

east#digital

02 / Juni 2026
www.eastdigital.ch

FACTS UND FIGURES AUS DER
DIGITALISIERUNGSMETROPOLE OSTSCHWEIZ



GOLDPARTNER



<IT>rockt!

PARTNER



LEADER^{digital}

Digitale Identität zwischen Sicherheit und Privatsphäre

Mit der Swiss e-ID wird digitale Identität in der Schweiz zum Alltagsthema. Digitale Nachweise versprechen einen einfacheren Zugang zu Dienstleistungen und reibungslosere Abläufe. Gleichzeitig stellt sich eine zentrale Frage: Wie lassen sich Sicherheit, Datenschutz und Benutzerfreundlichkeit so verbinden, dass Nutzer die Kontrolle über ihre Daten behalten?

Ein Gastartikel von Katerina Mitrokovska, Professorin und Leiterin des Fachbereichs Cybersicherheit an der Universität St.Gallen

Jeden Tag erkennen unsere Smartphones unsere Gesichter, Banking-Apps überprüfen Fingerabdrücke, und Online-Konten verlangen von uns, unsere Identität nachzuweisen. Diese Vorgänge sind schnell und bequem, und wir denken kaum darüber nach. Doch sie beruhen auf einer überraschend fragilen Annahme: dass Systeme zuverlässig zwischen uns und jemandem, der sich als wir ausgibt, unterscheiden können.

«Identität ist die neue Angriffsfläche.»

Im Alltag weisen wir unsere Identität auf vertraute Weise nach, etwa durch das Vorzeigen eines Ausweises, durch Unterschriften oder durch das Vorlegen von Diplomen. Diese Handlungen ermöglichen Zugang, schaffen Vertrauen und erlauben die Teilnahme am gesellschaftlichen Leben. In der digitalen Welt erfüllt Identität denselben Zweck, jedoch unter völlig anderen Bedingungen. Die Überprüfung erfolgt nicht mehr von Angesicht zu Angesicht, sondern aus der Distanz, oft automatisiert und über mehrere Systeme hinweg. Dadurch wird digitale Identität einerseits unverzichtbar, andererseits auch anfälliger.

Heute nutzen wir digitale Identität für Bankgeschäfte, Gesundheitsdienste, öffentliche Leistungen und universitäre Plattformen. Im Hintergrund stehen Passwörter, Geräte, biometrische Daten wie Fingerabdrücke oder Gesichtserkennung sowie digitale Nachweise. Funktioniert das Zusammenspiel dieser Elemente, erleichtert es unseren Alltag. Versagt es, können die Folgen unmittelbar sein.

Wenn Identität zum Angriffsziel wird

Viele Angriffe richten sich heute nicht mehr primär gegen technische Systeme, sondern direkt gegen die Identität. Phishing bringt Nutzer dazu, Zugangsdaten preiszugeben. Datenlecks legen Millionen von Passwörtern offen, die Angreifer anschliessend in verschiedenen Diensten wiederverwenden.

Gleichzeitig macht künstliche Intelligenz solche Angriffe überzeugender und schwerer erkennbar. Synthetische Stimmen, manipulierte Videos und personalisierte Nachrichten können genutzt werden, um vertrauenswürdige Personen oder Organisationen realistisch zu imitieren. Was früher grossen Aufwand erforderte, lässt sich heute automatisieren und skalieren.

Auch biometrische Systeme, die oft als besonders sicher gelten, bringen eigene Risiken mit sich. Im Gegensatz zu Passwörtern lassen sich biometrische Merkmale nicht einfach ändern. Werden sie kompromittiert, kann dies langfristige Folgen haben.

Es gibt bereits konkrete Beispiele: 2015 wurden bei einem Angriff auf das US Office of Personnel Management Daten von über 20 Millionen Personen gestohlen, darunter mehr als fünf Millionen Fingerabdrücke. 2019 führte eine Schwachstelle im BioStar-2-System dazu, dass Millionen biometrischer Datensätze öffentlich zugänglich waren, einschliesslich Fingerabdrücken und Gesichtsdaten.

Diese Entwicklungen machen Angriffe auf digitale Identität nicht nur häufiger, sondern auch



Katerina Mitrokotsa:
Datenschutz
schafft Vertrauen.

schwieriger zu erkennen und zu verhindern. Das Ziel bleibt dabei stets dasselbe: die Kontrolle über eine digitale Identität zu erlangen.

Sicherheit und Datenschutz in Einklang bringen

Um diesen Bedrohungen zu begegnen, sind stärkere Authentifizierungsverfahren notwendig. Gleichzeitig führt mehr Sicherheit oft dazu, dass mehr persönliche Daten erhoben und verarbeitet werden.

«Mehr Sicherheit bedeutet oft mehr Daten.»

Hier entsteht ein grundlegender Zielkonflikt. Regulierungen wie die DSGVO und das Schweizer Datenschutzgesetz betonen, dass nur die unbedingt notwendigen Daten verwendet werden sollen. In der Praxis werden Nutzer jedoch häufig aufgefordert, mehr Informationen preiszugeben als erforderlich, etwa ihr vollständiges Geburtsdatum oder ihre Adresse, selbst wenn nur ein einzelnes Detail benötigt wird.

Daraus ergeben sich zentrale Fragen: Wie viele Informationen sollten wir tatsächlich preisgeben, um uns zu identifizieren? Ist es möglich, Identität zu verifizieren, ohne sensible Daten offenzulegen? Und wie können Nutzer die Kontrolle über ihre Daten behalten?

Privacy by Design

Ein Ansatz besteht darin, Identitätssysteme von Anfang an datenschutzfreundlich zu gestalten. Das Prinzip ist einfach: Es sollen nur jene Informationen preisgegeben werden, die für einen bestimmten Zweck tatsächlich notwendig sind. Moderne kryptografische Verfahren machen dies möglich.

Ein Beispiel ist der Kauf von Alkohol. Um diesen zu erwerben, muss man nachweisen, dass man über 18 Jahre alt ist. Üblicherweise geschieht dies durch Vorzeigen eines Ausweises, der deutlich mehr Informationen enthält als notwendig.

Mit datenschutzfreundlichen Verfahren kann stattdessen nur eine einzige Tatsache überprüft werden: dass die Altersgrenze erfüllt ist. Das Geschäft erhält keine weiteren persönlichen Informationen. Nutzer können damit nachweisen, dass sie zum Kauf berechtigt sind, ohne ihre Identität oder ihr genaues Geburtsdatum offenzulegen.

Sichere Biometrie und mehr Kontrolle

Angesichts der Risiken biometrischer Verfahren stellt sich die Frage, wie diese sicher umgesetzt werden können. Ein vielversprechender Ansatz besteht darin, auf die Speicherung roher biometrischer Daten zu verzichten. Stattdessen werden geschützte Repräsentationen verwendet, die sich nicht rekonstruieren oder missbrauchen lassen. So kann ein System eine Person wiedererkennen, ohne die zugrunde liegenden biometrischen Daten offenzulegen.

Auch bei der Anmeldung bei Online-Diensten gibt es datenschutzfreundlichere Ansätze. Viele Plattformen ermöglichen heute die Anmeldung über bestehende Konten von Anbietern wie Google oder Facebook. Das ist bequem, bedeutet aber auch, dass diese Anbieter grundsätzlich beobachten können, wo und wann sich Nutzer anmelden.

Alternative Verfahren verfolgen das Ziel, denselben Komfort zu bieten, ohne diese Nachverfolgbarkeit zu ermöglichen. Nutzer sollen sich sicher anmelden können, ohne dass eine zentrale Stelle ihr Verhalten über verschiedene Plattformen hinweg beobachten kann.



Bedeutung für die Swiss e-ID

Diese Ansätze sind besonders relevant für die Swiss e-ID. Ein gut gestaltetes System könnte es ermöglichen, den Wohnsitz in einem Kanton nachzuweisen, ohne die vollständige Adresse offenzulegen. Ebenso könnten Berechtigungen bestätigt werden, ohne unnötige Details preiszugeben. Auch eine sichere Authentifizierung wäre möglich, ohne sensible Daten zentral zu speichern. Durch die Reduktion der weitergegebenen Daten werden sowohl die Sicherheit als auch der Datenschutz gestärkt.

Vertrauen als entscheidender Faktor

Digitale Identität wird zu einem grundlegenden Bestandteil unserer Gesellschaft. Sie bestimmt, wie wir auf Dienstleistungen zugreifen, wie Organisationen mit uns interagieren und wie Vertrauen im digitalen Raum entsteht. Schlecht gestaltete Systeme können Betrug, Überwachung und Kontrollverlust begünstigen. Gut gestaltete Systeme hingegen reduzieren Risiken und stärken das Vertrauen. Dabei geht es nicht nur

darum, Systeme sicherer zu machen, sondern Sicherheit und Datenschutz in Einklang zu bringen. Mit der weiteren Digitalisierung wird die Bedeutung datenschutzfreundlicher Identitätssysteme weiter zunehmen. Technologie allein reicht jedoch nicht aus. Auch Regulierung, Systemdesign und gesellschaftliches Bewusstsein spielen eine wichtige Rolle.

«Vertrauen ist die Grundlage digitaler Identität.»

Digitale Identität ist letztlich keine rein technische Frage. Sie betrifft das grundlegende Verhältnis zwischen Sicherheit, Privatsphäre und Vertrauen. Während die Schweiz die Einführung der e-ID vorantreibt, besteht die zentrale Herausforderung darin, diese Systeme von Anfang an so zu gestalten, dass Sicherheit, Datenschutz und Nutzerkontrolle integraler Bestandteil sind.

Bild: Marlies Beeler-Thurnheer



Weniger Kabelsalat – mehr chrisign

chrisign.ch – der Digitalisierungsspezialist
aus dem Thurgau



chrisign gmbh Walkenstrasse 11 8570 Weinfelden info@chrisign.ch www.chrisign.ch



Digital & Start-ups

Virtuelle Maus soll Tierversuche reduzieren

Forscher der Empa haben ein KI-gestütztes Computermodell entwickelt, das Tierversuche in der medizinischen Forschung künftig reduzieren könnte. Die sogenannte «virtuelle Maus» simuliert, wie sich Nanopartikel im Körper verteilen, und soll damit die Entwicklung neuer Therapien beschleunigen. Das Modell basiert auf Daten aus 18 früheren Mausexperimenten und nutzt maschinelles Lernen, um die Eignung von Nanopartikeln bereits vor deren Herstellung zu beurteilen. Langfristig wollen die Forscher das Prinzip auch auf den Menschen übertragen.



OST-Projekt erhält Anerkennungspreis

Das Forschungsprojekt «Gen-AI zur Produktionsdigitalisierung» der OST – Ostschweizer Fachhochschule ist mit dem Anerkennungspreis der Stiftung FUTUR ausgezeichnet worden. Die entwickelte Lösung iDIP

nutzt generative KI, um Produktionsprozesse in KMU einfacher zu digitalisieren. Ein KI-Beratungs-Bot übersetzt Anforderungen aus der Produktion in technische Spezifikationen, ein weiterer KI-Agent setzt Anpassungen direkt im System um. Dadurch soll der Implementierungsaufwand deutlich sinken.



Hostpoint startet Datei-transfer-Dienst

Der Rapperswiler Cloud- und Hostinganbieter Hostpoint erweitert sein Angebot mit dem Datei-transfer-Dienst «File Express». Die Plattform wird vollständig über Schweizer Server betrieben und positioniert sich als Alternative zu internationalen Diensten wie WeTransfer. Nutzer können Dateien in der Basisversion kostenlos und ohne Registrierung versenden. Registrierte Anwender erhalten zusätzliche Funktionen wie Transfer-Verwaltung, Passwortschutz und die Möglichkeit, Dateien anzufordern. Für Unternehmen stehen kostenpflichtige Abos mit erweiterten Sicherheitsfunktionen wie Ende-zu-Ende-Verschlüsselung und Geoblocking zur Verfügung.



I+D Campus startet eigene Community

Der I+D Campus in Kreuzlingen erweitert sein Angebot und lanciert eine eigene Community für Personen, Unternehmen und Organisationen aus den Bereichen Innovation, Digitalisierung und Unternehmertum. Mitglieder erhalten Zugang zu einem Netzwerk aus Partnern aus Forschung, Bildung, Wirtschaft und Start-up-Förderung sowie zu Veranstaltungen und Vergünstigungen für Co-working-Arbeitsplätze und Raumbuchungen. Der Anfang 2026 eröffnete Campus versteht sich als Drehscheibe für Innovation und digitale Transformation und bringt Wirtschaft, Wissenschaft und Bildung zusammen.

FileWave holt Gründerin zurück

Die Wiler Softwarefirma FileWave stellt ihre Führung neu auf. Firmengründerin Nurdan Eris kehrt als CEO zurück, während Nikola Gander die neu geschaffene Funktion des Co-CEO übernimmt. Mit der Doppelspitze will der Anbieter von Endpoint-Management-Lösungen die nächste Wachstumsphase einleiten und seine Position in sicherheitskritischen und regulierten Branchen stärken. FileWave mit Hauptsitz in Wil ist seit über 27 Jahren im Markt tätig und verwaltet nach eigenen Angaben weltweit Millionen von Endgeräten.

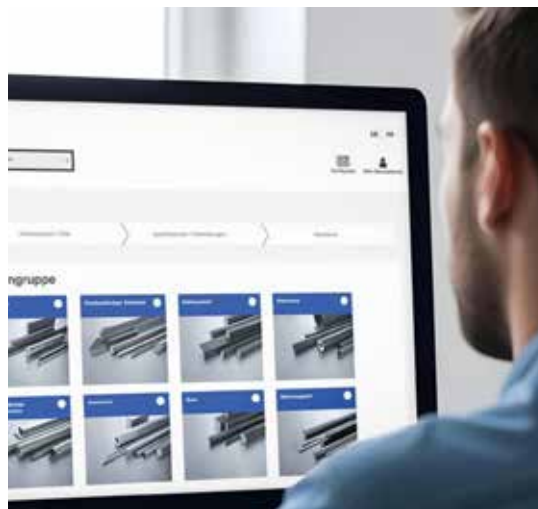


Gold für digitale Medikamentenplattform

Die Flawa Consumer GmbH ist mit ihrer digitalen Gesundheitsplattform Flawa iQ beim German Innovation Award 2026 mit Gold ausgezeichnet worden. Die App unterstützt Nutzer bei der sicheren Einnahme von Medikamenten und hilft dabei, Wechselwirkungen sowie Risiken bei der Selbstmedikation frühzeitig zu erkennen. Die Jury würdigte insbesondere die Verbindung von Gesundheitskompetenz, Benutzerfreundlichkeit und digitaler Innovation. Flawa iQ wurde in der Kategorie «Excellence in Business to Consumer» ausgezeichnet.

Schmobi erweitert digitales Stahlportal

Die Wiler Schmolz + Bickenbach Stahlcenter AG (Schmobi) hat ihr digitales Stahlportal um mehrere Funktionen erweitert. Neu erhalten Kunden bereits im Warenkorb Echtzeitinformationen zu Verfügbarkeit, Preisen und Lieferterminen. Zudem schlägt das System automatisch



Alternativen vor, wenn ein gewünschter Artikel nicht verfügbar ist. Bestellungen können neu auch dann abgeschlossen werden, wenn einzelne Positionen noch angefragt werden müssen. Laut Schmobi erfolgen bereits rund 80 Prozent der Preis-anfragen über das Portal, mehr als ein Drittel der Auftragspositionen wird direkt online bestellt.

Coachbetter erhält Millionenfinanzierung

Das Frauenfelder Sporttech-Unternehmen Coachbetter hat in einer Pre-Series-A-Finanzierungsrunde 6,4 Millionen Franken aufgenommen. Neu beteiligt sich auch der Deutsche Fussball-Bund (DFB) als strategischer Investor. Mit dem Kapital will Coachbetter seine Plattform für Vereins- und Teammanagement weiter ausbauen und die internationale Expansion vorantreiben. Die Lösung wird bereits von Spitzenvereinen, Verbänden und tausenden Amateurclubs genutzt.

KI soll Bewerbungen transparenter machen

Das St.Galler Start-up Humboldt AI entwickelt eine Plattform, die den Bewerbungsprozess für Stellensuchende transparenter machen soll. Mithilfe von Künstlicher Intelligenz analysiert die Lösung Stellenanzeigen und zeigt Bewerbern auf, wie gut ihr Profil zu einer ausgeschriebenen Stelle passt. Gleichzeitig erhalten Unternehmen strukturierte Einblicke in die Qualifikationen der Kandidaten. Ziel ist es, den Rekrutierungsprozess effizienter zu gestalten und die Erfolgchancen von Bewerbungen besser einschätzbar zu machen.

ALLE DIGITALNEWS DER OSTSCHWEIZ AUF EASTDIGITAL.CH

Der Hub «east#digital» der LEADER-Herausgeberin MetroComm AG begleitet den digitalen Wandel der Ostschweiz – dreimal pro Jahr mit einem Sonderteil im LEADER und mit der Newsplattform www.eastdigital.ch

 [eastdigital.ch](https://www.linkedin.com/company/eastdigital)





Digital Conference Ostschweiz 2026: Zwischen KI-Boom und Cyberrisiken

Am 8. September wird St.Gallen erneut zum Treffpunkt der digitalen Schweiz. Die Digital Conference Ostschweiz bringt im Einstein Congress Experten, Unternehmer und Entscheidungsträger zusammen. Im Zentrum steht ein Thema, das derzeit viele Unternehmen beschäftigt: «Cybersecurity trifft KI – Risiko oder Chance?» Special Guest ist Richard David Precht; Tickets sind ab sofort erhältlich.

Künstliche Intelligenz verändert Geschäftsmodelle, Prozesse und Entscheidungsmechanismen in rasantem Tempo. Gleichzeitig wachsen die Anforderungen an Sicherheit, Datenschutz und Resilienz digitaler Systeme. Die Digital Conference Ostschweiz 2026 greift diese Entwicklung auf und beleuchtet die Chancen, Risiken und strategischen Auswirkungen der Verbindung von KI und Cybersecurity.

Die Veranstaltung hat sich in den letzten Jahren als wichtige Plattform für digitale Zukunftsthemen in der Ostschweiz etabliert. Sie verbindet technologische Entwicklungen mit wirtschaftlichen und



gesellschaftlichen Fragestellungen und schafft Raum für Austausch und Vernetzung.

Hochkarätige Keynotes

Das Programm der Digital Conference Ostschweiz 2026 kombiniert technologische Expertise mit gesellschaftlicher Reflexion.

Zu den angekündigten Keynote-Speakern gehört der Philosoph und Publizist **Richard David Precht**. Er zählt zu den bekanntesten Intellektuellen im deutschsprachigen Raum und beschäftigt sich in seinen Arbeiten mit den Auswirkungen technologischer Entwicklungen auf Gesellschaft, Arbeit und Demokratie.

Mit **Jill Wick** steht eine Expertin für Security Awareness auf der Bühne, die den menschlichen Faktor in der Cybersicherheit ins Zentrum stellt. Die Wirtschaftspsychologin verbindet psychologische Erkenntnisse mit technologischen Fragestellungen und zeigt, wie Manipulation und Social Engineering in Cyberangriffen wirken.

Einen stark technologischen Fokus bringt **Anna-Lena Horlemann** ein. Die Professorin für theoretische Informatik und Mathematik forscht im Bereich Informationstheorie und Post-Quantum-

Kryptographie. Im Sommer 2026 wird sie an der HSG den neuen Lehrstuhl für Quantum Computing and Information Theory aufbauen.

Mit **Henriette Engbersen** ergänzt eine erfahrene Auslandskorrespondentin das Programm. Die frühere SRF-Korrespondentin in London befasste sich jahrelang mit politischen und gesellschaftlichen Entwicklungen in Grossbritannien. Heute leitet sie bei der SRG den Bereich «Public Value» und verantwortet Projekte zur Erkennung von Desinformation und Fake News.

Die Journalistin **Bigna Silberschmidt** führt durch den Anlass. Die frühere SRF-Moderatorin war unter anderem für «Einstein» und «10 vor 10» tätig und arbeitet heute selbständig als Moderatorin und Kommunikationsberaterin.

Auch die St.Galler Regierung ist Teil des Programms. Regierungspräsident **Beat Tinner** wird an der Konferenz einen Impuls zur digitalen Entwicklung und Standortattraktivität des Kantons geben.

Frühzeitige Anmeldung empfohlen

Die Digital Conference Ostschweiz zählt inzwischen zu den wichtigsten Digitalveranstaltungen



Bigna Silberschmidt, Moderation

der Region. Erwartet werden rund 300 Teilnehmer aus Wirtschaft, Technologie, Forschung und Verwaltung. Aufgrund der begrenzten Plätze empfehlen die Organisatoren eine frühzeitige Anmeldung.

Breakout-Sessions mit Praxisfokus

Neben den Keynotes setzt die Digital Conference auf interaktive Elemente. Vier Breakout-Sessions

ermöglichen vertiefte Diskussionen zu spezifischen Fragestellungen und fördern den Austausch zwischen Teilnehmern aus unterschiedlichen Branchen.

Thematisch reichen die Sessions von «Cybersecurity als Business-Enabler» über die Verbindung von KI und Compliance bis hin zu datenbasierten Geschäftsmodellen und Sicherheitsfragen rund um KI-Systeme und Prompt Injection.

Zu den Referenten der Breakout-Sessions gehören **Sylvain Luiset** von Zurich Insurance, **Christian Loser** und **Benedict Vuilleumier** von Acreo Consulting, **Hanspeter Pfändler** von MAIT Swiss, **Daniel Riedener**, Leiter Cyber Security bei der Ceruno AG sowie **Yannik Brühl**, Analyst für IT-Sicherheitsvorfälle und digitale Forensik bei der Arctic Wolf Networks Germany GmbH.

Kompaktes Programm mit Networking-Fokus

Das Programm ist bewusst kompakt strukturiert. Nach Registrierung und Welcome Coffee folgen Keynotes, Q&A-Sessions, Networking-Pausen sowie interaktive Formate. Den Abschluss bildet ein Apéro riche.

SPONSOREN

Presentingpartner

K Y O S

Goldpartner

ARCTIC WOLF

Silbersponsoren

Kanton St.Gallen



CONTENTHOUSE

st.gallen

valantic

dieMobiliar

ZURICH

Partner

Kanton St.Gallen
Amt für Wirtschaft
und Arbeit



ma't

Universität St.Gallen

1 CERUNO

acreo consulting
partnering
transformation

Netzwerkpartner

GEWERBEVERBAND
APPENZEL AUSSER RHODEN

**I + D
CAM
PUS**

**gewerbe
st.gallen**

**GEWERBE
THURGAU**

IHK
Industrie- und
Handelskammer
Thurgau

MOV'ING
LIGHT SOUND
MEDIA

START
NetzwerkThurgau

**SWITZERLAND
INNOVATION**
PARK OST

Award-Sponsoring

BVS St.Gallen

Hostpartner

E
EINSTEIN
ST. GALLEN



Keynote-Speaker
(von oben links)
Richard David Precht,
Jill Wick, Anna-Lena
Horlemann, Henriette
Engbersen

Zur Konferenz werden rund 300 Teilnehmer aus Wirtschaft, Verwaltung, Forschung und Technologie erwartet. Die Veranstaltung richtet sich sowohl an ICT-Fachkräfte als auch an Unternehmer, Führungskräfte und KMU-Entscheidungsträger, die sich mit digitalen Entwicklungen und deren Auswirkungen auf ihre Organisation beschäftigen.

Auszeichnung Digital Shaper Ostschweiz

Ein fester Bestandteil der Konferenz ist die Verleihung des Digital Shaper Ostschweiz. Die Auszeichnung würdigt Persönlichkeiten, die die digitale Entwicklung der Region prägen. Die Ehrung gilt inzwischen als wichtiger Gradmesser für Trends und Innovationen innerhalb der Ostschweizer Digitalwirtschaft.

Ostschweizer Plattform für digitale Zukunftsthemen

Organisiert wird die Digital Conference Ostschweiz von <IT>rockt!, LEADER und east#digital. Unternehmen, Start-ups, Forschungseinrichtungen und Institutionen kommen dabei gezielt miteinander ins Gespräch.

Damit spiegelt die Veranstaltung die zunehmende Bedeutung digitaler Technologien für die Region wider. Die Ostschweiz positioniert sich immer stärker als Standort für Innovation, Technologie und digitale Geschäftsmodelle. Die Digital Conference

verbindet dabei regionale Akteure mit internationalen Entwicklungen und Fragestellungen. Die Digital Conference Ostschweiz 2026 ist mehr als ein klassisches Branchentreffen. Sie zeigt, wie eng KI, Cybersecurity und gesellschaftliche Entwicklungen inzwischen miteinander verknüpft sind und welche Herausforderungen daraus für Unternehmen und Institutionen entstehen.

Text: Patrick Stämpfli Bilder: zVg

JETZT TICKET SICHERN

Die Digital Conference Ostschweiz 2026 findet am 8. September 2026 im Einstein Congress in St.Gallen statt. Freuen dürfen sich die Teilnehmer auf hochkarätige Keynotes, praxisnahe Breakout-Sessions, Networking und aktuelle Einblicke in die Themen KI, Cybersecurity und digitale Transformation.

Tickets können ab sofort über den QR-Code bestellt werden.



Weitere Informationen zum Programm, zu den Referenten sowie zum Ticketverkauf finden Sie unter: www.digitalconference.ch

Henriette Engbersen:
KI verschärft
Desinformation.



«Vertrauen ist das höchste Gut der Medien»

Desinformation entwickelt sich zunehmend zu einem Risiko für Wirtschaft, Politik und Gesellschaft. Henriette Engbersen, ehemalige SRF-Korrespondentin in London und heute verantwortlich für das Thema «Public Value» bei der SRG, erklärt, weshalb KI die Problematik verschärft, warum Nachrichtenkompetenz wichtiger denn je ist und welche Verantwortung Medien heute tragen.

Henriette Engbersen, Sie haben als SRF-Korrespondentin in London den Brexit aus nächster Nähe begleitet. Welche Parallelen sehen Sie heute zwischen den damaligen Informationskämpfen und der aktuellen Entwicklung rund um KI und Desinformation?

Nach der Brexit-Abstimmung im Jahr 2016 habe ich beobachtet, wie die Debatte darüber lanciert wurde, ob Desinformation auch in demokratischen Staaten politische Entscheidungen beeinflussen kann. Heute, zehn Jahre später, geht es nicht mehr um die Frage, ob das der Fall ist. Ein europäisches Beratungsunternehmen hat kürzlich berechnet, dass die Kosten von Desinformation für die Weltwirtschaft über 400 Milliarden US-Dollar betragen. Die Brisanz der Thematik hat sich durch KI in den

letzten Jahren deutlich verschärft. Ich beobachte nicht mehr nur, sondern befasse mich beruflich mit der Thematik und der zunehmenden Bedeutung von journalistischen Medienhäusern in diesem Umfeld.

Sie sind bei der SRG für das Thema «Public Value» zuständig und sind im Vorstand von «UseTheNews Schweiz». Sie beschäftigen sich mit der Erkennung von Desinformation. Wo stehen wir aktuell in der Schweiz bei diesem Thema – technologisch und gesellschaftlich?

Wir schneiden nicht gut ab. Beim Erkennen von Fake News liegt die Schweizer Bevölkerung laut einer Studie von Politoools unter dem Durchschnitt. Zudem gibt fast die Hälfte der Bevölkerung an, kaum noch Nachrichten zu konsumieren. Das ist eine problematische Tendenz für die demokratische Meinungsbildung. Wer auf Fake News hereinfällt und weniger Nachrichten konsumiert, misstraut auch öffentlichen Institutionen und politischen Entscheidungsprozessen eher. Als SRG haben wir den Auftrag zur Meinungsbildung beizutragen. Deshalb engagieren wir uns für Projekte rund um Nachrichtenkompetenz, mitunter zusammen mit Keystone-SDA und dem Schweizer Verlegerverband im Verein «UseTheNews».

KI ermöglicht es heute, Inhalte in hoher Qualität zu manipulieren oder komplett neu zu generieren. Wird die Unterscheidung zwischen wahr und falsch zur zentralen Kompetenz der Zukunft?

Die Nachrichtenkompetenz ist nicht neu, aber sie ist dringlicher geworden. Viele Länder haben das erkannt. Finnland hat etwa vor einigen Jahren den gesamten Schullehrplan umgestellt, um die Nachrichtenkompetenz auf allen Stufen zu stärken. In der Schweiz gibt es ebenfalls spannende Projekte. Etwa im Kanton Bern: Dort haben wir mit UseTheNews und anderen Partnern erstmals einen «Erste-Hilfe-Kurs» in Nachrichtenkompetenz für Jungbürger lanciert. Bei der SRG konnte ich zum Thema «Fake News» einen Schulzug mit der SBB sowie eine Ausstellung im Verkehrshaus als Projektleiterin betreuen. Weitere Projekte sind geplant, denn das Interesse ist hoch.

Welche Bedeutung hat verlässliche Information für das Funktionieren von Wirtschaft und Gesellschaft im Zeitalter von KI und Desinformation?

Desinformation ist mehr als ein digitales Problem, es kann die Grundlage untergraben, auf welcher wirtschaftliche Entscheidungen basieren. Deshalb stuft das World Economic Forum (WEF) das Thema Desinformation als eines der grössten globalen Stabilitätsrisiken ein. Vor einigen Mona-

ten haben international renommierte Ökonomen zudem dazu aufgerufen, verlässliche Information als fundamentalen Input für Wirtschaftswachstum, Regierungstätigkeit und gesellschaftliches Vertrauen zu verstehen. Für mich wiederum zentral, ebendiese Wirtschaftsexperten betonen, dass die Aufgabe von journalistischen Medienhäusern für eine stabile Wirtschaft in Zeiten von Desinformation wichtiger werden. Über diesen Konnex zwischen starken journalistischen Medien und einer stabilen Wirtschaft sollten wir vermehrt sprechen.

«Die Nachrichtenkompetenz ist nicht neu, aber sie ist dringlicher geworden.»

Welche Rolle sollten Medienhäuser heute im Umgang mit KI und Desinformation einnehmen – gerade auch im Spannungsfeld zwischen Geschwindigkeit und Verlässlichkeit?

Ich glaube, Medienhäuser haben heute eine doppelte Pflicht. Die Überprüfung von Fakten hat an Bedeutung gewonnen und gleichzeitig müssen wir das Vertrauen in die Medien hochhalten. Die Schweizer Medienbranche hat kürzlich mit ihrem gemeinsamen KI-Kodex ein Signal gesetzt: Vertrauen ist das höchste Gut der Medien – und KI darf dieses Vertrauen nicht untergraben, sondern muss transparent eingesetzt werden.

Es geht aber auch um eine aktive Rolle etwa im digitalen Raum, denn aus internationalen Studien ist bekannt, dass die Resilienz gegen Desinformation und Polarisierung in jenen Ländern höher ist, wo journalistische Medien, insbesondere auch öffentlich-rechtliche Medien stark sind und eine hohe Reichweite haben.

Mit Blick auf Ihre Keynote an der Digital Conference Ostschweiz: Welche zentrale Erkenntnis sollen die Teilnehmer aus Ihrem Vortrag mitnehmen?

Von der Hexenverfolgung über die dunklen Seiten des Radios bis hin zur künstlichen Intelligenz: Jede Kommunikationsrevolution hat neue Formen der Desinformation hervorgebracht. Die gute Nachricht ist, dass Gesellschaften immer Wege gefunden haben, damit umzugehen. Welche Lehren wir daraus für den Umgang mit KI ziehen können und welche konkreten Ansätze sich daraus auch für Unternehmen ergeben, darum geht es in meinem Vortrag.

Text: Patrick Stämpfli Bild: zVg

«Cybersecurity ist ein Führungsthema»

Sylvain Luiset zeigt an der Digital Conference Ostschweiz, wie Unternehmen Cyberrisiken strategisch steuern. Im Interview erklärt der Cyber-Resilience-Experte von Zurich Insurance, warum KMU besonders betroffen sind und wie sich Sicherheit zum Wettbewerbsvorteil entwickeln kann.

Sylvain Luiset, viele Unternehmen sehen Cybersecurity noch immer als reines IT-Thema. Wo liegt der Denkfehler?

Cybersecurity war lange stark mit technischen Fragen und Schwachstellen verbunden. In den letzten Jahren hat sie sich jedoch zu einem strategischen Thema entwickelt. Heute stehen Resilienz, Business Continuity und gezielte Investitionen in Schutzmassnahmen im Zentrum. Entscheidend ist, dass Organisationen diese Entwicklung erkennen und verstehen, dass Cybersecurity längst kein reines IT-Thema mehr ist.

«Cyberrisiken müssen als finanzielle Auswirkungen verständlich gemacht werden.»

Sie sprechen davon, Cyberrisiken «greifbar» zu machen. Was bedeutet das für KMU?

Viele KMU und Industrieunternehmen gehen davon aus, dass sie kein Ziel von Cyberangriffen seien und dass sich Cyberkriminelle eher auf Grossbanken oder internationale Konzerne konzentrierten. Das ist ein Irrtum! Die häufigste Angriffsform in der Schweiz, Ransomware, ist opportunistisch und wird in grossem Stil branchenübergreifend eingesetzt. Man muss also kein gezieltes Angriffsziel sein, um Opfer zu werden. Unsere Daten zeigen zudem, dass die meisten Ransomware-Opfer kleinere Organisationen sind; die Ostschweiz bildet dabei keine Ausnahme.

Risikoquantifizierung ist ein zentraler Teil Ihrer Arbeit. Wie bringt man ein abstraktes Cyberrisiko

auf eine Ebene, die für Geschäftsleitungen entscheidungsrelevant ist?

Cybersecurity ist heute ein strategisches Thema, deshalb müssen Risiken auch in einer Sprache dargestellt werden, die für die Geschäftsleitung verständlich ist. Wenn Cyberrisiken als potenzielle finanzielle Auswirkungen statt im technischen Fachjargon kommuniziert werden, können Entscheidungsträger fundierter entscheiden und Investitionen gezielt priorisieren. Ein wichtiger Teil unserer Arbeit sind das Verständnis des Geschäftsmodells und der Prozesse eines Unternehmens. Nur so lassen sich pragmatische und kosteneffiziente Lösungen entwickeln.

Unternehmen investieren zunehmend in Sicherheit, oft ohne klare Prioritäten. Wo sehen Sie die grössten Probleme?

Die Verbesserung der Cyber-Reife ist grundsätzlich nie falsch. Entscheidend ist die Priorisierung: Massnahmen müssen zum Reifegrad, zum Geschäftsmodell und zu den konkreten Risiken passen. Gerade bei KMU lässt sich die Cyber-Reife oft bereits mit wenigen gezielten Projekten deutlich erhöhen. Dazu gehören häufig Themen wie Monitoring und Incident Response, eine robuste Backup-Strategie sowie die Absicherung von Benutzerkonten. Ein strukturiertes Cyber-Assessment ist oft ein sinnvoller Ausgangspunkt.

Der Begriff «Cyber Resilience» wird häufig verwendet. Was unterscheidet resiliente Unternehmen denn von anderen?

Resiliente Organisationen kennen ihre Risiken, sind vorbereitet und können sich von Störungen oder Angriffen erholen. Wichtig ist ein klares Verständnis dafür, welche Ereignisse den Betrieb tatsächlich beeinträchtigen können. Das können nicht nur externe Angriffe sein, sondern auch interne Fehler, etwa durch einen privilegierten IT-Administrator. Entscheidend ist zudem, dass Prozesse nicht nur definiert, sondern auch regelmässig getestet werden. Ein Unternehmen mit Backups, das die Wiederherstellung nie geübt hat, wird im Ernstfall deutlich länger ausfallen als eines,



Sylvain Luiset:
Risiken strategisch steuern.

das diese Abläufe regelmässig überprüft. Cyber Resilience ist damit eine echte strategische Stärke.

Sie arbeiten an der Schnittstelle zwischen Technik und Business. Wo entstehen Reibungsverluste?

Die beiden sprechen oft unterschiedliche Sprachen, sei es technischer oder finanzieller Natur. Das führt dazu, dass beide Seiten in ihren Denkmustern bleiben und zu wenig miteinander interagieren. Dabei verfolgen sie letztlich dasselbe Ziel: den Geschäftsbetrieb zu sichern und Risiken zu beherrschen. Ein wichtiger Teil meiner Arbeit besteht darin, diese beiden Welten zusammenzubringen und technische Risiken in verständliche, umsetzbare und strategische Projekte zu übersetzen.

Cybersecurity wird oft als Kostenfaktor wahrgenommen. Wie wird sie tatsächlich zum Business-Enabler?

Es ist ein verbreitetes Missverständnis, dass Cybersecurity zwangsläufig teuer und aufwendig sein muss. Mit einer klaren Priorisierung entlang der tatsächlichen Geschäftsrisiken lassen sich viele Verbesserungen kosteneffizient umsetzen. Gleichzeitig sehen wir zunehmend, dass Unter-

nehmen mit konkreten Anforderungen ihrer Kunden im Bereich Cybersecurity konfrontiert sind. Wer diese nicht erfüllt, kann Wachstumspotenziale verlieren. In diesem Kontext wird Cybersecurity zu einem Wettbewerbsvorteil und damit zu einem echten Business-Enabler.

Was sollten die Teilnehmer der Digital Conference Ostschweiz nach Ihrer Keynote anders machen als zuvor?

Ich hoffe, dass Cybersecurity nicht mehr als trockenes, rein technisches Thema wahrgenommen wird, sondern als relevantes Führungs- und Geschäftsthema. Wichtig ist, Cyberrisiken und Cyber Resilience aktiv in strategische Diskussionen einzubringen, sowohl intern im Management als auch im Austausch mit Kunden und Partnern. Ein erster Schritt ist, sich mit den eigenen Risiken auseinanderzusetzen und zu verstehen, welche Szenarien den Geschäftsbetrieb tatsächlich bedrohen. Das schafft die Grundlage für fundierte Entscheidungen und wirksame Resilienz.

Text: Patrick Stämpfli Bild: zVg



**Jetzt mitmachen
beim
KI-Kompetenz Cluster
Ostschweiz
www.eastki.ch**



<IT>rockt!



Wer wird «Digital Shaper Ostschweiz 2026»?

Ab dem 1. Juli beginnt die zweite Runde der Wahl zum «Digital Shaper Ostschweiz 2026». Entscheiden Sie, wer den begehrten Titel erhalten soll.

Bereits zum vierten Mal macht sich der Digital Hub east#digital mit der Wahl zum «Digital Shaper Ostschweiz» auf die Suche nach den Ostschweizer Wegbereitern der digitalen Zukunft. Der Titel ist mehr als eine blosser Auszeichnung. Er zeigt, wie Einzelpersonen, Teams und Unternehmen aus unserer Region mit Innovationskraft und viel Engagement die digitale Transformation vorantreiben.

Noch bis Ende Juni können die Leser von east#digital und dem LEADER in der ersten Abstimmungsrunde aus über 50 Ostschweizer Persönlichkeiten bzw. Teams auswählen, die im vergangenen Jahr durch besondere Leistungen oder Erfolge aufgefallen sind.

Bis Redaktionsschluss erhielten folgende Personen bislang die meisten Stimmen (in alphabetischer Reihenfolge):

- **Adrian Eichrodt**, CEO, Verwaltungsrat und Partner Geoinfo
- **Enes & Bajram Emini**, Gründer, Meeting Metrics
- **Denis Forster**, Ausbildungsverantwortlicher Informatikberufe Bühler AG

- **Claudio Hintermann**, Co-CEO Abacus Research AG
- **Daniel Kara & Igor Mamuzic**, CEO & CIO Nägele Capaul AG
- **Erdin Kamoglu**, Leiter Jugendrotkreuz St.Gallen
- **Andy Kutter**, Partner & Direktor Kyos AG
- **Claudio Minder & Karl Müller**, Co-CEOs Kybun Joya
- **Christian Naef**, CEO und Co-Gründer RY3T
- **David Spoerle, Benjamin Vanzella, Lukas Naef, Lucas Roth & Michael Rey**, IDIP Solution AG

Die zweite Abstimmungsrunde beginnt am 1. Juli. In dieser kann bis am 31. August 2026 darüber abgestimmt werden, wer von den zehn Shortlist-Kandidaten «Digital Shaper Ostschweiz 2026» werden soll. Offiziell verliehen wird der Titel dann am 8. September 2026 an der Digital Conference Ostschweiz, die im Einstein Congress in St.Gallen stattfinden wird.

Text: Patrick Stämpfli Bild: zVg

Hier geht's zur
Abstimmung



«Ein Copilot antwortet. Ein Agent handelt»

Viele Unternehmen experimentieren mit ChatGPT oder Copilot. Der eigentliche Wandel beginnt laut Ishan Don aber erst jetzt. Im Gespräch erklärt der Gründer und Geschäftsführer der St.Galler Stack-Works AG, weshalb KI-Agents ganze Geschäftsprozesse übernehmen könnten und warum viele Firmen trotz Gen AI bisher kaum echten Nutzen sehen.

Ishan Don, ChatGPT und Copilot sind inzwischen in vielen Unternehmen angekommen. Weshalb sprechen Sie bei KI-Agents trotzdem von einer neuen Kategorie?

Kurz gesagt: Ein Copilot antwortet, ein Agent handelt. ChatGPT oder Copilot liefern Texte oder Code auf Anfrage. Der Mensch steuert weiterhin den Prozess. Ein Agent dagegen beobachtet Zustände, trifft Entscheidungen und führt selbstständig Aktionen aus, etwa im Postfach, im CRM oder im ERP-System. Damit verlassen wir die klassische Werkzeuglogik. Ein Agent schreibt nicht nur einen Vorschlag, sondern erledigt die Aufgabe.

Wo stehen Schweizer KMU beim Einsatz von KI aktuell?

Derzeit sehen wir zwei Arten von Unternehmen. Die einen haben ChatGPT, Gemini oder Copilot längst eingeführt und suchen nun den nächsten Schritt. Die anderen beobachten noch und warten ab. Gleichzeitig ist die Entwicklung brutal schnell. Dinge, die vor einem Jahr noch als Innovation galten, wirken heute teilweise bereits veraltet. 2026 dürfte aus meiner Sicht der eigentliche Wendepunkt werden: weg von «Menschen nutzen KI» hin zu «Prozesse nutzen KI».

«KI scheitert selten an der Technologie, sondern an Prozessen.»

Hinzu kommt ein weiterer Punkt: In vielen Firmen wird KI längst genutzt, oft ohne offizielle Freigabe. Genau diese Schattennutzung setzt Geschäfts-

leitungen derzeit unter Druck, das Thema endlich strukturiert anzugehen.

Welche Aufgaben übernehmen KI-Agents heute bereits konkret in Unternehmen?

Die Einsatzmöglichkeiten sind inzwischen sehr breit. Wir sehen Anwendungen bei der Offert-Erstellung, in der Buchhaltung oder im Bereich IT-Security. Besonders spannend finde ich derzeit den Einsatz im First-Level-Support.

Bei einem Schweizer Service-Unternehmen mit rund 100 Mitarbeitern übernimmt ein Agent heute die Mail-Triage, beantwortet Standardanfragen direkt, leitet komplexe Fälle ans richtige Team weiter und dokumentiert alles automatisch. Früher lag die Reaktionszeit bei zwei bis drei Stunden, heute bei unter einer Stunde. Das Team ist gleich gross geblieben, verbringt den Tag aber nicht mehr mit Mail-Triage, sondern kann sich wieder um komplexere Fälle kümmern.

Viele Unternehmen experimentieren mit Gen AI, sehen aber kaum echten Business-Impact. Weshalb?

Nach meiner Erfahrung gibt es dafür meistens drei Gründe. Erstens fehlt ein klarer Prozess. Viele Unternehmen führen KI-Tools ein, ohne sauber zu definieren, welches Problem sie eigentlich lösen wollen. Zweitens fehlt oft ein brauchbares Datengrundfundament. Wenn Daten chaotisch abgelegt oder unvollständig sind, kann auch KI keinen stabilen Mehrwert liefern.

Und drittens werden viele Projekte rein technisch gedacht. KI scheitert aber selten an der Technologie, sondern fast immer an Prozessen und Zuständigkeiten.

Welche Risiken oder Herausforderungen werden beim Einsatz von KI-Agents derzeit unterschätzt?

Viele Unternehmen bauen derzeit Agents, ohne sauber zu definieren, was diese überhaupt dürfen. Genau dort beginnt das Risiko, denn oft ist völlig unklar, welche Aktionen ein Agent eigenständig auslösen darf und in wessen Namen er handelt.



Ishan Don:
Agenten übernehmen
Prozesse.

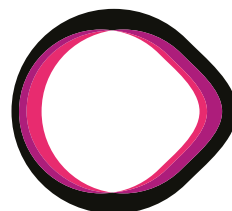


IMMER WEITER IN INFORMATIK.

Online-
Infoanlass:
9. September
ab 17 Uhr



Erfahre, wie dich unsere
30 Weiterbildungen
im Bereich Informatik
weiterbringen.
WO WISSEN WIRKT.



OST

Ostschweizer
Fachhochschule

Auch Datenschutz und Datenklassifikation werden häufig unterschätzt. Ein Agent kann nicht selbst erkennen, welche Informationen sensibel sind. Dazu kommt die Auditierbarkeit. Wenn ein Agent Bestellungen freigibt oder Tickets schliesst, muss jeder Schritt nachvollziehbar bleiben. In vielen Fällen braucht es deshalb weiterhin einen «Human in the Loop», also einen Menschen, der bewusst eingebunden bleibt.

Sie sagen, KI-Agents könnten 2026 zur Trennlinie zwischen schnellen und langsamen Unternehmen werden. Woran wird sich das konkret zeigen?

Sehr direkt im Alltag. Unternehmen, die Offerten in Stunden statt in Tagen erstellen, gewinnen schneller Aufträge. Wer den Support effizienter organisiert, ohne ständig zusätzliches Personal aufzubauen, hält die Marge stabil. Und wer Ideen oder Hypothesen innerhalb weniger Stunden testen kann, lernt schneller als der Wettbewerb. KI entscheidet dadurch zunehmend darüber, wie schnell und effizient Unternehmen arbeiten.

«Viele Unternehmen bauen Agents ohne klare Spielregeln.»

Was sollten Geschäftsführer heute konkret tun, wenn sie das Thema sinnvoll angehen wollen?

Zuerst muss KI zur Chefsache werden. Es braucht eine verantwortliche Person mit Mandat, Budget und Zeit. Das Thema einfach an die IT abzuschieben, funktioniert aus meiner Sicht nicht. Viele IT-Abteilungen denken primär in Systemen und Tools. Bei KI geht es aber zuerst um Prozesse. Zweitens sollten Unternehmen mit zwei oder drei konkreten Anwendungsfällen starten, bei denen heute Zeit oder Marge verloren geht, etwa bei Offerten, Support oder Buchhaltung. Dort lassen sich erste Projekte gezielt testen und Erfahrungen sammeln. Ohne klare Berechtigungen, eine aufgeräumte Datenbasis und nachvollziehbare Prozesse wird keine KI-Lösung langfristig skalieren können.

Text: Patrick Stämpfli Bild: Marlies Beeler-Thurnheer



**Ihre Zukunft
Ihr Projekt
Ihr Raum**



Hier finden Sie:

- Büroräume & Labore
- Co-Working Plätze
- Event- & Sitzungs-räume



Mehr dazu:



Presentingpartner

K Y O S

Digital Conference Ostschweiz

Zum Thema: Cybersecurity trifft KI –
Risiko oder Chance?

Di, 08. September 2026

Einstein Congress, St.Gallen

Richard David Precht
Philosoph



Jill Wick
Wirtschaftspsychologin



Anna-Lena Horlemann
Professorin



Henriette Engbersen
Fernsehjournalistin



Tickets ab Ende Mai erhältlich

www.digitalconference.ch

Organisation

<IT>rockt!

LEADER

east#digital