität. Ein Bericht darüber, warum Datenhoheit und Schweizer Partnerschaften besonders zählen, wenn die Sonne nicht scheint.

AUTOR:INNEN: SAMUEL STEINER UND CORNELIA AMMON

«Bei Schönwetter kann jede:r zu Berge gehen.» Dieses Sprichwort bewahrheitet sich in der IT immer wieder. Solange Systeme laufen, Zertifikate aktuell sind und Dienstleistungen verfügbar bleiben, ist der Betrieb einer Plattform Routine. Die Realität der digitalen Abhängigkeit zeigt sich oft erst, wenn unvorhergesehene Ereignisse schnelles Handeln erfordern.

Für swissICT trat dieses Szenario Ende 2024 ein, als die Infrastruktur sowie die technische Betreuung der Salärstudie unter hohem Zeitdruck migriert werden mussten. Der abstrakte Begriff der «Souveränität» wurde zur operativen Realität. Im Zentrum standen für swissICT weniger neue Features, sondern Werte wie Rechtssicherheit, Verfügbarkeit und das Vertrauen, sensible Lohndaten in einem Schweizer Rechtsraum zu wissen.

Nähe und Rechtsraum

Die Übernahme einer bestehenden Applikation (Ruby on Rails App) unter Zeitdruck ist herausfordernd. Kündigungsfristen drängen, Serverkonfigurationen müssen verstanden sowie Eigentumsverhältnisse und Zugriffsrechte geklärt werden. In solchen Krisen zeigt sich der Wert lokaler Verankerung. Es ist ein Trugschluss zu glauben, digitale Dienstleistungen seien ortsunabhängig. Es macht einen fundamentalen Unterschied, sich bei Problemen direkt an einen Tisch zu setzen. Souveränität bedeutet auch operative Handlungsfähigkeit. Die Möglichkeit, zum Telefon zu greifen oder persönlich vorbeizugehen, schafft operative Resilienz, die rein vertraglich kaum abzubilden ist. Gerade weil swissICT und die neue Technologiepartnerin Renuo AG im selben kulturellen und rechtlichen Umfeld agieren, konnten komplexe Fragen zur Migration pragmatisch und ohne interkulturelle Reibungsverluste gelöst werden.

Die Frage des Hostings

Ein Rechenzentrum in der Schweiz allein sagt wenig über die anwendbaren Rechtsräume aus. Werden Daten bei internationalen Hyperscalern gehalten, gelten deren rechtliche Rahmenbedingungen. In Kombination mit europäischen Regulierungen oder dem künftigen *AI Act* entstehen so reale Druckpunkte. Die Wahl rein schweizerischer Partner ist daher eine strategische Notwendigkeit für den Datenschutz und die Compliance-Sicherheit der Salärstudie.

Bei der Migration der Plattform stand eine strategische Entscheidung im Zentrum: Wo und wie betreiben wir die Applikation künftig? Der Entscheid fiel bewusst auf die Schweizer Plattform-as-a-Service-Lösung (PaaS) Deploio, welche auf offenen Standards basiert und keinen Vendor-Lock-in erzwingt.

Die Entscheidung für eine PaaS-Lösung auf offenen Standards verlangt eine technische Disziplin, die sich auszahlt. Durch die Trennung von Applikations-Code und Konfiguration steigen Portabilität und Sicherheit massiv an. Eine Software nach diesem Standard lässt sich jederzeit verschieben. Das ist die technische Definition von Unabhängigkeit.

Diese Architektur hat auch eine politische Dimension. Durch die Kombination eines lokalen Dienstleistungspartners, einem rein schweizerischen Hosting sowie einem Setup, das die Portabilität maximiert, entsteht eine durchgängige Swiss-Made-Kette. Von der Software-Entwicklung durch eine in der Schweiz ansässige Agentur über die Datenbank bis hin zum auslieferndem Server unterliegt die Wertschöpfung dem Schweizer Recht. Damit werden für den Betrieb und die Datenhaltung jegliche Berührungspunkte mit dem *US CLOUD Act* vermieden.

Rechtssicherheit als höchstes Gut

Digitale Souveränität definiert sich nicht nur über Technik, sondern über rechtliche Kontrolle. Die Eigentumsfrage des Codes ist bei der ICT-Salärstudie klar geregelt und liegt vollumfänglich bei swissICT. Das stellt sicher, dass der Verband jederzeit die Kontrolle über das Kern-Asset der Studie behält.

Ebenso wurden die Herausgabepflichten geregelt. Da alle Parteien ausschliesslich dem Schweizer Recht unterstehen, entfällt das Risiko, dass ausländische Behörden Zugriff auf die Daten fordern könnten. Eine Datenherausgabe ist damit klar definiert: Sie kann nur aufgrund einer Schweizer Verfügung erfolgen. Für die teilnehmenden Unternehmen bedeutet dies einen konkreten Schutz ihrer Anonymität, der fest im Schweizer Datenschutzgesetz (DSG) verankert ist.

Bereit für die Zukunft

Ein weiterer zentraler Baustein ist die externe Validierung der Partnerunternehmen. Sicherheit ist kein Zustand, den man einfach behauptet, sondern muss belegt werden. Darum setzt swissICT für den Betrieb der Plattform auf Technologiepartner, deren Standards durch anerkannte Labels wie *CyberSeal* zertifiziert sind. Ein klares Signal, dass swissICT die Messlatte für Auftragnehmende hoch legt. Selbst ist swissICT *Cyber*SAFE zertifiziert und trägt ebenso aktiv zur Sicherheit bei.

Die Migration der Salärstudie ist anfangs 2025 geglückt und hat bewiesen: Digitale Souveränität ist machbar. Im Fall von swissICT erforderte sie einen bewussten Entscheid für den sicheren Weg mit lokalen Partnerunternehmen. Die Salärstudie liefert damit nicht nur wertvolle Marktdaten, sondern vertritt auch in ihrer technischen DNA die Grundwerte der Schweizer ICT: Unabhängigkeit, Qualität und Sicherheit.

CyberSeal: CyberSeal ist ein Schweizer Gütesiegel, das von der Allianz Digitale Sicherheit Schweiz vergeben und vom Bundesamt für Cybersicherheit (BACS) unterstützt wird. Es zertifiziert, dass eine Organisation angemessene technische und organisatorische Massnahmen zum Schutz vor Cyberrisiken umgesetzt hat.

DIGITALSECURITYSWITZERLAND.CH

CyberSAFE: CyberSAFE ist ein Schweizer Cybersicherheits-Label, das Organisationen ein verantwortungsbewusstes Cyber-Risk-Management auf einem von öffentlichen und privaten Partnern als akzeptabel definierten Niveau attestiert. Es basiert auf einer neutralen, praxisorientierten Bewertung von IT-Systemen, Prozessen und menschlichen Kompetenzen.

CYBER-SAFE.CH

Technologiepartnerin Renuo AG

Renuo AG ist eine Schweizer Software-Agentur. Das 25-köpfige Team hat sich auf die Entwicklung von massgeschneiderten Webapplikationen auf Basis von Ruby on Rails spezialisiert. Als swissICT-Mitglied begleitet Renuo den Verband als technische Partnerin.

RENUO.CH

DIE AUTOR:INNEN

Samuel Steiner ist Geschäftsführer bei Renuo AG. Er verbindet strategischen Weitblick mit pragmatischer Umsetzung und begleitet Kund:innen von der Idee bis zur passenden digitalen Lösung.
Cornelia Ammon ist Produkt Managerin bei swissICT und verantwortlich für die Durchführung und Weiterentwicklung der ICT-Salärstudie.

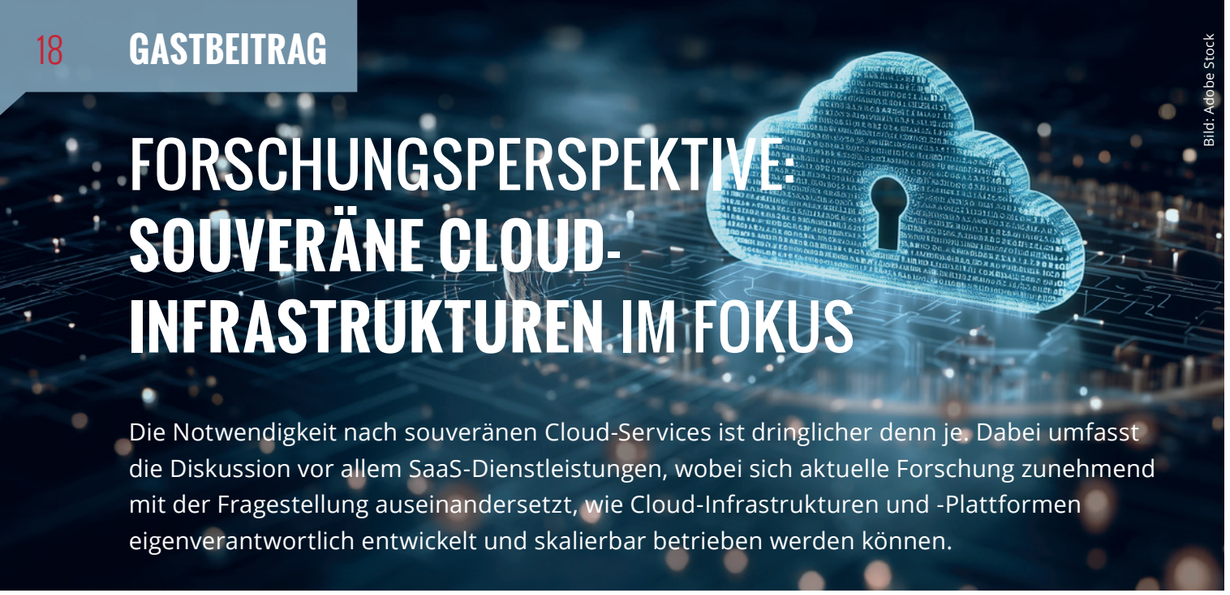


Bild: Adobe Stock

FORSCHUNGSPERSPEKTIVE: SOUVERÄNE CLOUD-INFRASTRUKTUREN IM FOKUS

Die Notwendigkeit nach souveränen Cloud-Services ist dringlicher denn je. Dabei umfasst die Diskussion vor allem SaaS-Dienstleistungen, wobei sich aktuelle Forschung zunehmend mit der Fragestellung auseinandersetzt, wie Cloud-Infrastrukturen und -Plattformen eigenverantwortlich entwickelt und skalierbar betrieben werden können.

AUTOR: SEBASTIAN GRAF

Die geopolitischen Entwicklungen der letzten Jahre stellen die Belastbarkeit von Zusicherungen seitens der Hyperscaler in Frage: Individuelle Sanktionen gegenüber Richter:innen des internationalen Strafgerichtshofs zeigen beispielsweise, dass amerikanische Firmen Garantien praktisch nicht einhalten können. Der Bundesrat definierte im November 2025, dass die Schweiz «über die erforderlichen Kontroll- und Handlungsfähigkeiten im digitalen Raum verfügen muss, um digital souverän zu sein». In der Folge muss das Spektrum technischer Massnahmen auf zwei Dimensionen ausgeweitet werden: Zusätzlich zur notwendigen Wahrung der Vertraulichkeit rückt auch die Verfügbarkeit in den Fokus der Forschung.

Vom politischen Anspruch zur technischen Umsetzung

Cloud-Services sind dabei nicht nur auf der Software-as-a-Service-Ebene (SaaS) zu betrachten. Hier gibt es bereits einige Vorstösse, die Monopolstellung von Microsoft und Google mit offenen und selbst gehosteten Office-Lösungen zu überwinden. Die grundlegende Fragestellung, wie eigenständig entwickelte und betriebene Cloud-Services matur, benutzerfreundlich und verfügbar bereitgestellt werden können, zieht sich dabei durch den gesamten Stack der IT.

Gerade auf Plattformebene definiert die Auswahl der Services, wie eng eine Applikation inklusive ihrer Daten an einen Hyperscaler gebunden ist. Diese Auswahl schlägt sich direkt auf die Handhabung von Workloads und Datenhaltung nieder. Um einen Vendor-Lock-in zu minimieren, muss diese Serviceauswahl flexibel und anpassbar gestaltet werden.

In diesem Kontext wird aktuell in verschiedenen Forschungsarbeiten evaluiert, unter welchen Bedingungen und mit welchen technischen Mechanismen Daten und Applikationen während des laufenden Betriebs auf mehrere Plattformen verteilt werden können. Entsprechende Verteilungsansätze unterliegen dabei vorgängig nichtfunktionalen Vorgaben wie zum Beispiel einer expliziten Handhabung von personalisierten Daten oder der Annahme, dass bestimmte Plattformen oder Cloud-Provider nicht verfügbar werden könnten. Plattformen müssen gleichzeitig so bereitgestellt werden, dass Applikationen cloud-unabhängig und transparent darauf entwickelt werden können. Im Umfeld der cloud-nativen Ökosysteme wie Kubernetes bestehen dabei bereits mature Technologien, welche auch schon von Projekten wie dem Sovereign Cloud Stack (SCS) und Neo-Nephos als Nachweis einer homogenisierten Umgebung verwendet werden.

Bild: zvg

SEBASTIAN GRAF

Sebastian Graf arbeitete nach seiner Promotion an der Universität Konstanz als Software-Entwickler, Software-Architekt und als Product Manager sowohl in Startups als auch grösseren Unternehmen. Seit 2022 ist er Professor für Cloud-Infrastrukturen und agilen Software-Betrieb an der Fachhochschule Nordwestschweiz.

Abstraktion als strategischer Hebel

Eine Zukunftsprognose hängt daher unmittelbar davon ab, wie erfolgreich diese Ansätze zur Abstrahierung von Hyperscaler-Infrastrukturen in der Praxis sein werden und wie sich diese weiterentwickeln. Um mittelfristig wirkliche Souveränität zu erreichen, müsste sowohl die Infrastruktur-Provisionierung als auch der Betrieb über verschiedene Provider abstrahiert werden. Jegliche souveränen, virtualisierten Systeme sollten als Software integrierbar werden, dass am Ende cloud-native Plattformen nicht nur verwendet, sondern direkt vorher provisioniert und betrieben werden könnten – on-premise wie auch auf hiesigen Clouds.

Die Grundvoraussetzungen sind gegeben: Viele cloud-native Plattformen wie Kubernetes sind heute schon offen im Sinne des Open-Source-Gedankens. In einem Best-Case-Szenario wäre damit nicht nur die Garantie gegeben, dauerhaft souverän Plattformen zu verwenden, sondern Open Source würde sich zu Open Plattform weiterentwickeln.

5. MAI 2026: #DIGITUP & GV

Am #DIGITUP mit anschliessender swissICT-Generalversammlung kommt unsere Community auch dieses Jahr wieder in Zürich zusammen. Ein besonderes Highlight sind die zahlreichen Workshops und Referate unserer Fachgruppen, die aktuelle Themen aus dem IT-Sektor praxisnah, kontrovers und zukunftsgerichtet beleuchten.

An der Generalversammlung werden Weichen gestellt, neue Persönlichkeiten willkommen geheissen und prägende Stimmen aus dem swissICT-Universum verabschiedet. Wer mitreden und mitgestalten will, sollte diesen Event nicht verpassen.

Und natürlich bleibt genug Raum für Austausch, Begegnungen und Networking. Es sind alle herzlich willkommen, die sich für IT und moderne Arbeitswelten interessieren.

ALLE INFOS AUF SWISSICT.CH/DIGITUP-GV-2026

ALLE EVENTS AUF EINEN BLICK

Unsere Eventagenda bündelt relevante ICT-Anlässe an einem Ort. Sie finden dort Fachveranstaltungen, Community-Events und Weiterbildungen aus der Schweizer ICT-Branche.
Die Agenda hilft Ihnen, passende Events zu finden oder eigene Veranstaltungen mit der swissICT-Community zu teilen. Bleiben Sie auf dem Laufenden und entdecken Sie spannende Events rund um Digitalisierung, Technologie und Arbeitswelten.
Schon länger nicht mehr vorbeigeschaut?

HIER GEHTS ZUR EVENTAGENDA: SWISSICT.CH/EVENTS

IMPRESSUM

Das swissICT Magazin ist das offizielle Publikationsorgan von swissICT und wird direkt an die Mitglieder versandt. Es erscheint zweimal jährlich und ist unter www.swissict.ch kostenlos als PDF erhältlich.

Herausgeber: swissICT, Vulkanstrasse 120, 8048 Zürich

Redaktionsleitung:
Romana Bleisch, romana.bleisch@swissict.ch und Philipp Binaghi, philipp.binaghi@swissict.ch

Anzeigen: Carol Lechner, carol.lechner@swissict.ch

Redaktionelle Mitwirkung: Thomas Flatt, Matthias Michel, Marc Holitscher, Matthias Stürmer, Florian Schütz, Nathalie Kern, Alina Matyukhina, Liisa Pakosta, Sven Kohlmeier, Matthias Ebneter, Alexander Hofmann, Samuel Steiner, Cornelia Ammon, Sebastian Graf

Grafik: Staudenmann Kommunikation AG

Druck: Druckerei Varicolor

Druckauflage: 3500 Exemplare

Eine fundierte Entscheidungs-grundlage für Ihre Lohnpolitik.

swissICT

SALÄRSTUDIE 2026

JETZT ANMELDEN >

Mit rund 40'000 Datensätzen ist die ICT-Salärstudie die zentrale Referenz für ICT-Gehälter in der Schweiz.

Ihr Beitrag stärkt die Datengrundlage der Branche und Sie profitieren von besseren Benchmarks.

Jetzt für die Studienteilnahme 2026 anmelden:
swissict.ch/salaere-der-ict-voranmeldung