

NACHLESE | CommunityConnect am 11. Mai 2026

Beim dritten CommunityConnect der Community Plattform Verwaltungsinnovation, organisiert von IÖB, BRZ, Wien IT und der Abteilung für Verwaltungsinnovation und Strategische Organisationsentwicklung des Bundeskanzleramts, drehte sich alles um das Thema „Digitale Souveränität und Sicherheit“.

Eröffnet wurde die Veranstaltung von Staatssekretär Alexander Pröll, der in seinen einleitenden Worten die Bedeutung digitaler Handlungsfähigkeit, europäischer Zusammenarbeit und resilienter Verwaltungsstrukturen hervorhob.

Im Anschluss beleuchteten drei Keynotes sowie eine hochkarätig besetzte Paneldiskussion unterschiedliche Perspektiven auf digitale Souveränität, von Open Source und Forschungsförderung bis hin zu Quantenkryptographie, KI und europäischen Datenräumen. Vertreterinnen und Vertreter aus Verwaltung, Forschung, Infrastruktur und Technologieentwicklung diskutierten gemeinsam darüber, wie digitale Unabhängigkeit gestärkt und gleichzeitig Innovation, Sicherheit und Zusammenarbeit gefördert werden können.

Bereits zu Beginn wurde deutlich: Digitale Souveränität ist längst kein abstraktes Zukunftsthema mehr, sondern betrifft die konkrete Arbeitsfähigkeit öffentlicher Institutionen, Unternehmen und kritischer Infrastrukturen. Im Zentrum standen Fragen nach technologischer Unabhängigkeit, resilienten IT-Systemen, Open-Source-Strategien, Cybersicherheit sowie der Rolle europäischer Kooperationen.

Keynote 1: Einführung von LibreOffice im BMLV/ÖBH

Der erste Impuls wurde von der Direktion 6 – IKT und Cyber des Bundesheers geliefert. Im Mittelpunkt stand die Einführung von LibreOffice im österreichischen Bundesheer und die Frage, wie digitale Souveränität in der öffentlichen Verwaltung konkret umgesetzt werden kann.

Eindrucksvoll wurde geschildert, wie der Wunsch nach langfristiger digitaler Handlungsfähigkeit zur bewussten Entscheidung führte, unabhängiger von einzelnen Technologieanbietern zu werden. Dabei wurde betont, dass es bei der Umstellung nicht primär um Kostenersparnis gehe, sondern um die Fähigkeit, auch ohne externe Cloud-Infrastrukturen oder geopolitische Abhängigkeiten arbeitsfähig zu bleiben.

Open Source wurde dabei nicht nur als technische Lösung verstanden, sondern als strategischer Ansatz zur Stärkung europäischer Wertschöpfung, Transparenz und

Zusammenarbeit. Gleichzeitig wurde deutlich gemacht, dass digitale Souveränität weit über Software hinausgeht: Prozesse, Standards, Kompetenzen und organisatorischer Wandel spielen eine zentrale Rolle. Change Management, Community-Arbeit und gemeinsame Weiterentwicklung wurden als entscheidende Erfolgsfaktoren hervorgehoben.

Keynote 2: Forschungsförderung für Souveränität und Sicherheit in Europa

Die zweite Keynote hielt Jeannette Klonk von der FFG Organisationseinheit Europäische und Internationale Programme. Sie gab einen Überblick über europäische Förderprogramme und Initiativen im Bereich Sicherheitsforschung, Cybersecurity und digitale Souveränität.

Vorgestellt wurden unter anderem Möglichkeiten innerhalb von Horizon Europe, dem Digital Europe Programme sowie Initiativen zur Förderung europäischer Sicherheits- und Innovationsprojekte. Besonders hervorgehoben wurde die Bedeutung grenzüberschreitender Zusammenarbeit zwischen Forschung, Verwaltung, Wirtschaft und Infrastrukturbetreibern.

Ziel sei es, europäische Lösungen für Herausforderungen wie Cyberbedrohungen, resiliente Kommunikationssysteme oder sichere KI-Anwendungen zu entwickeln. Dabei wurde deutlich, dass digitale Souveränität nicht isoliert erreicht werden kann, sondern gemeinsame Standards, Vernetzung und langfristige Investitionen in Forschung, Kompetenzen und sichere Technologien benötigt.

Keynote 3: Quantentechnologie Digi.Lab

Die dritte Keynote gestaltete Harald Schneider, Head of Competence Center Digi.Lab der Wien IT. Im Fokus standen aktuelle Entwicklungen rund um Quantenkryptographie und Quantensensorik sowie deren Bedeutung für die zukünftige Cybersicherheit.

Thematisiert wurde insbesondere die Frage, warum sich Organisationen bereits heute mit Post-Quantum-Verschlüsselung beschäftigen sollten, auch wenn leistungsfähige Quantencomputer noch nicht flächendeckend verfügbar sind. Diskutiert wurde die Gefahr, dass heutige Verschlüsselungsverfahren künftig durch Quantencomputer entschlüsselt werden könnten.

Gleichzeitig wurden neue Ansätze vorgestellt, die auf quantenphysikalischen Prinzipien basieren und künftig besonders sichere Kommunikationswege ermöglichen sollen. Neben Verschlüsselung standen auch Anwendungen der Quantensensorik im Fokus, etwa für hochpräzise Messungen, kritische Infrastruktur oder autonome Navigationssysteme. Der Vortrag zeigte eindrucksvoll, wie eng technologische Innovation, Sicherheit und strategische Zukunftsfragen mittlerweile miteinander verbunden sind.

Paneldiskussion zum Thema „Digitale Souveränität und Sicherheit“.

Im anschließenden Panel diskutierten Christian Braunsteiner (Wiener Stadtwerke), Mario Drobics (AIT Austrian Institute of Technology), Barbara Keck (BRZ) und Michael Plachy (Bundeskanzleramt) unter der Moderation von Manuel Schuler (Leiter der IÖB-Servicestelle) über konkrete Herausforderungen digitaler Souveränität in der Praxis.

Dabei wurde mehrfach betont, dass vollständige digitale Autarkie weder realistisch noch sinnvoll sei. Ziel müsse vielmehr sein, Entscheidungsfreiheit, Kontrolle über Daten und technologische Handlungsfähigkeit zurückzugewinnen.

Diskutiert wurden unter anderem:

- die Bedeutung von Open Source,
- der bewusste Umgang mit Cloud- und Plattformabhängigkeiten,
- europäische Datenräume,
- sowie der Aufbau eigener Kompetenzen innerhalb von Organisationen.

Auch künstliche Intelligenz spielte eine wichtige Rolle in der Diskussion. Neben technologischen Fragen standen organisatorische Voraussetzungen im Mittelpunkt: Welche Kompetenzen brauchen Mitarbeitende? Wie können Verwaltungen souverän mit KI-Systemen umgehen? Und wie gelingt es, Innovation mit Sicherheit, Datenschutz und regulatorischen Anforderungen zu verbinden?

Ein weiterer Schwerpunkt lag auf europäischen Datenökosystemen wie Gaia-X, die vertrauensvolle und kontrollierbare Datennutzung zwischen Organisationen ermöglichen sollen. Vertrauen, Transparenz und gemeinsame Standards wurden dabei als zentrale Voraussetzungen für funktionierende digitale Zusammenarbeit genannt.

Fazit: Digitale Souveränität braucht Zusammenarbeit, Kompetenzen und Mut zur Veränderung

Die Veranstaltung zeigte eindrucksvoll, dass digitale Souveränität weit mehr ist als eine technologische Frage. Es geht um strategische Entscheidungen, organisatorische Veränderung und den Aufbau langfristiger europäischer Handlungsfähigkeit.

Deutlich wurde auch: Viele Lösungen existieren bereits, von Open-Source-Ökosystemen über europäische Förderprogramme bis hin zu neuen Sicherheits- und Quantentechnologien. Entscheidend wird sein, diese Ansätze gemeinsam weiterzuentwickeln, Kompetenzen aufzubauen und Kooperationen zu stärken.

Der CommunityConnect machte damit sichtbar, dass Europa im digitalen Raum nicht nur reagieren, sondern aktiv gestalten kann, vorausgesetzt, Innovation, Sicherheit und Zusammenarbeit werden gemeinsam gedacht.