Platinsponsor

KYOS

Goldsponsor

st.gallen

www.leaderdigital
www.digitalconference.ch
August 2025 | CHF 5

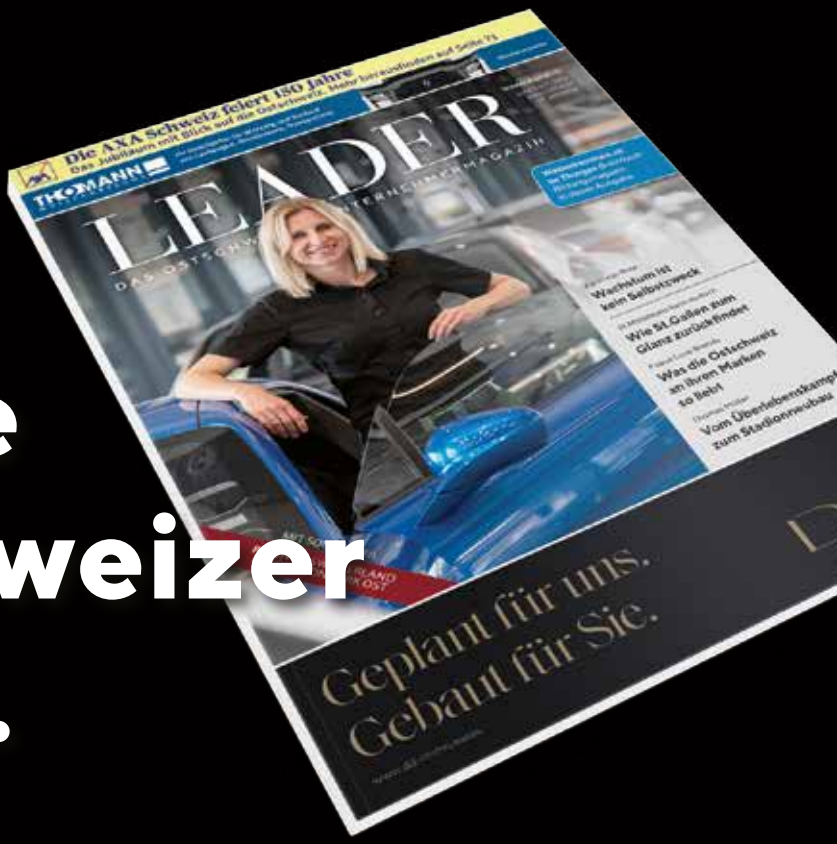
Digital Conference Ostschweiz

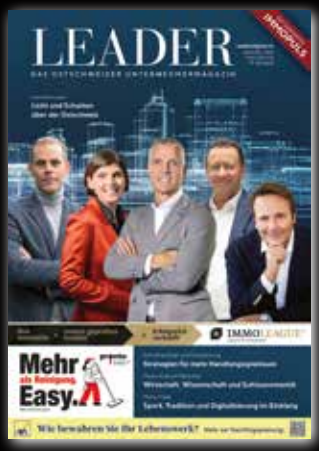
Die LEADER-Sonderausgabe zum Event am 26. September 2025 im Einstein Congress, St.Gallen

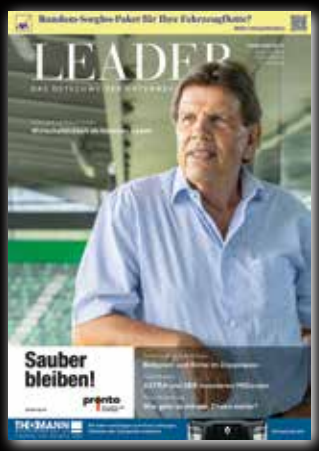
Organisation

<IT>rockt! LEADER east#digital

Die Stimme der Ostschweizer Wirtschaft.







www.leaderdigital.ch

Digitalisierung braucht Resilienz – willkommen zur Digital Conference Ostschweiz 2025

Die Digital Conference Ostschweiz geht in die dritte Runde – und ich freue mich, dass LEADER, east#digital und <IT>rockt! auch 2025 wieder gemeinsam die führende Digitalkonferenz unserer Region veranstalten. Die wachsende Teilnehmerzahl zeigt, wie wichtig Orientierung in der digitalen Transformation bleibt und wie gross das Interesse an einem Austausch auf Augenhöhe ist.

Dieses Jahr steht das Thema Cyber Resilience im Fokus. Die Digitalisierung eröffnet enorme Chancen, macht Organisationen aber auch verletzlich. Resilienz heisst, Risiken zu erkennen, ihnen vorzubeugen und dennoch innovativ zu bleiben. Genau hier setzt die DCONO an: Sie bietet Ihnen eine kompakte Plattform, um die neusten Trends und konkrete Ansätze kennenzulernen, Fachwissen zu vertiefen und praxisnahe Lösungen zu entdecken.

Ein Höhepunkt sind die hochkarätigen Keynotes, die aktuelle Perspektiven aufzeigen, sowie die Breakout-Sessions, die Raum für Diskussion und vertiefte Einblicke bieten. Nutzen Sie die Gelegenheit, mit Expertinnen und Experten ins Gespräch zu kommen, Ihr Netzwerk zu erweitern und die Zukunft Ihres Unternehmens aktiv zu gestalten.

Mein Dank gilt allen Partnern und Sponsoren, die dieses Programm möglich machen. Ich wünsche Ihnen eine inspirierende Lektüre des Vorschau-Specials und freue mich darauf, Sie am 26. September im Einstein Congress St.Gallen persönlich zu begrüssen.

Natal Schnetzer, Verleger LEADER / Inhaber MetroComm AG

Die Organisatoren der Digital Conference Ostschweiz: Eva De Salvatore (<IT>rockt!), Natal Schnetzer (MetroComm AG).

Mit diesem Vorschau-Special möchten wir Ihnen einen ersten Einblick in die Digital Conference Ostschweiz geben und Sie für die wichtigsten Themen der Digitalisierung sensibilisieren. Künstliche Intelligenz, vernetzte Systeme und neue Technologien verändern Wirtschaft und Gesellschaft grundlegend. Gleichzeitig wächst die Abhängigkeit von digitalen Infrastrukturen – Resilienz wird zur entscheidenden Fähigkeit.

Die DCONO bringt Fachleute, Innovatoren und Entscheidungsträger zusammen, um gemeinsam über die Chancen und Herausforderungen der digitalen Zukunft zu diskutieren. Mit hochkarätigen Keynotes und praxisorientierten Breakout-Sessions beleuchten wir aktuelle Entwicklungen und zeigen konkrete Ansätze für Unternehmen und die Region auf. Nutzen Sie die Möglichkeit, Wissen zu teilen, neue Kontakte zu knüpfen und die Innovationskraft der Ostschweiz weiter zu stärken.

Unsere Region zählt zu den bedeutendsten IT-Standorten der Schweiz. Mit der DCONO wollen wir dazu beitragen, diese Stärke weiter auszubauen und gemeinsam zukunftsfähige Lösungen zu entwickeln.

Ich wünsche Ihnen eine spannende Lektüre und freue mich, Sie am 26. September im Einstein Congress St.Gallen persönlich zu begrüssen.

Eva De Salvatore, Geschäftsführerin Verein IT St.Gallen (<IT>rockt!)

Sponsoren und Partner

Platinsponsor

KYOS

Goldsponsor

st.gallen

Silbersponsor

CONTENTHOUSE

Partner

OST Ostschweizer Fachhochschule

Kanton St.Gallen Amt für Wirtschaft und Arbeit

SWITZERLAND INNOVATION PARK OST

Netzwerkpartner

GEWERBE THURGAU

Wirtschaft Region St.Gallen

gewerbe st.gallen

START NetzwerkThurgau

wpo Wirtschafts Portal Ost Lebens- und Arbeitsregion Wil

IHK Industrie- und Handelskammer Thurgau

Award-Sponsor

BVS St Gallen

Hostpartner

EINSTEIN ST. GALLEN

Anfahrt, Programm und Tickets

Adresse
Einstein Congress
Wassergasse 3
9000 St.Gallen

Programm
Hier finden Sie das detaillierte Programm >>

Anfahrt mit öffentlichen Verkehrsmitteln
Ab HB St.Gallen: Bus Nr. 11 (Richtung Abacus-Platz) bis «St.Gallen, Einstein»

Anfahrt mit dem Auto / Einstein Parking
Adresse für Navigationssystem: Wassergasse 7, 9000 St.Gallen
Unseren Gästen stehen 245 Parkplätze zur Verfügung.

Tickets
Tickets kosten CHF 350 pro Person. Die Anzahl Plätze ist beschränkt ist, eine rasche Anmeldung lohnt sich. >>

«Resilienz heisst: Vorbereitet sein, nicht unverwundbar.»

Dr. Benedikt van Spyk
Staatssekretär
Kanton St.Gallen

Die digitale Transformation eröffnet enorme Chancen – für Innovation, Effizienz und neue Formen der Zusammenarbeit. Doch sie bringt auch neue Risiken mit sich. Cyberangriffe betreffen längst nicht mehr nur globale Konzerne oder kritische Infrastrukturen. Auch Verwaltungen, Schulen und Spitäler geraten zunehmend ins Visier. Cyberresilienz ist deshalb weder ein rein technisches Thema noch eines, das sich einfach delegieren lässt. Sie ist eine strategische Grundvoraussetzung für das Vertrauen in den digitalen Staat und das stabile Funktionieren unserer Gesellschaft.

Resilienz entsteht durch Zusammenarbeit, gegenseitiges Vertrauen und kontinuierliches Lernen. Kein Unternehmen, keine Behörde kann dies allein leisten. Cyberresilienz ist eine gemeinsame Aufgabe. Sie erfordert eine enge und systematische Kooperation zwischen Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft – lokal, regional, national.

Die Ostschweiz bringt dafür gute Voraussetzungen mit: kurze Wege, starke Akteure, eine gewachsene Vertrauenskultur – und zahlreiche bestehende Kooperationsformen, auf denen wir aufbauen können: Der Schutz vor Cyberrisiken ist Teil der Schwerpunktplanung der Regierung des Kantons St.Gallen. Die Weiterbildung Cyber Security für Führungskräfte (CSF-HSG) bietet die Möglichkeit, das strategische Bewusstsein für dieses Thema zu verankern. Die gemeinsame Beschaffung von SIEM/SOC-Dienstleistungen durch die Ostschweizer Kantone schafft einheitliche operative Grundlagen. Formate wie die CyberSecurity Days Ostschweiz oder die Erfa-Gruppe Cyber Security von <IT>rockt! fördern den persönlichen und fachlichen Austausch.

Die verschiedenen Initiativen verlaufen jedoch oft parallel und Synergien werden noch zu wenig genutzt. Was es daher braucht, ist eine langfristige strategische Zusammenarbeit der relevanten Akteure im ICT-Bereich in der Ostschweiz. Die Digital Conference Ostschweiz bietet eine gute Gelegenheit, eine solche Koordination über Sektor- und Kantonsgrenzen hinweg anzustossen.

Ich wünsche Ihnen eine inspirierende Veranstaltung und gute Gespräche. <

Impressum

Magazin LEADER, MetroComm AG, Bahnhofstrasse 8, 9000 St.Gallen, T 071 272 80 50, F 071 272 80 51, leader@metrocomm.ch, www.leaderdigital.ch
Verleger: Natal Schnetzer | **Chefredaktor:** Stephan Ziegler, Dr. phil. I, sziegler@metrocomm.ch | **Autoren:** Patrick Stämpfli, Stephan Ziegler | **Fotografie:** Marlies Beeler-Thurnheer, zVg | **Gestaltung:** Doris Hollenstein, dhollenstein@metrocomm.ch | **Herausgeberin, Redaktion und Verlag:** MetroComm AG, Bahnhofstrasse 8, 9000 St.Gallen, T 071 272 80 50, F 071 272 80 51, www.leaderdigital.ch, www.metrocomm.ch, leader@metrocomm.ch | **Geschäftsleitung:** Natal Schnetzer, nschnetzer@metrocomm.ch | **Verlags- und Anzeigenleitung:** Oliver Iten, oiten@metrocomm.ch | **Marketingservice, Aboverwaltung:** Fabienne Schnetzer, info@metrocomm.ch | **Abopreis:** CHF 61.50 für 18 Ausgaben | **Erscheinung:** Der LEADER erscheint 9 x jährlich mit Ausgaben Januar/Februar, März, April, Mai, Juni/Juli, August, September, Oktober, November/Dezember, zusätzlich 9 Special-Ausgaben | **Produktion:** Ostschweiz Druck AG, 9300 Wittenbach. Die mit «Profil» gekennzeichneten Beiträge sind Sponsored Content.

ISSN 1660-2757

Cyber Resilience wird zur Pflicht

Die Digital Conference Ostschweiz 2025 stellt die Frage nach digitaler Handlungsfähigkeit in Krisenzeiten ins Zentrum. Bereits zum dritten Mal versammelt sich die Branche in St.Gallen, um konkrete Lösungen für Unternehmen, Behörden und Institutionen zu diskutieren.

Auch 2025 wird St.Gallen wieder zum digitalen Brennpunkt der Schweiz. Die Konferenz im Einstein Congress bringt am 26. September führende Köpfe aus Wirtschaft, Verwaltung, Forschung und IT zusammen. Veranstaltet von <IT>rockt!, dem Unternehmermagazin LEADER und dem Netzwerk east#digital, steht die Praxisnähe im Vordergrund: Statt abstrakter Visionen geht es um reale Bedrohungen, bewährte Ansätze und konkrete Massnahmen. Thematischer Schwerpunkt ist diesmal Cyber Resilience – wie Organisationen auch in Ausnahmesituationen funktionsfähig bleiben.

«Die Digital Conference lebt von ihrer Praxisnähe und der Verankerung in der Region. Hier wird nicht über Digitalisierung geredet – hier wird sie konkret gestaltet», erklärt Natal Schnetzer, Verleger MetroComm und Herausgeber des LEADER.

Keynotes mit Relevanz

Das Tagesprogramm beginnt mit Katja Dörlemann von SWITCH. Sie spricht über Security Awareness als Schlüssel zur Resilienz – und darüber, warum der Mensch im Zentrum jeder Sicherheitsstrategie steht. Am Nachmittag folgt Marco Brenner von IBM Quantum Schweiz. Seine Keynote dreht sich um Verschlüsselungstechnologien der Zukunft – ein Thema, das durch KI und Quantencomputing enorm an Brisanz gewinnt. Den Abschluss macht Florian Schütz, Direktor des Bundesamts für Cybersicherheit (BACS). Er spricht über nationale Strategien und den konkreten Beitrag, den Unternehmen leisten müssen.

Vertiefung in Breakout-Sessions

Zwischen den Keynotes erhalten die Teilnehmer in sechs Breakout-Sessions Einblicke in die Realität moderner Cyberbedrohungen und resilienzorientierter Ansätze. Christina Vintila von Google thematisiert in ihrer englischen Session, wie sichere KI- und Cloud-Systeme gestaltet werden müssen – nicht nur technologisch, sondern auch organisatorisch und ethisch. Als Expertin für Kryptosysteme und Engineering Security vermittelt sie eine globale Perspektive auf lokale Herausforderungen.

Thomas Fröhlich, langjähriger Security Architect bei Inventx, richtet den Blick auf die Finanz- und Versicherungsbranche. Seine Erfahrung reicht von UNIX-Administration über ISO-Zertifizierungen bis zum Aufbau von SOCs – ideale Voraussetzungen, um über branchenspezifische Risiken und praktikable Massnahmen zu sprechen.

Angela Meier, Geschäftsführerin der Outvision GmbH zeigt, wie Resilienz in Unternehmen entsteht – durch gute Führung, klare Prozesse und gelebte Verantwortung. Michael Stahlberger (Leiter Departement IT, HOCH Health Ostschweiz) beleuchtet Cyber Resilience aus ganzheitlicher Sicht: Was geschieht vor, während und nach einem Angriff? Welche Rolle spielen Mensch, Technik und Kommunikation? Tobias Meier, CTO der MTF Solutions AG präsentiert die Chronik eines realen Cyberangriffs – ein seltener, offener Einblick in das Innenleben eines Incident-Response-Prozesses. Und KYOS-Direktor Andreas Kutter sensibilisiert für eine einfache, aber oft unterschätzte Wahrheit: Ein Klick kann teuer werden –

besonders für KMU. Er zeigt, wie sich auch kleinere Unternehmen sinnvoll schützen können.

Raum für Austausch

Die Konferenz ist bewusst als Tagesanlass konzipiert – kompakt, fokussiert, vernetzt. Es gibt keine Panels oder Workshops, sondern gezielte Inhalte mit hoher Relevanz. Der persönliche Austausch ist dennoch zentral. «Digitalisierung gelingt nicht im Alleingang. Sie braucht das Zusammenspiel unterschiedlicher Akteure – Wirtschaft, Verwaltung, Forschung und IT», sagt Eva De Salvatore, Geschäftsführerin von <IT>rockt!.

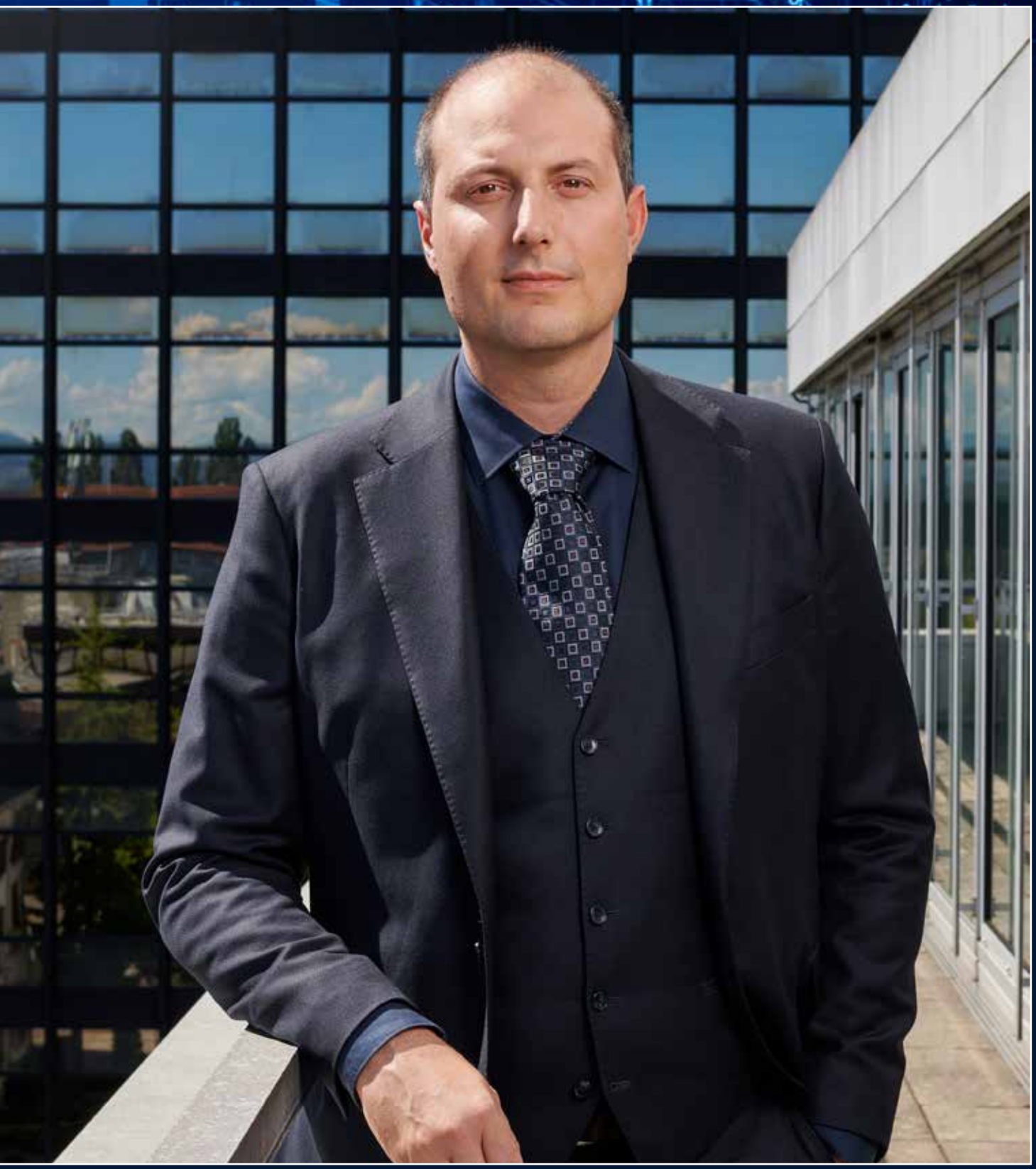
Moderiert wird der Anlass von SRF-Journalistin Bigna Silberschmidt. Zudem wird der «Digital Shaper Ostschweiz 2025» gekürt – eine Auszeichnung für Persönlichkeiten, die Digitalisierung in der Region voranbringen.

Jetzt anmelden

Die Digital Conference Ostschweiz 2025 steht für Substanz, regionale Verankerung und persönliche Begegnung. Der Einstein Congress bietet den passenden Rahmen – mit klaren Inhalten, spannenden Referenten und viel Raum für Gespräche.

Der Tag endet mit einem Apéro – die ideale Gelegenheit, Erkenntnisse zu vertiefen und neue Kooperationen anzustossen. <

Das vollständige Programm, Speaker-Infos und Anmeldung:
digitalconference.ch



«Cyberresilienz ist Chefsache – nicht nur ein IT-Thema»

Cyberangriffe bedrohen Wirtschaft, Staat und Gesellschaft gleichermassen. Florian Schütz, Direktor des Bundesamts für Cybersicherheit, erklärt, warum Cyberresilienz mehr als Technik ist, welche Fortschritte die Schweiz gemacht hat und was Organisationen jetzt tun müssen.

Florian Schütz, was bedeutet für Sie persönlich der Begriff «Cyber Resilience» – und wie unterscheidet er sich von klassischer IT-Sicherheit?
Cyberresilienz beschreibt die Fähigkeit einer Organisation, nach einer Beeinträchtigung ihrer digitalen Systeme möglichst rasch wieder geordnet arbeiten zu können. Dazu gehören sowohl technische als auch organisatorische Massnahmen: die Sensibilisierung der Mitarbeitenden, Notfallkonzepte, regelmässige Cyberübungen, um die Wirksamkeit der Massnahmen zu überprüfen und erkannte Lücken zu schliessen.

Worin liegt der Unterschied zur klassischen IT-Sicherheit?
Während klassische IT-Sicherheit vor allem auf Prävention abzielt – also darauf, Angriffe zu verhindern –, geht es bei der Cyberresilienz darum, vorbereitet zu sein, im Ernstfall schnell reagieren und sich rasch erholen zu können. Idealerweise wird eine Beeinträchtigung ganz vermieden, aber man muss immer auch den Ernstfall einkalkulieren.

Heisst das, Resilienz setzt immer auch beim Menschen an?
Ja, denn Technik allein reicht nicht. Viele Cyberangriffe beginnen mit einem menschlichen Fehler: Ein unachtsam geöffneter E-Mail-Anhang oder ein Klick auf einen Phishing-Link können schwerwiegende Folgen haben. Zwar lassen sich Schäden oft mit technischen Mitteln eindämmen, besser ist es aber, wenn es gar nicht erst so weit kommt. Sensibilisierung, klare Prozesse und regelmässige Übungen sind entscheidend, damit im Ernstfall jeder weiss, was zu tun ist.

Wo sehen Sie aktuell die grössten Schwachstellen bei der Cyberresilienz in der Schweiz?
Wir sehen durchaus Fortschritte, aber auch noch einige Schwächen. Veraltete IT-Systeme, fehlende Notfallpläne und zu wenig Schulungen sind nach wie vor häufig.

Gibt es Unterschiede zwischen grossen Unternehmen und kleineren Organisationen?
Ja, insbesondere KMU und Gemeinden sind oft nur teilweise auf Cyberangriffe vorbereitet, da dort meist das notwendige Wissen und die Ressourcen fehlen. Umso wichtiger sind einfache, praxisnahe Hilfestellungen und Sensibilisierungskampagnen.

Was sind die grössten Herausforderungen bei der Umsetzung der Nationalen Cyberstrategie (NCS)?
Die NCS verfolgt einen ganzheitlichen Ansatz mit fünf strategischen Zielen: Selbstbefähigung der Bevölkerung, Schutz kritischer Infrastrukturen, Sicherheit digitaler Dienstleistungen, Bekämpfung der Cyberkriminalität und internationale Zusammenarbeit. Die grösste Herausforderung bleibt die koordinierte Umsetzung mit Kantonen und Wirtschaftsverbänden.

> «Cyberangriffe machen nicht an Grenzen halt.»

Wo sehen Sie bislang die grössten Erfolge?
Es gibt konkrete Fortschritte: Die per 1. April 2025 eingeführte Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist ein wichtiger Meilenstein. Auch der Aufbau branchenspezifischer «Cyber Security Centres» (CSC) schreitet voran. Für den Finanzsektor gibt es den FS-CSC, für das Gesundheitswesen steht ein H-CSC kurz vor der Gründung, und auch im Bahnsektor sind die Vorbereitungen weit fortgeschritten. Diese CSC stärken die Resilienz in besonders exponierten Branchen erheblich.

Seit Anfang 2024 leiten Sie das neue Bundesamt für Cybersicherheit (BACS). Was hat sich dadurch gegenüber dem früheren NCSC verändert? >

Sankt Digital

Entdecke spannende Unternehmen und Jobs in St.Gallen.

meine-stadt.sg

> Das NCSC wurde per Januar 2024 in das BACS überführt. Als Bundesamt verfügen wir über eine klarere Struktur und eigene Ressourcen für Supportfunktionen wie HR und Controlling. Das gibt uns mehr Flexibilität bei der Planung und Priorisierung.

«Notfallkonzepte sind ein wichtiger Faktor der Cyberresilienz.»

Gab es auch inhaltliche Veränderungen?
Ja. Wir haben nicht nur die bisherigen Dienstleistungen übernommen, sondern deutlich ausgebaut. Dazu gehören die verstärkte internationale Zusammenarbeit, der Ausbau der Anlaufstelle für die Bevölkerung bei Cybervorfällen sowie die Plattform für den Informationsaustausch mit Betreibern kritischer Infrastrukturen. Wir haben eine gute Basis geschaffen, um die Leistungen zu skalieren und mit der zunehmenden Bedrohung im Cyberraum mitzuhalten.

Was bedeutet das konkret für Unternehmen?
Der direkte Informationsaustausch mit dem BACS gibt Unternehmen frühzeitig Hinweise auf aktuelle Bedrohungen, Schwachstellen und Angriffsmuster, sodass sie ihre Schutzmassnahmen gezielt anpassen können. Wir führen zudem Sensibilisierungskampagnen und unterstützen beim Aufbau von Notfallkonzepten. Wichtig ist uns auch eine Balance zwischen Regulierung und Anreizen. Schweizer Unternehmen, die international tätig sind, sollen nicht mit widersprüchlichen Anforderungen konfrontiert werden.

Welche Rolle spielt dabei die internationale Zusammenarbeit?
Eine sehr zentrale. Cyberangriffe machen nicht an Grenzen halt. Als Vorsitzender der OECD-Arbeitsgruppe «Security in Digital Economy» arbeite ich mit anderen Staaten an politischen Analysen und Empfehlungen, um Vertrauen in die digitale Transformation zu schaffen. Ziel ist auch, regulatorische Rahmenbedingungen zu harmonisieren.

Welche Risiken für kritische Infrastrukturen sehen Sie aktuell als besonders relevant?
Ein längerer andauernder Ausfall beispielsweise der Stromversorgung hätte weitreichende Folgen für viele andere Sektoren. Deshalb unterstützen wir die Betreiber kritischer Infrastrukturen intensiv beim Schutz vor Cyberbedrohungen, bieten mit dem Cyber Security Hub eine Plattform für den vertrauensvollen Austausch über aktuelle Bedrohungen und leisten im Ernstfall technische und operative Unterstützung.

Wie wichtig ist es, den Faktor Mensch zu adressieren?
Sehr wichtig. Viele Angriffe beginnen mit einem Klick. Deshalb führen wir regelmässig Sensibilisierungskampagnen und Pilotprojekte durch. Ein Beispiel ist das Projekt mit der Planzer Transport AG. Ziel war es, Unternehmen konkrete Hilfsmittel an die Hand zu geben, um ihre Resilienz entlang der Lieferkette zu stärken. Neben der technischen Absicherung haben wir dabei auch die Krisenkommunikation thematisiert – ein oft unterschätzter Faktor.

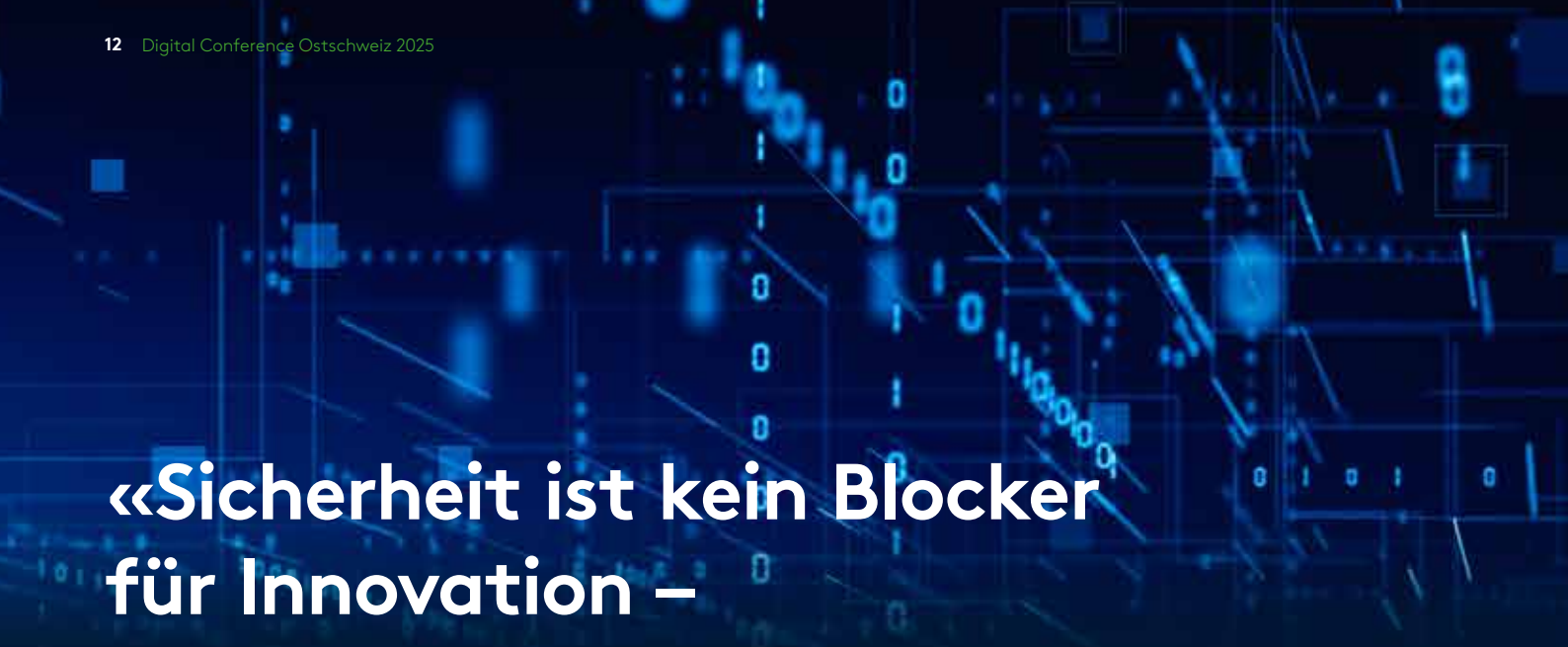
«Cyber gehört ins Risikomanagement.»

Was erwarten Sie sich von der Digital Conference Ostschweiz – und was wollen Sie mit Ihrer Keynote vermitteln?
Ich erwarte praxisnahe Einblicke und einen intensiven Austausch mit den Teilnehmenden und Referierenden. In meiner Keynote möchte ich zeigen: Jeder kann und muss zur Cyberresilienz beitragen. Es geht nicht darum, Angst zu schüren, sondern Verantwortung zu übernehmen.

Und was raten Sie Organisationen, um morgen resilient zu sein?
Cyber gehört ins Risikomanagement. Eine fundierte Business Impact Analyse hilft zu entscheiden, wo Investitionen notwendig sind und welche Risiken man bewusst trägt. Diese Entscheidungen müssen von der Geschäftsleitung getroffen und vom Verwaltungsrat mitgetragen werden. Cyberresilienz ist Chefsache – nicht nur ein IT-Thema. <


Bild: BACS

Florian Schütz ist seit 2024 Direktor des Bundesamtes für Cybersicherheit (BACS) und damit direkt dem Departementsvorsteher des VBS unterstellt. Er ist Ansprechperson für Politik, Medien und Bevölkerung zu Fragen der Cybersicherheit und verantwortlich für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS). Schütz verfügt über einen Master in Computerwissenschaft sowie einen Master of Advanced Studies in Sicherheitspolitik und Krisenmanagement der ETH Zürich.



«Sicherheit ist kein Blocker für Innovation – sondern ihr Motor»

Cristina Vintila von Google Cloud erklärt im Interview, wie Unternehmen Cyber Resilience in KI-gestützten Cloud-Umgebungen umsetzen können, warum Sicherheit von Anfang an mitgedacht werden muss und was gute Führung mit Resilienz zu tun hat.

Cristina Vintila, wie lässt sich Cyber Resilience in KI-gestützten Cloud-Umgebungen wirksam umsetzen?
Cyber Resilience in solchen Umgebungen erfordert einen vielschichtigen Ansatz, der auf Partnerschaften, robuste Frameworks und kontinuierliche Sicherheit setzt. Bei Google Cloud verfolgen wir ein «Shared Fate»-Modell: Wir arbeiten eng mit unseren Kunden zusammen, stellen Frameworks, Best Practices und Ressourcen bereit, um ihre Cloud-Umgebungen abzusichern.

Cristina Vintila ist seit rund 20 Jahren in verschiedenen Funktionen in den Bereichen Antivirus, 4G/LTE-Sicherheit, NFC-Mobilzahlungen, Telekommunikation, Google-Kundenservice und Sicherheit bei Google beschäftigt. Sie hat einen Doktortitel in Sicherheit und einen EMBA der IMD & Universität Lausanne. Sie ist leidenschaftlich daran interessiert, Geschäftsmodelle zu verstehen und nachhaltig Werte für Kunden zu schafft.

Wichtige Strategien sind unser Secure AI Framework (SAIF), umfassende Sicherheitspraktiken wie Zugriffskontrollen, MFA, sichere Softwareentwicklung, Business Continuity und Kryptografie – also die Basics richtig umzusetzen. Ebenso zentral ist der Zero-Trust-Ansatz, bei dem jede Identität und jedes Gerät authentifiziert und validiert wird, um die Angriffsfläche zu minimieren.

Was sind die grössten Risiken, wenn Unternehmen KI-Lösungen ohne Sicherheitskonzept einführen?
Ohne «Security by Design» riskieren Unternehmen die Integrität ihrer Daten, den Schutz der Privatsphäre und ihre operative Stabilität – und erhöhen den technischen Schuldenberg. Typische Risiken sind unbeabsichtigte Datenlecks, schwache Zugriffskontrollen, Prompt-Injection-Angriffe oder schlecht gesteuerte Integrationen.

Wie lässt sich Sicherheit von Beginn an in den Entwicklungszyklus von KI-Systemen integrieren?
Das ist entscheidend für robuste und widerstandsfähige Systeme. Bei uns sensibilisieren wir schon im Design mit den Produktteams, bauen «well-lit paths» in die Architektur ein, überwachen kontinuierlich und führen regelmässig Red-Teaming durch. Wir wenden konsequent unsere Prinzipien für verantwortungsvolle KI an, testen sorgfältig und implementieren Schutzmechanismen, um unerwünschte Folgen zu minimieren.

Viele sehen Sicherheit immer noch als Innovationsbremse. Wie begegnen Sie diesem Vorurteil?
Es braucht Führung, die Sicherheit als Geschäftsfaktor und Innovationstreiber versteht. Permanente Angriffe verhindern Innovation. Sicherheit gehört wie Zuverlässigkeit und Compliance fest in den Lebenszyklus. Als Security-Managerin erkläre ich das «Warum» hinter unseren Anforderungen und schaffe ein Bewusstsein dafür.

> «Resilienz erfordert Anpassung und Mut zu Fehlern.»

Was bedeutet für Sie langfristiger Kundennutzen in der Cloud-Sicherheit?
Das geht weit über Produktfeatures hinaus: Es geht um eine nachhaltige Partnerschaft auf Basis von Vertrauen, kontinuierlicher Verbesserung und dem Ermöglichen von sicherem Wachstum und Innovation.

Sie fördern Führungskräfte in Produktivität und Karriere. Was verbindet Resilienz in der IT mit guter Führung?
Es geht darum, die Basics richtig zu machen. Effektive Führung bedeutet, Teams zu befähigen, ihre Arbeit zu machen – und dann nicht im Weg zu stehen. Das funktioniert nur mit Vertrauen. Resilienz in Cyber Security funktioniert genauso wie das Bauen resilienter Teams: durch Vertrauen, Zusammenarbeit und kontinuierliche Verbesserung.

> «Ohne Sicherheit von Anfang an häufen sich technische Schulden.»

Wie verändert sich die Bedrohungslage durch den Einsatz von KI in kritischer Infrastruktur?
KI eröffnet neue Angriffsflächen, aber sie stärkt auch Verteidiger: Sie hilft, Bedrohungsszenarien schneller zu erkennen, Gegenmassnahmen effizienter zu entwickeln und Systeme sicherer zu gestalten. Sie ermöglicht kürzere Produktionszyklen und bessere Tests durch Simulationen.

Was erwarten Sie von der Digital Conference Ostschweiz?
Ich freue mich auf den Austausch mit anderen Teilnehmenden und auf neue Perspektiven von Partnern, Kunden und Forschern. Meine Breakout-Session wird zeigen, wie ich eine kleine Security-Einheit führe und soll einen anregenden Dialog über unterschiedliche Sichtweisen anstossen.

Sie haben Ozeane überquert und waren in der Antarktis. Was hat das mit Cyber Resilience zu tun?
Wahre Resilienz erfordert Anpassung, Innovation und die Bereitschaft, kalkulierte Risiken einzugehen. Ich erwarte von meinem Team auch nicht, mir zu vertrauen, wenn ich nicht selbst neue Wege gehe, Fehler mache, Verletzlichkeit zeige und mich verbessere. Ich versuche, als Führungskraft, Kollegin und Mensch widerstandsfähiger zu werden und Teams zu formen, die anpassungsfähig und wirksam auf die Herausforderungen reagieren – gerade im Bereich KI und Sicherheit. <

Weitere Informationen zu den von Cristina Vintila erwähnten Konzepten

Secure AI Framework (SAIF)
cloud.google.com/use-cases/secure-ai-framework

Shared Fate-Modell für Cloud-Sicherheit
cloud.google.com/security/shared-fate

Security by Design
cloud.google.com/architecture/framework/security/implement-security-by-design

«Awareness muss kontinuierlich gelebt werden»

Katja Dörlemann von Switch stellt den Menschen ins Zentrum der Cybersicherheitsstrategie. Im Interview erklärt sie, warum Awareness mehr als Schulung ist, weshalb Empathie zählt und welche Rolle Führungskräfte für Cyber Resilience spielen.

Katja Dörlemann, wie definieren Sie Cyber Resilience aus der Perspektive des «Faktors Mensch»?
Cyber Resilience heisst für uns als Nutzerinnen und Nutzer: zu verstehen, was im Ernstfall zu tun ist, und ein Gefühl für den Kontext der Bedrohungslage zu haben. In Organisationen spielt der Faktor Mensch eine Schlüsselrolle. Vorfälle melden, bearbeiten, nachbereiten – das alles passiert durch Menschen. Und wenn diese in ihrer Rolle vorbereitet sind und wissen, wie sie mit dem Stress umgehen können, wird die Organisation als Ganzes widerstandsfähiger.

Was sind typische Verhaltensmuster, die IT-Systeme angreifbar machen – und wie lässt sich das Bewusstsein dafür stärken?

Schwaches Passwortmanagement und Phishing sind die Klassiker. Das Bewusstsein, dass das ein Problem ist, fehlt meistens gar nicht – viele wissen durchaus Bescheid. Aber wenn der sichere Weg meine Arbeit behindert und ich keinen Nutzen darin sehe, nehme ich den Mehraufwand oft nicht in Kauf. Da reicht dann auch das beste Training nicht aus.

Warum ist Security Awareness kein einmaliger Akt, sondern ein Prozess?
Weil Organisationen und ihre Mitarbeitenden sich permanent verändern. Die meisten wissen, wie sie sich richtig verhalten sollten – und tun es trotzdem nicht. Warum? Oft, weil im sich stetig wandelnden Arbeitsalltag Prozesse und Tools nicht passen oder weil Vorbilder fehlen. Awareness ist nicht einfach ein Kurs, sondern eine Haltung der gesamten Organisation, die ständig erneuert und gelebt werden muss.

Wo sehen Sie die grössten Lücken im Sicherheitsverhalten?
Ich sehe die grössten Schwächen oft auf Seiten der Organisationen. Es ist nicht immer einfach für Mitarbeitende, sich sicher zu verhalten, wenn ihnen die passenden Mittel fehlen. Gibt es einen Passwortmanager? Wurde er erklärt? Gehört es zu meinen Zielen, Sicherheitsvorgaben umzusetzen? Das muss gewährleistet sein.

Wie wichtig ist die Community für den Fortschritt in der Awareness-Arbeit?
Sehr wichtig. Awareness ist ein junges Feld. Wir können nicht auf jahrzehnte-

lange Erfahrung zurückgreifen wie andere Disziplinen. Deshalb ist der Austausch mit anderen unerlässlich – um voneinander zu lernen und schneller besser zu werden.

Welche Rolle spielt Empathie in der Cybersicherheitskommunikation?
Empathie ist absolut zentral. Wer Menschen überzeugen will, muss verstehen, was sie bewegt, und ihre Sprache sprechen. Schuldzuweisungen bringen nichts – am besten vermeidet man sie gleich von Anfang an.

Als Präsidentin der Swiss Internet Security Alliance: Wo setzt die Allianz Schwerpunkte?
Wir fördern den Austausch zwischen Fachleuten und Praktikern und bereiten Informationen für Internetnutzer und -nutzerinnen auf, etwa über iBarry.ch. Das sind unsere Kernaufgaben.

«Vorbereitung macht Organisationen resilient.»

Wie kann man Führungskräfte dafür sensibilisieren, dass Cybersicherheit kein reines IT-Thema ist?
Indem man sich ehrlich mit ihnen auseinandersetzt. Wer weiss, was Führungskräfte antreibt, kann das Thema entsprechend platzieren – als Wettbewerbsvorteil, Risikominimierung, Reputationsgewinn. Wenn Cybersicherheit für sie trotzdem keine Priorität hat, bleibt nur: die Risiken aufzeigen und die Entscheidung akzeptieren.

Was möchten Sie mit Ihrer Keynote an der Digital Conference Ostschweiz bewirken?
Mir ist wichtig, dass der Mensch in der Cybersicherheitsdiskussion nicht zu kurz kommt. Mitarbeitende müssen von Anfang an mitgenommen werden – nicht erst ganz am Ende via eLearning, wenn schon alles entschieden ist. Meine Botschaft richtet sich an Verantwortliche und Führungskräfte, die diesen blinden Fleck noch haben.

Was kann die Geisteswissenschaft der Cybersicherheit beibringen?
Literatur zeigt, wie man Botschaften in Geschichten verpackt, die Menschen berühren. Wir lernen an Beispielen, in einem verständlichen Kontext. Das funktioniert in der Cybersicherheit genauso gut. <

Katja Dörlemann ist Security-Awareness-Expertin bei Switch. Als Teil der Schweizer Stiftung unterstützt sie die Bildungs-, Forschungs-, Innovations- und Internet-Community im Umgang mit dem Faktor Mensch in der Informationssicherheit. Sie ist Präsidentin der Swiss Internet Security Alliance und Vorstandsmitglied bei Women in Cyber Switzerland.

«Cyberresilienz ist keine Einzelleistung, sondern ein kollektives Ziel»

Thomas Fröhlich ist Cyber Security Architect bei der Inventx AG. Im Interview erklärt er, warum Cyberresilienz in der Finanz- und Versicherungsbranche weit über klassische IT-Sicherheit hinausgeht – und wie auch kleinere Institute ihre Widerstandsfähigkeit gezielt stärken können.

Thomas Fröhlich, wie definieren Sie Cyber Resilience im Kontext der Finanz- und Versicherungsbranche – und worin liegt der Unterschied zur klassischen IT-Sicherheit?
Cyber Resilience beschreibt die Fähigkeit, Cyberangriffe nicht nur zu verhindern, sondern auch darauf zu reagieren, sich davon zu erholen und den Geschäftsbetrieb – mindestens für kritische Prozesse – aufrechtzuerhalten. Es geht um Widerstandsfähigkeit, nicht nur um Schutz. Während klassische IT-Sicherheit auf Prävention fokussiert, zielt Resilienz auf das gesamte Krisenmanagement – inklusive Wiederherstellung und kontinuierlicher Verbesserung.

Welche Schwachstellen sind bei Banken und Versicherungen besonders kritisch?
Assume Breach gilt auch hier. Gezielte Angriffe durch Cyberkriminelle oder staatliche Gruppen, kombiniert mit Insider Threats, Phishing oder Social Engineering, sind alltäglich. Schlechte Patchstände, veraltete Systeme oder ungesicherte Lieferketten erhöhen das Risiko zusätzlich. Zero-Trust-Architekturen und konsequentes Monitoring sind daher unerlässlich, um Angriffsflächen so klein wie möglich zu halten.

Wie hat sich das Verständnis von Sicherheit in der Branche verändert?
Früher war Sicherheit ein rein technisches Thema. Heute ist sie ein strategischer Unternehmensfaktor. Nach der Perimetersicherheit folgten Netzwerkschutz und Intrusion Detection. In der Digitalisierungsphase rückten Compliance, Governance und Cyber Resilience in den Fokus. Heute sind wir in einer

adaptiven, KI-gestützten Ära angekommen, in der Sicherheit dynamisch, risikobasiert und eng mit Geschäftsprozessen verzahnt sein muss.

Was sind typische Fehler beim Aufbau resilienzfähiger Systeme?

Fehlende Zuständigkeiten, ungenügende Tests, zu starke Technikorientierung. Viele Institutionen investieren punktuell, statt ganzheitlich zu denken. Wer Risiken wirklich reduzieren will, sollte eine Assume-Breach-Mentalität leben, Zero Trust einführen, Red Teaming und Tabletop-Übungen nutzen, Drittparteien aktiv einbeziehen und das Sicherheitsbewusstsein im Unternehmen gezielt fördern. Resilienz erfordert laufende Pflege und organisatorische Verankerung.

Wie können kleinere Institute Resilienz auch ohne grosses Budget stärken?

Durch fokussiertes und pragmatisches Vorgehen. Der erste Schritt ist die Identifikation geschäftskritischer Prozesse – etwa Zahlungsverkehr oder Kundenkommunikation – und die Entwicklung von Notfallplänen, die auch ohne IT tragfähig sind. Auch mit beschränkten Mitteln lassen sich wirkungsvolle Massnahmen umsetzen: Multi-Faktor-Authentifizierung, Least Privilege, rollenbasierte Zugriffskontrollen, automatisiertes Patchmanagement – das sind starke Pfeiler einer soliden Grundabsicherung.

Wie wichtig ist Zusammenarbeit innerhalb der Branche?

Sie ist absolut zentral. Cyberresilienz ist keine Einzelleistung, sondern ein kollektives Ziel. Ein funktionierendes Frühwarnsystem, sektorübergreifender Informationsaustausch und gemeinsame Übungen erhöhen die Widerstandsfähigkeit des gesamten Finanzökosystems. Leider ist die operative Zusammenarbeit in der Schweiz noch fragmentiert – hier besteht Potenzial, das dringend genutzt werden sollte.

«Assume Breach gilt auch für Banken und Versicherungen.»

Wie wichtig sind Vorgaben wie ISO 27001 oder DORA – und wo stossen sie an Grenzen?

Beide sind essenziell, aber nicht ausreichend. ISO 27001 ist ein etabliertes Fundament für Informationssicherheit. DORA ist ein regulatorischer Meilenstein, der Cyberresilienz europaweit stärkt. Doch formale Vorgaben ersetzen keine gelebte Sicherheitskultur. Echte Resilienz entsteht nicht durch Dokumente, sondern durch Praxis, Verantwortung und laufende Verbesserung.

Was müssen Verwaltungsräte und Geschäftsleitungen über Cyberresilienz wissen?

Sie müssen sich nicht die Frage stellen, ob ein Vorfall eintritt – sondern wann. Cyberresilienz ist kein IT-Projekt, sondern ein Führungsauftrag. Verwaltungsräte und Geschäftsleitungen müssen sicherstellen, dass Risiken verstanden, Massnahmen umgesetzt und Ressourcen bereitgestellt werden. Wer vorbereitet ist, schützt nicht nur Systeme, sondern auch das Vertrauen von Kunden, Partnern und Aufsichtsbehörden.

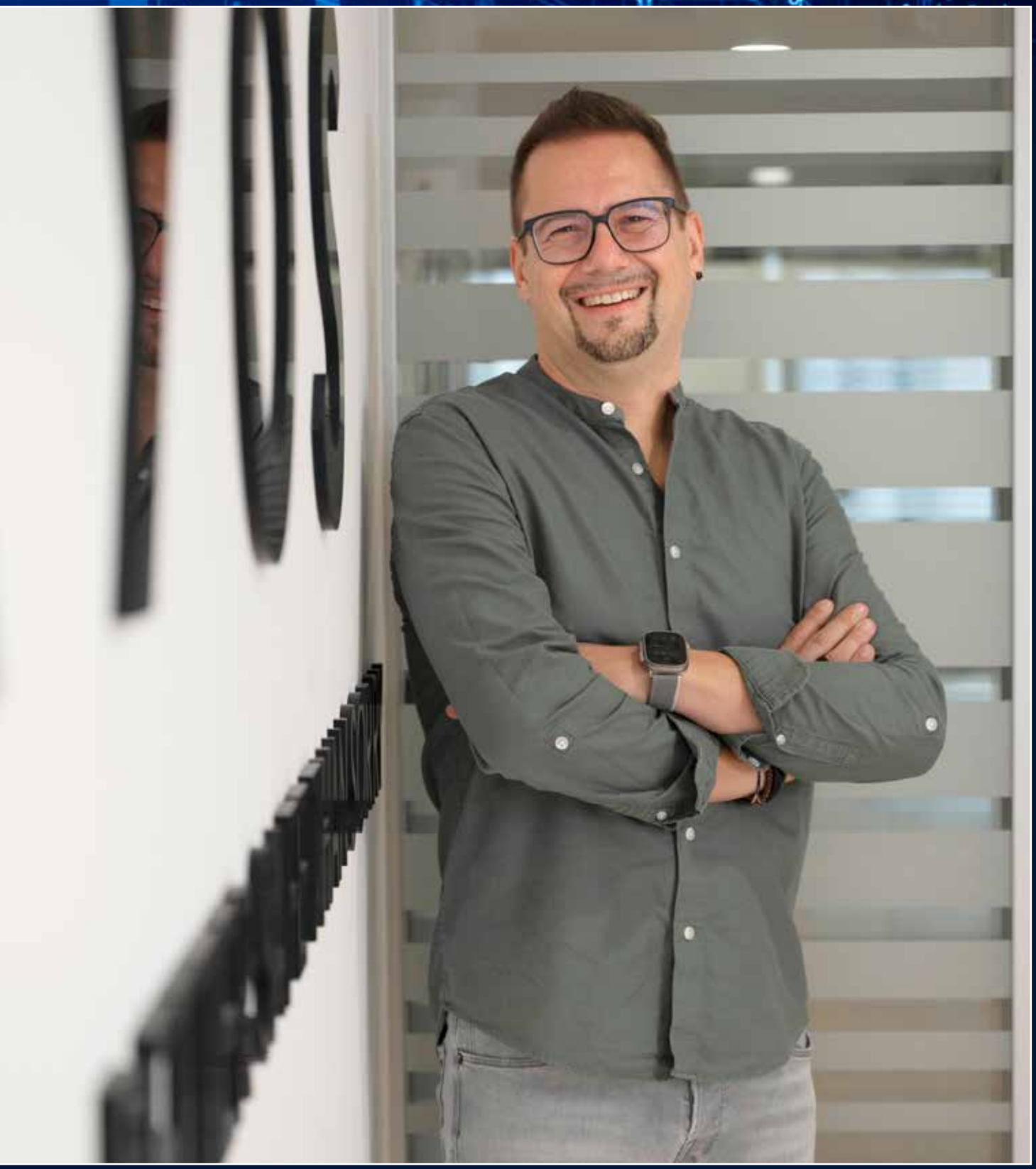
Was möchten Sie den Teilnehmern Ihrer Breakout-Session mitgeben?

Cyberresilienz beginnt nicht mit Technologie, sondern mit Klarheit, Verantwortung und Zusammenarbeit. Es gibt kein Patentrezept – aber es gibt vorbereitete Organisationen und überraschte. Ich werde keine «Step-by-step»-Lösung präsentieren. Wichtig ist, die eigenen Risiken realistisch einzuschätzen und im Ernstfall rasch reagieren zu können. Wer die Möglichkeit hat, sollte auf ein professionelles SOC mit 24/7-Überwachung setzen – das kann im Ernstfall entscheidend sein.

Was ist wichtiger: Technik, Prozesse oder Menschen?

Alle drei sind essenziell. Aber ohne den Menschen funktioniert weder die Technik noch der Prozess. Der Mensch ist das Fundament, Prozesse das Rückgrat und Technik das Werkzeug. Nachhaltige Resilienz entsteht nur, wenn alle drei Komponenten zusammenspielen – mit Verantwortung und Überzeugung. <

Thomas Fröhlich verfügt über mehr als 30 Jahre Erfahrung im Bereich IT-Security – von der UNIX-Systemadministration über Security Engineering und Enterprise Architektur bis hin zu Audits und Erstzertifizierungen. Aktuell ist er im Cyber Resilience Center (SOC) der Inventx AG tätig. Zuvor verantwortete er während zehn Jahren die CISO-Rolle beim Schweizer IT- und Digitalisierungspartner für führende Finanz- und Versicherungsunternehmen.



Cybersecurity für KMU: Einfach umsetzen, wirksam schützen

Andy Kutter, Partner und Direktor bei Kyos sowie Presentingpartner der Digital Conference Ostschweiz, spricht am Anlass über reale Gefahren und die teuren Folgen von Cyberangriffen. Im Interview erklärt er, warum gerade KMU besonders gefährdet sind – und wie sie mit pragmatischen Massnahmen ihre Cyberresilienz steigern können.

Andy Kutter, Ihre Präsentation trägt den Titel «Was kostet ein Klick?». Was steckt dahinter?
Es geht um alltägliche Situationen. Ein Mitarbeiter klickt auf eine scheinbar harmlose E-Mail – etwa eine gefälschte Rechnung. In einem konkreten Fall führte genau das zu einem Schaden von 87'000 Franken und zwei Wochen Betriebsunterbruch bei einer Schreinerei. Ein einziger Klick kann katastrophale Folgen haben – das ist leider Realität für viele KMU.

Wie hoch ist die tatsächliche Bedrohung für kleinere Unternehmen?
Sehr hoch. In der Schweiz waren bereits 72 % der KMU Ziel eines Cyberangriffs. Viele wiegen sich in falscher Sicherheit, weil sie sich für zu klein oder uninteressant halten. Doch Hacker setzen automatisierte Angriffe ein – da spielt die Grösse keine Rolle. KMU sind oft weniger gut geschützt und dadurch ein leichtes Ziel.

Welche Angriffsmethoden kommen am häufigsten vor?
Phishing, Ransomware und Social Engineering gehören zu den Klassikern. Dabei werden Mitarbeitende gezielt getäuscht oder Schwachstellen in der IT ausgenutzt. Auch einfache Versäumnisse wie schwache Passwörter oder fehlende Zwei-Faktor-Authentifizierung öffnen Tür und Tor.

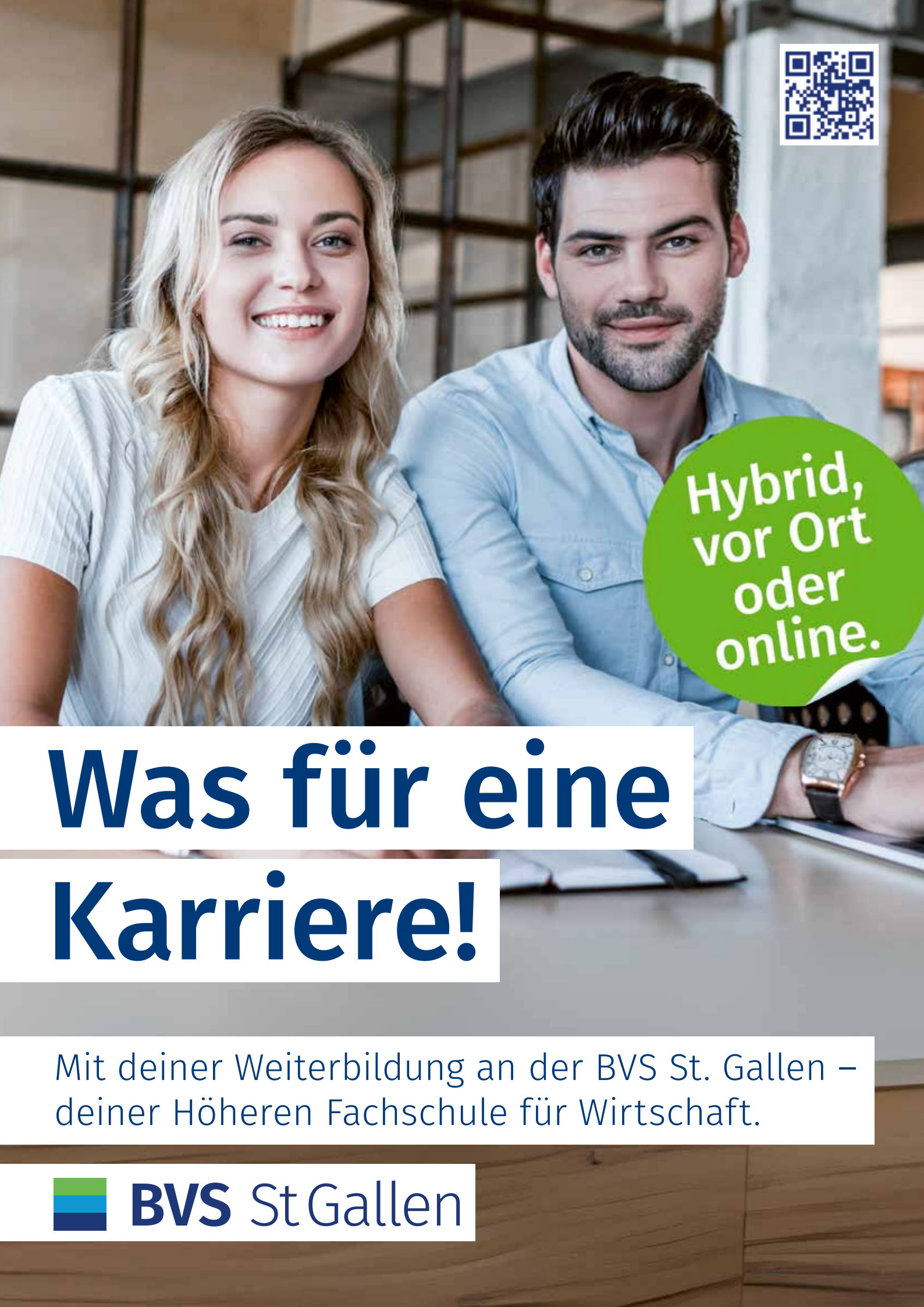
Wo liegen die häufigsten Schwächen bei KMU?
In der falschen Einschätzung des Risikos. Cybersicherheit wird oft als unnötiger Kostenfaktor gesehen. Es fehlt an klaren Prozessen, an Schulungen – und oft auch an grundlegenden Massnahmen wie regelmässigen Backups oder der Filterung von E-Mails.

Welche konkreten Massnahmen empfehlen Sie?
Zuerst die Basics: starke Passwörter mit Passwortmanager, Zwei-Faktor-Authentifizierung, regelmässige Schulungen und getestete Backups. Diese Massnahmen sind kostengünstig, aber sehr wirksam. Wichtig ist auch ein Notfallplan – bevor es zum Ernstfall kommt.

Mit welchen Kosten muss man rechnen, wenn man das Thema ernst nimmt?
Für einen soliden Basisschutz genügen bei KMU oft 2000 bis 5000 Franken im Jahr. Angesichts eines durchschnittlichen Schadens von 45'000 Franken pro Angriff ist das ein sehr gutes Verhältnis von Aufwand zu Nutzen.

Ihr Fazit?
Cybersicherheit ist Chefsache – aber gleichzeitig eine Teamleistung. Wer seine Mitarbeitenden sensibilisiert und einfache Schutzmassnahmen umsetzt, ist klar im Vorteil. Entscheidend ist, frühzeitig zu handeln – nicht erst, wenn es zu spät ist. <

Zur Person
Andreas Kutter ist Partner und Direktor bei Kyos, einem führenden Schweizer IT-Sicherheitsunternehmen mit über 20 Jahren Erfahrung. Seit mehr als zehn Jahren prägt er die Entwicklung des Unternehmens mit – gestützt auf zwei Jahrzehnte Erfahrung in der Finanzbranche und ein HSG-Studium im Key Account Management.
Kyos zählt heute über die Hälfte der Top-Ten-Unternehmen der Schweiz zu seinen Kunden. Als Thales Top Partner in Europa bietet das Unternehmen massgeschneiderte Sicherheitslösungen – von Penetrationstests über strategisches Consulting bis hin zu hochspezialisierten Netzwerkteams. Im Fokus steht dabei immer: praxisnahe, kosteneffiziente IT-Sicherheit – auch für KMU.



Was für eine Karriere!

Mit deiner Weiterbildung an der BVS St. Gallen – deiner Höheren Fachschule für Wirtschaft.

BVS St Gallen

Weitere Speaker im Überblick

Keynote

1 Marco Brenner
Program Executive, IBM Quantum Schweiz
Als Experte für Kryptographie und Datenschutzlösungen bei IBM Quantum verbindet Marco Brenner Forschung und Kundenpraxis. In seiner Keynote beleuchtet er die Auswirkungen von Quantencomputing auf die Cybersicherheit – und erklärt, welche Technologien die Verschlüsselung der Zukunft bestimmen könnten.

Breakout Sessions

2 Angela Meier
Geschäftsführerin, Outvision GmbH
Führung entscheidet, wenn es ernst wird: In ihrer Session zeigt Angela Meier, wie Unternehmen ihre Resilienz durch gezielte Auswahl und Entwicklung von Führungskräften stärken können – mit Fokus auf Menschen, Werte und Passung.

3 Michael Stahlberger
Leiter Departement IT, HOCH Health Ostschweiz
Als CIO der grössten Spitalgruppe der Ostschweiz bringt Michael Stahlberger den Blick aus dem Gesundheitswesen ein. Er zeigt, wie Cyber Resilience vom technischen Schutz bis zur organisationalen Reaktion reichen muss – und was es dazu braucht.

4 Tobias Meier
CTO, MTF Solutions AG
In seiner Session gibt Tobias Meier einen Einblick in einen realen Sicherheitsvorfall – Schritt für Schritt, offen und direkt. Eine Gelegenheit, den Ablauf eines Cyberangriffs aus der Innenperspektive nachzuvollziehen.

Sensorlösungen für Ihr KMU – von der Idee bis zur Serienreife

Sie haben eine Anwendung, für die es noch keinen passenden Sensor gibt?

Wir unterstützen Sie dabei:

- Entwicklung und Forschung rund um Sensorik
- Miniaturisierung, Photonik, Mikro-/Elektronik
- Systemintegration und Datenanalyse
- Prototyping und Applikationsentwicklung

si-hub.ch

powered by

OST Ostschweizer Fachhochschule

RhySearch Das Forschungs- und Innovationszentrum Rheintal

SWITZERLAND INNOVATION PARK OST

Die Moderatorin der DCONO 2025


Bild: Mirjam Kluka

bignasilberschmidt.ch
bigna-silberschmidt-20b972a9
bignasilberschmidt

Bigna Silberschmidt
Bigna Silberschmidt schloss an der Universität Fribourg mit einem Bachelor in Medien- und Kommunikationswissenschaften sowie Zeitgeschichte und einem trilingualen Master in Betriebswirtschaftslehre ab. Zudem absolvierte sie an der Universität Bern das CAS «Leadership and Inclusion».
Nach diversen Stationen bei Radio, Print und als stellvertretende Geschäftsführerin einer Kommunikationsagentur war Bigna Silberschmidt während zehn Jahren beim Schweizer Fernsehen SRF tätig. Sie realisierte zahlreiche Reportagen und moderierte unter anderem beim Wissensmagazin «Einstein» und zuletzt die Informationssendung «10 vor 10». 2025 machte sich die Journalistin und Kommunikationsspezialistin selbständig. Sie moderiert Podien und Veranstaltungen in den Bereichen Wissenschaft, Gesellschaft, Umwelt und Wirtschaft, berät und referiert – mit Spezialgebieten konstruktive Kommunikation, Nachhaltigkeit und Inklusion.

Profil

St.Gallen: Ein Hotspot für KI-Innovation

Künstliche Intelligenz verändert aktuell Wirtschaft, Bildung und Forschung und St.Gallen ist mittendrin. Wie die vor kurzem erschienene Marktstudie zum Schweizer ICT-Markt 2025 von Netzmedien zeigt, profitieren insbesondere Consulting-Unternehmen und die Softwareentwicklung von der hohen Nachfrage nach KI-gestützten Lösungen. Hier sticht der Ostschweizer Trumpf: Viele Unternehmen in der Region sind in diesem Bereich tätig und ein entscheidender Treiber für den Erfolg ist die enge Verbindung zwischen Wissenschaft, Bildung und Wirtschaft. Dabei spielt auch das Netzwerk des Vereins <IT>rockt! eine zentrale Rolle. Die Universität St.Gallen und die Fachhochschule OST bilden mit ihren starken Ausbildungsgängen neue Fachkräfte aus und ermöglichen den hiesigen Firmen den Zugang zu kompetenten Mitarbeitenden. Gepaart mit der

hohen Lebensqualität zwischen Bodensee und Säntis sowie als Bindeglied zwischen den starken Wirtschaftsräumen München und Zürich bietet die Stadt St.Gallen damit den idealen strategischen Standort.

Wählen Sie Ihren «Digital Shaper Ostschweiz» 2025

In den vergangenen Monaten konnten die Leser von east#digital aus 55 Ostschweizer Persönlichkeiten und Teams ihre drei Favoriten für die Auszeichnung «Digital Shaper Ostschweiz 2025» wählen. Die zehn Personen, die bis Anfang Juli am meisten Stimmen erhalten haben, sind auf der Shortlist.

1 Elisabeth Wenzler & Michael Bernasconi
Projektleiter <IT>rockt!
Digitale Kompetenzen in der Ostschweiz gezielt fördern – mit diesem Ziel haben Elisabeth Wenzler und Michael Bernasconi 2024 zwei zentrale Initiativen lanciert. Erfa-Gruppen zu Cyber Security und KMU-IT-Trends bieten Fachkräften eine Plattform für praxisnahen Austausch, während neue KI-Kurse, entwickelt in Zusammenarbeit mit der TKF AG, speziell Führungskräfte, Content Creators und die Generation 50+ ansprechen. Mit diesen Angeboten schafft <IT>rockt! wertvolle Weiterbildungsmöglichkeiten und unterstützt Unternehmen sowie Einzelpersonen dabei, das Potenzial der Künstlichen Intelligenz optimal zu nutzen.

2 Thomas Hepp
Key-Account-Manager OriginStamp AG
Datenschutz und künstliche Intelligenz in Einklang zu bringen, ist das Ziel eines neuen KI-Chatbots «swiDoc», den Thomas Hepp und sein Team bei der Weinfelder OrginStamp AG entwickelt haben. Speziell für Schweizer KMU konzipiert, ermöglicht die Lösung eine sichere und effiziente Verwaltung vertraulicher Dokumente – ohne dass Nutzerdaten für Trainingszwecke genutzt oder das geschützte System verlassen werden. Diese konsequente Datenschutzpolitik gewährleistet die Vertraulichkeit und Integrität sensibler Unternehmensdaten.

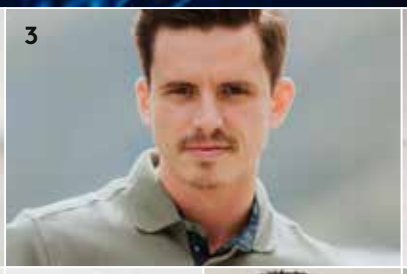
3 Nimrod Malinas
CEO Robonnement
Flexible Robotik für KMU: Nimrod Malinas wurde 2024 in die Forbes-Liste «30 Under 30» aufgenommen. Seit der Übernahme des Altstätter Traditionsunternehmens 2020 hat er es zu einem führenden Anbieter von Roboter-as-a-Service (RaaS) umgewandelt. Das Modell ermöglicht es Unternehmen, Roboter flexibel zu mieten, was insbesondere KMU den Zugang zur Automatisierung erleichtert. Für seine innovativen Ansätze wurde Robonnement mehrfach ausgezeichnet, zuletzt im November 2024 mit dem Digital Economy Award in der Kategorie «Digital Excellence Commercial».

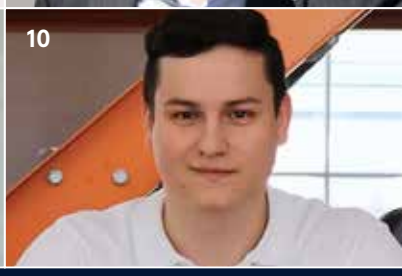
4 Reto Rutz
Geschäftsführer Valantic CEC Schweiz
Effizienz und Benutzerfreundlichkeit standen im Mittelpunkt der neuen Webseite der Sonepar Suisse AG – ein Projekt der Valantic CEC Schweiz AG. Diese digitale Lösung überzeugte beim Best of Swiss Web Award 2024 und wurde mit Bronze in der Kategorie Productivity ausgezeichnet.

5 Reto Gutmann
CEO Abraxas Informatik AG
Die Abraxas Informatik AG in St.Gallen wurde beim Best of Swiss Web Award 2024 mit zwei Bronze-Auszeichnungen geehrt. Die Web-App «VOTING Ausmittlung», entwickelt für die Staatskanzlei St.Gallen, überzeugte in den Kategorien Public Value und Innovation. Diese Anerkennung bestätigt die führende Rolle von Abraxas in der Digitalisierung von Verwaltungsprozessen. CEO Reto Gutmann und sein Team treiben damit die Modernisierung des öffentlichen Sektors weiter voran.

6 Daniel Baur
Mitgründer emonitor AG
Digitalisierung im Immobilienvertrieb: Daniel Baur ist Mitgründer der St.Galler emonitor AG. Diese wurde auf der Expo Real in München mit dem Immobilienmarketing-Award in der Kategorie «Digitale Marketing Tools» ausgezeichnet. Das prämierte Tool «transactionhub» digitalisiert den gesamten Verkaufsprozess von Renditeimmobilien – von der Identifikation bis zur Angebotsabgabe. Diese Innovation ersetzt zeitaufwendige manuelle Abläufe durch eine effiziente, transparente und datenbasierte Lösung, die Investoren den Zugang zum Markt erleichtert.

7 Catherine Ferris
Projektleiterin PHSG
Wie lassen sich Online-Übersetzungstools sinnvoll in den Schulunterricht integrie-





ren? Mit dieser Frage beschäftigte sich das Projekt «Tools@Schools» unter der Leitung von Catherine Ferris an der Pädagogischen Hochschule St.Gallen (PHSG). Das Team entwickelte Aufgaben, die Schüler der Sekundarstufe I dazu anleiten, diese Tools reflektiert im Sprachunterricht zu nutzen. Nach erfolgreichen Tests an verschiedenen Schulen des Kantons St.Gallen fliessen die Erkenntnisse nun in die Aus- und Weiterbildung angehender Lehrpersonen ein. Für diese wegweisende Forschungsarbeit erhielt das Projekt den ersten PHSG Bridge Award.

8 Dennis Eitner & Sandro Pezzutto

OST-Absolventen

Technologie gegen Einsamkeit: Dennis Eitner und Sandro Pezzutto, Absolventen des MAS Human Computer Interaction Design an der OST, entwickelten den Sprachassistenten Alfred, der Senioren durch sprachgesteuerte Interaktionen unterstützt. Alfred hilft älteren Menschen, Erinnerungen wachzurufen, positive Momente zu teilen und so ihr Wohlbefinden zu steigern. In ersten Tests überzeugte das System mit eindrücklichen Ergebnissen – eine Seniorin führte ein 16-minütiges Gespräch mit Alfred. Mit dieser Innovation leisten Eitner und Pezzutto Pionierarbeit und setzen sich dafür ein, Alfred weiterzuentwickeln und noch mehr Menschen zugänglich zu machen.

9 Boryana Milova

Projektleiterin Stiftung MyHandicap

Inklusion aktiv mitgestalten – dieses Ziel verfolgt die Plattform EnableMe Insights, die Boryana Milova mit ihrem Team bei der Stiftung MyHandicap in St.Gallen ins Leben gerufen hat. Das partizipative Konzept stellt sicher, dass Menschen mit Behinderungen direkt in die Entwicklung und Gestaltung von Produkten und Dienstleistungen einbezogen werden. Für dieses Engagement wurde das Projekt im Oktober 2024 mit dem ersten Platz der Swiss Sustainability Challenge.

10 Stefan Bamberger

CEO Fluidbot AG

Roboter für die Trinkwasserversorgung: Stefan Bamberger erhielt 2024 mit seinem Team eine bedeutende Förderung vom Schweizerischen Verein des Gas- und Wasserfaches (SVGW). Das 2022 gegründete Start-up aus Gossau entwickelt hochpräzise Roboter zur Überwachung und Instandhaltung von Trinkwasserleitungen. Diese Technologie ermöglicht eine frühzeitige Schadenserkennung und verbessert die Nachhaltigkeit der Wasserversorgung. Die Förderung bestätigt das Potenzial von Fluidbot, einen wichtigen Beitrag zur Infrastruktur der Zukunft zu leisten.

Bis Ende August können Sie darüber abstimmen, wer von diesen zehn Personen/Teams «Digital Shaper Ostschweiz 2025» werden soll. Die Auszeichnung erfolgt im Rahmen der Digital Conference Ostschweiz 2025, die am 26. September im Einstein Congress in St.Gallen stattfinden wird.

Hier geht's zur Abstimmung >>

Contenthouse – Ihr Partner für starke Videokommunikation

Mit Standorten in St. Gallen und Olten ist Contenthouse im gesamten deutschsprachigen Raum für Kunden aus verschiedensten Branchen tätig.

Wir unterstützen Unternehmen, Organisationen und Institutionen bei der Entwicklung professioneller Brandkits und individualisierter Video-Vorlagen für gängige Kreativ-Tools wie Canva oder CapCut. Damit können Inhalte effizient, markengerecht und kanalgerecht produziert werden – flexibel inhouse oder gemeinsam mit uns.

Benjamin Pipa

Unser Ziel: Videokommunikation, die auffällt, relevant ist und sich mit überschaubarem Aufwand realisieren lässt. Als Full-Service-Agentur decken wir die gesamte Bandbreite ab – von Ideenfindung und Storytelling über den Dreh vor Ort bis zur Postproduktion, inklusive Schnitt, Motion Design, Animation und Vertonung.

So werden Markenbotschaften nicht nur sichtbar, sondern bleiben im Gedächtnis – effizient produziert, modern inszeniert und perfekt auf Ihre Zielgruppe abgestimmt.

Contenthouse GmbH
Lerchenfeldstrasse 3, 9014 St.Gallen
Hauptgasse 33, 4600 Olten

Kontakt
Benjamin Pipa
info@contenthouse.ch
+41 58 255 06 06
contenthouse.ch

Cyber-Security Basis Workshop

Sicherheitsbewusstsein von Anfang an. Ob für Ihre persönlichen Daten oder die Sicherheit Ihres Unternehmens – in unserem interaktiven Workshop erfahren Sie durch unsere Experten von KYOS SA aus erster Hand, wie Hacker vorgehen und wie Sie sich wirksam verteidigen können. Gerade neue Mitarbeitende benötigen eine fundierte Einführung in Ihre Cybersicherheitskultur. Ohne gezielte Schulung bleiben sie unbewusst ein Risiko für Ihr Unternehmen.

Zwei Buchungsoptionen

Einzelpersonen
Ideal für Privatpersonen oder punktuelle Schulungen – inkl. interaktive Szenarien,
Kosten: 500 CHF pro Person

Unternehmen
Kontinuierliche Awareness Schulungen – Perfekt für Onboarding & regelmässige Updates
Kosten: 980 CHF pro Jahr für bis zu 5 Mitarbeitende

Termine 2025 & Anmeldung

21. Oktober | 9. Dezember
jeweils 13–17 Uhr – inklusive Snacks und Getränke

Infos zu Rabatten für <IT>rockt! Mitglieder oder Gewerbe Stadt St.Gallen finden Sie ebenfalls auf der Kursseite.

<IT>rockt!

Buchen Sie jetzt Ihren Platz als Einzelkurs oder im Abo-Modell
www.itrockt.ch/ki-kurse/cyber-security-basis

KYOS

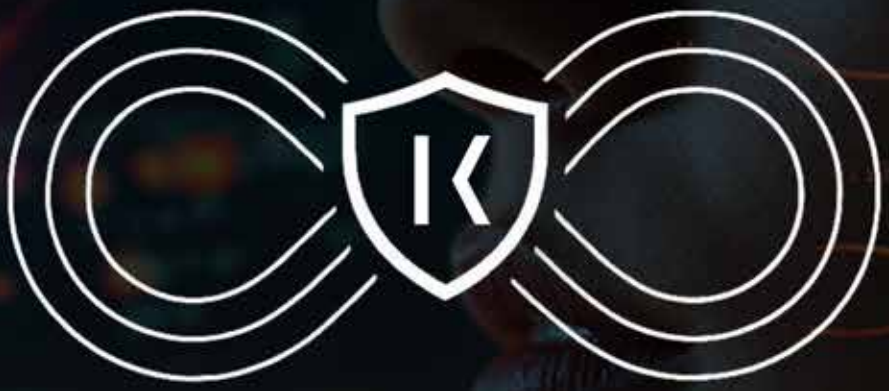
Make IT Simple

PROTECT

- Risk & Compliance Management
- Threat Detection & Response
- Identity & Access Security
- Business Continuity & Policy

CONSULTING SERVICES

- Cloud Security
- Penetration Testing
- Security Architecture & Design
- Security Audits



DATA SECURITY

- Application Security
- Secure Software Development
- Data Privacy
- Encryption & Cryptography

NETWORK INFRASTRUCTURE

- Network Security
- Wifi
- Network
- Telephony

KYOS St. Gallen
Breitfeldstrasse 13
9015 St. Gallen
+41 71 566 70 30
st.gallen@kyos.ch

KYOS Genève
Ch. Frank-Thomas 32
1208 Genève
+41 22 566 76 30
info@kyos.ch